MARCH 2017 VOL. 15 ISS. 03
CYBERTREND.COM

CyberTrend®

TECHNOLOGY FOR BUSINESS

TODAY'S DIGITAL THREAT LANDSCAPE

PLUS: AN ONLINE SCHEME THAT RAKED IN MILLIONS

ALSO IN THIS ISSUE

Top Data Center Mistakes To Avoid

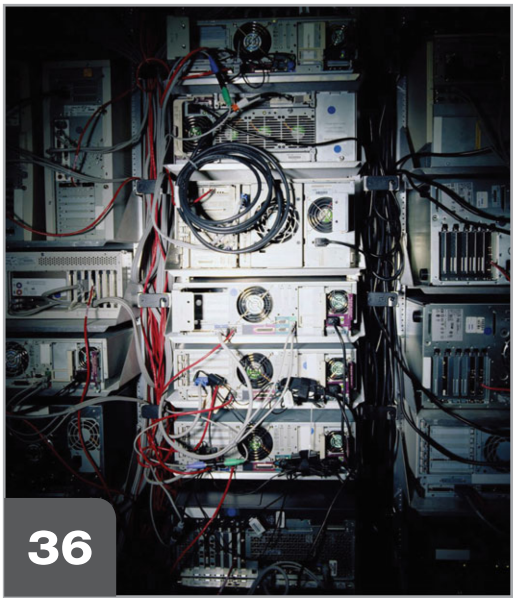
Better Business Travel

How To Measure Cloud ROI

PROCESSOR
Special Section For IT Managers

Table of Contents

Volume 15 : Issue 03 : March 2017



PROCESSOR

Special Section For IT Managers

CONTACT US
P.O. Box 82545
Lincoln, NE 68501

or

120 W. Harvest Drive
Lincoln, NE 68521

Advertising: Fox Associates
800-440-0231 ext. 116
AdInfo.snh@FoxRep.com
Circulation: (800) 334-7458
Fax: (402) 479-2123
www.cybertrend.com
Email: feedback@cybertrend.com

CyberTrend®

Sandhills Publishing®

Only Modest Growth Now Expected For 2017 IT Spending

› Research firm Gartner has slightly down-graded its forecast for 2017 global IT spending from 3% to 2.7%, with spending on devices expected to remain about the same as in 2016. "2017 was poised to be a rebound year in IT spending," says John-David Lovelock, research vice president with Gartner, citing the convergence of "cloud, blockchain, digital business, and artificial intelligence" among other important trends. "However," he says, "some of the political uncertainty in global markets has fostered a wait-and-see approach, causing many enterprises to forestall IT investments." The accompanying chart shows Gartner's worldwide IT spending forecast for the next two years, and illustrates the widening gap between gains in enterprise software/cloud computing and a slowdown in data center systems.

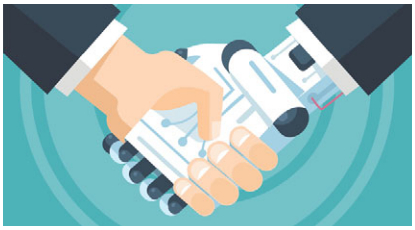
Worldwide IT Spending Forecast (In Billions Of U.S. Dollars)

	2016 Spending	2016 Growth	2017 Spending	2017 Growth	2018 Spending	2018 Growth
Data Center Systems	170	-0.6%	175	2.6%	176	1.0%
Enterprise Software	333	5.9%	355	6.8%	380	7.0%
Devices	588	-8.9%	589	0.1%	589	0.0%
IT Services	899	3.9%	938	4.2%	981	4.7%
Communications Services	1,384	-1.0%	1,408	1.7%	1,426	1.3%
Overall IT	3,375	-0.6%	3,464	2.7%	3,553	2.6%

SOURCE: GARTNER

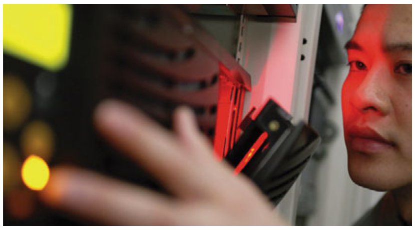
PC Market Growth Continues Its Five-Year Decline

› The traditional PC market's downward trend, which began in 2012, is continuing worldwide as mobile device usage grows, according to Gartner. "The broad PC market has been static as technology improvements have not been sufficient to drive real market growth," explains Mikako Kitagawa, principal analyst with Gartner. Lightweight laptops with longer battery life have been a bright spot in the market, she adds, but not enough to compensate for slow growth elsewhere. Gartner says 269.7 million PCs shipped in 2016, a 6.2% decline from 2015.



Spending On Robotics Is Up As New Markets Welcome Benefits

› Research firm IDC expects global spending on robotics to reach $188 billion in 2020, twice the $91.5 billion spent last year. "Innovators in the field of robotics are delivering robots that can be used to perform a broader range of tasks, which is helping to drive the adoption of robotics into a wider base of industries," says John Santagate, research manager with IDC. The most prominent use cases today are assembly, welding, and painting (24% of the market); mixing (20.1%); consumer (7.1%); and automation in mining, bottling, and other areas (6%), says IDC.

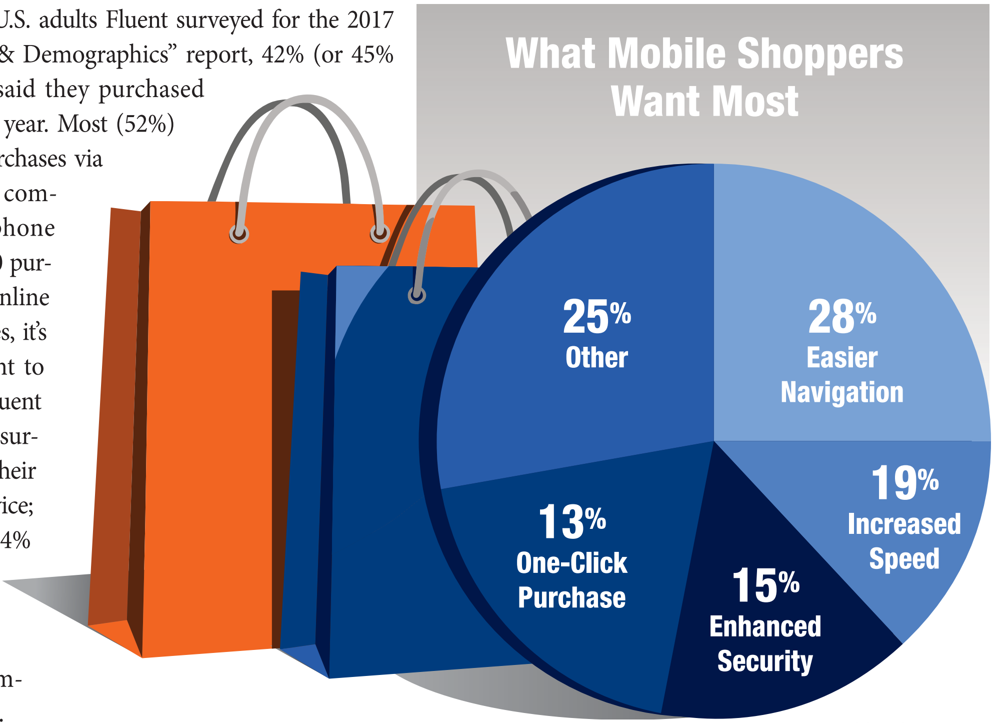


ESG & ISSA Point Out Impact Of Cybersecurity Skills Shortage

› A report from the Enterprise Strategy Group and the Information Systems Security Association indicates 46% of the organizations it surveyed "claim to have a problematic shortage of cybersecurity experts," with 69% of those organizations reporting that those effects are currently tangible. Areas of impact include workload increases for existing staff (54% of organizations reported this), the necessity of hiring and training junior employees (35%), and an inability to fully learn or utilize some security technologies to their utmost potential (35%).

Online Retailers Take Note Of These Consumer Barriers To Mobile Shopping

❯ Of the approximately 3,000 U.S. adults Fluent surveyed for the 2017 edition of its annual "Devices & Demographics" report, 42% (or 45% of women and 40% of men) said they purchased something via smartphone last year. Most (52%) made between one and five purchases via smartphone, while 11% were comfortable enough with smartphone shopping to make more than 20 purchases throughout 2016. For online retailers seeking to increase sales, it's becoming ever more important to take mobile into account, as Fluent also reports that 55% of those surveyed spend more time using their smartphones than any other device; runners-up were desktops at 14% and laptops at 12%. Also consider the accompanying chart, which highlights consumers' desired areas of improvement for mcommerce sites.



SOURCE: FLUENT

Augmented Reality For Business To Come Into Its Own In 2018

❯ "2016 was a year of discovery for AR, with the industry focusing on initial ROI metrics," said Eric Abbruzzese, senior analyst with ABI Research, in February, speaking about AR in enterprise as a whole. Abbruzzese expects this "pilot phase" to continue this year and ramp up next year, with shipments of smart glasses in particular experiencing a 227% CAGR and reaching 28 million shipments in 2021. This echoes an ABI forecast from December that focused on industrial AR applications; the firm expects 400% growth in that area this year compared to 2016.

Number Of IoT "Things" Forecast To Increase 31% This Year

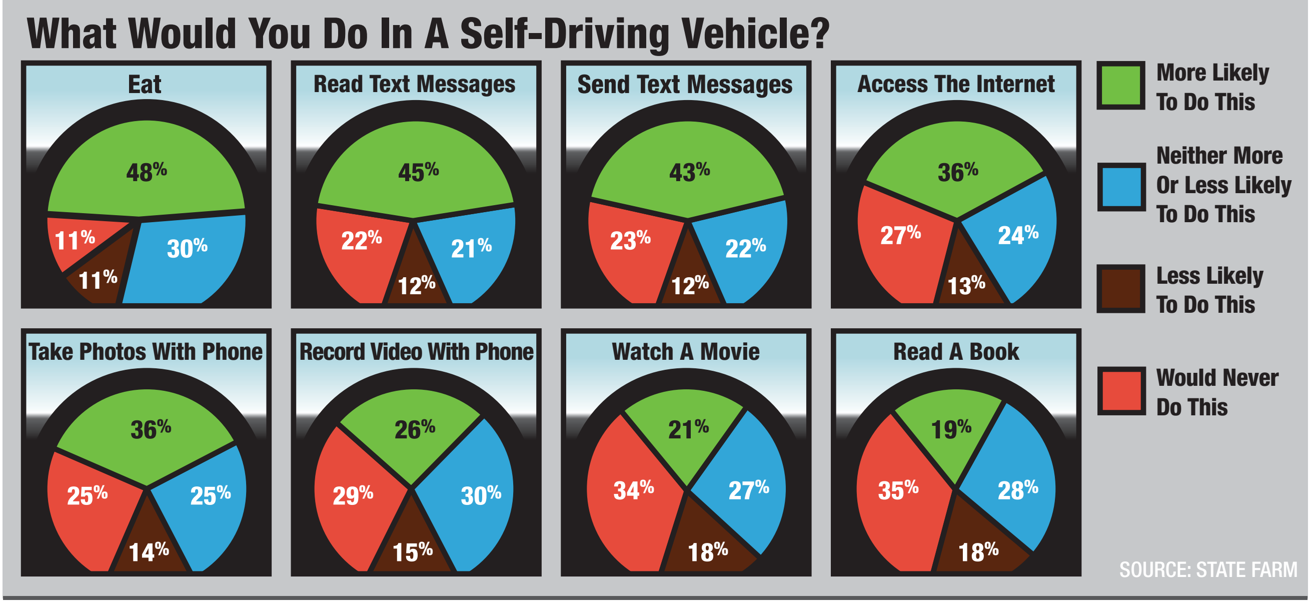
❯ Like cloud computing before it, the collection of technologies that fall under the IoT (Internet of Things) banner has caught on and is now growing at a predictably rapid pace. Gartner is among the research firms tracking IoT's growth, and its latest forecast indicates there will be 8.4 billion connected things worldwide by the end of 2017, a 31% increase over last year. The consumer IoT segment is the largest in terms of installed units, nearly three times that of cross-industry business. Gartner predicts there will be 20.4 billion connected things by 2020.

Banks Must Prepare For Digital To Keep Up With Demand

❯ The number of digital banking users could reach 3 billion, or about half of the world's population, by 2021, according to a new forecast from Juniper Research. "Technology is currently the big differentiator for all types of banks, including traditional banks and the so-called challenger banks," says report author Nitin Bhas. With increased demand comes increased expectations for all banks, so the pressure is on to invest more in banking technology. Juniper expects larger banks to acquire challengers, including startups and digital-only banks, in 2017.

What Would You Do In A Self-Driving Vehicle?

› For its "Autonomous Vehicles" report, State Farm surveyed 961 drivers to find out what they might want most from a self-driving vehicle. Most wanted help avoiding obstacles or dangers, with 54% wanting help backing up, 53% wanting the vehicle to alert them when they get sleepy, and 48% desiring a little help with parking. But what about the freedom a self-driving vehicle might bring? The accompanying chart shows what respondents would (and wouldn't) want to do if their vehicle did all the driving for them.



SOURCE: STATE FARM

Data & Analytics Solutions To Get Lift From Cybersecurity Trend

› The trend of incorporating machine learning technologies into cybersecurity solutions will help increase spending on big data, intelligence, and analytics solutions to $96 billion by 2021, according to ABI Research. Currently used in SIEM (security information and event management) solutions, which monitor for abnormal behaviors and activities, machine learning will also make its way into "traditional [antivirus], heuristics, and signature-based systems within the next five years," says Dimitrios Pavlakis, industry analyst with ABI Research.

Executives Remain Hopeful About The Future Of IT

› Business intelligence software vendor ChristianSteven Software recently surveyed 500 C-level executives about their technology concerns for 2017. Although 53.1% reported having some degree of worry about new competitors disrupting their market share, 91.4% said they were hopeful about the future of information technology. General concerns were split among security (46.5%), data (30.2%), and automation (23.3%), with 54.8% reporting data security as their top concern. And although automation was a concern, 59.1% said they don't view it as a threat to their business.

What People Think About When They Think About Virtual Reality

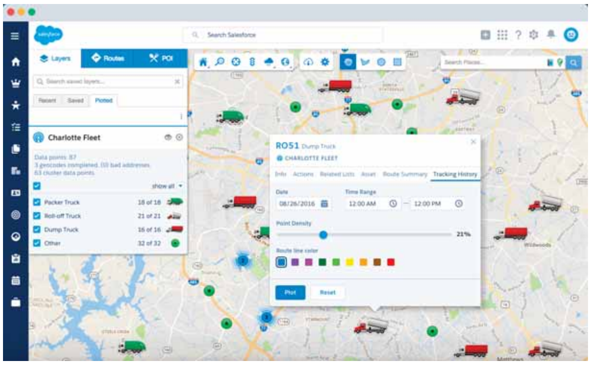
› VR (virtual reality) has its enthusiasts but hasn't yet captivated the mainstream imagination. A recent ReportLinker study based on multiple surveys of hundreds of U.S. consumers found that while 57% had heard of VR, only 31% considered themselves "very familiar" with VR, and 12% hadn't heard of it. When asked to name the first VR headset brand that comes to mind, 35% said none; but there were improvements for Samsung, as 28% said Samsung came to mind first compared to 9% three months earlier. Sony (11%) and Oculus (10%) took the No. 2 and No. 3 spots.

Videoconferencing Startup Zoom Raises $100M From Sequoia

❯ Founded in 2011 and based in San Jose, Calif., Zoom offers a cloud-based platform that's focused on videoconferencing but also ties in group messaging and other collaboration features. Zoom has become wildly popular, particularly among other tech companies, and claims to have more than 450,000 customers. Zoom recently announced that Sequoia led a $100 million Series D round of financing for Zoom, with AME Cloud Ventures (Yahoo co-founder Jerry Yang's firm), Emergence Capital, and Qualcomm Ventures also participating. Also, Sequoia partner Carl Eschenbach was named to Zoom's Board of Directors.

Startup Offers Mapping Layer For Salesforce, Raises $33.1 Million

❯ There's often a clunky separation between CRM (customer relationship management) systems and mapping software, with businesspeople having to switch from one to the other to coordinate information about where they are at a given moment and where they need to be. MapAnything, a Charlotte, N.C.,-based startup founded in 2009, offers a suite of desktop and mobile location-based applications that bridge the gap between customers' Salesforce data and maps. Its MapAnything For Salesforce application, for instance, literally puts CRM data on a map so field sales and service people can identify new opportunities nearby. MapAnything recently announced it had raised $33.1 million in Series B funding, which the company will channel into further development and expansion.



Charlotte Fleet

Data points: 87
3 geocodes completed. (0) bad addresses
63 cluster data points

☑ Packer Truck 18 of 18
☑ Roll-off Truck 21 of 21
☑ Dump Truck 16 of 16
☑ Other 32 of 32

RO51 Dump Truck
CHARLOTTE FLEET

Date: 08/26/2016
Time Range: 12:00 AM — 12:00 PM
Point Density: 21%
Route line color

Cloud Communications Firm Closes $104M Funding Round

❯ Since its founding in 2006, Fuze has enjoyed a rather quick ascent to a top spot in the cloud-based communications market. Based on the performance and popularity of its UCaaS (unified communications as a service) platform, the Cambridge, Mass., company has raised more than $300 million in funding, including a $104 million round in February. Founder and CEO Steve Kokinos says the new investment will go toward "geographic expansion to service our large global customers" and "product innovation in ways that align with our long-term growth strategy."

Neurala Delivers Artificial Intelligence For The Mainstream

❯ Artificial intelligence is clearly a hot topic these days, with big players such as Google and IBM gaining most of the media attention for their supercomputing AI systems. The 11-year-old Boston-based company Neurala, however, designed its neural networks platform, The Neurala Brain, for use in mainstream commercial products including drones, cameras, toys, and even self-driving vehicles. Neurala has landed some prominent customers, including Parrot and Teal Drones, for its NASA-based platform, and recently raised $14 million in a Series A funding round.

Startup Exabeam Seeks To Upset The Big Names In SIEM

❯ Traditional security measures focus predominantly on external attacks, and although the top digital security firms are adapting to help organizations fight internal threats, there is room for competition. San Mateo, Calif.,-based startup Exabeam is getting major attention for its SIEM (security information and event management) solutions, including those that target internal behaviors and provide automated incident response. Exabeam recently raised $30 million in a Series C funding round led by Lightspeed Venture Partners and Cisco.

Look For *CyberTrend* Magazine At These Technology Events

FEBRUARY

Industry of Things World USA 2017
Hard Rock Hotel
San Diego
February 20-21, 2017
The Industry of Things World team invites you to connect with over 500 Industrial Internet experts to challenge current thinking and unveil latest innovations at the must-attend Industrial IoT event.
www.industryofthingsworldusa.com

AITP San Antonio
San Antonio
February 15, 2017
www.aitp.org/group/174

CIO Summit Denver
Denver
February 21, 2017
www.ciodenversummit.com

Green Data Center Conference
The San Diego Supercomputing Center
San Diego
February 21-23, 2017
www.greendatacenterconference.com/san-diego-2017

Data Center World Dallas
AT&T Stadium
Arlington, Texas
February 22, 2017
http://local.datacenterworld.com/dallas/2017

AITP St. Louis
UMSL Cybersecurity Room
St. Louis
February 23, 2017
www.aitp.org/group/55

CIO Summit D.C.
Washington, D.C.
February 23, 2017
www.ciodcsummit.com

CIO Public Sector Summit
Washington, D.C.
February 23, 2017
www.ciopublicsectorsummit.com

CISO Public Sector Summit
Washington, D.C.
February 23, 2017
www.ciopublicsectorsummit.com

AITP Pittsburgh
Pittsburgh
February 27, 2017
www.aitp-pgh.org

MARCH

SecureWorld Charlotte
Charlotte Convention Center
Charlotte, N.C.
March 2, 2017
https://events.secureworldexpo.com/details/charlotte-nc-2017

CIO Summit Charlotte
Charlotte, N.C.
March 7, 2017
www.ciocharlottesummit.com

CISO Summit Charlotte
Charlotte, N.C.
March 7, 2017
www.cisosummit.us

Internet of Manufacturing Business Conference
Hyatt Magnificent Mile
Chicago
March 7-8, 2017
The Only Event Exclusively for Manufacturers Capitalizing on the IoT Opportunity: Powering Scalable Processes, Competitive Products & Smarter Performance.
www.internetofbusiness.net/manufacturingchicago

AFCOM NYC/NJ Metro
Location TBD
March 9, 2017
www.afcomnycnj.com

CIO Summit Chicago
Chicago
March 9, 2017
www.ciochicagosummit.com

CISO Summit Chicago
Chicago
March 9, 2017
www.cisosummit.us

CyberTrend®

Look For *CyberTrend* Magazine At These Technology Events

MARCH

National Healthcare CIO Summit 2017
The Langham Huntington
Pasadena, Calif.
March 13-14, 2017
www.nhciosummit.com

DatacenterDynamics Enterprise
New York Marriott Marquis
New York City
March 14-15, 2017
www.dcdconverged.com/conferences/enterprise

ISSA Blue Ridge
Blue Ridge CTC Tech Center
5550 Winchester Ave.
Martinsburg, W.Va.
March 14, 2017
www.issa-blueridge.org

AITP San Antonio
San Antonio
March 15, 2017
www.aitp.org/group/174

AITP Twin City
Ozark House
704 McGregor
Bloomington, Ill.
March 16, 2017
www.twincityaitp.org

AFCOM Greater Tampa Bay
Tampa Bay, Fla.
March 17, 2017
www.afcom.com/GreaterTampaBay

CIO Summit Dallas
Dallas
March 21, 2017
www.ciodallassummit.com

CISO Summit Dallas
Dallas
March 21, 2017
www.cisosummit.us

SecureWorld Boston
Hynes Convention Center
Boston
March 22-23, 2017
https://events.secureworldexpo.com/details/boston-ma-2017

AITP St. Louis
UMSL Cybersecurity Room
St. Louis
March 23, 2017
www.aitp.org/group/55

AFCOM Chicago
Chicago
March 27, 2017
www.afcom.com/chicago

AITP Pittsburgh
Pittsburgh
March 27, 2017
www.aitp-pgh.org

APRIL

CIO Summit U.S.
Miami
April 2-4, 2017
www.ciosummit.us

CISO Summit U.S.
Miami
April 2-4, 2017
www.cisosummit.us

CIO Cloud Summit
Miami
April 2-4, 2017
www.ciosummits.com

Data Center World Global
Los Angeles
April 3-6, 2017
http://global.datacenterworld.com/dcwg17

CIO Finance Summit
Miami
April 4-5, 2017
www.ciosummits.com

CISO BFSI Summit U.S.
Miami
April 4-5, 2017
www.cisobfsisummit.us

Visit www.cybertrend.com for a complete list of upcoming events.

CyberTrend

Digital Threat Landscape 2017

FILELESS MALWARE, SOCIAL ENGINEERING, RANSOMWARE, HYBRID ATTACKS & MORE

WITH EVER-GREATER FREQUENCY, new security threats arise that either didn't exist previously or are more sophisticated versions of older types of attacks and now have a better shot at getting past existing security measures. There is no doubt that companies are continually playing catch-up with hackers and other bad actors, which means that security vendors are having to ramp up their efforts in turn against ever-evolving threats. But let's face facts: no matter what solutions these vendors make available, there will always be another uncovered vulnerability, another hole in the general security fabric that attackers find a way to exploit.

“In terms of technology, you just have to have tight control and take a whitelist approach where you only allow things you know to run on your network. You have to be very controlling in what you let in. Instead of trust and verify, you have to verify first and then trust.”

AVIVAH LITAN
Vice President and Distinguished Analyst
Gartner

KEY POINTS

- Fileless malware is dangerous because it hides in memory rather than on a hard drive, making it more difficult to detect.
- Ransomware occurrences will continue to accelerate and may become part of larger hybrid attacks where they’re combined, for example, with DDoS.
- Mobile security issues are slowly increasing, but there is set to be a boom in security incidents involving IoT.
- Risk assessments are crucial to understanding your company’s unique vulnerabilities and security requirements.

By all accounts, 2017 is going to be no different than previous years when it comes to the continual rollout of digital security threats. With a combination of brand new types of threats as well as older ones rearing their ugly heads in new ways, everyone is going to have their hands full from a security perspective. It’s a constantly changing landscape where one threat vector gets the most attention and then hackers move onto the next one. We’ll give you a quick look at some of the threats organizations and consumers will face over the coming year, why some types of threats will be especially prevalent, and a few tips on what you can do to protect yourself against them.

Fileless Malware

The most successful forms of malware have a way of hiding from antivirus solutions or tricking security systems into thinking they aren’t there at all. With recent research from Kaspersky Labs, it was discovered that fileless malware was present in the systems of over 140 organizations in 40 countries. What made these programs particularly unique, however, is that they were hiding in memory, such as your computer’s RAM, and not on hard drives, so they were much more difficult to detect than traditional malware files.

Fileless malware programs have been used in the last few months to steal password, and that’s actually how Kaspersky Labs found out about this phenomenon in the first place. The key with these types of attacks is that although they can be discovered by traditional security solutions if they are located in a computer’s RAM, for instance, hackers have targeted forms of memory that are used or accessed less frequently, where the malware can lie in wait and steal data, making them much more difficult to find and much more dangerous.

"The rise of fileless malware is one issue that organizations aren't prepared for," says Avivah Litan, vice president and distinguished analyst at Gartner. "We saw this in the retail and financial services space. Now it's moving into the enterprise more where it's basically the malware doesn't write itself to disk. It's just in-memory the whole time. That's an old attack," she explains. "[Supermarket chain] Target had that type of attack a few years ago, but it hadn't really moved to the enterprise yet and organizational security. But now you're seeing it. The old defenses just don't work and they have to upgrade their new defenses. They also have to keep their systems patched and more secure. These attacks are just very difficult to see and protect against."

Social Engineering

When we asked analysts whether or not there were any security threats that were overplayed, we consistently heard the response "no," but there were some types of attacks that were underplayed, and one of those, according to Litan, is social engineering. Social engineering is a style of attack where a hacker essentially tries to manipulate their human target into clicking on a link, providing sensitive personal information in response to an email, or downloading an email attachment. The goal is to make the incoming message, which is typically done via email but can include virtually any other form of messaging, look as legitimate as possible. An attacker might, for example, pose as a financial institution, a coworker, or even your boss or company owner.

Social engineering attacks can be either rapid or slow and methodical. In some cases, the goal is to present a sense of urgency and thereby elicit an immediate response, such as a fake message from a manager requesting specific information. In other cases, the threat is a multi-part affair where the hacker attempts to gather some basic information about you, and, if you unwittingly provide it, proceeds to craft an attack against you.

And while you've probably heard about these types of phishing scams for quite some time, social engineering is becoming much more sophisticated. Perhaps the most dangerous aspect of these attacks is that they are targeted directly at individuals, which means they can often circumvent the security measures designed to stop them. Once malware is installed on the target's machine or sensitive information is stolen, it can then be used to either strike at the individual or as a gateway to go after a connected network or the company as a whole.

