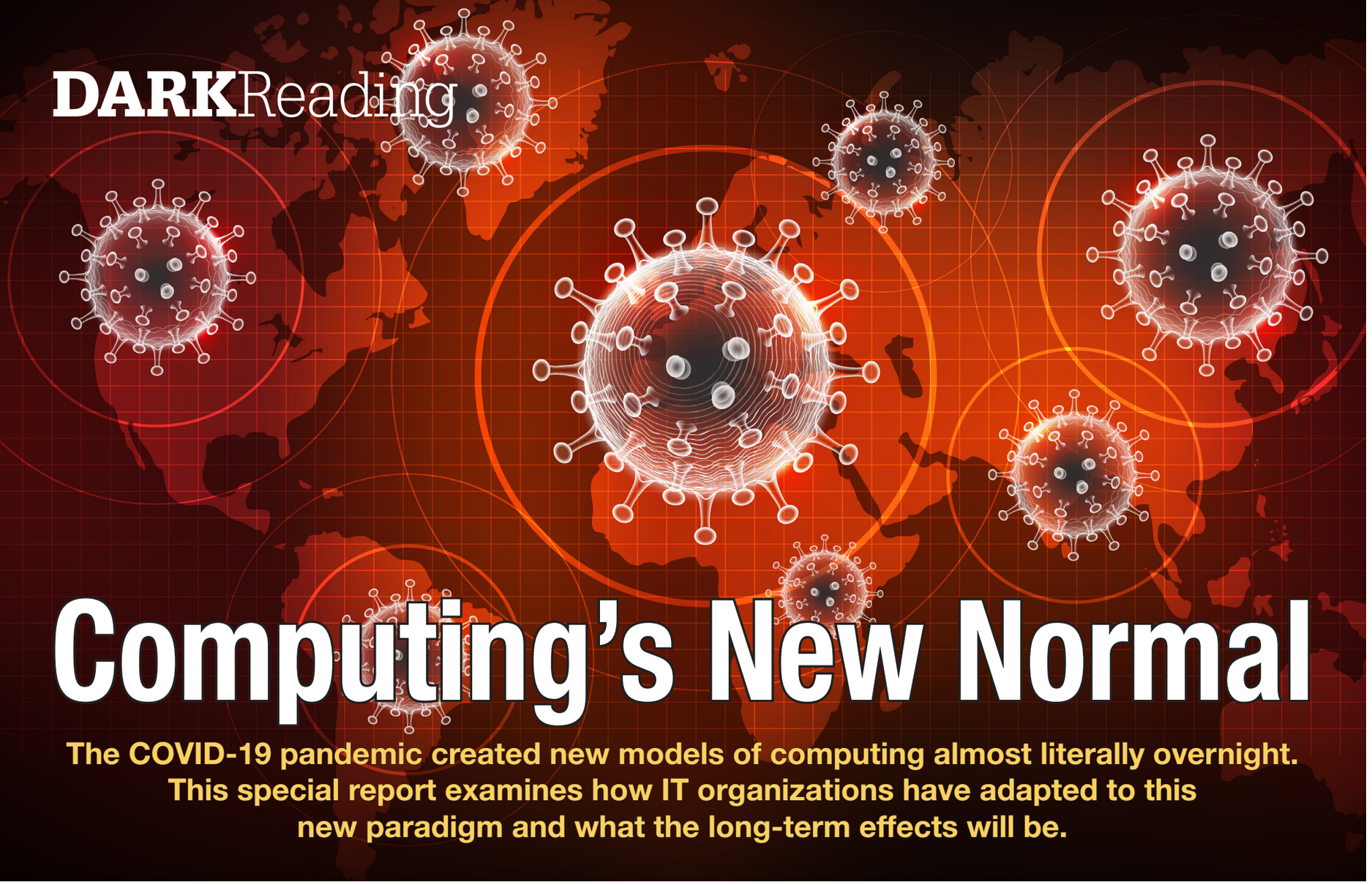


Computing's New Normal

The COVID-19 pandemic created new models of computing almost literally overnight. This special report examines how IT organizations have adapted to this new paradigm and what the long-term effects will be.

INSIDE:

Next

informa tech
Enterprise IT Network | DARKReading | DataCenter Knowledge | InformationWeek | ITPro Today | NETWORKComputing | OMDIA

A Different Type of Incident Response

How the work-from-home movement driven by the COVID-19 pandemic is shifting IT security priorities and processes.