DO ANALYSTS CONSIDER ANY SECURITY THREATS TO BE OVERHYPED? THE ANSWER IS INVARIABLY "NO."

"You need people-centric security where your staff are really your front line and your consumers are your front line," says Litan. "People just have to become much more aware and on top of things. The technology has to be upgraded. Keep your systems up-to-date, secure; and patch your vulnerabilities. A lot of the attacks that take place exploit common vulnerabilities. You have to keep your systems clean, secure, and controlled, and have more visibility into them, but you also need to keep your people aware. People fall for social engineering attacks. You have to raise the level of awareness in the U.S. population, or wherever you're talking about. A lot of people are still very naïve about the threats."

Ransomware & Hybrid Attacks

Ransomware is a type of attack that has surged over the past couple of years. A good example of a ransomware attack might involve a hacker gaining control of your PC and locking you out of it until you pay a fee, or ransom. Michela Menting, research director at ABI Research, says these types of attacks are particularly successful, and that "many organizations find they don't have backups and are obliged to pay out in order to retrieve their files." That success, unfortunately, means that "there are many new threat groups carrying out such attacks, and not all can guarantee that they will return your files," Menting adds. In those situations, there's a chance that you will not only end up paying a fee, but you will also lose those files, or access to those files, entirely. "These types of attacks are spreading to cloud-based services, as well—see MongoDB as the most recent victim—so organizations cannot solely rely on cloud platforms, either," she says.

To make matters worse, there are also hybrid attacks where, for instance, there is some form of malware delivery that is grouped together with a DDoS (distributed denial of service) attack. When both of these attack methods are launched in tandem, most resources will go toward getting a website, service, or application back online while the ransomware or other form of malware goes at least temporarily undetected and can do some damage. But things are about to get worse, according to Menting, because these types of attacks are going to pull—and indeed have already started pulling—IoT (Internet of Things) devices into the mix for greater impact and reach.

"Ransomware will evolve to hijack connected IoT devices," says Menting. "The health care industry has been hard hit by ransomware, and attacks against IT

> "I don't think any threats have really been overplayed. Most networks, platforms, and devices are so insecure that even the oldest bugs are still causing havoc (despite existing patches) and many continue to use outdated and unsupported systems. Organizations, and end-users, are unprepared and often unaware of the abounding vulnerabilities and insecurities of the internet. To consider any threat to have been overplayed or hyped would be to seriously underestimate the inherent weakness of all things connected."

MICHELA MENTING
Research Director
ABI Research

systems and databases holding patient records. In time, it is likely that such attacks will render medical devices unusable until a ransom has been paid. This will directly affect patient safety. Ransomware, and DDoS using IoT devices, will be rampant in all types of businesses."

Nation-State Espionage

If you think it's scary to picture a lone wolf hacker building a custom piece of malware and using it to target your company or your personal data, then imagine what it would be like for that hacker, or a group of hackers, to have support from their own government. That's what has reportedly been occurring in Russia, China, and other countries where state-sponsored hacking groups target the U.S. government and related entities on a regular basis. In some cases, these attacks are blatant and can be traced by intelligence agencies back to the governments themselves, but in other cases the attacks come from standalone groups and are only discovered to be state-sponsored after the fact. "Nation-state espionage has been around for a while, but the Russians and Chinese are just much deeper into our systems than anyone imagines," says Litan. "That's a big problem."

There's a great deal of controversy surrounding the reported hacking of the Democratic National Convention in 2015-2016, but one thing that most intelligence agencies agree on is that the Russian government was involved the attacks. In this case, Russia was able to steal emails and other pieces of information, which were then released to the public and served as a major political issue throughout the 2016 presidential campaign. These attacks are particularly dangerous because they can come from multiple angles and involve a wide range of bad actors. For one, you may have a double agent of sorts working inside the U.S. government and sending secrets to a foreign government. Or, it could be a hacker working remotely and spoofing their connection to look mundane as he steals valuable information for personal financial gain and/or for their country's government.

Mobile & IoT Security

When it comes to threats to mobile devices, Menting says that thing haven't evolved much over the past few years. She says, interestingly enough, that innovation has been slowed because "the operating systems are so diverse" and "it's difficult to target a large group with just one strain." Every time there's a new version of an operating system, the malware would have to be tweaked in some way, which is "more costly in time and resources for the attacker," Menting adds. Returning to the topic of nation-state and related attacks, she says that mobile devices "remain the prerogative of state actors who are keen to leverage them for espionage purposes." But when it comes to general cybercriminals, mobile devices aren't the best possible tool, but Menting says they are still "a significant threat factor."

One thing you'll find with mobile device security is there are many "good news, bad news" situations. On the bad news side, according to Patrick Hevesi, research director at Gartner, "network-based attacks were more prevalent than malware in 2016." He says hackers are going to start attacking mobile container boundaries, there are more configuration-based attacks occurring where hackers change settings on devices, and there is now mobile malware that can essentially lock your screen until you pay a fee as already occurs with desktops. But the good news is that security vendors are working to get a handle on mobile threats and are getting more relevant data than ever before.

"The vulnerabilities are there for iOS and Android and will continue to be discovered. We saw the IoT DDoS attacks last year, [and] in the future we could see similar attacks on the pool of billions of mobile devices in the world. The main challenge is spreading the malware or taking control of the devices at scale."

PATRICK HEVESI
Research Director
Gartner

"The biggest challenge we have with mobile threats and understanding how widespread the threats are is the lack of real world numbers," says Hevesi. "This [began] to improve in 2016 due to the fact that mobile threat defense vendors [are] getting their agents on more mobile devices. This is allowing us to get better statistics, but we are still far from where we need to be to completely understand the full risk yet. That being said, when we see attacks like Pegasus, Gooligan, Dirty COW, QuickSand, XcodeGhost, Youmi, mobiSage, JSPatch and AceDeceiver, these have the capability to cause damage and exfiltrate corporate data. But just because one device is infected," Hevesi adds, "that does not mean my whole enterprise is under attack. We have not seen propagation like desktop viruses, for example, that infect one endpoint and then tries to scan the enterprise network and infect other devices yet on mobile devices."

However, the news isn't as good when you look at the impact of IoT-related security threats. You can look to the many IoT-related DDoS attacks that occurred last year, and Hevesi says there could be "similar attacks on the pool of billions of mobile devices in the world" in the future. Menting agrees and says the issue is complicated further when you think about the sheer number of devices out there that could be brought into an organization by employees or "that form part of building automation systems," just to name a couple of examples. "They provide a threat vector that cybercriminals can leverage to penetrate an enterprise, or can be used in DDoS attacks," she says. "Organizations will need to consider these devices in their security policies."

What You Can Do Now

For even more bad news, Menting says that companies simply aren't doing enough to protect themselves from potential attacks. "Many organizations tend to rely on basic defense appliances, such as basic authentication to endpoints like PCs, antivirus, firewall, and some encryption," she says. "Many do not have incident response plans, or security policies that cover devices other than PCs. Many haven't thought about third-party applications where employees are using company data, or personally liable smartphones that are connecting to corporate networks. Many organizations don't perform risk assessment or put in place information governance programs. They don't assess risks and prepare for potential attacks. Security is an ongoing activity—it cannot just be thought about once and left to machines to tackle. It requires input from the organizations based on its needs, requirements, and acceptable levels of risk, and is therefore an exercise that needs to be undertaken on a continual basis."

So what can companies do to get themselves back on the right security track? Well, there's actually quite a lot that can be done. As a start, companies need to perform risk assessments to get a baseline on where they're at and measure against their specific security goals. And they need to have a plan in place for when an incident does occur. "This will help significantly in planning for the appropriate security mechanisms to implement and keep costs at a reasonable level," says Menting.

For Hevesi, the key is to look at what your company does and focus on the specific needs of your organization from a security perspective. For example, if your application or service requires users to sign in and perform certain tasks, you can put behavioral monitoring solutions in place to track unexpected actions. You can put more complex network protections in place to make it as difficult as possible for hackers to get in without compromising performance for end users. But most of all, Menting suggests, you simply need to put security top of mind and constantly assess your organization for potential threats. "Many organizations spend on ineffective security solutions that are simply not adapted because they do not understand their own vulnerabilities or risks," says Menting. "This is almost as bad as not thinking about security at all." C

Methbot's Millions

HOW GREED BROUGHT DOWN A SOPHISTICATED AD FRAUD PROGRAM

KEY POINTS

- Digital ad fraud isn't new by any means, but Methbot was a particularly sophisticated attack perpetrated by hackers.
- When the hackers behind Methbot ramped up the number of fraudulent ads in play, White Ops took notice and was able to coordinate a shutdown.
- White Ops hopes that Methbot's shutdown will result in more money going to content creators in the long run.
- To prevent fraud, publishers need more robust auction systems, and advertisers need to use third parties to validate purchases.

EVERY NOW and again in the cybersecurity world, an unprecedented attack happens that either causes massive damage and sends people scrambling or unites an entire community to fight back. Then there was Methbot, a sophisticated digital advertising ring that not only took money out of the pockets of advertisers and publishers alike, but also caused a swift and decisive retaliation. Although this story could've ended with the typical post-attack damage control, it instead turned into a galvanizing event for the digital-advertising industry that could prove to prevent similar attacks in the future.

How Digital Ad Fraud Works

Digital advertising fraud is nothing new. In fact, Michela Menting, research director at ABI Research, says ad fraud is "a particularly lucrative operation because the online advertising market is so highly profitable." Online advertising is handled through a process called programmatic ad buying, where a website essentially auctions off open ad slots to the highest bidder. Once the transaction is complete, the ad shows up on the website in the specified slots and in front of the eyes of visitors.

"Every time a user loads a page, a massive bidding war is going on behind the screen for the right to advertise on that page to that particular user," says Menting. "This is done through advertising networks where advertisers, and other third parties serving the ad market, play. The various ad players will look to see if they have any cookies on that user and, based on the information they have on that user, decide which ad to display and how much the ad is worth. It's a highly lucrative market for advertisers, and of course a click on that ad is worth more than just an impression."

Methbot, in particular, took advantage of a specific segment within the overall digital ad market called pre-roll video ads. These are ads that play before YouTube videos, for example, and often have links that viewers can click to go to the advertiser's website. What these hackers were able to do was "build a complicated system of robotic ad viewers that looked like browsers spread out across the whole [United States] and were visiting websites and watching ads," says Michael Tiffany, CEO and co-founder of White Ops, the company responsible for discovering Methbot and, ultimately, helping bring it down.

The real secret of the attack is that instead of targeting one company or a small group of companies, these hackers went after 6,000 of the most popular sites on the internet even though they, obviously, weren't in control of any of them. "These guys figured out that they could exploit a loophole in the way that programmatic ad buying works to create auctions that appeared to be name-brand ad inventory on popular sites," says Tiffany. They were creating these counterfeit ad opportunities and then serving them to their army of robots and basically pocketing the money. They could counterfeit just a little bit of ad inventory from every single one of those domains. In many respects, this is the perfect kind of crime because instead of hitting just a few victims hard, they were stealing just a little bit of money from a lot of victims."

Committing One Of The Seven Deadly Sins

So, there Methbot was, humming along and generating revenue by pooling funds from thousands of different touchpoints, but then it made the mistake of going too big too fast and getting on the radar of White Ops. "We are in the business of identifying robotic, fake traffic in advertising, because it's a very profitable scheme overall, generating more money than any other form of mass cybercrime," says Tiffany. No. 2 on that list, he says, is ransomware, because it's been growing so fast. "Ad fraud, by being so profitable, has attracted a whole bunch of cybercriminals to try their hand at it, and White Ops is a company built to identify that and stop it."

> "The ad networks look at specific characteristics to see if the ad request is legitimate, and if those clicking are legitimate. If it passes such a threshold, there is no secondary audit to see if they were real or not. It's really up to fraud-detection engines to root out IP addresses and other URLs to add to blacklists that these automated programs can refer to. It's a cat-and-mouse game, with ad fraud groups seemingly always one step ahead."
>
> ***MICHELA MENTING***
> *Research Director*
> *ABI Research*

In the beginning, Methbot didn't do much to stand out from other ad-fraud operations that White Ops deals with on a day-to-day basis, but then there was a spike in the total amount of counterfeit inventory near the end of September and another, much larger spike in October where the program ramped up to the point where it could generate millions of dollars a day on fraudulent ads. These spikes grabbed the curiosity of White Ops, and so the company started a more in-depth investigation into what was going on.

"Because they ramped up so aggressively, that got more of our attention, and that's when we saw one of the most unusual and, frankly, most sophisticated aspects of the operation," says Tiffany. "They were actually doing the crime out of data centers. There were just three of them, two in Dallas and one in Amsterdam, but they had created fake entries in the internet's RIR (regional internet registries). The internet only has five of these RIRs that administer all of the IP address base for the entire internet. These are organizations like ARIN, which covers North America, and RIPE NCC, which covers Europe, and AFRINIC, APNIC, and LACNIC."

What the hackers were able to do was create fake entries for IP addresses that they controlled in the right regional internet registries so they wouldn't stand out. Rather than looking like one huge entity, it was instead divided up into several smaller ones spread across multiple ISPs around the country, including Time Warner Cable (now Charter), Comcast, and Cox, among others. Tiffany points out that no one had ever seen an attack quite like this before, but because it was so advanced, it actually turned into somewhat of an Achilles' heel. Where other ad-fraud operations used botnets and malware, this one used a bot farm "using this carefully crafted IP address base," Tiffany says.

Although greed initially put Methbot on the White Ops radar, it was the sophistication of the program itself that ultimately led to its downfall. "That's when we spotted our opportunity for a globally coordinated shutdown," says Tiffany. "That IP space is not easily changed, so if we could circulate among the entire ad industry the information that we had put together about the operation and importantly about the IP space that they used, then everyone could inoculate themselves. On Dec. 20, we gave this a whirl and, using an organization called Tag, we coordinated among all of the major ad tech players that needed to do something to inoculate their systems, and I'm happy to report that was a success. And so this operation that had grown in size quite considerably was totally off the internet within 24 hours."

How Advertisers & Publishers Will Protect Themselves

The problem with defending against an attack like Methbot is that it made victims of both advertisers buying ads and publishers selling ads, which means that "for every dollar that went to a Methbot impression, that's a dollar that didn't go to someone's legitimate ad opportunity," Tiffany says. For that reason, it takes both sides coming up with their own security solutions and checks and balances to ensure that something like this doesn't fly under the radar ever again.

On the publisher side, Tiffany says it's important to realize that this isn't a situation where someone "fell asleep at the wheel" because it was such a difficult flaw to exploit in the first place. There were quite a few moving pieces, which is why he says "there's nothing shameful about not having a defense in place." Still, publishers were shocked at how well Methbot was able to counterfeit ads, which is leading to some system redesigns.

"White Ops is working with publishers to help them defend themselves, and that's some very important work because this is the kind of thing where when you're getting your inventory counterfeited, there are no indications that it's happening," says Tiffany. "The publishers that were victims here couldn't tell that they were being victimized. We're setting up monitoring systems to identify when someone is selling inventory that they don't really have."

On the advertiser side, Tiffany says the main course of action is to "engage with an independent third party to validate that they're truly getting what they paid for." He also points out that this process is nothing new in the business world. He compares it to the first time that American enterprises went online and saw both the massive opportunity, but also the major risks associated with the internet. "It's something that other departments in any corporation had to learn themselves," says Tiffany. "First you're online, and then you go, 'Oh my God, I can't believe all of the opportunity, but also all of the bad stuff out here.' Then, you need to start budgeting for security. It's a process we've all gone through, even individuals in buying antivirus software."

"We are in the business of identifying robotic, fake traffic in advertising, because it's a very profitable scheme overall, generating more money than any other form of mass cybercrime. [No. 2], because it's been growing so fast, is ransomware. Ad fraud, by being so profitable, has attracted a whole bunch of cybercriminals to try their hand at it, and White Ops is a company built to identify that and stop it."

MICHAEL TIFFANY
CEO & Co-founder
White Ops

Long-Term Impact Of Methbot

When something as far-reaching as Methbot is discovered, it makes sense to think about the potential long-term implications of such an attack. The fortunate part, depending on how you spin it, is that "marketers are aware that some of their budget will be going to fraud," says Menting. "Ad networks are also aware that some of their revenue will be generated by bots. It's an accepted risk, but the online ad market is so lucrative that it is one most are willing to accept. Companies like Yahoo, Google, Amazon, et al. make excellent use of user behavior (despite bot activity) and are more than willing to take the risk in exchange for the vast troves of information they can gather on user behavior."

What does make Methbot unique, however, is in how it was shut down so quickly by a large and well coordinated effort. Once the hackers started getting a little too greedy, White Ops quickly caught on to what was happening, let the parties involved in on the situation, and then worked together to bring it all down. "That's amazing, because what will happen if we keep this fight up and we take it all the way to victory, then it means we're going to be cleaning up all of the bogus inventory that is distorting the ad market, and that's ultimately really good news for your content creators."

In fact, what Methbot may have done is open the door for preventing or, at the very least, quickly addressing ad fraud in a way that helps content creators better engage with a real human audience. If all of those dollars that were previously going to bots and ad counterfeiting rings actually made it to the content creators and publishers, then it would bring more success to all of the parties involved and encourage more opportunities in the future. It's a true high tide raising all boats scenario where fraud is eliminated, and revenue goes to the right people.

"We're talking about creating a more vibrant and fairer system that's rewarding creators better and ending this crazy downward price pressure that's been making it harder and harder to be a content creator because it seems like prices are down all the time," says Tiffany. "The reason why prices are down all the time is because a glut of fake inventory pushes prices down. If there's artificial oversupply, then of course prices drop. What I'm seeing is a leveling of the playing field, and the elimination of all of these fakes is making this a more honest and fairer system, which is ultimately good for the people creating great content on the web."

How To Measure Cloud ROI

COMPARE COSTS, BUT KEEP IN MIND FLEXIBILITY & PERFORMANCE GAINS

KEY POINTS

- Estimates show that companies spend about 20% of their overall IT budgets on cloud-based solutions and services.
- Companies that only focus on meeting cloud ROI expectations might be missing out on getting the best possible return through optimization.
- Measuring cloud application costs against on-premises is important, but other factors also need consideration.
- Backing away from the cloud or migrating can be difficult and expensive, so choose a trusted cloud provider up front.

ONE OF THE most important aspects of investing in a new technology, a new piece or equipment, or a new service is to make sure you get a solid return on said investment. After all, companies are in the business of making money, so it makes sense that they need to get something back for every dollar they spend. Cloud computing is no different. Surely you've heard the argument for years, that moving to the cloud will result in cost savings, help you consolidate your internal infrastructure, and provide more agility in how you're able to spin up new resources and push your business forward.

While all of that may sound great on the surface, actually achieving those goals, let alone measuring the corresponding results, is something else entirely. There are so many factors to take into account when judging the ROI (return on investment) of cloud-based commitments that it can be difficult to determine, when all is said and done, whether or not you've actually lowered costs and are spending less than you did when you focused more on physical equipment and on-premises servers. The key here is to not only develop a baseline that you can measure against, but also to keep track of every facet of your organization in which the cloud is making a difference.

Cloud Computing & IT Budgets

According to Ed Anderson, research vice president at Gartner, organizations, on average, "spend about 20% of their IT budgets on cloud computing," but when asked if that is not enough, just enough, or too much, he points out that it's all subjective based on the company

"For me, for cloud to really empower enterprises, it has to be part of a digital transformation. In other words, companies that want their technology to scale quickly on-demand to changing business requirements also need their businesses to change quickly–so being more flexible in terms of business processes, financial, and budgets, and empowering employees with some flexibility to choose and run the best cloud tools for their jobs."

OWEN ROGERS
Research Vice President
451 Research

at hand. "Smart organizations have aligned their spending on cloud commensurate with the value they get from using cloud," says Anderson. "This value may be in the form of cost savings, agility, innovation, or other things. Organizations that see the value from cloud and do not invest to capture that value are underspending. Organizations that haven't quantified the value from cloud computing, and yet invest in cloud solutions, are over spending. In general, I think IT spending is shifting to cloud at a reasonable rate."

These rules of thumb are helpful when trying to determine whether or not your current investment in cloud computing makes sense for your company, but they aren't the whole story. One underappreciated aspect of the cloud is the flexibility it offers in terms of giving employees meaningful tools to use in day-to-day operations. If you think about how cloud computing fits into your overall IT budget, of course it's important to focus on the actual contracts and service agreements, but it's also important to consider the impact it may be having on your workforce. Achieving that understanding may require going against one of the major selling points of cloud computing, which is to spend less money.

"A crucial mistake I hear of a lot is [organizations] expecting cloud to make cost-savings over traditional infrastructure," says Owen Rogers, research vice president at 451 Research. "For me, if you are using cloud in its most efficient manner, you will probably be spending more than you did before. Why? Because cloud means you can rapidly address demands in ways you didn't expect in a matter of minutes. If you are using cloud in its most exciting way, employees should be able to utilize the cloud when and how they want to (within reason) to help the company achieve its goals."

One the most interesting aspects of the cloud is that, due to growing maturity, it's simply becoming table stakes for a lot of companies. In fact, Ryan Martin, senior analyst at ABI Research, says "we are at the point where the ability to operate at cloud-scale is a minimum requirement for companies to be competitive in the long run." This means that focusing on the cloud as part of your IT budget is going to be more important, and potentially more difficult, as it starts to touch more and more parts of the business. The cloud complements, the cloud replaces, and the cloud enhances, which can make measuring success and managing a budget more complex. Plus, the cloud continues to evolve and go beyond the basic benefit of storage, so there will always be new metrics to consider as you move forward.

"The commoditization of cloud storage means that providers are under pressure to build out and bake in a better suite of capabilities equipped for heavy lifting," says Martin. "Today, the cloud is about much more than storage. It is about the centralization of compute power, resource, and intelligence across an increasingly disparate and diverse technology landscape. The challenge is that even though cloud providers continue to expand the app, analytic, and data management capabilities that come with their respective offerings, it doesn't mean that companies consuming these services, especially those that already subscribe, are aware of them, let alone willing and able to train teams on how to use these new tools."

"Organizations should shift their IT budgets and financial models to an operating expense basis (rather than capital expenses). They should also be very clear about what the shift to cloud services means for their organization. Cloud services are highly standardized offerings so they should accept them as such. This may mean giving up some custom features they may have implemented in their non-cloud systems as they move to cloud."

ED ANDERSON
Research Vice President
Gartner

Getting The ROI You Expect vs. The ROI That's Possible

Determining the success of a given technology investment is going to vary wildly from company to company depending on expectations as well as expertise. For example, if you have never worked with the cloud before, you move an application over to a SaaS (software-as-a-service) provider, and you lower spending as a result; then you've achieved the ROI you expected, but that may not the best possible ROI. If a company is well-versed in the cloud, then it may have higher expectations and therefore get closer to that optimal ROI.

In general, Anderson says, there are several types of cloud usage, which means there are multiple ways to measure value and ROI. As an example, Anderson says that a "simple life-and-shift" implementation where you just move an application from on-premises to the cloud "often falls short of ROI expectations, whereas developing a new application from the ground up in the cloud "typically meets or exceeds ROI expectations." And if a company decides to go with a prebuilt SaaS application, it "usually results in the ROI the organization expects."

Where things tend to get more interesting is when you look at what's actually possible, which is an area where Anderson thinks a lot of companies are falling short. You may see benefit from merely moving an application to the cloud, but it's in the optimization that you start to see real gains. To help with this process, Anderson lays out a few steps to follow. The first is to "monitor and profile the application to determine the optimal resources needed by the application," he says. The second is to migrate the application to the cloud or build it from scratch in the cloud. And the third, Anderson says, is to "monitor and profile the application running the cloud."

From there, it's time to do some tinkering. Steps one and two are all about adjusting "the resources used by the application" and leveraging "the elastic nature of the cloud to expand the application resources when needed, on demand," Anderson says. This is the step where you fine-tune the application to the point where it not only meets your existing needs, but is also flexible and malleable enough to mold to future needs. The final step, according to Anderson, is to return to steps three, four, and five until you feel that the app is fully optimized. "Most organizations do step two, and some organizations will do steps one and two, but most don't do the subsequent optimization, which means they don't realize the greatest potential ROI," Anderson says.

How To Measure Cloud ROI

When it finally comes down to measuring cloud ROI, Anderson says that most companies start by measuring against "a baseline of spending established in their traditional data center," which means trying to "compare the costs of running the application in a traditional mode and then compare the costs of running the application in the cloud." From there, he says, companies can start to take agility, innovation, and performance into account as potential metrics that may play into the overall ROI of the cloud.

It's in this area that Martin likes to talk about time-to-value as an important metric, which is when, instead of checking off boxes, "it is something that needs to be continually revisited to ensure a cloud investment is optimized over the entirety of its tenure."

"One of the most attractive success metrics is time-to-value. This doesn't just mean checking off a box; it is something that needs to be continually revisited to ensure a cloud investment is optimized over the entirety of its tenure."

RYAN MARTIN
Senior Analyst
ABI Research

However, Rogers says that one mistake to avoid when measuring the success of a cloud implementation is confusing TCO (total cost of ownership) with return on investment. "It's important to distinguish between TCO and ROI," he says. "If an ecommerce site has 10 times the usual demand, then the TCO of the cloud meeting that demand is going to be 10 times greater than usual, but TCO is irrelevant here. If the company makes 10 times the revenue as a result, then the ROI is going to be huge. The same issue applies if departments increase productivity as a result of easy and quick access to technology, or if a new geography is quickly targeted as a response to a need."

Another area that Rogers likes to focus on with cloud ROI is the flexibility of giving employees access to the resources they need as they need them. He says that "for the cloud to really empower enterprises, it has to be part of a digital transformation" Companies need to focus on scaling on demand and changing their business processes and budgets to keep up with that demand. The key is to not lock in budgets to the point where the company becomes rigid, as doing so results in losing out on many potential cloud benefits. Instead, it's best to put tools in place to help monitor cloud usage, and then use that data to come to an ROI and budgeting conclusion.

"I like cloud tools that allow end-users to access cloud services, but with a degree of governance, and CloudHealth and CloudCheckr spring to mind," says Rogers. "These tools let enterprises users consume on-demand cloud services with a degree of choice, but [allow] spend and security to be controlled by the IT department. Yes, you can measure usage of cloud services, with the cloud providers typically some reporting on this. What is harder to do is reconcile how revenue is growing as a result of increased cloud use and spend, although companies like Apptio and Cloud Cruiser offer tools to help measure this."

The Difficulty & Cost Of Backing Out

The final piece of the pie, according to Anderson, is to understand the complexities and potential costs of disengaging from a given cloud service or solution in the event that it no longer works well for your organization. He points to "expensive data export fees, complex data integrations, management tools dependencies, lack of an alternative location to host the application, lack of personnel" and "long-term contractual commitments" as just a few stumbling blocks that can occur when trying to migrate from one cloud solution to another. That's why it's so important to find a cloud provider that you trust up front, and fortunately, Anderson says, that's the case for most companies.

"If they have built their application (and cloud usage) to utilize the most basic capabilities of cloud—[for example,] provisioning virtual machines—then it's easier to move off of cloud," says Anderson. "As soon as the application starts using native platform capabilities, integrating with cloud APIs, using cloud management tools, etc., it becomes harder and harder. For these reasons, plus the fact that most organizations are reasonably happy with the cloud services," he adds, "we don't see many organizations move from cloud back to their non-cloud environment, or to another cloud provider."

Travel Management

FLIGHTS, HOTELS, EXPENSES & EASY-TO-READ REPORTS VIA THE CLOUD

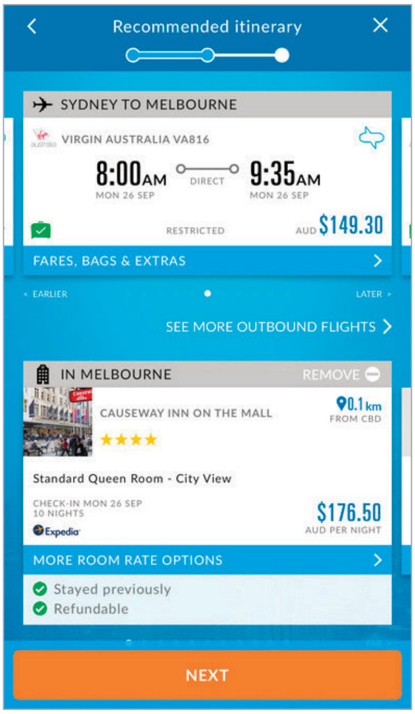
KEY POINTS

- Dozens of vendors today offer services that can handle all or most business travel booking and travel management needs.
- Many travel management solutions offer tiers of service, so explore the differences between tiers to ensure you get all of the features you expect.
- The main benefit of using a travel management service is that it helps travelers and companies alike stay organized.
- Check for support offerings. Some services, including FCM Travel Solutions, also offer emergency support.

ONE OF THE BIGGEST HEADACHES of business travel is having to track every little detail from the point at which trip planning begins to the moment you're back in the office. Finding a good hotel rate, booking a flight, reserving a rental car, and planning out meetings are only part of the fun. Next comes following a meal budget, keeping track of receipts, and reporting the whole works when the trip is done.

If your organization is still stuck in the past, relying on the employee to keep all receipts and invoices, build spreadsheets or other travel documents, and then present them to the HR department to hash out all of the details for reimbursement and approval, this article is for you.

In today's world of enterprise-focused applications and the power of cloud computing, we are no longer bound to the tired old methods. Dozens of vendors offer services, typically available for desktop and mobile devices alike, that can help you do everything from booking a flight and storing ticket information to populating an expense report with any relevant data from the entirety of a trip. What follows are a few examples of vendors that offer flexible, feature-rich, cloud-based travel management services.



With Serko, travelers can get recommendations for flight and hotel rates, making it easier to pay the best possible price very time.

Certify lets you keep track of receipts and expenses via the cloud on a mobile devices or your computer.

Certify

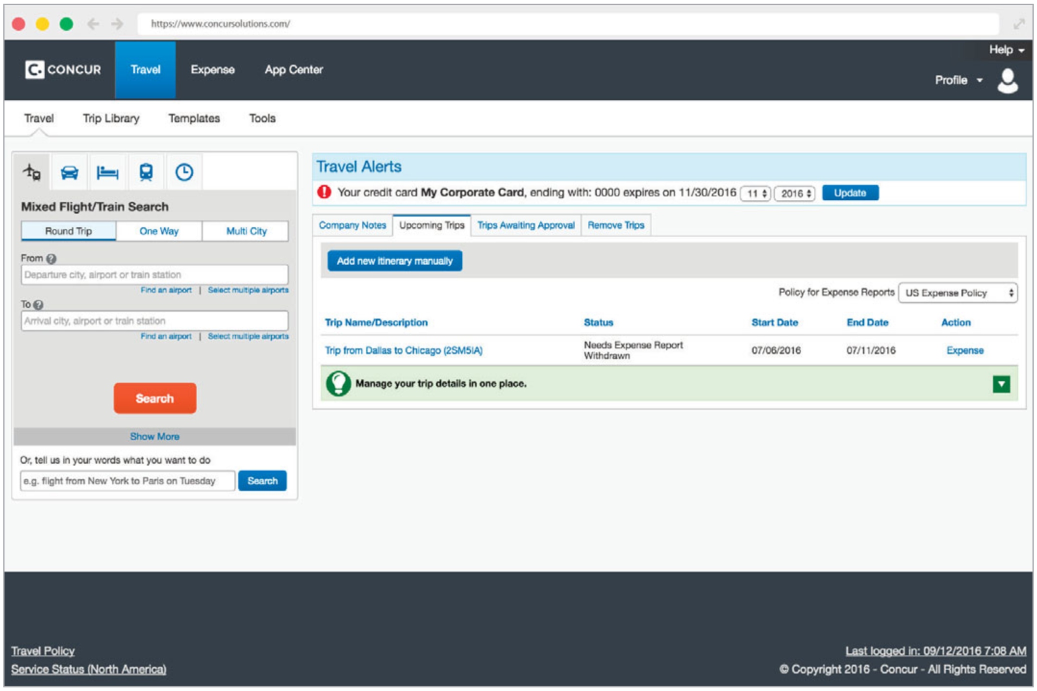
The best travel management services are flexible enough to support companies of all sizes, whether that be a small business with 10 employees or a larger corporation with hundreds of workers. Certify understands that one solution doesn't necessarily fit all, which is why it offers three different plans, each of which come with base features plus a few extras as you move up the tiers. For example, all plans from Certify Now! to the Professional and Enterprise versions offer a free mobile app for creating reports, receipt scanning with autofill, unlimited cloud storage for receipts, automated expense reports, travel analytics, role designation for employees, live technical support, and the ability to build reports using over 140 different currencies. Plus, you also get the option of creating custom categories within your report, which is great for companies that have unique internal policies and processes with regard to business travel.

With the Professional version of Certify, you add the ability to integrate not only business credit cards, but also personal credit cards into the service and your reports. This makes it much easier to track transactions while on the go. And to make sure you always have a clear trail to follow, Certify Professional also offers backup for receipts. The Enterprise edition adds HMS (health care management system) and ERP (enterprise resource planning) integration as well as support for 64 different languages.

With each version of Certify, you can either get access to a free trial or request a demo so you can try it out before you signing up for the service. If you like what you see, then you can choose a plan depending on how many employees you need it to support, which also impacts cost. For example, Certify Now! (one to 25 employees) is $8 per user per month, Professional (25 to 200 employees) carries a monthly service fee that depends on the number of users, and the Enterprise version (over 200 employees) is available at an annual fixed price.

Serko

While many travel management vendors focus on the solutions themselves and how they'll work for you, something that tends to get lost in the details is how well their solutions integrate with companies' other



Mixed Flight/Train Search

From: Departure city, airport or train station

To: Arrival city, airport or train station

Or, tell us in your words what you want to do: e.g. flight from New York to Paris on Tuesday

Travel Alerts

Your credit card **My Corporate Card**, ending with: 0000 expires on 11/30/2016 11 2016

Policy for Expense Reports: US Expense Policy

Trip Name/Description	Status	Start Date	End Date	Action
Trip from Dallas to Chicago (2SM5IA)	Needs Expense Report Withdrawn	07/06/2016	07/11/2016	Expense

Manage your trip details in one place.

Last logged in: 09/12/2016 7:08 AM

© Copyright 2016 - Concur - All Rights Reserved

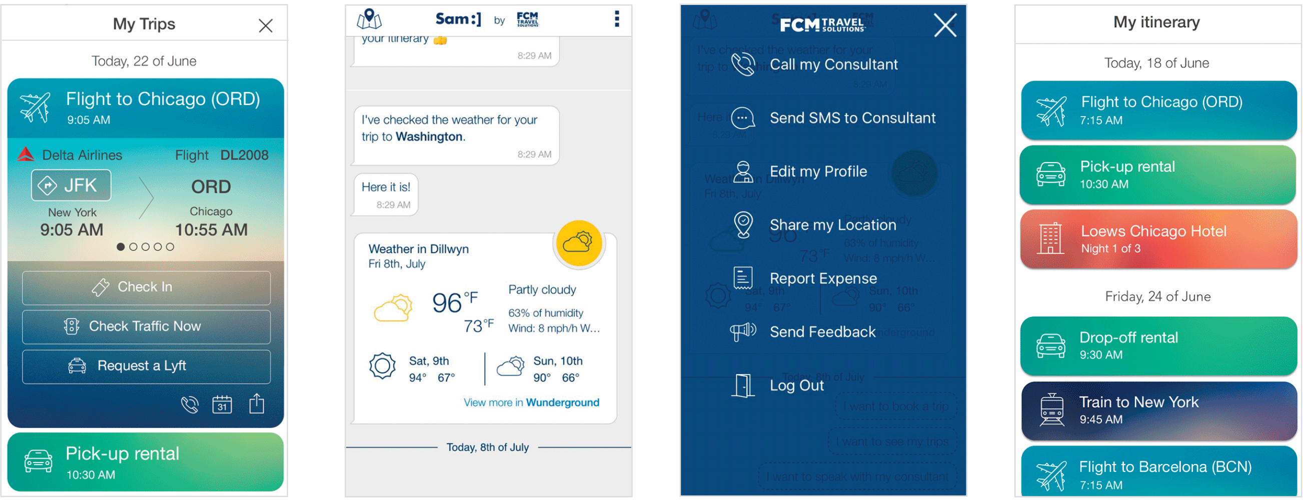
With Concur's Travel tools, employees can keep track of every aspect of their trips, including flights, rental cars, hotels, transit trips, and more.

software and infrastructure. Serko makes this perfectly clear with its overarching Serko Online service and its Serko Expense and Serko Mobile solutions. The Serko Cloud is where a lot of the magic happens because it serves to automate much of the monitoring, approval, and reporting processes that happen after a trip. In fact, you can set it up so that once Serko Online has received all of the data from a trip, it can check to make sure the total expenses are under the pre-approved estimation for the trip and then automatically send it to the finance team rather than force the employee to go through manual processes.

The focus of Serko Expense, by contrast, is on tracking receipts, which can be approved or rejected directly from the mobile app. What's particularly useful here is that if you pay for something with a corporate credit card, both the card statement and the captured receipt can then be sent to the Serko Expense Cloud, combined into a matching record, and then pushed through for submission. Additionally, Serko Mobile is available for iOS and Android devices so you can take pictures of receipts and track other elements of your trip without having to sit down at a PC or enter information via a web portal. Everything comes together seamlessly to take a lot of the guesswork out of travel management.

Concur

If you follow the travel management market or have used such solutions at any point in time, then you're probably familiar with Concur, which is an SAP company. Concur is among the few companies that have become synonymous with business travel, and for good reason. The secret to Concur's success is in how it offers a broad assortment of tools meant to cover nearly all of the bases in terms of business travel. For example, there is Concur Invoice for automating accounts payable processes, which not only relates to travel but also to day-to-day operations. There's also Concur Expense, which is more focused on trip tracking, receipt auto-uploads, and managing other expenses related to business travel. And then there's Concur Travel, which aids in the travel planning process, keeps track of electronic receipts, and helps you build reports. Most, if not all, of these solutions are available browser-based or PC



your itinerary 8:29 AM

I've checked the weather for your trip to **Washington**. 8:29 AM

Here it is! 8:29 AM

FCM Travel Solutions offers a mobile application where you can track your entire itinerary and even get weather updates.

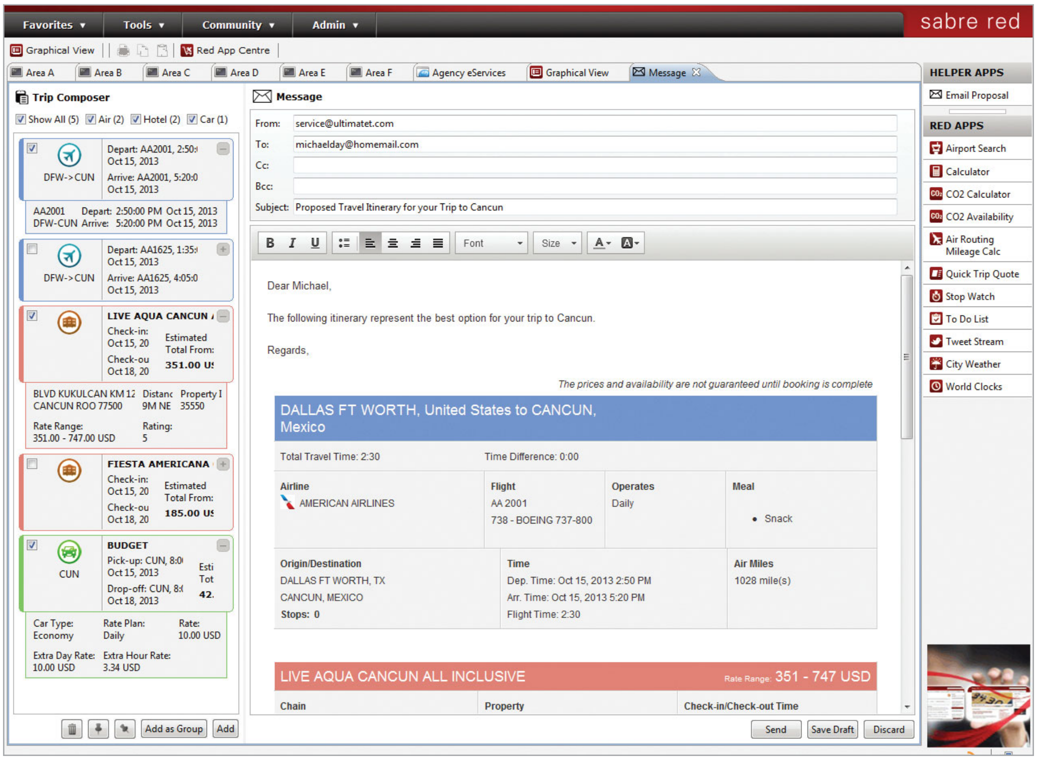
services as well as being part of the Concur Mobile application.

Perhaps the most interesting aspect of Concur is in how it also tailors its solutions to specific industries and use cases. The company breaks these down into five different categories: small business, federal government, health care, higher education, and life sciences. Within each of these categories, Concur features tools that are customizable and flexible enough to meet the needs of financial managers, travel administrators, and, of course, travelers. Concur understands that traveling for business isn't only reserved for large enterprises, which is why it offers advice and best practices for companies in a wide range of industries that still need to track the ins and outs of travel. Whether it's a teacher taking students on a school trip or a doctor visiting a faraway hospital for a quick consultation, they can both take advantage of the same features to stop worrying about expenses and instead focus on the task at hand.

FCM Travel Solutions

In the travel management industry, it can be difficult for vendors to differentiate themselves from the competition because almost all of them offer the same fundamental capabilities. You'll be able to track your expenses, you'll be able to use the data you gather throughout your trip to build a report at the end, and you'll more than likely be able to take advantage of most of these features from the comfort of your smartphone or tablet. Where FCM Travel Solutions takes things one step further is with its series of Smart services, which give companies the option to essentially piece together a travel management solution that leaves no stone unturned.

SmartSuite combines FCM 360 Services, FCM 360 Technology, and FCM 360 Travel into one packed platform. With this solution, you'll not only be able to book flights and track expenses, but also fine-tune the travel management experience to fit your business. FCM SmartPay can essentially replace corporate credit cards with Virtual Card alternatives that are easier to track and much more secure. FCM SmartFare makes sure you always find the best flight for the lowest price with regular updates and notifications. And FCM SmartRate works similarly to SmartFare but focuses on hotels.



Trip Composer

☑ Show All (5) ☑ Air (2) ☑ Hotel (2) ☑ Car (1)

☑ DFW->CUN Depart: AA2001, 2:50: Oct 15, 2013 Arrive: AA2001, 5:20:0 Oct 15, 2013

AA2001 Depart: 2:50:00 PM Oct 15, 2013
DFW-CUN Arrive: 5:20:00 PM Oct 15, 2013

☐ DFW->CUN Depart: AA1625, 1:35: Oct 15, 2013 Arrive: AA1625, 4:05:0 Oct 15, 2013

☑ LIVE AQUA CANCUN Check-in: Oct 15, 20 Check-ou Oct 18, 20 Estimated Total From: 351.00 U

BLVD KUKULCAN KM 12 CANCUN ROO 77500 Distanc 9M NE Property I 35550

Rate Range: 351.00 - 747.00 USD Rating: 5

☐ FIESTA AMERICANA Check-in: Oct 15, 20 Check-ou Oct 18, 20 Estimated Total From: 185.00 U

☑ CUN BUDGET Pick-up: CUN, 8:0 Oct 15, 2013 Drop-off: CUN, 8: Oct 18, 2013 Esti Tot 42.

Car Type: Economy Rate Plan: Daily Rate: 10.00 USD

Extra Day Rate: 10.00 USD Extra Hour Rate: 3.34 USD

Message

From: service@ultimatet.com
To: michaelday@homemail.com
Cc:
Bcc:
Subject: Proposed Travel Itinerary for your Trip to Cancun

Dear Michael,

The following itinerary represent the best option for your trip to Cancun.

Regards,

The prices and availability are not guaranteed until booking is complete

DALLAS FT WORTH, United States to CANCUN, Mexico

Total Travel Time: 2:30 Time Difference: 0:00

Airline	Flight	Operates	Meal
AMERICAN AIRLINES	AA 2001 738 - BOEING 737-800	Daily	• Snack

Origin/Destination	Time	Air Miles
DALLAS FT WORTH, TX CANCUN, MEXICO Stops: 0	Dep. Time: Oct 15, 2013 2:50 PM Arr. Time: Oct 15, 2013 5:20 PM Flight Time: 2:30	1028 mile(s)

LIVE AQUA CANCUN ALL INCLUSIVE Rate Range: 351 - 747 USD

Chain	Property	Check-in/Check-out Time

Sabre makes it easier to keep track of invoices, flight information, and other data relevant to a trip.

In addition to the Smart portfolio of solutions, FCM offers its Secure travel risk management service. One of the biggest concerns for companies, especially with employees that travel internationally, is to make sure their trips are as safe as possible. FCM Secure offers 24/7/365 emergency support on a global level, traveler monitoring, updates on events happening around the world, and alerts as to whether those events are escalating. If your employees ever find themselves in an emergency situation, FCM Secure is meant to serve as a way not only for the company to keep track of them, but also for the employee to have access to advice and even rescue and recovery services as needed.

Sabre

One aspect of travel management solutions that is often overlooked is exactly how extensive the vendor's GDS (global distribution system) is—that is, how many agencies are supported. Sabre's GDS, for example, covers approximately 750,000 hotels, 400 airlines, 36 car rental companies, and 17 cruise lines. What this means is that Sabre is capable of tracking information going to and from these agencies as well as working as a go-between to obtain the best possible deal every step of the way. With Sabre's solutions, you get access to all the features you'd expect, including booking, itinerary, expense tracking, payments, and more. But the company also provides a few extra services that you might not think about or expect from a travel management company.

One such service is the ability to develop applications that work hand-in-hand with Sabre's solutions and it expansive GDS network of agencies. With Sabre Dev Studio, you get access to tools where you can build custom applications for consumers and businesses alike.

You can then work to become a Sabre Red App Certified Provider or a Sabre Authorized Developer to let potential customers know that your applications are designed to work seamlessly with the Sabre Travel Network. This program is particularly useful because whereas most travel management companies give you the basic features, not many of them will also take the step to work with third-party vendors and provide access to their resources. This ensures that new features and tools will be added on a consistent basis and make Sabre products even more beneficial for business travelers.

ArborLinks

An exclusive private club located on Nebraska's pristine Arbor Day campus

Warm atmosphere

Premium dining

Elegant accommodations

ArborLinks™

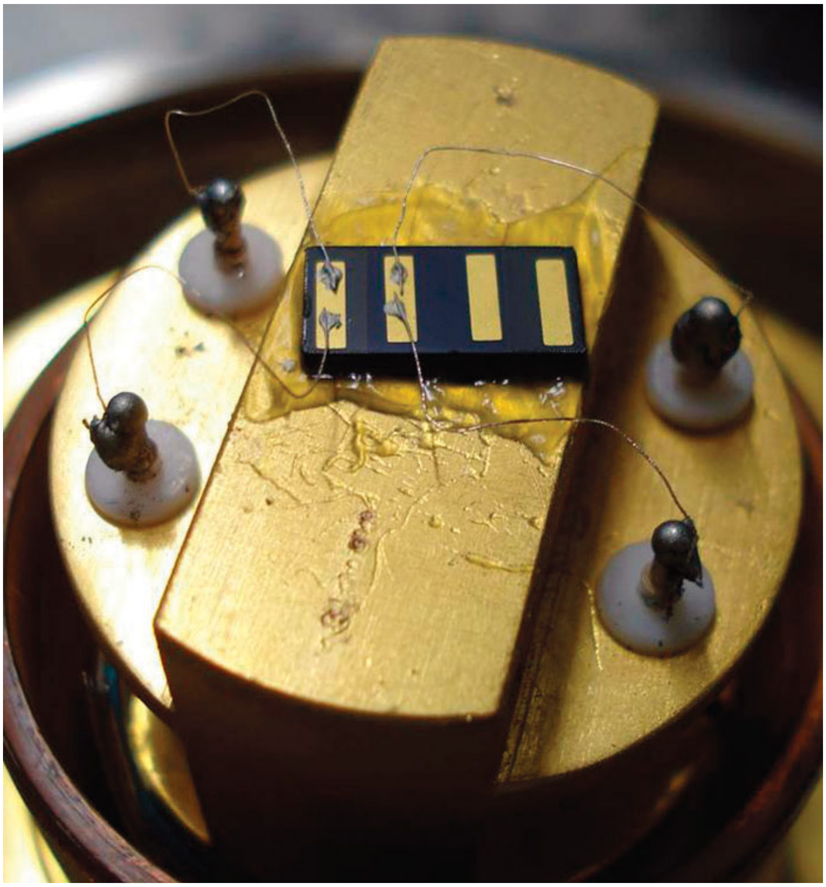
6038 H Road | Nebraska City, Nebraska 68410 | (866) 272-7453 | www.ArborLinks.com

Ranked among Nebraska's best golf courses by *Golf Digest*

Greenovations

ENERGY-CONSCIOUS TECH

The technologies that make our lives easier also produce some unwanted side effects on the environment. However, many researchers, manufacturers, and businesses are developing solutions that are designed to keep us productive while reducing energy demands to lessen our impact on the environment. Here's a look at some of the newest such initiatives.



CREDIT: UNIVERSITY OF GÖTTINGEN, MAX PLANCK INSTITUTE FOR BIOPHYSICAL CHEMISTRY

At the University of Göttingen, a team of interdisciplinary physicists has developed a method to reduce energy loss from solar cells (such as the one shown here) at extremely low temperatures.

Look To Perovskite Research For Solar Efficiency Gains

› Solar energy is abundant, but procuring it poses efficiency challenges and can therefore be costly. Researchers have looked to perovskite in recent years because when a thin layer of the mineral is incorporated into solar cells, it has been shown to increase efficiency by around 25%. Researchers currently exploring ways to improve solar cells with perovskite include a team at the University of Göttingen in Germany, which has found a way to slow electrons and vibrations within cells and thereby reduce energy loss; this was accomplished in extremely low temperatures, however, so the team is looking for ways to make its work feasible in ordinary climates. Oxford Photovoltaics, a spin-out of the University of Oxford, made many of the earliest strides in perovskite research and remains a leading researcher in the area. And perovskite research underway at Cambridge may lead to even greater efficiency boosts, perhaps 30% to 50%.

IMAGE COURTESY OF KAWA AUSTRALIA / CONERGY

Conergy began constructing its massive, $42.5 million solar-and-storage project, a first for Australia and the largest such utility-scale project in the southern hemisphere, in August 2016.

Solar-Storage Project Offers Scale Unmatched In Southern Hemisphere

› Built on a 50-hectare site and scheduled for completion this spring, Conergy's colossal solar-and-storage project will produce enough electricity to power 3,000 homes 24/7. Combining a 10.8-megawatt array of 41,440 solar panels and a 1.4MW/5.3MWh storage solution, the site will deliver continual power even under cloudy skies. "We want to demonstrate how this technology can provide an effective and consistent supply to the grid or operate in islanding mode, particularly in fringe-of-grid locations, paving the way for this integrated model to be used more widely around the world," says David McCallum, Conergy managing director.

Lighting Science Delivers Lighter, Brighter, Less Expensive LED

› As the LED lighting market continues to mature, manufacturers are seeking ways to compete better on both features and price. Lighting Science serves as an example of this trend, particularly with the introduction of its L-Bar lighting solution. Designed to replace a standard 2x4-foot fluorescent troffer, each L-Bar weighs 19 ounces compared to the standard troffer's 25 lbs. (which means it can be affixed directly to a ceiling), uses 95% less material and 80% less packaging, and "costs 50% less than both traditional LED and legacy fluorescent solutions," according to Lighting Science. The L-Bar is also wet-rated, so it can be used in commercial locations and outdoor areas such as parking garages.

CREDIT: LIGHTING SCIENCE

Lighting Science says just one of its L-Bar LED luminaire produces 4,500 lumens, which means it can adequately replace a typical 4-light 2x4-foot fluorescent troffer.

Green Numbers

About **24 gigawatts of new utility-scale generating capacity was added to the U.S. power grid in 2016**. For the third year in a row, most new capacity came from renewable sources, mainly solar and wind. **Renewable energy accounted for 63% of new capacity** in 2016, 66% of new capacity in 2015, and 51% of new capacity in 2014.

Source: U.S. Energy Information Administration.

According to the U.S. Department of Energy, **there are now about 1 million Americans working in the renewable and alternative energy sectors** at or near full-time, about five times as many as work in fossil fuel industries.

Source: "2017 U.S. Energy and Employment Report," U.S. Department of Energy.

According to the latest forecast from research firm IHS Markit, **15% to 35% of all vehicles sold in 2040 will be electric** vehicles.

Source: IHS Markit.

Sales of all types of electric cars were up 59% in January 2017 compared to January 2016. Breaking that down, sales of hybrids were up 86% and sales of fully-electric cars were up 41%. The top sellers this January were the Tesla Model S (approximately 1,900 sold), Chevy Volt (1,611 sold), and Tesla Model X (approximately 1,500 sold).

Source: EVObsession.

Europe's offshore wind installations now provide 12,631 megawatts of power. **European nations installed 1,558 megawatts of new offshore wind capacity in 2016 alone**, the result of more than $19.2 billion in wind farm investments.

Source: WindEurope.

Cargo Tracking Technology

GPS TRACKING, ENVIRONMENTAL MONITORING, THEFT PREVENTION & MORE

KEY POINTS

- Today's asset tracking devices combine GPS and sensors into one package to relay more information back to the carrier, manufacturer, and/or retailer.
- IoT is helping push cargo tracking forward as sensors communicate with one another as well as send information back to PCs and mobile devices.
- Vendors offer a wide range of solutions from modules and sensors to monitoring services.
- Cargo tracking technology will shift to 4G networking in the future, which will also encourage growth in the market.

SUCCESSFULLY TRACKING assets as they make their way from the factory to the retail store can be challenging. It's not only important to make sure that products are always in stock and arrive in a timely manner; there's also the issue of keeping shipping companies accountable as those products travel over long distances, whether by land, sea, or air. Add to this the fact that some items are perishable and require special shipping conditions, and the fact that some cargo is highly sought after by criminals, and thorough tracking clearly becomes a more critical and complex task.

In the past, you had to take the shipping company's word for it that your shipments were in good hands, and rely on paper documents and phone calls to make sure items were moving in a timely fashion. Eventually wireless and location-based technologies "made it possible for a company to monitor the goods inside the shipment while being transported anytime, anywhere," says Raquel Artes, industry analyst at ABI Research. Today, asset tracking technologies are advanced enough to generate immediate notifications when shipments are lost or stolen, or if there have been potential counterfeit-related attacks during transit.

The technology behind this level of tracking revolves around "compact, portable, and rechargeable GPS systems, which fit cellular and satellite components into one device," Artes says. This means you can use both satellite and cellular tracking at the same time to make sure that regardless of where your items are located, you can get reliable information. These devices are specifically designed to stay powered up over long periods of time and be versatile enough to fit in a wide range of cargo containers and trailers. Plus, as we've mentioned, you can get the added security benefit of having sensors go wherever your goods do, even when they fall into the wrong hands.

"Since these devices are small, [they] can be covertly hidden inside the product, packaging, box, or pallet and monitored via the internet using SaaS [software as a service] . . . and provide alert notification real-time for any breaches that occur," says Artes. "Cargo thieves may have difficulty in detecting these devices. In addition, it allows companies to track their goods even in a situation in which goods have been transferred/reloaded to a different container or vehicle owned by cargo thieves while in transit. This gives companies the opportunity to act promptly and help facilitate the speedy recovery of their products."

Impact Of Sensors & The Internet Of Things

One of the biggest innovations in the cargo and asset tracking industry has come about because of growth in the IoT (internet of things) space as well as the increased versatility of sensors. Companies in a variety of industries can take advantage of these technologies and the general concepts behind IoT to keep tabs on almost any type of product imaginable. "Sensors could provide full visibility of goods inside the shipment container or trailer while in-transit and ensure products reach their final destination in good condition, particularly temperature-sensitive products, such as pharmaceutical products, biological samples, blood, and food," says Artes.

These sensors are able to monitor more types of products because they come packed with features capable of measuring temperature, shock, light exposure, humidity, barometric pressure, and other factors, and then transmit the data they collect wirelessly. This allows for an entirely new level of asset tracking that goes beyond location to include almost any environmental condition you can imagine.

"When transporting perishable and temperature-sensitive products, such as pharmaceutical products, biological samples, life sciences, blood, and food, companies will be informed real-time when temperature deviates from a pre-determined level, whether that be caused by freezer compressor failure, defective thermostat, or something else," says Artes. "These sensors were designed to protect a product shelf life and reduce packaging cost. Meanwhile, sensors could also detect light exposure, which sends an alert to companies when a package or shipment has been opened before it reaches its final destination. This device is designed to mitigate pilferage on shipments while on the move."

In addition to being able to monitor multiple conditions, sensor designs have improved from a foundational perspective. Artes points to new innovations including LPWAN (low-power wide-area network), which is intended "to interconnect a wide array of IoT and machine-to-machine [M2M] devices, and utilize the LTE network." This technology is particularly important because it allows for the modules themselves to maintain low power consumption while still providing the wide-area coverage necessary for asset and cargo tracking.

When it comes to the actual data being exchanged between sensors or modules, low-bandwidth connections are used for IoT and M2M purposes to "transmit a small amount of data only to its SaaS server in regular intervals," says Artes, which could be anywhere from every five minutes to every 24 hours depending on the situation. Because these devices don't have to handle more resource-intensive traffic that a traditional network might, such as high-definition video streaming, it allows for the modules to have longer lasting battery life and lower power consumption so they can be used in more applications. In fact, many modules feature power saving modes and eDRX (extended discontinuous reception), which Artes says can offer "huge benefits to battery-operated IoT and M2M devices left unattended over a period of time," because "battery replacement or recharging while on the road would be challenging."

Vendors & Solutions

If you think about the sheer number of cargo shipments that occur on a daily basis in the United States alone, it makes sense that the asset tracking industry is large enough to hold dozens, if not hundreds of vendors covering multiple facets. For example, there are asset tracking service providers, including FreightWatch International, Starcom, 3Si Security, and Rockwell; third-party logistics providers, including FedEx and DB Schenker; telecom operators such as AT&T; module vendors, including Telit and U-blox; and chipset vendors such as Qualcomm and MediaTek. All of these vendors bring something different to the table when it comes to cargo tracking and they all have

"[W]hen transporting perishable and temperature-sensitive products, such as pharmaceutical products, biological samples, life sciences, blood, and food, companies will be informed in real-time when temperature deviates from a pre-determined level, whether the cause is freezer compressor failure, defective thermostat, or something else. . . . [Sensors are also] designed to mitigate pilferage on shipments while on the move."

RAQUEL ARTES
Industry Analyst
ABI Research

unique products and services tailored for general use cases as well as industry-specific ones.

FreightWatch International, for example, offers its GEO F4 Tracker, which "is a portable, battery-powered tracker that covertly tracks high-value assets while on the move" and "uses a cellular-based GPS technology, which augments GPS signals with cell tower triangulation, and sensors to provide the shipment's location real-time and monitor environment conditions," Artes says. It features multiple battery options, antennas, and sensors, so it can be used in a variety of setting and under different environmental conditions. This makes it a perfect solution for sealed trailers and containers where GPS tracking can typically be unreliable.

ORBCOMM also offers an asset tracking sensor with its CS 100. Among its standout features is its ability to use ultrasonic technology to send an alert when the load status of a shipping container or trailer changes. One of the benefits of this technology is that shipping companies can ensure that trailers are either empty or full, depending on the situation, and know when it's time to pick up a container. Another benefit has to do with potential theft, where the CS 100 can let you know if assets are being moved at an unscheduled time and location or if the sensor itself has been damaged or removed.

3Si Security Systems is another company that helps shipping providers, manufacturers, and retailers prevent theft and track stolen cargo. 3Si's solutions are all discretely designed so that they won't be noticed by criminals. They can be used with phones, ATM systems, jewelry, pharmaceuticals, cash, and any other goods and assets that require a little extra protection. The data its sensors gather can then be used to aid law enforcement in tracking down and apprehending thieves, and potentially recovering your stolen goods.

Sendum is an example of a cargo tracking vendor that is taking advantage of sensor innovation to pack as many features into one module as possible. Its PT300 is a cellular-based tracker and datalogger in one that can send information back to a computer or mobile device for real-time monitoring. As with many other modules, it is full of useful sensors for not only tracking location, but also monitoring temperature, shock, vibration, and even orientation for those special "this side up" shipments.

FreightWatch International's GEO F4 Tracker has an always-on setting and an only when moving setting so you can decide whether you need 24/7 monitoring or if you want to preserve battery power when at rest.

Cargo Tracking In The Future

It's obvious from the many solutions on the market that innovation isn't a problem in cargo trucking. The industry is also pegged for solid growth, with ABI Research estimating growth at a 13% CAGR from 12.9 million units in 2016 up to 23.4 million units in 2021. Artes, for one, attributes this growth to rising incidents of cargo theft, among other issues, such as trade liberalization on the Trans-Pacific Partnership and the mandated migration away from 2G and 3G technologies over to 4G. That last one is particularly important because these sensors rely on those connections to relay information, and all parties want those connections to be as fast and reliable as possible.

"3GPP announced the 3 LPWA standard connectivity platform designed for IoT and M2M applications that offers vital solutions toward 4G network deployment across emerging technologies," says Artes. "Why is this important? Internet connectivity is essential to M2M applications (for example, goods/asset tracking devices, commercial telematics, etc.) and the type of connectivity platform is vital to the ecosystem. Currently, these devices utilize 2G or 3G networks; however, wireless communications providers across the world announced shutting down their 2G and 3G networks this year, and some operators already shut down their 2G/3G network. As such, a wide array of devices (mobile phones, tablets, IoT, M2M, etc.) that need internet connectivity are required to make their devices 4G future-proof."

As modules, sensors, and monitoring solutions start to take more advantage of 4G, it will not only make all of the base features even better, but also open up more opportunities for the cargo tracking industry. Sendum's PT300 is already involved in this by making it possible to monitor shipments on your smartphone, and it's that use case could allow cargo tracking to find its stride and encourage market growth. By giving companies more ways to track their assets and more platforms on which to view that information, it should help ease some of the headaches around cargo tracking and improve the process across the board.

Smart DCIM Improves Data Centers

BETTER SENSORS & CLOUD-BASED SOLUTIONS MEAN MORE INSIGHTS

KEY POINTS

- DCIM (data center infrastructure management) relies on external sensors to gather environmental data, so incorporating other IoT concepts makes sense.
- Cooling and power consumption are two areas where companies can see a quick return by using smart DCIM solutions.
- When DCIM starts to bring more automation into the fold, IT teams will be able to respond more quickly to issues.
- On-premises DCIM will still be important when it comes to UPSes, backup power, and other critical physical infrastructure.

THE INTERNET OF THINGS is one of those concepts that seems to be creeping into nearly every branch of technology, and for good reason. There are many benefits to be had by connecting more and more devices to one another in an effort to generate more information and use that information to make better decisions. Whether the data gathered is used by individuals to improve processes or in a more automated manner by the connected devices themselves, there's no doubt that IoT is having a major impact on technology across the board.

One area of technology that adopted the foundational concepts of IoT long ago and continue to rely on them is DCIM (data center infrastructure management). At its core, DCIM is about giving IT and data center managers more control over their assets, which includes all of the physical infrastructure as well as the software running inside the facility. DCIM solutions depend on sensor-related monitoring data to keep track of environmental conditions and the general health status of mission-critical systems to ensure everything runs properly.

Rhonda Ascierto, research director, data center technologies, at 451 Research, says you could consider DCIM to be "IoT for the data center to the point where DCIM platforms are being repurposed as IoT back engines." Ascierto does warn that there is significant IoT "whitewashing" out there, where some technologies claim to be IoT but don't truly fall under that category. However, DCIM isn't one of those areas, because "if you really strip down the components of what DCIM is, it is aggregating sensor data and other data, normalizing that data, and running algorithms on that data. And if you combine DCIM tools with IoT-related sensors and monitoring equipment, you can start to make meaningful changes inside the data center.

Impact Of DCIM & The Internet Of Things On Cooling

While one of the main functions of using sensors as part of an overall DCIM strategy typically involves alarms where you set up a sensor to detect a given occurrence and then receive a notification, there is a lot more you can do with that basic concept, especially with regard to cooling. "It's things like dynamic cooling optimization, which has been around for a number of years, whereby the racks have a high volume of sensors, so maybe top, middle, bottom, front, and back," says Ascierto. "Using that data and applying machine learning to that data, you can determine when the cooling unit set point temperature should change or when the fan speed should change in real time according to the environmental conditions of that rack."

One vendor in this area is Vigilent, which offers a solution that promises dynamic control. The idea is that sensors are constantly measuring temperature and sending that information back to an analyzation engine. That analysis is then used to determine where to set the temperature level in a given rack as well as how to best regulate the fan speed for optimal cooling. Ascierto points out that while Vigilent is a relatively small company, its dynamic cooling solutions are authorized to be resold by Schneider Electric as part of its "comprehensive DCIM suite." Vigilent and similar companies often not only provide the sensors that measure temperature and other factors, but also the software and analytical intelligence necessary for the systems to work.

In addition to larger vendors taking advantage of solutions from smaller players to bolster their product offerings, some of those vendors are also working to embed more monitoring software, including DCIM-related tools, directly into the cooling units themselves. One example is Vertiv, formerly Emerson Network Power, which is adding more intelligence into its solutions as a way to encourage dynamic cooling approaches. "The barrier is lower because they actually have software inside the equipment, inside the CRAH [computer room air handler] and the CRAC [computer room air conditioner]," says Ascierto. "We see that trend increasing."

"The cost to monitor, manage, and maintain a data center can make this resource one of the most intensive OPEX line items for a company. The ease of use with which we assimilate modern data management systems—whether part of a private, public, or hybrid cloud environment—obfuscates the dynamic and resource-intensive requirements that need to be met to keep things up and running."

RYAN MARTIN
Senior Analyst
ABI Research

Impact On Issues Related To Power & Energy

While cooling is often a primary focus for the data center, the Yin to that Yang is power and energy consumption. Ryan Martin, senior analyst at ABI Research, says that "IoT adds to the complexity of DCIM in a number of ways," but adds that "the same technologies that amplify the need for more intelligent, more capable infrastructure management capabilities are also the ones that offer some of the most tangible near-term opportunities to optimize these systems." One such near-term opportunity is in gathering as much information as possible about power sources within the data center facility as well as the equipment that taps into those power sources. This is a place where gathering data from sensors can help aid in improving your PUE (power usage effectiveness) among other important data center performance metrics.

"At its core, DCIM is about facilities management," says Martin. "This includes the ability to manage the core functionality of the facility—data storage and access in this case—as well as HVAC, lighting, and other controls that historically adjusted with the flip of a switch, press of a button, or turn of a dial. There is no reason these processes cannot—and should not—be automated, particularly given the repetitive and highly predictable nature of their operation in the real-world. If we trace energy consumption back to the source—production—we can also see massive improvements in the way the production and distribution of power is handled."

Impact Of Cloud-Based DCIM On IT Teams

In addition to power and cooling, IoT can help DCIM in the overall IT management arena by giving teams access to more information than ever before as well as more automation for routine tasks. One example of adding more DCIM-related capabilities to products is with Intel Data Center Manager, which is essentially "firmware that comes with all modern Intel servers, and can be applied to non-Intel servers," Ascierto says. She adds that all leading DCIM platforms support Intel DCM, which gives IT administrators "access to board-level environment data and activity," which can then be sent back to the DCIM system for further processing. As more of the process is automated, we move toward a future in which Ascierto believes artificial intelligence, machine learning, and other newer technologies will continue to play a role.

While these potential benefits may sound great to companies, the glaring issues with DCIM have always been cost and complexity. However, vendors such as Schneider Electric, with its StruxureOn solution, offer cloud-based DCIM with remote monitoring capabilities. Ascierto says these solutions make it possible to have a third-party monitor your data center and deliver information to your mobile device without having to install software, all "within a matter of hours." This enables companies with relatively small IT budgets to take advantage of DCIM capabilities.

"This is a really big deal because one of the barriers to DCIM has been deployment," says Ascierto. "The reason for that is there are a lot of operational processes required to support DCIM. You have to make sure data gets into the system and stays current. Once organizations realize that, and I think most of them do now, there's a recognition that this more than just applying software. This is going to require some operational change. This is a much bigger project than buying and putting software in. We're seeing a lot of data center operators hesitate on their purchasing decisions around DCIM, because they understand this is a bigger thing. With DCIM cloud-based services, it takes away this very important barrier."

Because cloud-based DCIM platforms gather data related to multiple clients, large data lakes of aggregated customer data are created. This empowers companies to see monitoring information from data centers of all shapes and sizes, analyze that data, and come up with insights that simply couldn't be achieved by someone running an in-house DCIM solution using only their own data.

"That's where you start getting into IoT-type outcomes for the data center," says Ascierto. "These are things like recommended actions, industry benchmarking. For example, if you're a data center in the health care industry and of a certain size, how does your PUE and data center utilization compare to your peers? That industry benchmarking is something that's just not possible if you're running it on-premises. Recommended actions are possible, but you're not benefitting from the wealth of hundreds of your compatriots around the world that have this similar situation."

Long-Term Outcomes

Many potential gains from cooling, power consumption, and improved management are somewhat low-hanging fruit in the grand scheme of things for IoT and DCIM; this doesn't make them any less important, but there are bigger fish to fry. For example, Ascierto sees a future where companies can use aggregated data from sensors and DCIM solutions to make better purchasing decisions around mission-critical data center equipment, which is an area where many companies avoid saving money in an effort to make sure they have the seemingly best and most reliable products on the market.

IN ADDITION TO POWER AND COOLING, IOT CAN HELP DCIM IN THE AREA OF OVERALL IT MANAGEMENT.

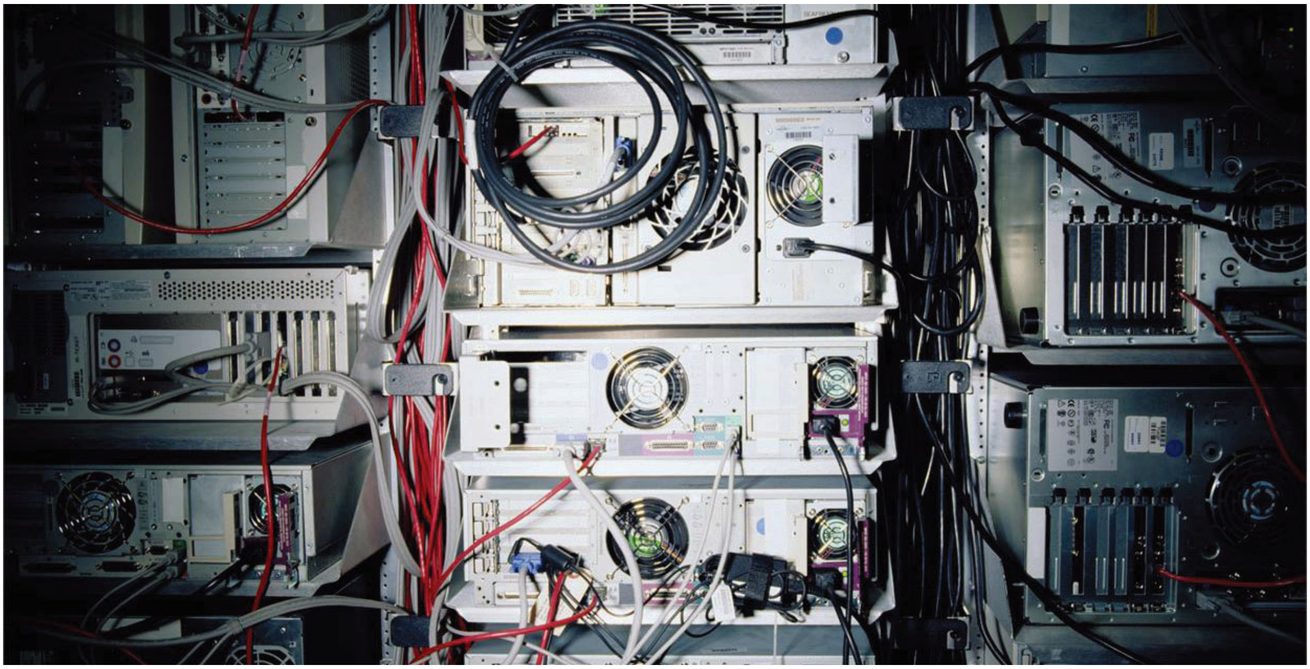
"We expect this to lead to being able to lease critical infrastructure equipment, like a UPS or generator, which is a very expensive piece of equipment, and turn that huge CAPEX into an OPEX cost," says Ascierto. "Then, you can have the maintenance and service contracts tied into that. The other thing that cloud-based DCIM services are doing so far is that they're tied into the field services, like maintenance, because Schneider and Eaton, which is the other provider that is early to market with this, are huge field service businesses. They sell the equipment and then sell services whether it's their equipment or not."

For an example of how to take advantage of all of this IoT and DCIM data, look no further than Google, which has hyperscale data centers large enough to form its own comprehensive data lakes. In 2014, the company acquired DeepMind in an effort to improve its overall cooling operations. By being able to monitor the environment and automate the process of adjusting cooling parameters and fan speeds in real-time, Google was able to lower it's overall cooling bill by about 40%, which is a sizable chunk of change for an organization that large. "[Google has] gotten some pretty impressive reductions in their PUE when they were using DeepMind compare to when they weren't," says Ascierto. "We're in the very early stages of data center management transforming into a remote, smart, big data-driven, and outcome-based service."

On-Premises DCIM Will Still Have A Place

With all of this talk of automation and cloud-based DCIM solutions, it may seem as though on-premises DCIM is on its way out, but that's not the case. In fact, there are going to be situations, specifically with equipment including UPSes (uninterruptible power supplies) and backup power solutions, where onsite DCIM is necessary because "you can't wait for that data to go over the Internet, process, and then come back to you as an alert," Ascierto says. But as the technology continues to evolve, it will start to take over more and more of those functions and find a place in organizations of all sizes.

"Generally speaking at a high level, the value of these AI-driven, smart cloud data center services are going to be really powerful," says Ascierto. "It's going to take some time though, because there are barriers like the risk and comfort level of operators to send data about their critical infrastructure off-premises to a cloud. It's a risk vs. benefit always, and I think once these services mature and more of these outcome-based services become available, the benefits will overweigh concerns. It's all fully encrypted, but risk is still an important consideration."



Data Center Mistakes To Avoid

OVERBUILDING, OVERUTILIZATION & EVERYTHING IN BETWEEN

KEY POINTS

- It can be difficult to find the right balance between right-sizing and overbuilding, but it's necessary to prevent wasting time and money.
- About half of the total cost of ownership for a data center is incurred over the first six years of operation.
- Colocation and cloud computing are two avenues for adding extra capacity without physically expanding.
- Modular data center components can be used in new builds and expansion projects for on-demand scalability.

BUILDING A DATA CENTER, or even just expanding one, can be a stressful, expensive, and time-consuming process. There is an extensive planning process that requires estimating not only how much capacity you need right away, but how much you may need 10, 20, or even 30 years down the road. Then you have to make sure that there is adequate space, power, and cooling to support all of the equipment and components you wish to install. And once all of that is said and done, you need to strive for the best possible power and cooling efficiency in order to get the most bang for your buck while still meeting compute requirements.

Needless to say, there are plenty of steps in the process where mistakes can and probably will be made. That's often difficult to admit, but the truth is that even with the most in-depth planning, there will be unexpected hiccups along the way that must be handled quickly and accurately so situations don't spiral out of control. It all starts with proper planning and a clear vision of future positioning as an organization. From there, you'll need to take advantage of all of the different technologies available to you to meet capacity demands without painting your business into a corner.

Right-Sizing & Overbuilding

Within the planning process and afterward, one of the biggest concerns companies face regarding data center builds is running out of capacity in the future. The last thing you want to do is spend millions of dollars on a new facility and fill it with equipment only to find out you've hit maximum capacity sooner than expected and it's already time to expand. This is a relatively common mistake.

For organizations that don't take right-sizing into account, it's often the case that they focus more energies on the current needs of the organization without fully considering future growth and scalability needs. This may help save money in the short-term by not overdoing it on the initial build, but it means having to incur incremental costs along the way that will certainly add up.

A related problem, which especially occurs when there is constant expansion, is overutilization. If, for example, servers are run too hot or overloaded with compute processes, the risk of running those servers into the ground increases. It's always best to operate equipment within the parameters specified by the vendor, as pushing it too far negatively impacts its overall life cycle. What's more, if you overutilize your data center and overstuff it with physical infrastructure, you may run into power and cooling concerns where there is simply not enough capacity to keep pace with demand. This can result in downtime, which for service providers in particular is something that simply can't happen.

However, too much concern for running out of capacity can swing an organization too far in the other direction, resulting in overbuilding the data center. In this scenario, there is an assumption that a certain amount of capacity will be needed in the next few years or decades. The data center is then built with that in mind so that all of the expected scaling can be accommodated. But then, due to unforeseen circumstances or improper planning, the organization never fully takes advantage of that extra space and the money spent is essentially wasted. What's more, there is an ongoing drag on operations by having to cool and maintain unused space, further eroding its value. That's why it's so crucial to use monitoring and measuring tools, which not only help establish a baseline for performance, but also help estimate how much capacity may be needed in the future.

> "What we're seeing is that a lot or organizations that are facing a capacity issue within their on-premises privately held data center is they are looking to outsource as much as possible rather than commit to a new build. They are making decisions around which workloads can be hosted remotely in a public cloud and which ones they need to have more control over. Typically, they'll choose a colocation facility. That's a big challenge at the moment and for most organizations, it's a bit of a moving target."
>
> **RHONDA ASCIERTO**
> *Research Director*
> *451 Research*

"In terms of new builds, the big challenge of capacity management is that most organizations don't really monitor or measure their data center capacity," says Rhonda Ascierto, research director at 451 Research. "They may have an understanding of how much empty space they have, but they may not have a good grasp on available power capacity vs. actual power utilization, for example, and how much of that is being used for work. You can have servers spun up and there may be CPU activity on those, but that CPU activity actually revolves around things nascent to that server, like caching and firmware or software upgrades, but not actually doing useful work. That's something that most organizations still don't have good visibility into. That feeds into DCIM [data center infrastructure management] where you actually have visibility into the utilization of the assets in place."

Total Cost Of Ownership

Another major challenge when building a data center or expanding it is weighing the initial capital expenditures vs. the operation expenditures. Ascierto says that in a typical 15-year TCO (total cost of ownership) calculation for a 3-megawatt data center build, you can expect to incur half of the costs of that entire TCO within the first six years of operation. "You're committing significant funds in the first six years of that data center's life, and the degree to which you actually utilize it over the 15-year TCO is an unknown," she says. What this realization ultimately leads to is that companies are finding ways to cut down on internal capacity and expanding via other avenues.

"What we're seeing is a lot of data center consolidation," says Ascierto. "It may be a new build or an expansion of a core centralized data center, but we are seeing a fair amount of compute in regional localized data centers being consolidated into centralized, premium facilities. That's the trend at the moment in terms of getting a handle on our longer term capacity requirements. Should we be building? Should we be outsourcing, and if so, what should our outsourcing look like?"

Colocation & Cloud Computing

With consolidation on the rise and growing fears of either building too much capacity or not enough, companies are turning to more flexible alternatives to traditional data center builds. The reason for that, according to Ascierto, is that capacity requirements are often in flux, so you can't even plan ahead for future demands because you simply don't know what they will be. This has a bit to do with how much choice the market offers in terms of solutions. You can choose between on-premises systems, cloud-based services, or even solutions hosted in a third-party data center.

Expanding on that last example, Ascierto says that there is significant growth in colocation facilities "where you lease space in a third-party data center, install your own IT, and are responsible for running your own IT." Colocation offers you a way to expand capacity while maintaining control over your infrastructure even though it's hosted in a provider's data center. Another way to achieve similar gains is to invest more in cloud offerings where you can completely (or almost completely) offload certain applications and free up internal resources for other projects or for consolidation if necessary. Whichever option you choose, it's clear that companies are opting more for outsourcing than new builds at least for the time being.

"What we're seeing is that a lot or organizations that are facing a capacity issue within their on-premises privately held data center are looking to outsource as much as possible rather than commit to a new build," says Ascierto. "They are making decisions around which workloads can be hosted remotely in a public cloud and which ones they need to have more control over. Typically, they'll choose a colocation facility [for the latter]. We're also seeing the growth of public cloud services exploding. And when you look at the workloads that go to the public cloud, oftentimes an organizations decides what's mission critical, and what they need to control, vs. what's not mission critical to the business and can move to a public cloud."

Prefabricated & Modular Data Center Builds

It's important to remember that even though the cloud and colocation are attractive options and will solve certain problems, there are some companies that still want to build new data centers onsite or expand existing facilities with additional capacity. In those situations, in order to avoid the aforementioned mistakes and challenges, it's possible to opt for prefabricated and modular data center builds. This is a concept that has been popular in health care and industrial sectors for quite some time, but one that's only just now growing in popularity in the data center space.

"It's something that's often overlooked because it's relatively new, so when people think we need to build a new data center, they're probably looking at replicating what they've done in the past, which is a traditional brick-and-mortar build," says Ascierto. "Generally, they're probably going to be doing a new build because they have a certain amount of capacity that they can project with a high degree of confidence. This is a big commitment, and as I said, half of the costs are committed up front. The question is what's the right size? How big should we build this data center? That's a tricky thing to do."

COLOCATION OFFERS A WAY TO EXPAND CAPACITY WHILE MAINTAINING CONTROL OVER YOUR INFRASTRUCTURE

Instead of taking that approach, companies can go the prefabricated route either with a fresh build or with an expansion. On the new build side, you can calculate how much capacity you need now and within the first few years after the initial build, and then you can add capacity with modular components as it becomes necessary to do so. Or, if you simply need to expand, you can take advantage of the same modular data center components to bring in more power, cooling, or IT-related processing power depending on the situation. Plus, you get the added bonus of faster time to market because modular data center projects often take a fraction of the time of traditional builds.

"The biggest advantage with prefab is being able to manage capital expenditures," says Ascierto. "You don't have this big commitment up front. You're able to modularly build in increments as needed. And [in terms of] lead times for prefab, we hear lead times of six weeks, and that's certainly possible, but that generally costs quite a bit of money. Hyperscale can do that, but more realistically for an enterprise, instead of a building project taking at least 12 months to two years, and there are a lot of people involved in that. With prefab, the performance and outcome are pretty much guaranteed by the supplier."

Another important factor with prefabricated and modular data centers is that they are highly customizable. Not only are the components all tested offsite to ensure quality and performance, but you can also put your own stamp on them within reason. Ascierto points out that there are "literally catalogs full of modular products and SKUs that you can pick to meet the capacity your organization will require and the increments in which you'll require them." Once you make a decision, it often takes around six months for a build and then you have a modular, scalable data center that looks "indistinguishable from what you would get from brick and mortar," she says.

And if you need an idea of how popular and primed for growth this particular market segment is, look no further than the types of vendors and providers that need this brand of scalability and flexibility the most. "It's something that more people are talking about, and it's certainly being adopted by some of the more forward-thinking corporations, including colocation providers," says Ascierto. "It's colocation builders and providers, and public cloud providers as well. We really see that as the future and the industrialization of the data center build. We certainly see that as a strong and growing trend."

What Is WiGig?

ONE STEP CLOSER TO AN ALL-WIRELESS FUTURE

WI-FI AND OTHER over-the-air technologies have changed the way people connect to the Internet and interact with their devices. In the past, you'd have to plug an Ethernet cable into your desktop, laptop, gaming console, you name it, in order to access the Internet. Vendors over the years have worked to break that tether through the use of Wi-Fi, Bluetooth, 4G LTE, and many other wireless technologies that make it easier to connect regardless of location and distance.

Those same vendors continue to work on improving base connections, but they're also moving on to other types of connections, like those between a smartphone and a television, or a PC and an access point. This idea of streaming from one device to another or ensuring high-speed data transfers when running resource-intensive applications is driving the Wi-Fi industry forward and has led to a few major innovations in the past few years.

One of those innovations, which specifically focuses on streaming and related connections where speed is of the utmost importance, is WiGig. WiGig is a Wi-Fi standard that, instead of using the 2.4GHz or 5GHz spectrum, utilizes the 60GHz band, which is often less congested, to ensure the best possible performance and speed. This allows for multiple gigabit-per-second data transfer speeds, which is perfect for this new era of 4K streaming as well as for removing bottlenecks inside enterprise data centers.

There are many potential use cases for WiGig technology, both in the consumer and enterprise spaces, and multiple vendors including Dell and Intel have already jumped onboard with products that support the newer standard. And while these implementations have been somewhat few and far between to date, many analysts believe that 2016 and 2017 will be crucial years for the technology as it releases deeper into the mainstream and makes its presence felt in a wider range of applications.

Major Use Cases

Philip Solis, research director at ABI Research, is one of the analysts who believe 2017 and beyond will mark the time when WiGig makes a big splash in the technology world. He expects a much higher volume of WiGig product releases that fall into the smartphone, PC, and even virtual reality headset categories. One of the reasons for this is that the millimeter wave spectrum is getting much more attention from vendors do the fact that you can fit more WiGig connections into the same frequency without losing as much speed and performance. This impacts other wireless spectrums used with Wi-Fi standards, for example, because those frequencies can't handle too many connections at once without performance degradation.

As an example of where WiGig started and how it continues to evolve, Solis uses the example of PC docking. This was one of the initial applications for WiGig, and it has been expanded upon to improve connectivity and even add a few extra capabilities. "The chipsets out now work better than [the] initial chipsets, which required placing the laptop in a certain way to achieve a connection, and all the major chipsets are interoperable," says Solis. "Many of these docks will be absorbed into monitors. You will just place your portable PC on your workstation and it will wirelessly charge and connect to the dock via WiGig. All the connections to the monitors [and] peripherals via Bluetooth, and Internet via Wi-Fi or Ethernet, will occur between the dock and the peripherals and access point."

In addition to PC docking and wireless charging, Solis points out that WiGig is going to have a place in enterprise settings and in the IoT (Internet of Things) space, as well. He says the 60GHz band is being used more and more with backhaul applications because it offers so much additional capacity. "Previously, it was not that usable, but with beamforming, it is much more reliable now," Solis says. Beamforming involves the use of directional antennas or Wi-Fi chip-based signal amplification and phasing to improve wireless coverage between access points and devices.

When it comes to IoT, Solis sees WiGig being used with kiosks, industrial robots, and industrial automation "to connect cameras to networks for machine vision applications." Any applications where a higher data rates or multiple high-speed connections are necessary, WiGig is going to find a place as long as vendors add support for it to their products.

"WiGig is about speed, but also capacity and avoiding interference. Its disruptiveness come from the use of millimeter wave spectrum to vastly increase speed and capacity, even as the other Wi-Fi protocols evolve to 802.11ax."

PHILIP SOLIS
Research Director
ABI Research

Potential Impact

According to Solis, "WiGig is going to be very disruptive to the wireless connectivity space," but the question remains "how long this will take." As it stands right now, newer versions of the Wi-Fi standards 802.11n and 802.11ac—that is, 802.11ac Wave 2 and 802.11ax—are backward-compatible with previous standards and will continue to serve many applications well.

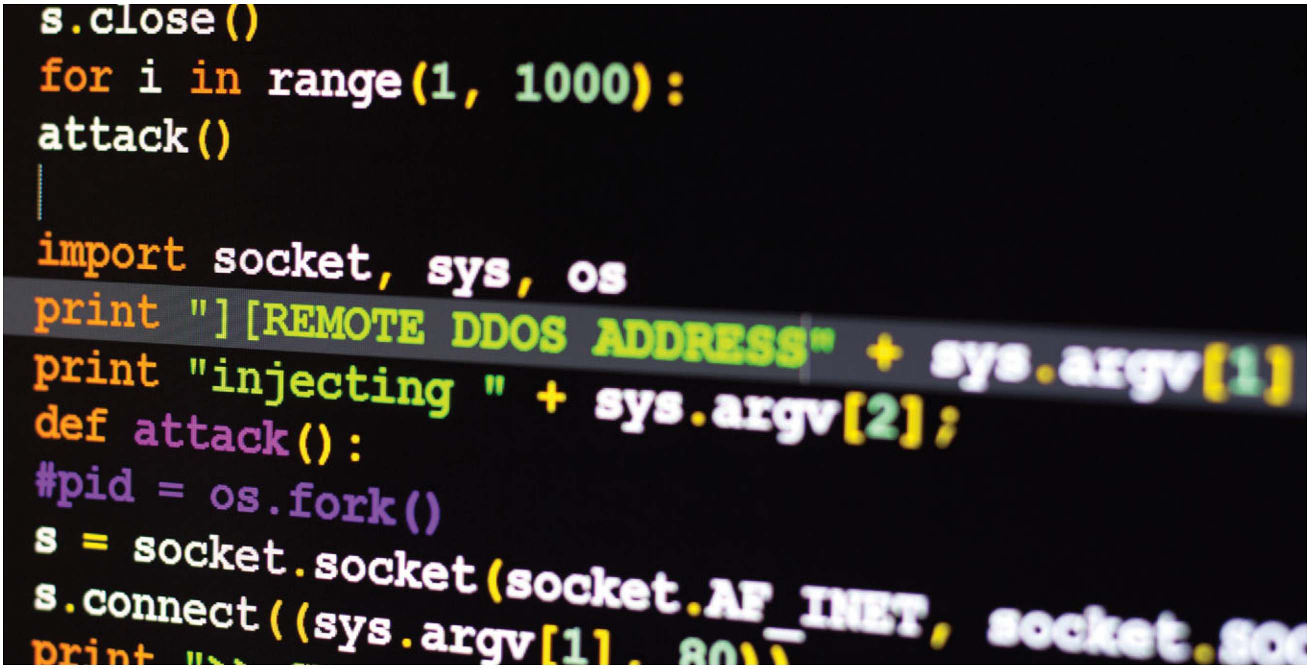
The issue, however, is that these bands are limited in capacity and are vulnerable to interference, which is a problem both for large families trying to use devices and applications at the same time as well as employees of a business trying to finish important tasks over the Internet. The more crowded an environment is with devices trying to connect to the network, the more performance will suffer without a standard designed specifically for that purpose.

"Some houses have a family of several people, a few of whom are streaming 1080p or even 4K video now," says Solis. "This will go 4K HDR video and 8K video. On top of that, there might be a PC or two being used and smartphones with many applications pinging the Wi-Fi access point constantly. Or you might have an apartment in a dense city with one person in it surrounded by dozens of personal and business access points. The solution," Solis explains, "will be to divide traffic and use not just the smaller 2.4GHz band and larger 5GHz band, but also the 60GHz band."

Interestingly enough, one of the potential weaknesses of WiGig and the 60GHz band in general is that it is somewhat limited by obstructions, but that could actually end up being a strength for the standard. Solis says that longer-range connections can use 2.4GHz, bandwidth-heavy applications and whole-home coverage scenarios can use 5GHz, and shorter-range situations that put a major emphasis on speed and data transfer can take advantage of the 60GHz spectrum through WiGig. This range of spectrums makes it possible to categorize different connections and choose the best possible standard for a given use case.

With so many potential use cases for WiGig, it's easy to see why the technology is poised to disrupt the Wi-Fi marketplace in a big way once it finally hits the mainstream. Imagine using Wi-Fi to connect to the Internet, Bluetooth to connect keyboards and mice, and WiGig to connect your device to a monitor. The only wire you'd need is one for charging the device itself, which Solis calls "the last piece" of this puzzle when it comes to making portable computers 100% wireless.

Indeed, wireless charging is a technology that many vendors in the smartphone space are already working on. If the ultimate goal of the mobility trend is to enable businesspeople and consumers alike to become as mobile as possible with no tethers or limitations whatsoever, WiGig will certainly play a significant role.



```
s.close()
for i in range(1, 1000):
attack()

import socket, sys, os
print "][REMOTE DDOS ADDRESS" + sys.argv[1]
print "injecting " + sys.argv[2];
def attack():
#pid = os.fork()
s = socket.socket(socket.AF_INET, socket.soc
s.connect((sys.argv[1], 80))
print "
```

DDoS Attack Mitigation

TAKE ADVANTAGE OF ON-PREMISES & CLOUD-BASED SOLUTIONS TO PROTECT YOUR NETWORK & SERVICES FROM DISTRIBUTED DENIAL-OF-SERVICE ATTACKS

KEY POINTS

- DDoS attacks essentially flood a network or service with illegitimate traffic and prevent real users from getting through.
- These attacks use botnets, which are groups of computers that have been infected with malware and have become "zombies" for the hacker to use.
- The goal of a DDoS attack may be to bring down a service or to hijack it until a fee is paid to release it.
- You can choose between on-premises, cloud-based, and hybrid solutions to protect yourself from DDoS attacks.

DENIAL-OF-SERVICE, or DoS, attacks and DDoS (distributed denial-of-service) attacks are the bane of any service provider's or web host's existence. From the user's perspective, if you've ever tried to load up a web-based service only to find a message waiting for you that says it's either over capacity or down for an indefinite period of time, then there's a chance the site was hit with a DDoS attack that overwhelmed it with fake traffic and is now keeping legitimate users from getting through.

DDoS attacks are surprisingly common because the tools themselves are relatively easy and inexpensive to acquire, and they are also difficult to predict and mitigate without the proper tools. Fortunately, once you get over the hurdle of actually understanding why someone would want to perpetrate a DDoS attack, you can start putting yourself in the best possible position to limit the damage.

How DDoS Attacks Work

A DDoS attack starts with a botnet, which is essentially a group of computers that have been infected with malware and can be controlled as one entity by an outside party. These are private computers that have been hacked without the user's knowledge and can then be used to attack networks or services in a variety of ways. For example, one DDoS attack might use spam messages to overwhelm an email service and cause issues, while another may use those computers to send fake traffic to a service such as Twitter and temporarily bring it down.

"Effectively, the botnet is ordered to repeatedly access a certain system," says Michela Menting, research director at ABI Research. "Each time a request to view a specified page is sent, information flows between the user's system and the website in order for the page to appear on the user's screen. If a great number of requests are sent, the server on which the page is hosted can be overwhelmed and becomes unable to respond to all the demands, sometimes becoming submerged and unable to respond altogether, thus denying service to all requests. DDoS are simply distributed attacks, meaning the botnet is composed of usually thousands of bots, and perhaps several botnets are used. It is simply an increase in scale."

The interesting thing about botnets is that they are widely available on the black market for a range of prices and a variety of use cases. For example, for $200 to $500 you can buy a turnkey botnet with maybe 50 "zombies," which is the term for the infected computers. For varying fees, you can rent larger botnets with thousands of bots by the hour. The goal of the attack, as well as the target, will determine what type of botnet needs to be used and for how long.

Jim Davis, senior analyst at 451 Research, also points out that there are different types of DDoS attacks that go after specific targets. There are the standard volumetric DDoS attacks, which are network-based and "have the effect of exhausting server resources and/or consuming available bandwidth with spurious requests," he says. And then there are application-layer DDoS attacks, which, although less common, are growing in popularity. "The techniques are different in that the attacker targets web, application, and database resources," says Davis. "These attacks require more sophisticated knowledge of features and vulnerabilities but can be done without large botnets. These attack types can be harder to detect and harder to mitigate. When done in conjunction with a volumetric attack, they can be quite devastating."

The Goals Of A DDoS Attack

With DDoS attacks, it can sometimes be tough to tell the attacker's desired outcome, but in other instances, they wear their goals on their sleeves. An example of this would be the 2010 series of DDoS attacks referred to as Operation Payback and Operation Avenge Assange. These attacks were perpetrated by Anonymous and other notorious hacker groups in an effort to take down opponents of piracy, in the case of Operation Payback, and payment providers that refused services to WikiLeaks and its founder, Julian Assange, after the group started leaking U.S. government documents. In the latter attack, Visa, MasterCard, PayPal, and many other financial institutions were taken offline for hours, and it disrupted service to the user base. The hacker groups even made fliers laying out the exact reasons why they were conducting the attacks and why those specific companies and services were targeted.

Attacks such as Operation Payback are less about financial gain and more about sending a message, but that doesn't mean that money-based DDoS attacks don't exist. "DoS and DDoS attacks can be used to blackmail or immobilize any website," says Menting. "In exchange for money, the perpetrator agrees to cease an attack or to desist from carrying one out. Commercial organizations can lose important financial gains because of their inability to trade due to a DoS attack. Even just the threat of an attack could be sufficient for the perpetrator to successfully extort money. With the sale and rental of botnets, it has become a lucrative business and perpetrators are not all necessarily technology experts. They need not even launch the attack themselves but can rent a service from a criminal organization specializing in this type of activity."

Then there's the idea of causing damage within an organization or picking up leaked information during a DDoS attack that can then be used to extort money from a company. These types of attacks often come from disgruntled workers or hacktivists who want to bring down a perceived foe. "The offender can also be a discontented employee, a lone actor, or a competitor seeking out sensitive information using methods such as social engineering, spyware, system penetration, device theft, data interception, and unauthorized disclosure of information from the inside," Menting says. Attackers either use the DDoS attack as a distraction to pull security resources away from the real target, or they can be used to attack the company from multiple directions and make it more difficult to defend against.

On-Premises, Cloud-Based & Hybrid Solutions

When it comes to mitigating DDoS attacks, there are many different approaches, but the end goal is to ultimately absorb the brunt of the attack and divert it away from your primary servers and networks until it can be stopped. Many vendors offer on-premises solutions, including A10 Networks, F5 Networks, and Radware, which require you to handle everything in-house, so you may need some extra infrastructure in place. This is a good

"Enterprises with significant revenue from web operations (e.g., e-commerce, online gaming) should consider placing web infrastructure behind a CDN provider to increase protection from DDoS attacks, which leverage CDN content and application-delivery functions to offer better end-user experiences."

JIM DAVIS
Senior Analyst
451 Research

"There are various ways to mitigate a DoS/DDoS attack using network defenses (IPS, firewalls, and others). These are primarily on-premises methods. Alternatively, traffic can be passed through a cleaning or scrubbing center before going to the intended user. This is often offered as a cloud-based service because the platform can be scaled depending on attacks. Of course there is also the possibility of sinkholing botnets [redirecting them to research machines for study], but that requires a coordinated, intelligence-based offensive approach."

MICHELA MENTING
Research Director
ABI Research

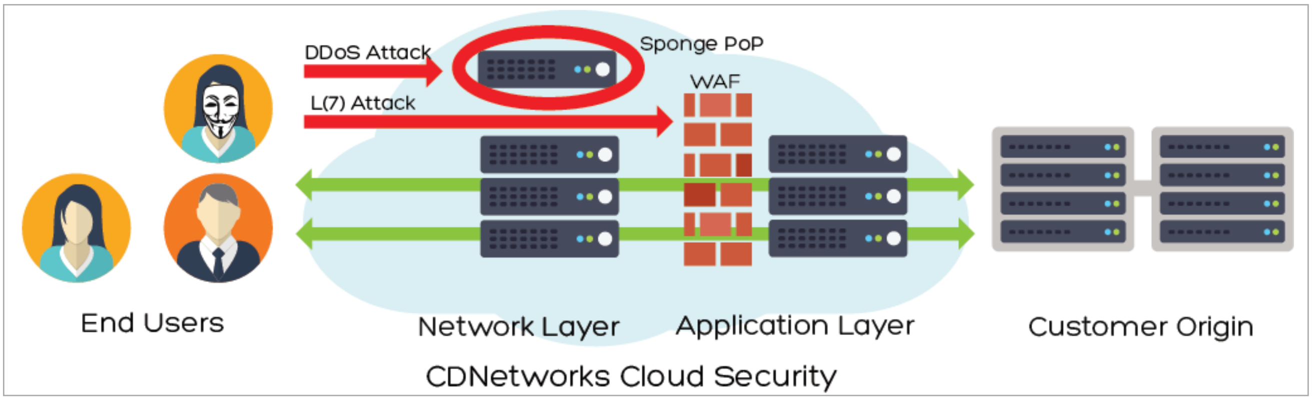
approach for organizations that are attacked on a relatively consistent basis and know how to handle the traffic.

From there, you have cloud-based solutions such as CloudFlare and CDNetworks, which tend to come in one of two flavors. There are CDN (content delivery network) solutions, which are designed to deliver content to users based on geographic location and can also be used to mitigate DDoS attacks. There are also cloud-based scrubbing services, "which consist of several points of presence that ingest traffic bound for the customer, mitigate attacks, and send clean traffic on its way to the customer," says Davis. "These services can be deployed in always-on fashion, but smaller enterprises may not always be able to justify the cost of this option. If services are not deployed in an always-on fashion, there can be delays in defending against attacks (typically between 15 to 20 minutes) as traffic gets re-routed."

One example of a cloud-based CDN provider is CDNetworks. It creates a filter of sorts in the cloud that directs unwanted traffic to a "sponge" server that can absorb the impact while still letting legitimate traffic through. But this approach can also help stop secondary attacks that can sometimes accompany the DDoS and tend to go after the application layer. That attack would run into a WAF (web application firewall) that prevents it from impacting any applications or the data stored within. The key to these cloud-based service providers is that they have enough bandwidth, and probably more than most companies have, to absorb the traffic without having it impact other services, which is exactly what you need during a DDoS attack.

There are also hybrid on-premises/cloud solutions that let you keep some control onsite but then you can take advantage of scrubbing services as needed. The important thing to remember is that you need to take a layered approach to security, especially when dealing with DDoS attacks. "Not all services mitigate all types of attacks," says Davis. "Web application firewall technology may be useful in supplementing protection against application-layer DDoS attacks."

"In general," Davis adds, "leveraging cloud-based services for protection from DDoS attacks is a must as attacks continue to scale in size beyond what on-premises solutions alone can handle. Additionally, they promise faster deployment and easier management."



This illustrates how traffic from legitimate end users is allowed to travel through the CDN (content delivery network) and WAF (web application firewall) unimpeded while the DDoS attack and secondary attack run into security measures, are absorbed, and can't impact service to actual clients.

Net Neutrality & Zero Rating

WADING THROUGH THE GRAY AREA OF WHAT CONSTITUTES A FREE & OPEN INTERNET

KEY POINTS

- There seemed to be a lull in the net neutrality debate in recent months, but the FCC under a new administration appears to be shaking things up.
- App creators are concerned because while some could afford to pay for better performance, smaller ones may not be able to compete.
- Carriers believe they should be able to charge more for apps that most heavily use resources.
- Zero rating is the concept of not making certain apps and services count against your data plan cap.

IF YOU FOLLOW technology-related news (which you clearly do, and thank you for that) then there's a solid chance you've heard about issues around net neutrality. In a nutshell, net neutrality is the idea that no specific applications, websites, or providers should get preferential treatment over others in terms of access to network resources. An example of this would be an ISP (internet service provider) giving Amazon Prime Video more bandwidth than Netflix, or throttling the bandwidth of one of those providers while letting the other operate freely. An important piece of this concept is that no provider should be able to pay for preferential network treatment because it could discourage competition from smaller players in a wide range of markets.

Over the past few months, and really over the past year and change, the talk of net neutrality has actually fallen away considerably as many of the policies passed by the Federal Communications Commission generally favored consumers and providers, while carriers (at least publicly) weren't expending much visible energy fighting the rules. However, with the recent shift from the Obama administration to the Trump administration and the appointment of a new FCC chairman, the debate around net neutrality is heating up again. While many of the old net neutrality concepts still remain, the new FCC chairman is taking a more carrier-friendly perspective, at least from the outset, which is causing concern for some application, website, and service providers.

The Evolving Argument

As with any argument, there are two sides to the coin, and with net neutrality, you have the carriers on one side and users and application providers on the other. Jennifer Pigg Clark, vice president at the 451 Research, explains that the carrier side of the argument is relatively simple to understand. “The carriers believe they are carrying an inordinate amount of traffic from certain applications providers,” says Clark. “If 40% of your network traffic is generated by Netflix, the carriers are of the opinion that Netflix should be compensating them for clogging up their pipes.”

Carriers also believe that because services such as YouTube and Netflix are so demanding on networks and “very susceptible to latency, performance, and jitter,” Clark adds, it makes sense that these service providers should pay extra for improved performance. That part is particularly important because in order to give their customers the experience they expect, ISPs have often had to build out their infrastructure to meet demand, which is a cost that application providers don’t have to worry about. In other words, some ISPs want these companies with higher network demands to pay more to help offset those expansion and upgrade costs.

On the other side of the coin, which is where the users and app providers live, a lot of the talk is around competition. If ISPs are able to charge app and content providers extra to get better performance, then larger corporations could find a way to take on that cost while smaller providers may not have the funds to compete. In other words, the companies taking up the most bandwidth will be able to continue to do so, and get better performance to boot, while smaller ones will remain stuck on the same bandwidth level. This trickles down further because users of a given application from that smaller provider are essentially being punished or not getting the best possible experience simply because the provider can’t afford to pay for extra bandwidth.

And then there’s the argument that carriers being able to throttle or bolster whichever services they desire could lead to a mild form of censorship. “The fear on the part of the end users is that the carriers will negatively impact traffic [which] they are, for some reason, determined that the users shouldn’t see,” says Clark. “It all gets wrapped up in things like BitTorrent, where peer-to-peer traffic was traditionally throttled by the carriers. They were differentiating between applications A through Z and BitTorrent applications. Peer-to-peer video traffic used up a lot of bandwidth on the upstream side, rather than on the downstream side. There were all sorts of reasons why the carriers felt that they were well within their rights to throttle this traffic.”

Interestingly enough, Clark says that many of these net neutrality points are waning or are simply not talked about as much as they used to be, at least for the time being. Thinking about mobile devices in particular, most of the carriers moved to tiered plans with data caps, but some of them still offer unlimited plans for particularly heavy users. Clark points out that some people are even in favor of bandwidth throttling in certain situations where their children, for example, might frequently go over their data cap, and it’s a service they can request from the carrier if the limit is within reach. That, of course, doesn’t tell the whole story, but it shows that both carriers and end users are still dancing around the issues and still figuring out how to maneuver through them.

Zero Rating

One of the ways mobile wireless providers in particular have been trying to balance out this issue of instituting data caps is through the practice of zero-rating. Zero-rating is where a carrier can make it so that a certain application, such as YouTube, Facebook, or Netflix, doesn’t count against your data cap, regardless of how much you use it. Clark refers to this as “a marketing tool” for many of

CURRENT FCC STANCE

While the Obama administration was largely seen as a supporter of net neutrality laws, the Federal Communications Commission under the Trump administration is swiftly making moves in the opposite direction. Ajit Pai, the FCC’s new chairman, was already a somewhat controversial pick for the position in pro-net neutrality circles because he previously worked as a lawyer for Verizon and was a vocal critic of the Open Internet Order, which was passed in 2015 and sought to “protect free expression and innovation on the internet and promote investment in the nation’s broadband networks,” according to the FCC’s official website.

At the outset, Pai announced the FCC would close an investigation into certain zero-rating policies implemented by Verizon, AT&T, and (perhaps most notably) T-Mobile to prevent certain services from counting against customer data caps. He also nixed a proposal meant to spur competition in the cable box market by requiring television providers to offer their services on third-party set-top boxes and applications. Pai was also against the move to officially consider broadband internet a utility, which opened the possibility for net neutrality rules in the first place. It’s difficult to predict how this will shake out, but at least for right now, it appears that net neutrality supporters likely have another fight on their hands.

the carriers to try to sell families with heavy users of these applications on their service plans. These types of programs are particularly interesting because although YouTube and other streaming services were often cited as the reason why carriers wanted to start charging for better performance, they are now often the exact services offered under zero-rating policies.

Clark, however, says she hasn't "seen a lot of revenue generated from that type of marketing." In fact, she says, zero-rating certain applications might make more sense in countries like India and Brazil that have high concentrations of prepaid phone users who are more concerned about monthly limits and would benefit from such a move. And zero-rating apps may also be an incentive for users that don't have consistent access to Wi-Fi but do have a 4G LTE connection, which is not only faster than previous 2G, 3G, and even original 4G standards, but is also often faster than many of the Wi-Fi connections out in the wild.

"I frequently find myself turning off Wi-Fi because it's driving me crazy and performance on 4G is better," says Clark. "That's something that we've been predicting for a while. Yeah, Wi-Fi is good when you're in a building, have good access points, or are in your home where it's really built around providing really good quality. When you're walking around in a store or are in a Starbucks on public Wi-Fi, you may be less than thrilled with the performance and 4G is more what you're looking for. Plus," she adds, "if you don't have Wi-Fi, we have a lot of people turning their phones into access points. They're using their 4G phone as an access point for their computer, and there goes your mobile data allotment right there. There are all sorts of ways to eat up your data allotment."

How Carriers Are Adjusting

As previously mentioned, carriers have had to change the way they approach their networks and services due to net neutrality concerns and trying to attract more customers, and this is especially true for wireless carriers. One of those attempts was to introduce data caps and then zero-rating, but there is also a push to go back to the old days of unlimited data plans, which is something AT&T decided to do recently and Verizon was exploring as we wrote this. Clark says the reason for this is because networks are "not only getting faster, but more flexible with the help of virtualization technologies." There is a level of scalability in place now that is making it possible for carriers to "keep up with the pace with this incredible demand" without having to bend over backwards, she adds.

Clark also thinks it's important to look back and realize that what the carriers were asking for wasn't necessarily unreasonable, and that they made strides to regulate themselves from the very beginning. The fear, she says, was that these companies would abuse the power they were given and spiral into a worst case scenario where the wealthiest and most successful corporations could pay for better bandwidth while the smaller players were left behind. But at the end of the day, the reason why carriers wanted to put these policies was in place is because Netflix, for example, was taking up about 40% of their traffic and they didn't feel as though they should have to "build out their networks for something they were not being paid for, pure and simple," Clark explains.

Now, as the technology is starting to catch up, carriers are starting to realize that it isn't just Netflix that's giving them headaches, but rather a wide swath of applications and services. And this realization has led to carriers investing more money in their infrastructure, which in turn has led to many efficiency and performance gains. At least for the time being, carriers are able to keep up with the demand, but that doesn't mean the issue won't come back in the future.

"The pain has now spread," says Clark. "They've caught up with the network. The carriers' role was a little bit more rational than users gave them credit for, but nevertheless, to just say to the carriers, 'charge what you want,' invites abuse. In the future, I think it has become less of an issue because users are experiencing good performance all around. If performance should start to degrade and suddenly they're finding that one application they depend upon that isn't from a global app provider suddenly doesn't have great performance and Netflix does, then that's when the problem will rear its ugly head again."

"The carriers' role was a little bit more rational than users gave them credit for, but nevertheless, to just say to the carriers, 'Charge what you want,' invites abuse. I think it has become less of an issue because users are experiencing good performance all around. If performance should start to degrade and suddenly they're finding that one application they depend upon that isn't from a global app provider suddenly doesn't have great performance and Netflix does, then that's when the problem will rear its ugly head again."

JENNIFER PIGG CLARK
Vice President
451 Research

Why Bother With Reddit?

IT'S A POWERFUL AGGREGATOR FOR CONSUMING & SHARING INFORMATION

KEY POINTS

- Reddit thrives on an active community of readers, submitters, and moderators that follow specific rules and guidelines.
- Submissions that receive the most upvotes will show up on the Reddit front page and at the top of individual subreddits.
- Subreddits are essentially more specific categories within Reddit where users can share similar posts with one another.
- Submitting to Reddit is relatively easy and after you sign up for an account, you can choose to share pre-existing information or offer up something new.

AT SOME POINT in the recent past, people grew tired of having to visit multiple websites on the Internet to get access to all of the information they needed. If you were a person of many tastes back in the early days of the World Wide Web, you often had to search far and wide for specific outlets that covered news and topics that were of interest to you. Today, a select few organizations understand the power and importance of aggregation. They understand that people want access to everything relevant to them in one place, or in as few places as possible. You have the social media side of things, including Facebook and Twitter, where friends, family members, colleagues, or just people you like can share information and relevant links. And then you have tools like Google News, which is a customizable information aggregator that helps you find articles about politics, world news, sports, entertainment, and much more.

But there is also a website out there that combines both of these philosophies. It's a combination information/news aggregator and a social network of sorts, where people can come together to share stories after the fact. Reddit, cleverly enough, refers to itself as "the front page of the internet," and it's not necessarily wrong to make that claim. Whether you choose to visit the front page of Reddit to find general news items and interesting stories that have received the most community votes or you dig down into the subreddits, or subcategories, to find more specific topics, Reddit contains something for almost everyone. And how much you get out of Reddit depends on exactly how deep you want to dig.

How It Works

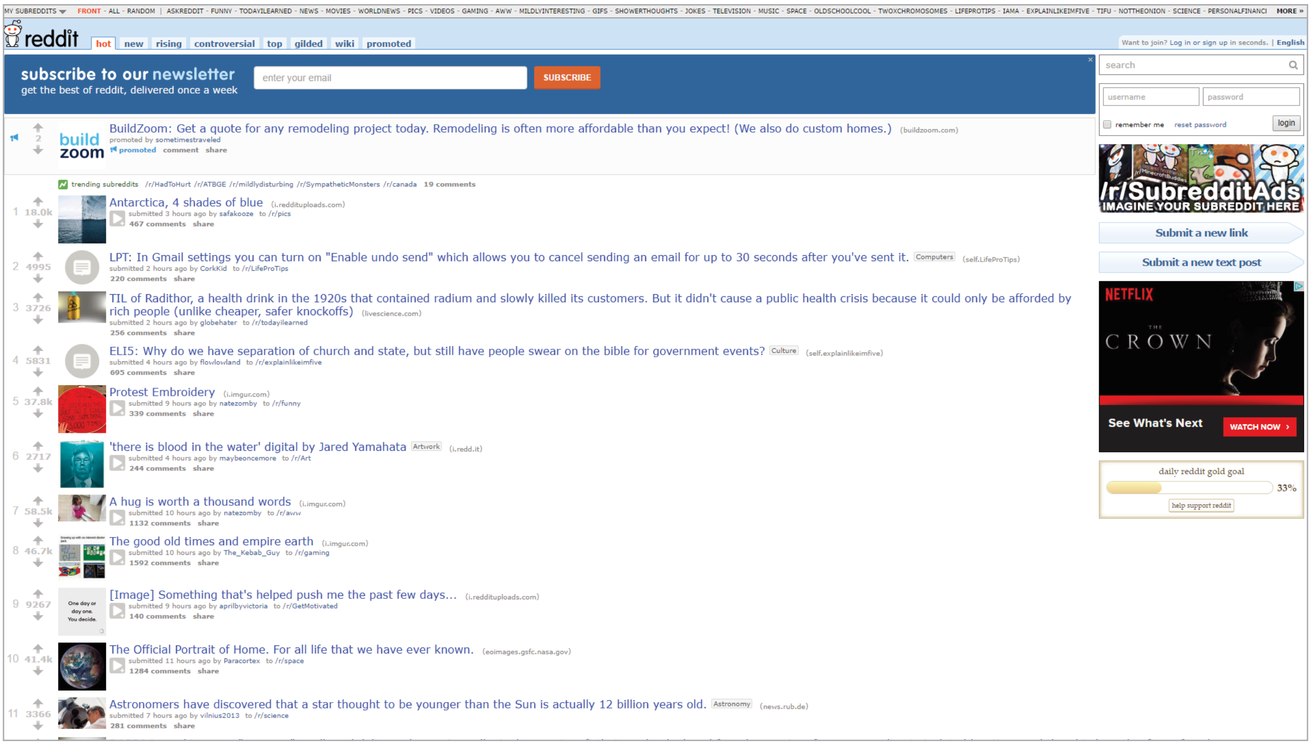
Reddit may appear daunting on the surface, and it does come with its own quirks and sets of rules, but for all intents and purposes it's a pretty simple website. Someone decides to post a link, an image, a video, or some other form of content and then the community chooses to either "upvote" (elevate) or "downvote" (demote) that submission based purely on opinion. If a post gets enough upvotes, then chances are it will show up on the front page. Reddit's front page is essentially a "most popular" page showing everything that people are enjoying most on a given day, and the "page" portion is a bit of a misnomer as it can in fact go dozens of pages deep.

However, just because the front page is cultivated by the community at large doesn't mean you don't have any say in what shows up there. In fact, when you first sign up for a Reddit account, you're given the option to customize what sorts of stories you'll see most often, and you can make changes to that list whenever you feel like it. For example, if you want to make sure news, entertainment, and pictures of cute animals are prioritized over other categories, you can do that. You can also dig much deeper into Reddit's options to filter out NSFW (not suitable for work) content, choose whether or not to show thumbnails next to links, etc. Reddit may be an aggregator, but it also has quite a few tools to make sure you mainly see what truly matters to you.

The mobile application also offers its own collection of settings and preferences for users to sort through. You can change the view of the feed on your smartphone or tablet, adjust the text size, choose whether or not videos should autoplay when they appear, and even change the overall theme. The goal of Reddit is to give you access to relevant information without getting in the way of the sharing process. You get to choose what categories you see most often and how that information is displayed on your computer or mobile device.

Subreddits

Speaking of categories, another major aspect of Reddit is the subreddit, and if you want to become a more active user of the service, it's something you'll want to become familiar with. You'll notice when you look at the front page that under every post there is a line that says who a post was submitted by, when it was submitted, and to what subreddit it was submitted. Think of subreddits as subcategories or topics where


MY SUBREDDITS ▾ FRONT - ALL - RANDOM | ASKREDDIT - FUNNY - TODAYILEARNED - NEWS - MOVIES - WORLDNEWS - PICS - VIDEOS - GAMING - AWW - MILDLYINTERESTING - GIFS - SHOWERTHOUGHTS - JOKES - TELEVISION - MUSIC - SPACE - OLDSCHOOLCOOL - TWOXCHROMOSOMES - LIFEPROTIPS - IAMA - EXPLAINLIKEIMFIVE - TIFU - NOTTHEONION - SCIENCE - PERSONALFINANCI MORE »
reddit
hot new rising controversial top gilded wiki promoted
Want to join? Log in or sign up in seconds. | English
search
username
password
□ remember me
reset password
login
/r/SubredditAds
IMAGINE YOUR SUBREDDIT HERE
Submit a new link
Submit a new text post
NETFLIX
THE CROWN
See What's Next
WATCH NOW ›
daily reddit gold goal
33%
help support reddit
SUBSCRIBE
enter your email

subscribe to our newsletter
get the best of reddit, delivered once a week

2 BuildZoom: Get a quote for any remodeling project today. Remodeling is often more affordable than you expect! (We also do custom homes.) (buildzoom.com)
promoted by sometimestraveled
promoted comment share

trending subreddits /r/HadToHurt /r/ATBGE /r/mildlydisturbing /r/SympatheticMonsters /r/canada 19 comments

1 18.0k Antarctica, 4 shades of blue (i.reddituploads.com)
submitted 3 hours ago by safakooze to /r/pics
467 comments share

2 4995 LPT: In Gmail settings you can turn on "Enable undo send" which allows you to cancel sending an email for up to 30 seconds after you've sent it. Computers (self.LifeProTips)
submitted 2 hours ago by CorkKid to /r/LifeProTips
220 comments share

3 3726 TIL of Radithor, a health drink in the 1920s that contained radium and slowly killed its customers. But it didn't cause a public health crisis because it could only be afforded by rich people (unlike cheaper, safer knockoffs) (livescience.com)
submitted 2 hours ago by globehater to /r/todayilearned
256 comments share

4 5831 ELI5: Why do we have separation of church and state, but still have people swear on the bible for government events? Culture (self.explainlikeimfive)
submitted 4 hours ago by flowlowland to /r/explainlikeimfive
695 comments share

5 37.8k Protest Embroidery (i.imgur.com)
submitted 9 hours ago by natezomby to /r/funny
339 comments share

6 2717 'there is blood in the water' digital by Jared Yamahata Artwork (i.redd.it)
submitted 4 hours ago by maybeoncemore to /r/Art
244 comments share

7 58.5k A hug is worth a thousand words (i.imgur.com)
submitted 10 hours ago by natezomby to /r/aww
1132 comments share

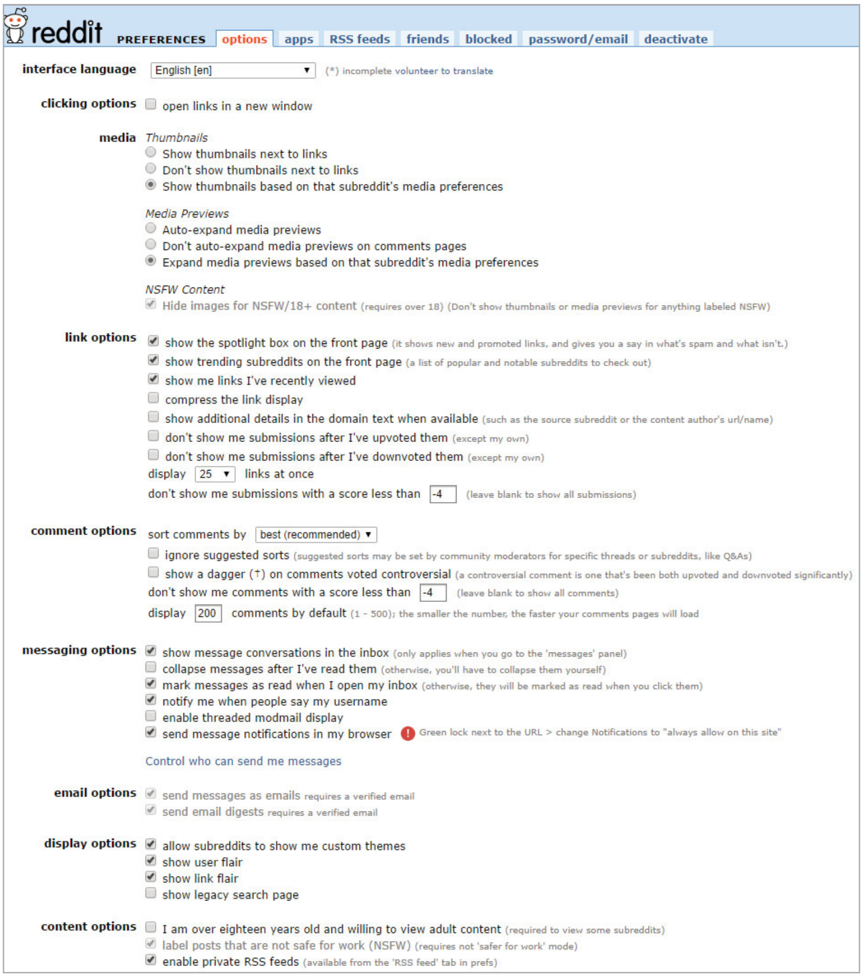
8 46.7k The good old times and empire earth (i.imgur.com)
submitted 10 hours ago by The_Kebab_Guy to /r/gaming
1592 comments share

9 9267 [Image] Something that's helped push me the past few days... (i.reddituploads.com)
submitted 9 hours ago by aprilbyvictoria to /r/GetMotivated
140 comments share

10 41.4k The Official Portrait of Home. For all life that we have ever known. (eoimages.gsfc.nasa.gov)
submitted 11 hours ago by Paracortex to /r/space
1284 comments share

11 3366 Astronomers have discovered that a star thought to be younger than the Sun is actually 12 billion years old. Astronomy (news.rub.de)
submitted 7 hours ago by vilnius2013 to /r/science
281 comments share

Check the small print: the front page of Reddit is a no-frills list of articles, images, videos, and original content that have been upvoted by the community.



reddit PREFERENCES options apps RSS feeds friends blocked password/email deactivate

interface language English [en] ▾ (*) incomplete volunteer to translate

clicking options □ open links in a new window

media *Thumbnails*
○ Show thumbnails next to links
○ Don't show thumbnails next to links
● Show thumbnails based on that subreddit's media preferences

Media Previews
○ Auto-expand media previews
○ Don't auto-expand media previews on comments pages
● Expand media previews based on that subreddit's media preferences

NSFW Content
☑ Hide images for NSFW/18+ content (requires over 18) (Don't show thumbnails or media previews for anything labeled NSFW)

link options ☑ show the spotlight box on the front page (it shows new and promoted links, and gives you a say in what's spam and what isn't.)
☑ show trending subreddits on the front page (a list of popular and notable subreddits to check out)
☑ show me links I've recently viewed
□ compress the link display
□ show additional details in the domain text when available (such as the source subreddit or the content author's url/name)
□ don't show me submissions after I've upvoted them (except my own)
□ don't show me submissions after I've downvoted them (except my own)
display 25 ▾ links at once
don't show me submissions with a score less than -4 (leave blank to show all submissions)

comment options sort comments by best (recommended) ▾
□ ignore suggested sorts (suggested sorts may be set by community moderators for specific threads or subreddits, like Q&As)
□ show a dagger (†) on comments voted controversial (a controversial comment is one that's been both upvoted and downvoted significantly)
don't show me comments with a score less than -4 (leave blank to show all comments)
display 200 comments by default (1 - 500); the smaller the number, the faster your comments pages will load

messaging options ☑ show message conversations in the inbox (only applies when you go to the 'messages' panel)
□ collapse messages after I've read them (otherwise, you'll have to collapse them yourself)
☑ mark messages as read when I open my inbox (otherwise, they will be marked as read when you click them)
☑ notify me when people say my username
□ enable threaded modmail display
☑ send message notifications in my browser ! Green lock next to the URL > change Notifications to "always allow on this site"

Control who can send me messages

email options ☑ send messages as emails requires a verified email
☑ send email digests requires a verified email

display options ☑ allow subreddits to show me custom themes
☑ show user flair
☑ show link flair
□ show legacy search page

content options □ I am over eighteen years old and willing to view adult content (required to view some subreddits)
☑ label posts that are not safe for work (NSFW) (requires not 'safer for work' mode)
☑ enable private RSS feeds (available from the 'RSS feed' tab in prefs)

You can dig deep into Reddit's settings to filter out certain types of content and even decide the upvote/downvote threshold for viewing comments.

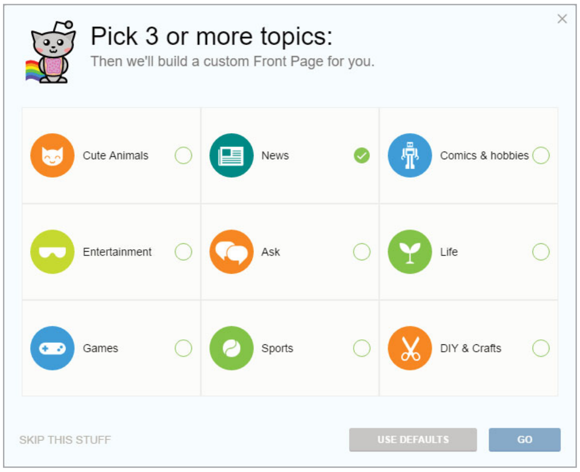
you will find a series of like-themed posts that all fit a given theme. For example, if you visit the r/worldnews subreddit, you'll find world news, if you visit the r/pics subreddit, you'll find pictures, and so on.

The reason why subreddits exist is to perform a bit of aggregation before the larger aggregation can begin (confusing, we know, but stick with us). Members of a subreddit will only post content related to that topic, and if that content gets enough upvotes within than specific community, it will more than likely end up transcending the subreddit and moving onto the front page. In other words, subreddits work as a way to let you get more granular in terms of what you want to see, but also to find the best of the best of each subreddit before letting those submissions make it to the main aggregation site.

The important thing to remember about subreddits is that they often have very specific and detailed rules as to what can be posted in them. These rules are absolutely crucial because they make sure only relevant content shows up in a given feed and is accurately categorized for future aggregation. These subreddits are often policed by the people, where members are encouraged to downvote and report posts that don't fit a given category; they are also monitored by moderators who are tasked with keeping subreddits as clean as possible.

Let's look at the r/worldnews subreddit as an example. Under this subreddit's rules, you'll find that purely domestic U.S. news posts, items with misleading titles, opinion pieces, petitions, and older news articles aren't permitted. You also can't post any images, videos, or audio clips, nor can you post items from social media sites including Facebook, Tumblr, and Twitter. The goal of this specific subreddit is to aggregate only posts about world news, so it makes sense to filter out certain types of content to keep that feed on-topic.

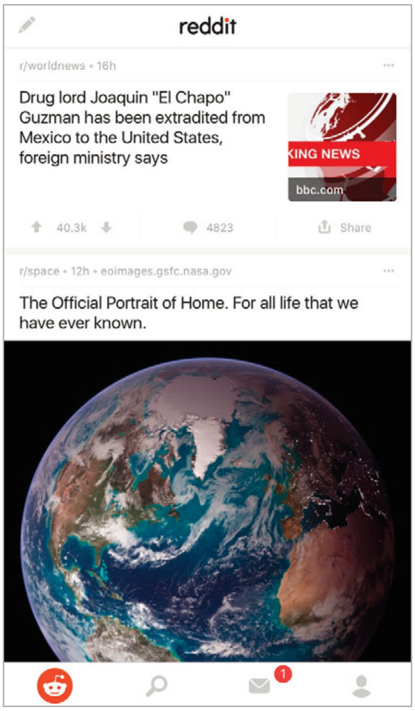
This subreddit also has a list of rules for actions that aren't allowed in the comments section of each submission. For example, no bigoted remarks, personal attacks on other users, or generally offensive content are allowed, and even memes and GIFS are



Pick 3 or more topics:
Then we'll build a custom Front Page for you.

Cute Animals ○ News ✓ Comics & hobbies ○
Entertainment ○ Ask ○ Life ○
Games ○ Sports ○ DIY & Crafts ○

When you sign up for an account, you can choose which categories you want to see more of on your personalized Reddit front page.



reddit

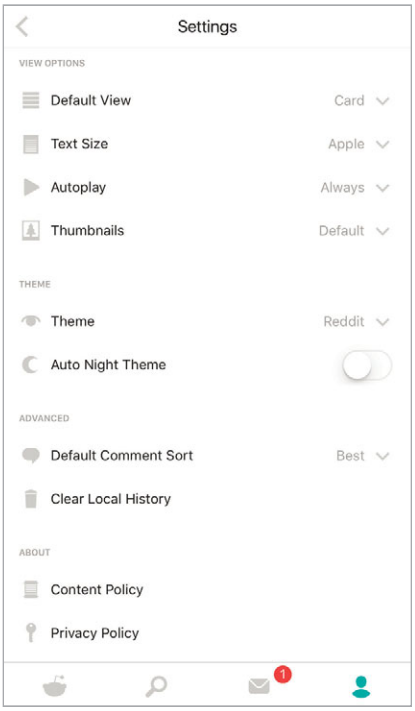
r/worldnews • 16h

Drug lord Joaquin "El Chapo" Guzman has been extradited from Mexico to the United States, foreign ministry says

r/space • 12h • eoimages.gsfc.nasa.gov

The Official Portrait of Home. For all life that we have ever known.

The Reddit app offers an experience fine-tuned for mobile devices, often with larger images and autoplay videos.



Settings

VIEW OPTIONS

Default View — Card

Text Size — Apple

Autoplay — Always

Thumbnails — Default

THEME

Theme — Reddit

Auto Night Theme

ADVANCED

Default Comment Sort — Best

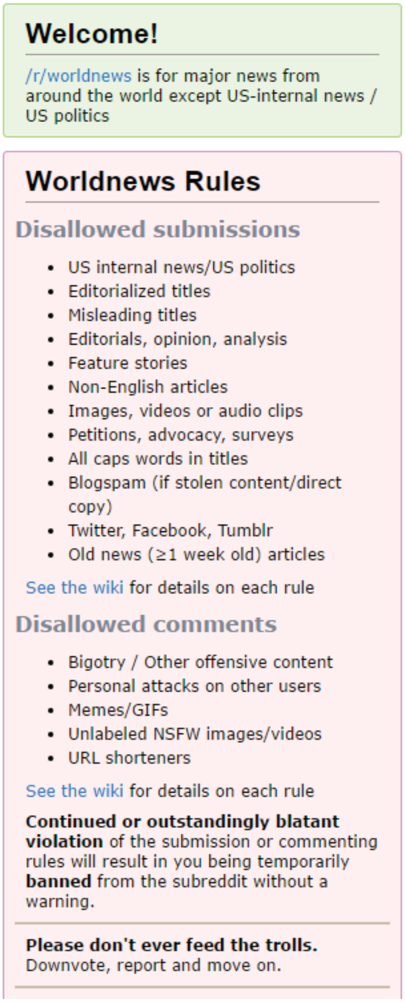
Clear Local History

ABOUT

Content Policy

Privacy Policy

Similar to how the main site works, you can dig into the settings on the Reddit mobile app to choose text size, themes, and more.



Welcome!

/r/worldnews is for major news from around the world except US-internal news / US politics

Worldnews Rules

Disallowed submissions

- US internal news/US politics
- Editorialized titles
- Misleading titles
- Editorials, opinion, analysis
- Feature stories
- Non-English articles
- Images, videos or audio clips
- Petitions, advocacy, surveys
- All caps words in titles
- Blogspam (if stolen content/direct copy)
- Twitter, Facebook, Tumblr
- Old news (≥1 week old) articles

See the wiki for details on each rule

Disallowed comments

- Bigotry / Other offensive content
- Personal attacks on other users
- Memes/GIFs
- Unlabeled NSFW images/videos
- URL shorteners

See the wiki for details on each rule

Continued or outstandingly blatant violation of the submission or commenting rules will result in you being temporarily **banned** from the subreddit without a warning.

Please don't ever feed the trolls. Downvote, report and move on.

Be sure to pay attention to the specific rules of a given subreddit when thinking about making a post to make sure you're working within the guidelines of that community.

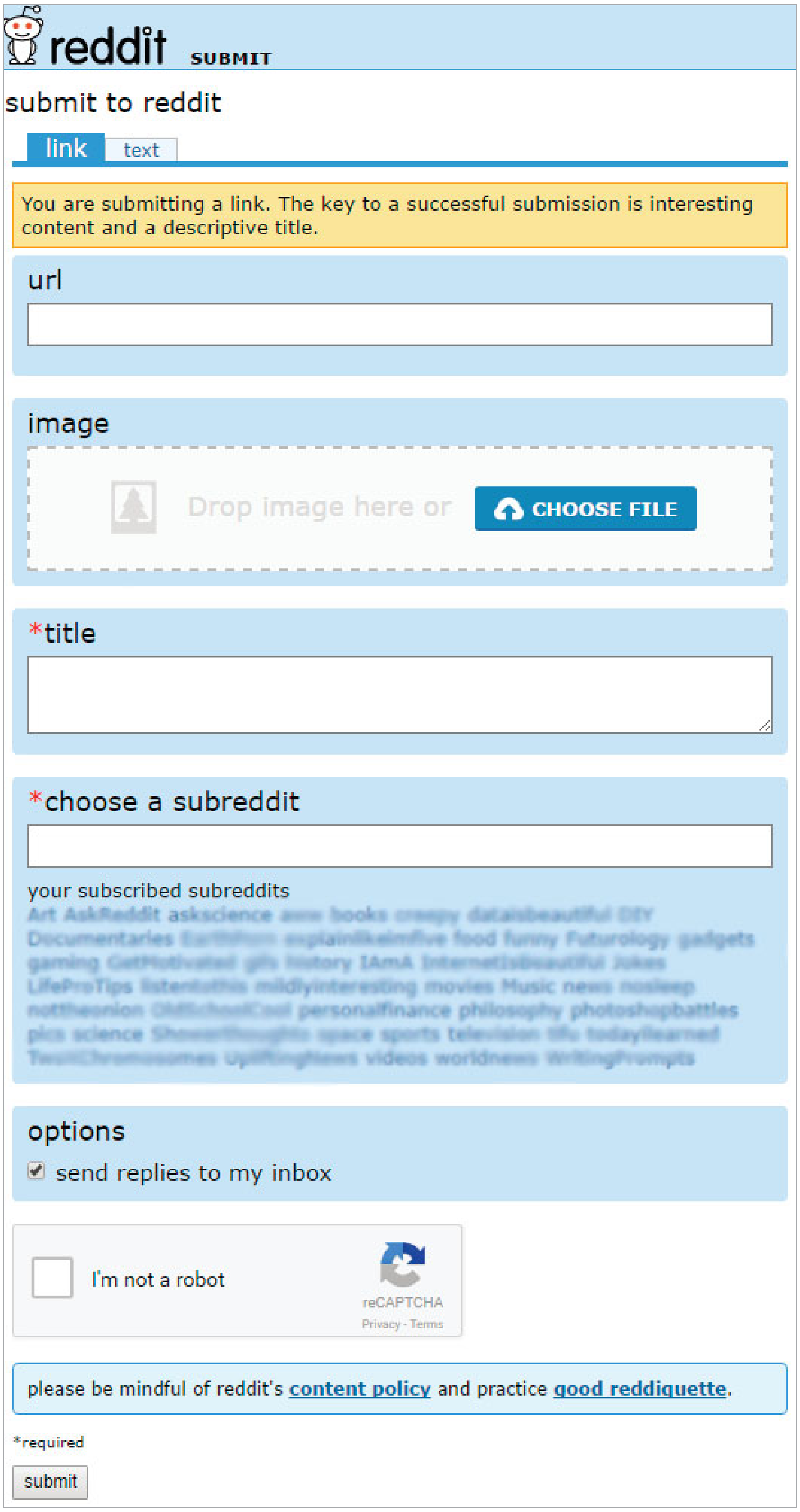
not permitted in the comments section. Having these types of policies helps foster a community where news is taken seriously and more reasoned discussions are encouraged. That, of course, isn't the case on all subreddits, as many of them are dedicated to humor, video games, movies, the aforementioned cute animal pictures, and almost any other topic you can imagine. The key is to find the subreddits that fit your personality the most and stay away from the others so you don't get in over your head.

Lurkers & Submitters

There are generally two different groups of people that tend to use Reddit. There are the lurkers, which are those who may not even have Reddit accounts but like to use the website as a general news aggregator. And then there are people who more actively use the site in a variety of ways, including people who actually submit links and other content to the site. Of course, there are more granular and nuanced subcategories within those two groups, not unlike Reddit itself, but we'll focus on the folks that just look at the site and then those who use it to its full potential.

If, after being a lurker for a given amount of time, you decide you want to jump in and get involved, it's really as easy as signing up for an account, customizing your categories, and then downvoting, upvoting, and submitting to your hearts content. You will have to pay attention to the aforementioned rules of the road for a given subreddit, but as long as you work within those parameters, the worst thing that can happen is your submission doesn't make an impact and you move on to the next one.

When it comes to submitting a post, it's almost as easy as signing up for an account. The first option is to submit a link either to an article, video, or image. You get to choose which URL the submission directs to, what image Reddit users will see next to the submission, the title of the post, and which subreddit it will appear in. The submission form shows a list of subreddits you're currently subscribed to, which makes it much easier to find a relevant place to make your submission. Then, when you're done, you can click "Submit" at the bottom of the page. From



submit to reddit

You are submitting a link. The key to a successful submission is interesting content and a descriptive title.

url

image

*title

*choose a subreddit

your subscribed subreddits

Art AskReddit askscience aww books creepy dataisbeautiful DIY Documentaries EarthPorn explainlikeimfive food funny Futurology gadgets gaming GetMotivated gifs history IAmA InternetIsBeautiful Jokes LifeProTips listentothis mildlyinteresting movies Music news nosleep nottheonion OldSchoolCool personalfinance philosophy photoshopbattles pics science Showerthoughts space sports television tifu todayilearned TwoXChromosomes UpliftingNews videos worldnews WritingPrompts

options

☑ send replies to my inbox

□ I'm not a robot

please be mindful of reddit's content policy and practice good reddiquette.

*required

When you make a submission to Reddit, you have the opportunity to give it a title, include an image to garner more attention for the post, and choose which subreddit it will appear in.

there, you can track the impact of your post from your account page and even receive notifications to your Reddit inbox when someone makes a comment. If a post gets more upvotes than downvotes, then it'll contribute to your overall "karma rating," which appears next to your user name and serves as a way to show other users your batting average on submissions.

In addition to sharing an already existing URL to Reddit, you can also choose to post a text submission where you have more freedom and can add a personal touch. One popular type of lighthearted submission in this category is called Showerthoughts where people offer up original, often humorous posts based on things that might pop into your mind while taking a shower. One highly upvoted post, for example, was entitled "On TV, once the 'bad guy' gets caught in a lie and admits it, everyone assumes they're always telling the truth suddenly." This particular subreddit shows the conversational side of Reddit where users can share ideas with one another in a more social-media manner.

The important thing to remember about Reddit is that it only remains daunting if you don't take the time to explore it. As long as you follow the rules of the site as a whole and each individual subreddit, there's really no wrong way to use it. It's an invaluable tool where you can get a snapshot of important current events across a wide range of topics without having to visit dozens of different websites. In a world where many people want to cut to the chase, get access to the information they need as quickly as possible, and sometimes have a venue for hashing out ideas with like-minded individuals, Reddit serves as an example of what can be achieved with a little bit of organization and an easy-to-use interface. C

Description
PC Today is the essential guide to business technology for executives and company owners.

Digital Diversions

THE LATEST PREMIUM ELECTRONICS

A Laptop That's Ready For Anything

Not satisfied with your laptop's performance? Many consumers have discovered that models built for serious gaming offer better speed, graphics, and audio than ordinary models, making them excellent all-around laptops. The GS63VR Stealth Pro from MSI Computer (www.msi.com) is just such a model. If you happen to be into gaming (or if you're searching for a gift for a gamer), all the better. The GS63VR is a Windows 10 PC that features the latest 6th Gen. Intel Core i7 processor and the newest GeForce GTX 1060 graphics with 6GB GDDR5, as well as DDR4-2400 memory (maximum 32GB), optional SSD (solid-state drive), and a 15.6-inch FHD (1,920 x 1,080 resolution) IPS LCD display that provides exceedingly vivid imagery. A full complement of ports supports the latest peripherals and accessories, and the GS63VR supports DirectX 12, virtual reality gear, multiple displays, and more.

Still On The Cutting Edge

If you've been hesitant to upgrade your smartphone, there's still the Galaxy S7 edge from Samsung (www.samsung.com) to consider. In addition to high-end specs inside, the edge features a water-resistant shell on the outside and works with Gear VR goggles and a host of other Samsung accessories. Samsung launched both the Galaxy S7 and the Galaxy S7 edge last year, and the chief difference between them is their size: the edge has a 5.5-inch Quad HD Super AMOLED display compared to the standard model's 5.1-inch display. Other specs are the same for both versions of this Android 6.0 (aka Marshmallow) phone, including your choice of 32GB or 64GB data storage (expandable via microSD card to 256GB), Fast Charging technology (including wireless charging capability), and a dual pixel camera with autofocus and the ability to take clear photos even when the lights are low.

Quick Cloud Collaboration

KEEPS PROJECTS IN SYNC

AS THE NUMBER OF employees doing business outside the walls of the traditional office environment increases, companies of all sizes are adopting new ways of getting work done. Namely, they're moving toward more flexible, efficient cloud-based services. Although the purposes of online SaaS (software as a service) options vary, users are taking advantage of seamless conferencing, file sharing, idea generating, and so much more. Read on to find a service that suits your collaborative needs.

Take Documents Offline

It seems inevitable that wireless internet availability determines when and where you edit online documents while you are on the road. But with the help of the right device-specific offline app, you don't have to postpone work until you are within range of a Wi-Fi hotspot. Some basic apps primarily let you read docs offline, whereas more feature-packed options let you edit and save changes to collaborative documents, spreadsheets, and presentations. Microsoft, for instance, provides a solution for offline workers via Office 365's (products.office.com/en-US/business) SharePoint Online. Using the program's MySite tool, you can create copies of documents on your PC and work on them when you are offline. Then, when you connect to the cloud again, SharePoint automatically syncs your work.

Don't Forget Your Webcam

Collaboration is accomplished on an international level these days, which means that face-to-face conversations with globetrotting team members are commonly conducted via LCD touchscreens. Whether you're working on a smartphone, tablet, laptop, or PC, using your webcam as a collaboration tool connects you to colleagues and clients more intimately than the routine conference call. We suggest using a videoconferencing app or software that supports multiuser conversations. Some options let you incorporate shared whiteboards and simultaneous document editing.

Consider Using File-Sharing Tools

If you need to share documents that don't contain particularly sensitive data, you can do so using a file-sharing service. Most file-sharing services let you securely upload and store a limited number of gigabytes (2 to 5GB is common) of data. Some services also give you the tools to organize your files. Sharing from your mobile device makes on-the-go collaboration convenient, so it's beneficial to check out file-sharing apps appropriate for your device.

Consider Online Productivity Tools

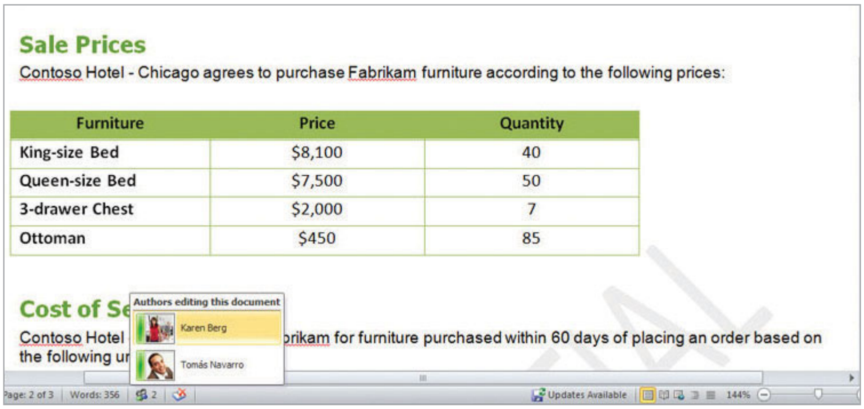
A plethora of web apps fall under the umbrella of "productivity," but in no way is that a bad thing because there is an app for practically every task, priority, project, and goal. For instance, you can use project management tools to juggle deadlines, manage to-do lists, track workflows, and more. Adding to these capabilities, Microsoft Office 365 gives team members shared access to master documents via user-created intranet sites, so they can edit in real-time and manage file access among customers and partners.

Use Whiteboards

When you can't meet in person, members of your virtual team can interact and brainstorm on full-featured online whiteboards. Browser-based whiteboards typically let you invite meeting participants to create and sketch on the same board. A number of whiteboard apps also support real-time collaboration in which everyone in the session is an equal participant. This is a good tool for tablet users who want to share ideas on the go but need input from others.

Accomplish More With Web Apps That Combine Different Capabilities

Multitaskers take note: Not only can you collaborate with more team members in the cloud than ever before, but you can also complete more tasks within the same service. Want to walk your team through a live slide show from a presentation sharing service? No problem. Need to create flow diagrams and share relevant images with your colleagues online? There's a service for that. And, if your team and a third-party developer are working on a website, for example, you can work together in a virtual space where anyone can add comments, crop images, and more.



Sale Prices

Contoso Hotel - Chicago agrees to purchase Fabrikam furniture according to the following prices:

Furniture	Price	Quantity
King-size Bed	$8,100	40
Queen-size Bed	$7,500	50
3-drawer Chest	$2,000	7
Ottoman	$450	85

Cost of Se

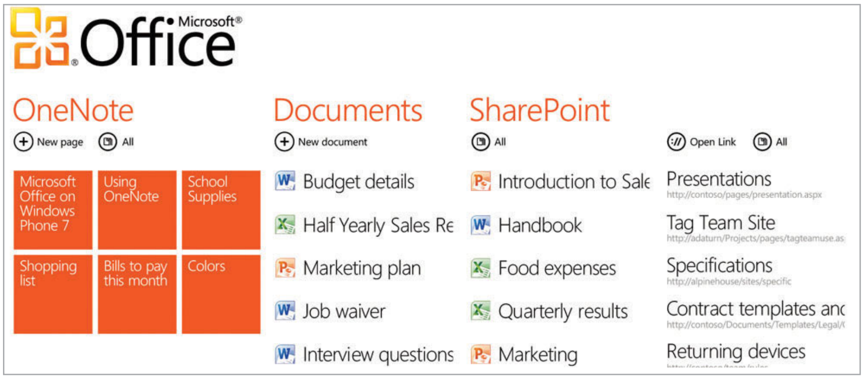
Contoso Hotel brikam for furniture purchased within 60 days of placing an order based on the following ur

Authors editing this document

Karen Berg

Tomás Navarro

With a cloud service such as Microsoft Office 365, you can co-author Word documents, Excel sheets, and other files with colleagues. Unlike traditional Office products, you don't have to save a separate version for yourself or wait until another person closes the file.



Microsoft® Office®

OneNote

Microsoft Office on Windows Phone 7

Using OneNote

School Supplies

Shopping list

Bills to pay this month

Colors

Documents

Budget details

Half Yearly Sales Re

Marketing plan

Job waiver

Interview questions

SharePoint

Introduction to Sale

Handbook

Food expenses

Quarterly results

Marketing

Presentations
http://contoso/pages/presentation.aspx

Tag Team Site
http://adaturn/Projects/pages/tagteamuse.as

Specifications
http://alpinehouse/sites/specific

Contract templates anc
http://contoso/Documents/Templates/Legal/(

Returning devices

If you're a Windows Phone user, you can easily access Office 365 apps from your device. Specifically, you can start a new OneNote page, create a new Office document, or edit files saved in SharePoint.

Manage Time & Tasks

Organizing schedules and all the associated meetings, deadlines, projects, and so forth can become a daunting task. Among the available cloud-based sites and mobile device apps, you can find apps and services that will help you manage your work life. Consider utilizing event-based planners, group-oriented reminder apps, services for meeting coordination, and visual to-do lists to keep your busy life on track.

Print Documents

When you need to print content from your mobile device, you can use one of many available apps to print documents to supported printers anywhere in the world. For example, if you are working on a presentation on your tablet while traveling and need to distribute copies to colleagues, you can print the presentation to a printer in your main office. Some mobile printing apps let you search a directory for nearby printers (such as those in hotels or airports) or locate a printer via GPS, so if you need to print a boarding pass or other content from your device while traveling, you can do that, too.

Some cloud-based printing apps and services also provide the option to print by sending an email attachment to a supported printer, or to print documents saved in an online storage service. Ⓒ

Isolate Malware

HOW TO COMBAT ATTACKS

An unfortunate fact about using an Internet-connected computer these days, whether it is a personal or company-issued notebook, is the constant threat of malware infection. Even when taking preemptive action to combat malware attacks, there's a fair chance one will eventually hit your notebook anyway, if for no other reason than the sheer volume of malware that attackers introduce daily. Frighteningly, **a leading security software maker reportedly detected more than 20 million new malware strains between January and March 2015 alone**. Of this number, Trojan horses accounted for 72.75% of all newly detected malware threats, and were responsible for 76.05% of all global computer infections. What's startling is that **these attacks included zero-day threats in which, as the name suggests, zero days expire between when a given vulnerability is discovered and when attackers release malware targeting the vulnerability**. With malware being so prevalent and persistent, a large part of combatting it is being able to recognize signs that a system may be infected and then knowing how to troubleshoot the problem. Also important is what security tools are available to detect, protect against, and remove malware.

WHAT ARE THE DANGERS?

MULTIPLE THREATS

New malware variants are constantly being developed and released.

There are several common groups, including viruses, worms, rootkits, spyware, Trojans, keyloggers, adware, and ransomware.

MULTIPLE AIMS

Malware can be designed to steal personal or company data, hold it for ransom, or simply wreak havoc.

One thing all malware has in common is an aim to infect its victims' systems.

MULTIPLE POINTS OF ENTRY

One good thing about malware is that it can often be avoided.

Infections can occur when visiting an infected website, installing infected software or an app, using an infected USB drive, or clicking a bad link.

WARNING SIGNS

SLOW PERFORMANCE

One of the most common warning signs is slow performance. You may notice that applications and/or the Internet is running noticeably more slowly than is ordinary. If this is happening, malware could be using resources in the background to fuel whatever nefarious activity it was designed to do.

WHAT TO CHECK

Updates running in the background, whether overall system updates or security software updates, can cause temporarily slow performance, so check to ensure updates aren't running before concluding your system has been compromised.

DISAPPEARING FILES

In addition to slow performance, you might also notice that certain programs, files, or folders take longer to open or don't open at all. Or your computer may take longer than usual to shut down, or it may refuse to shut down at all.

WHAT TO CHECK

An easy check for system performance issues on Windows computers is to look at the processes running in Task Manager. Press Ctrl-Alt-Delete to open Task Manager, and pay especially close attention to memory or CPU resource usage. Don't stop anything from running, though, if you're not sure what it is.

OTHER ODDITIES

If you find your notebook's battery drains quickly, your computer beeps, or your system's fans speed up for no obvious reason, something could be messing with your system. Also watch out for such things as unusual error messages, browser toolbars or software you didn't install, or the disappearance of shortcuts.

WHAT TO CHECK

These are common signs of malware, particularly adware or spyware if your browser is affected. Scour your installed programs for anything new, and check your browser settings to make sure an extension wasn't installed without your knowledge.

WHAT TO DO NEXT

SHUT IT DOWN

Switch off your internet connection immediately if you suspect malware is attempting to infect your system.

If your system appears frozen, or if you seem to be locked out from doing anything onscreen, perform a cold shutdown by pressing and holding the power button.

Sometimes shutting down prevents malware from installing fully, enabling you to turn it back on and use a malware removal tool.

USE A REMOVAL TOOL

In addition to built-in tools and your installed security software, there are numerous malware-removal tools available for free via the web.

Many software suites include malware-removal tools. Programs dedicated to the task include:

Malwarebytes
www.malwarebytes.com

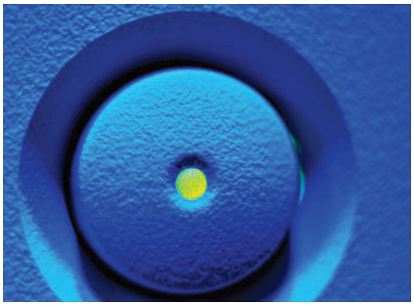
Spybot
www.safer-networking.org

DON'T LET IT HAPPEN AGAIN

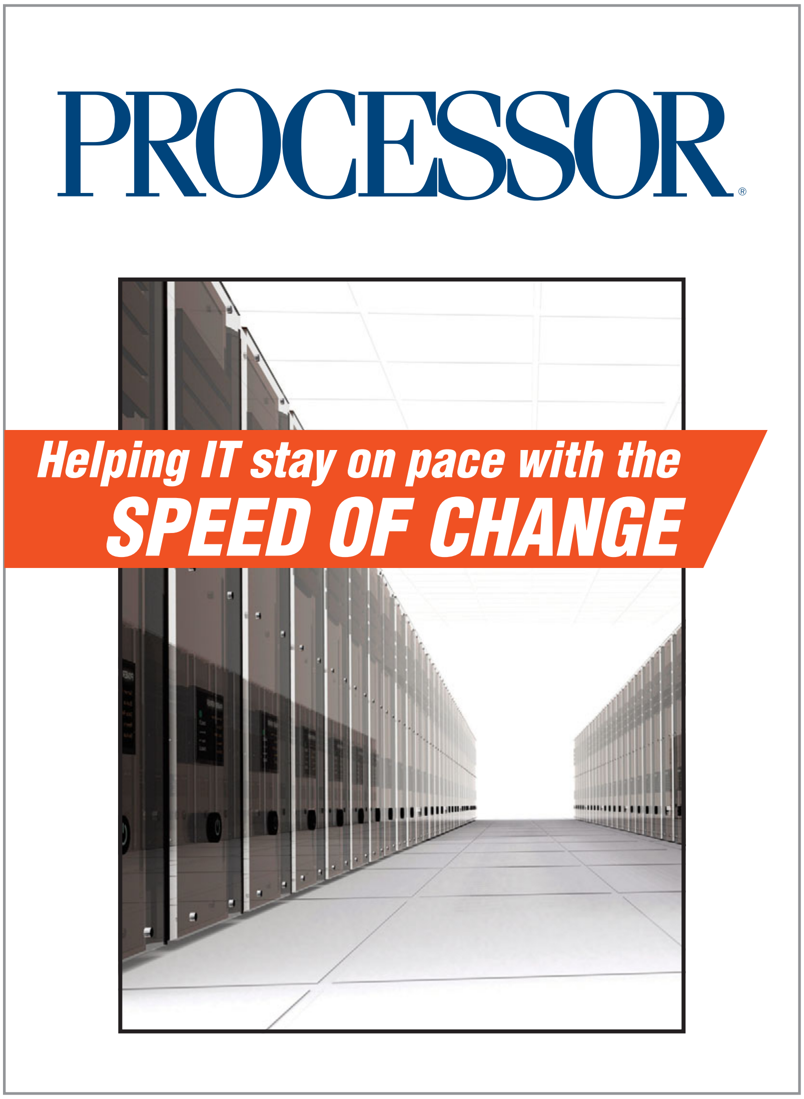
Prevention is the best method for never having to deal with malware. Ransomware, in particular, can rarely be dealt with in any other way than to pay off the hacker.

Ensure that, at minimum, there is a firewall running on your computer at all times. It's also vital to install security updates whenever available.

Make sure you don't inadvertently click a link or open an email attachment that is in any way questionable.



SPECIAL ADVERTISING & CONTENT FROM OUR *PROCESSOR* PARTNERS



Processor is designed for the IT world, covering the hardware and technologies that power today's data centers.

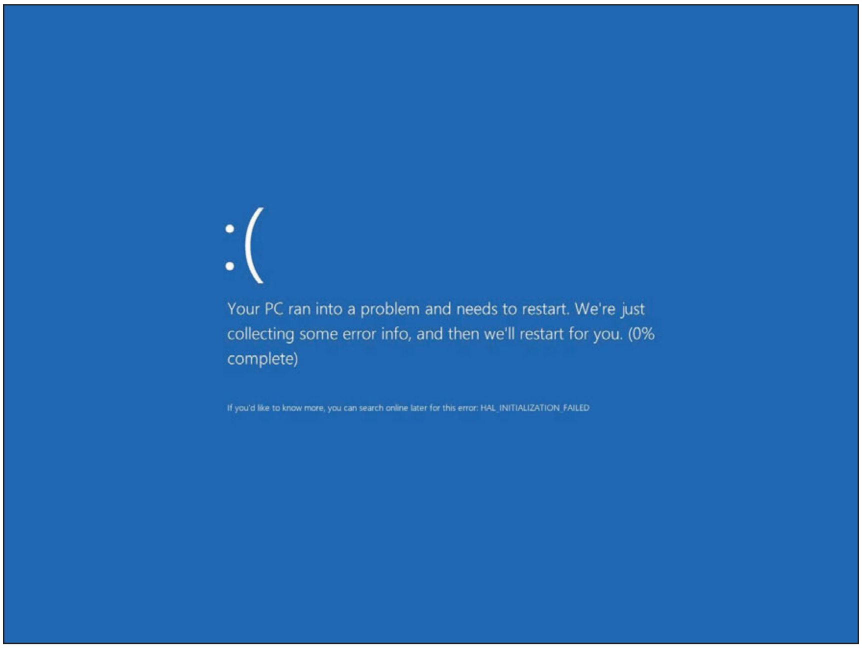
Blue Screen Of Death In The Age Of Windows 10

Banish The BSOD Blues

Don't you just hate it when your system thread exceptions aren't handled? Have you caught your DPC watchdog snoozing on the job? Is your IRQL consistently not less or equal? And you know, those bad pool callers need to seriously shape up. Or else!

It's 2017 and Windows PCs are more user-friendly than ever, yet despite more than four decades of advances and refinement in software and hardware, novice and expert PC users alike still encounter a special class of errors that the system is unable, seemingly even unwilling, to sufficiently explain. We're talking about blue-screen errors, or colloquially, the BSOD (blue screen of death). Even Windows 10's frowny-face emoji and a lighter shade of blue do little to lessen the impact of these Windows stop errors.

BSODs are most frequently caused by hardware or driver failures. Sometimes, software that has low-level access to the kernel can generate a BSOD, but these are the exception rather than the rule. Although BSODs can lead to data loss and often bode ill for the state of one or more of your PC's components, drivers, or settings, they can be really beneficial. For one thing, they usually only happen when something is seriously wrong, and if left running, your components might end up corrupting software, overloading circuits, burning out, or worse. They're also fairly good at leaving behind hints as to what caused the problem. The downside is that those hints can be pretty darn cryptic.



:(

Your PC ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you. (0% complete)

If you'd like to know more, you can search online later for this error: HAL_INITIALIZATION_FAILED

Look familiar? Although blue screens of death are annoying and can lead to data loss, they can also be beneficial and help you avoid more serious problems.

Forum Failures

What do most of us do when we encounter one of these system-stalling speed bumps (after the panic subsides and our pulse slows back to normal)? We perform a web search using the seemingly nonsensical string of words or alphanumeric characters we saw on the BSOD to determine what others have done in the same situation. Often, we scour forum posts until we find a solution that is reported to have worked for one user, try it ourselves, and then plunge right back into the forums when that fix doesn't solve the problem.

The trouble is that there tends to be any number of culprits behind a given Windows stop error, making solving these issues a hit-and-miss process. For instance, the IRQL_NOT_LESS_OR_EQUAL stop error refers to a kernel-mode process or driver that tried to access a memory location without permission, and it is most often caused by faulty software or incompatible hardware. The dodgy device or corrupt code that caused this error in one user's system is rarely identical to what caused it in another. That being said, we've also run into this error when overclocking.

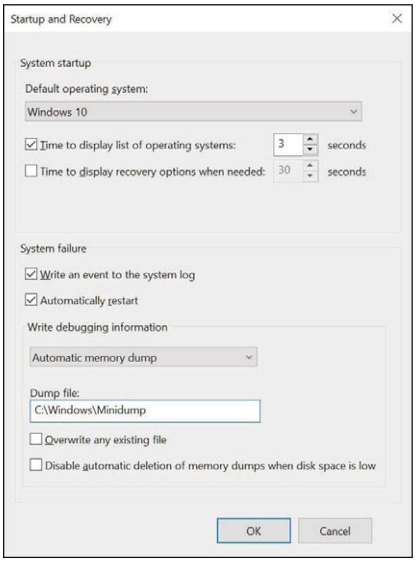
Although trial and error is a proven method for finding the best overclock, it's not the best way to get to the bottom of Windows stop errors. For this article, it's not our goal to solve your every last

BSOD, but rather to give you some tried-and-true sleuthing strategies that are sure to put you on a path to solving them on your own, every time you encounter one.

Start Your Search At The Dump

For most of us, Windows stop errors are blessedly uncommon, but one thing that we've picked up in the countless hours spent forum lurking is that the key to understanding a particular error lies within the dump (.DMP) files. This is the first thing any grizzled forum sage worth her salt will ask you for if your issue is deemed worthy of a response. A .DMP file is essentially a log file that Windows creates in the event of an error that forces the system to shut down. In fact, these files are usually created and saved as the BSOD is displayed.

Your system can create multiple types of .DMP files, and they vary in size and thoroughness. Most often, they contain bits and pieces of data that was stored in memory at the time of the error. Some .DMP files can be quite large, and other, more application-specific, dump files contain just the most pertinent data relating to the error and are respectively small enough to easily post in a forum without getting flamed. We'll go more in-depth regarding the size and types of .DMP files later, but first, let's make sure your system is configured to generate them in the first place.



Startup and Recovery

System startup

Default operating system:

Windows 10

☑ Time to display list of operating systems: 3 seconds

□ Time to display recovery options when needed: 30 seconds

System failure

☑ Write an event to the system log

☑ Automatically restart

Write debugging information

Automatic memory dump

Dump file:

C:\Windows\Minidump

□ Overwrite any existing file

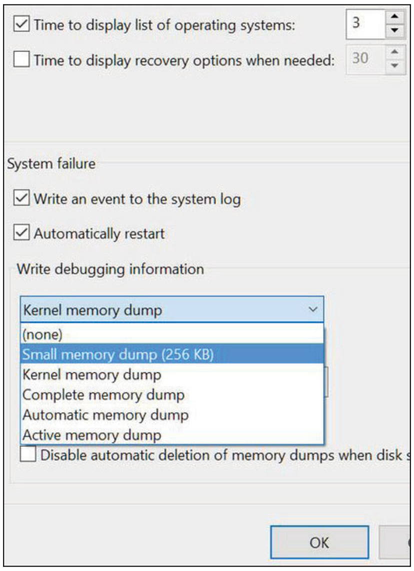
□ Disable automatic deletion of memory dumps when disk space is low

The Startup And Recovery dialog box is where you'll enable crash dump writing.

DMP Files, Coming In Hot

The formal phrase for what we're doing is enabling kernel-mode dump files. Often, the system is configured to automatically generate one of several types of .DMP files, but just to make sure, we'll need to jump into the Advanced System Properties dialog box. To access it, right-click the Start button in Windows 10 and click System (also found in Control Panel, System And Security, System). Then click the Advanced System Settings hyperlink on the left of the window and click the Settings button from the Startup and Recovery section. In the resulting dialog box, we're most interested in the settings in the System Failure section at the bottom.

The checkboxes for Write An Event To The System Log and Automatically Restart should be checked by default, so leave them that way. There's a drop-down list in the Write Debugging Information area that you can use to select the type of .DMP file you want the system to create.



☑ Time to display list of operating systems: 3

□ Time to display recovery options when needed: 30

System failure

☑ Write an event to the system log

☑ Automatically restart

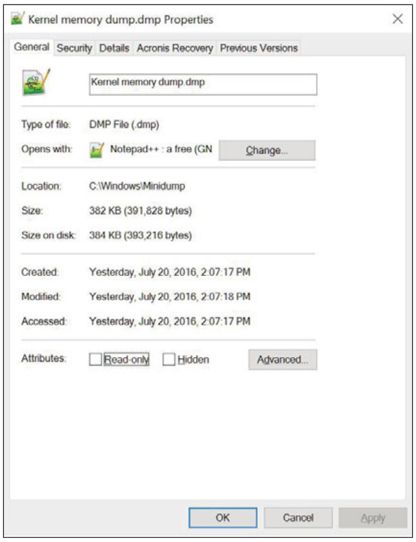
Write debugging information

Kernel memory dump

(none)
Small memory dump (256 KB)
Kernel memory dump
Complete memory dump
Automatic memory dump
Active memory dump

□ Disable automatic deletion of memory dumps when disk s

There are several options for how you want your system to handle debugging information.



Kernel memory dump.dmp Properties

Kernel memory dump.dmp

Type of file: DMP File (.dmp)

Opens with: Notepad++ : a free (GN

Location: C:\Windows\Minidump

Size: 382 KB (391,828 bytes)

Size on disk: 384 KB (393,216 bytes)

Created: Yesterday, July 20, 2016, 2:07:17 PM

Modified: Yesterday, July 20, 2016, 2:07:18 PM

Accessed: Yesterday, July 20, 2016, 2:07:17 PM

Attributes: □ Read-only □ Hidden

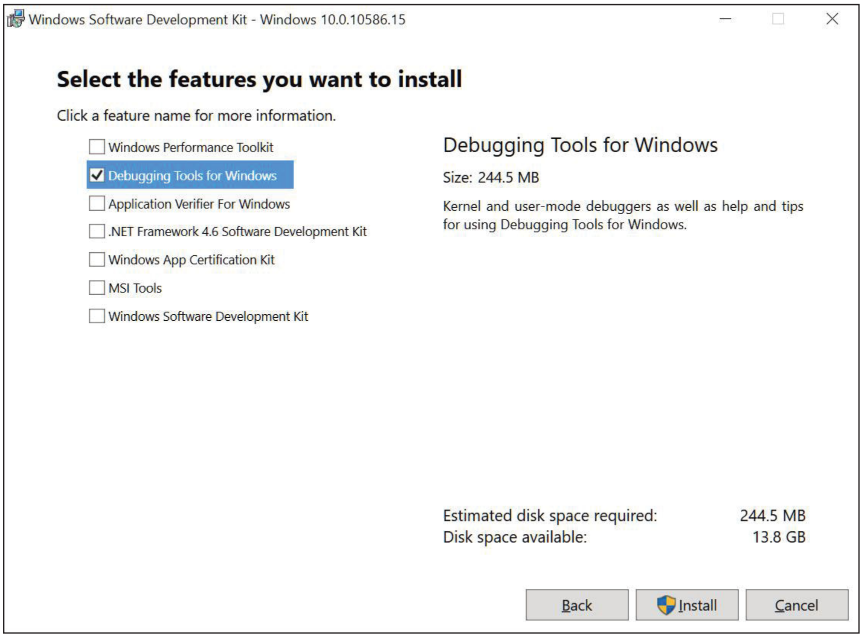
Microsoft recommends selecting Kernel Memory Dump, so that's what we'll do.

The text box labeled Dump File shows you the default location for storing dump files, typically C:\WINDOWS\MINIDUMP. You can manually change this location, but leaving it at this default setting is also a viable option. Later, when we're deciphering these dump files, we may need to copy them to another location to grant third-party applications access.

At the bottom of this dialog box you'll find a checkbox for overwriting existing files, which you can deselect if you suspect that you're tracking down multiple problems. The last checkbox lets you disable the automatic deletion of memory dumps when disk space starts to get low.

Diff'rent Dumps For Diff'rent Folks

When you expand the drop-down list on the Write Debugging Information area to select a type of



Windows Software Development Kit - Windows 10.0.10586.15

Select the features you want to install

Click a feature name for more information.

- ☐ Windows Performance Toolkit
- ☑ Debugging Tools for Windows
- ☐ Application Verifier For Windows
- ☐ .NET Framework 4.6 Software Development Kit
- ☐ Windows App Certification Kit
- ☐ MSI Tools
- ☐ Windows Software Development Kit

Debugging Tools for Windows

Size: 244.5 MB

Kernel and user-mode debuggers as well as help and tips for using Debugging Tools for Windows.

Estimated disk space required: 244.5 MB
Disk space available: 13.8 GB

You can dramatically speed up the installation of the Windows Debugger by unchecking any unnecessary components.

dump file you want your system to create, you'll get six options, with (None) being the first.

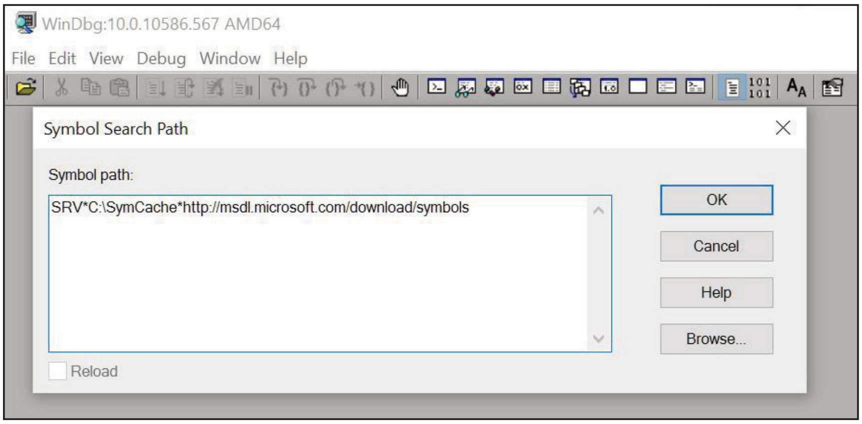
Automatic Memory Dump. This is the default write debugging setting, and the dump files it produces are indistinguishable from those generated using the Kernel Memory Dump setting. The system picks this one whenever the page file is set to a system-managed size, and the respective size of the paging file in this instance is designed to be large enough to capture a vast majority of the kernel memory dumps your system will potentially generate. Although we won't touch on manually adjusting the paging file in this article, Microsoft recommends making sure it is capacious enough to store one or more of your chosen memory dump types.

Small Memory Dump (256KB). As its name implies, this is designed to be a lightweight memory dump that's easy to share online. The small memory dump we created actually weighed in at 260KB, but that's still a compact file. It includes the BSOD information, a list of drivers that were loaded at the time of the stop error, process information, and a small amount of kernel data. It isn't as thorough as other memory dumps, but you can usually rely on it to pinpoint the problem.

Complete Memory Dump. This granddaddy of memory dumps includes everything contained in physical memory. Some sources report that if there's 8GB of system memory occupied at the time of a crash, then the complete memory dump will be 8GB in size. When we generated a complete memory dump on an otherwise idle system, the complete memory dump was a whopping 15.8GB in size, which is the amount of addressable RAM installed on our system. In either case, this memory dump type likely contains significantly more information than you'll need to troubleshoot a BSOD problem. Because of their unwieldy size, complete memory dumps typically get purged shortly after creation unless you click the checkbox to disable automatic deletion.

Active Memory Dump. Win10 brings a new dump type to the table in the form of the Active Memory Dump, which is significantly more svelte than a Complete Memory Dump but includes kernel and user-mode space data stored in active memory. This type is a godsend for developers afflicted with slow networks.

Kernel Memory Dump. This type of memory dump will tend to include more data than the small variety, but it can be as large as one-third of the amount of RAM installed on the system. If you have 16GB of memory for instance, that could result in a kernel memory dump of more than 5.3GB. When we generated a kernel memory dump, admittedly with the sys-



WinDbg:10.0.10586.567 AMD64

Symbol Search Path

Symbol path:

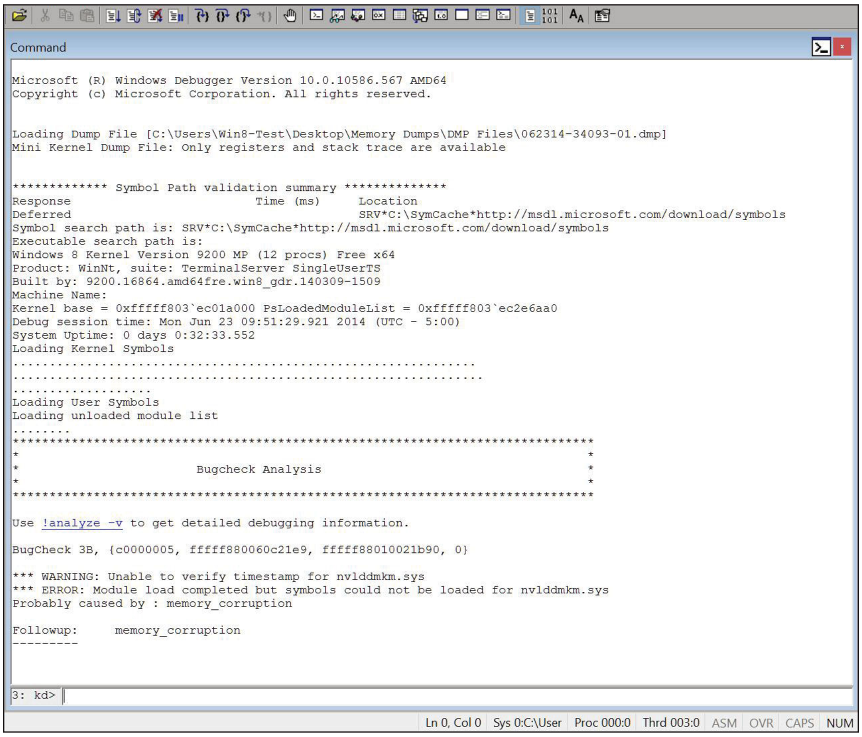
SRV*C:\SymCache*http://msdl.microsoft.com/download/symbols

☐ Reload

The SymCache folder provides a place to store the symbols you need to decipher dump files.

tem relatively idle, the file was a mere 383KB (we're using a system with 16GB of system memory). Microsoft reports that this dump file type includes memory allocated to the Windows kernel, hardware abstraction level, kernel-mode drivers, and other kernel-mode programs, but it excludes unallocated memory and memory set aside for user-mode applications. Microsoft also claims that this memory dump is the most useful for users like you and me, who are just trying to track down problems.

Microsoft knows a thing or two about Windows, so we see no reason not to heed the firm's advice here. Let's set Kernel Memory Dump as our preferred method for writing debugging information, click OK to close the Startup and Recovery dialog box, and then close the System Properties box.



```
Microsoft (R) Windows Debugger Version 10.0.10586.567 AMD64
Copyright (c) Microsoft Corporation. All rights reserved.


Loading Dump File [C:\Users\Win8-Test\Desktop\Memory Dumps\DMP Files\062314-34093-01.dmp]
Mini Kernel Dump File: Only registers and stack trace are available


************* Symbol Path validation summary **************
Response                         Time (ms)     Location
Deferred                                       SRV*C:\SymCache*http://msdl.microsoft.com/download/symbols
Symbol search path is: SRV*C:\SymCache*http://msdl.microsoft.com/download/symbols
Executable search path is:
Windows 8 Kernel Version 9200 MP (12 procs) Free x64
Product: WinNt, suite: TerminalServer SingleUserTS
Built by: 9200.16864.amd64fre.win8_gdr.140309-1509
Machine Name:
Kernel base = 0xfffff803`ec01a000 PsLoadedModuleList = 0xfffff803`ec2e6aa0
Debug session time: Mon Jun 23 09:51:29.921 2014 (UTC - 5:00)
System Uptime: 0 days 0:32:33.552
Loading Kernel Symbols
...............................................................
................................................................
...................
Loading User Symbols
Loading unloaded module list
........
*******************************************************************************
*                                                                             *
*                        Bugcheck Analysis                                    *
*                                                                             *
*******************************************************************************

Use !analyze -v to get detailed debugging information.

BugCheck 3B, {c0000005, fffff880060c21e9, fffff88010021b90, 0}

*** WARNING: Unable to verify timestamp for nvlddmkm.sys
*** ERROR: Module load completed but symbols could not be loaded for nvlddmkm.sys
Probably caused by : memory_corruption

Followup:     memory_corruption
---------

3: kd>
```

Clicking the !analyze –v hyperlink will display the detailed Bugcheck Analysis.

Don't Ask The Experts, Become One

Now that the system is generating dump files, we need to install a utility that will let us open them and make some sense of the data within.

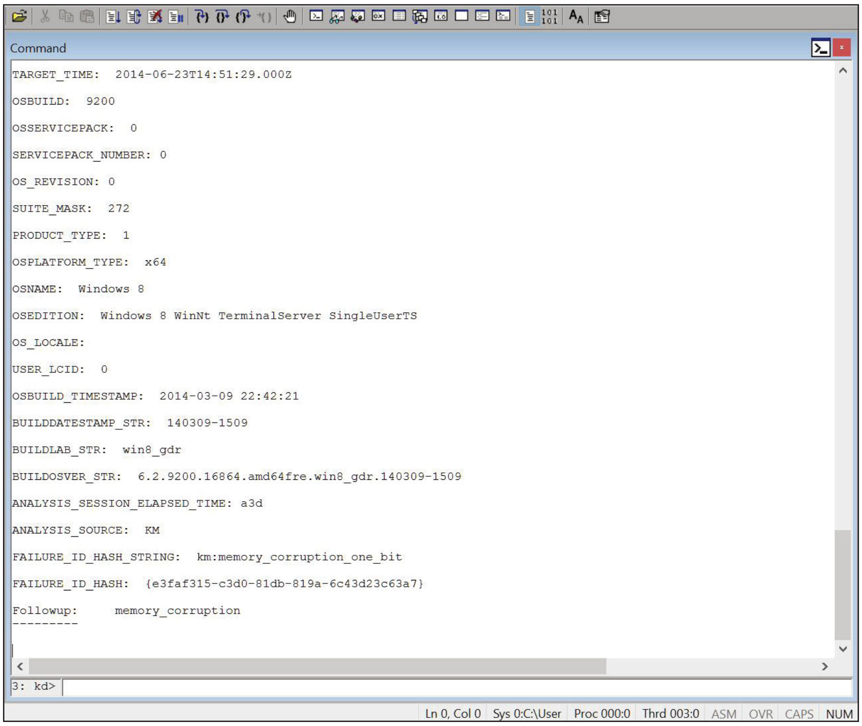
To download the Windows Debugger (WinDbg.exe) tool, visit http://bit.ly/2aKs48B and click the Get Debugging Tools For Windows (WinDbg) (from the SDK) hyperlink. The SDKSetup.exe file will quickly download. When it's finished downloading, navigate to its location, typically the DOWNLOADS folder, and double-click it to launch the installer.

If you're using the PC that you're trying to diagnose, then you can leave the first screen at the default settings, which installs the SDK at C:\PROGRAM FILES (x86)\WINDOWS KITS\10\. If not, choose a download path for the standalone installer of the SDK. Click Next to proceed. Choose whether or not to participate in Microsoft's CEIP (Customer Experience Improvement Program) and click Next. Accept the license agreement on the next screen to continue, deselect everything but the Debugging tools For Windows, and then click Install. When complete, click the Close button. To find the utility, navigate to C:\PROGRAM FILES (x86)\WINDOWS KITS\10\DEBUGGERS\x64\ and then double-click Windbg.exe.

The next step is to configure dump files to automatically open within the utility. Start by right-clicking the Win10 Start button and clicking Command Prompt (Admin). As long as you left the install directory alone during the installation, you can type **cd\Program Files (x86)\Windows Kits\10\Debuggers\x64\** at the prompt and press *ENTER*. Next, type **windbg.exe –IA** into the prompt and press *ENTER* again. If you did it correctly, the Windows Debugger will launch and a pop-up message will inform you that the procedure successfully associated the .DMP, .HDMP, .MDMP, .KDMP, and .WEW file types with the utility, which means that anytime you double-click one of those types of files, it'll load automatically in the Windows Debugger. Click OK to close it.

With that out of the way, our next task is to configure the WinDbg Symbol Path. To begin, launch the Windows Debugger by clicking Start, All Apps, Windows Kits, WinDbg (X64). Next click File, Symbol File Path and then type **SRV*C:SymCache*http://msdl.microsoft.com/download/symbols** into the text box and click OK. If performed correctly, this creates the C:\SYMCACHE folder and uses it as a place to download and store the symbols necessary for deciphering dump files. To save your changes and exit, click File, Save Workspace and then close the utility.

Now, when you double-click any dump file, it should open automatically in WinDbg, but the first time you do this, the dump file will



```
TARGET_TIME:  2014-06-23T14:51:29.000Z

OSBUILD:  9200

OSSERVICEPACK:  0

SERVICEPACK_NUMBER: 0

OS_REVISION: 0

SUITE_MASK:  272

PRODUCT_TYPE:  1

OSPLATFORM_TYPE:  x64

OSNAME:  Windows 8

OSEDITION:  Windows 8 WinNt TerminalServer SingleUserTS

OS_LOCALE:

USER_LCID:  0

OSBUILD_TIMESTAMP:  2014-03-09 22:42:21

BUILDDATESTAMP_STR:  140309-1509

BUILDLAB_STR:  win8_gdr

BUILDOSVER_STR:  6.2.9200.16864.amd64fre.win8_gdr.140309-1509

ANALYSIS_SESSION_ELAPSED_TIME: a3d

ANALYSIS_SOURCE:  KM

FAILURE_ID_HASH_STRING:  km:memory_corruption_one_bit

FAILURE_ID_HASH:  {e3faf315-c3d0-81db-819a-6c43d23c63a7}

Followup:     memory_corruption
---------

3: kd>
```

Our crash dump seems to indicate that our system suffered some sort of memory corruption.

take a while to fully appear. That's because this initial run is when the system downloads symbols to the SYMCACHE folder, which can balloon to more than a gigabyte in capacity. (You can also navigate to crash dumps within WinDbg by clicking File, Open Crash Dump and then navigating to the location of the dump file.)

To scan the dump file, click the !analyze –v hyperlink, which displays the exception record and stack trace of the function that caused the Windows stop error. In our dump file, we noticed that "memory_corruption_one_bit" appeared throughout the dump file, so we took a closer look at our system memory. We had recently installed a new motherboard, and this BSOD occurred upon our first reboot. We swapped out the kit with another we had on hand, and the system was once again stable.

Cloudy With a Chance Of Answers

Although there's a fair amount of work involved in setting up the Windows Debugger, once it's done, it's simple to look at any crash dump your system generates. Even so, that doesn't mean the utility will offer up a plain-English tutorial on how to fix the problem. Instead, it'll give you a few bread crumbs to get you looking in the right direction. If you still need to trust in the wisdom of those tech sages we mentioned earlier, having a crash dump analysis handy will earn you all kinds of good karma on the forums.

TIP: FORCE A BSOD

If you want to set up the Windows Debugger but don't have any BSOD-generated dump files with which to test, count yourself lucky. But don't count yourself out; there's a way to manually generate BSODs and their resulting dump files with a simple keyboard shortcut.

To begin, you first need to enable your system to generate crash dumps, which is a procedure we walked you through in the main article. The next step involves creating a Registry key, but the key's contents will vary depending on whether you're using a USB or PS/2 keyboard.

For those using a USB keyboard, click in the search box by the Win10 start button and type **regedit**, then press *ENTER*. Next, navigate to HKEY_LOCAL_MACHINE\SYSTEM\CURRENTCONTROLSET\SERVICES\KBDHID\PARAMETERS and then right-click in the right pane, click New, then click DWORD (32-bit Value).

Right-click the new item and click Rename, then type **CrashOnCtrlScroll** and press *ENTER*. Then double-click the item and put a "1" into the Value Data text field. Click OK, exit the Registry Editor, and restart your PC to make sure the change sticks.

If you're using a PS/2 keyboard, navigate to HKEY_LOCAL_MACHINE\SYSTEM\CURRENTCONTROL SET\SERVICES\i8042prt\PARAMETERS and right-click in the right pane, click New, then click DWORD (32-bit Value). Right-click the new item and click Rename, type **CrashOnCtrlScroll** and press *ENTER*. Double-click the item and put a "1" into the Value Data text field. Click OK, exit the Registry Editor, and restart.

Once the system has booted again, you can launch a MANUALLY_INITIATED_CRASH BSOD at any time by pressing and holding the right *CTRL* key then pressing *SCROLL LOCK* twice.

Wire Partition Below The Floor

For Full Enclosure & Secure Data Center Segregation, A Below-Floor Wire Partition Is Often Key

For cloud computing servers or any data center containing CPU hardware for two or more clients, wire partitions are typically used for full security. But simply building a five-sided box over the top of a server may not be enough—some also require the security of a cage extending below the floor for full enclosure and secure segregation.

Data Center Segregation

WireCrafters (www.wirecrafters.com) takes pride in its 10-gauge wire mesh partition server cages, but says the real challenge comes into play when securing the bottom vector of your, or your client's, server hardware.

WireCrafters installs a roughly 12-inch high partition under the computer floor to match the footprint of the cage above. With a full coverage floor for the entire data center, you can run cables beneath, preventing all manner of mishaps and tampering.

Fully Customizable Partitioning

WireCrafters' panels and components come in a range of sizes with a full array of fastening components and features specially designed to suit your data center needs, with precision and strength for optimal security.

With a wide selection of standard-sized stackable panels, custom-sized panels, and custom cages with multiple options, WireCrafters is prepared to meet specific data center needs. Specialized security may include subfloor meshing, and seismic bracing may be used to protect sensitive equipment.

Easy, Clean Installation

WireCrafters' experts install security cage systems quickly, leaving no mess—just a clean, strong, safe, and robust cage to store your data systems. Options include hinged, double-hinged, or sliding doors. And adjustments can be made on-site by your own data security systems teams. Cage equipment can be adjusted, for example, using WireCrafters' modular panel system.

All of WireCrafters' doors can be outfitted with basic key locks. Added security options include keypad locks, self-closing doors, card readers, fingerprint scanners, and emergency exit push bars.

For more information or to request a quote for custom security cages, visit www.wirecrafters.com. P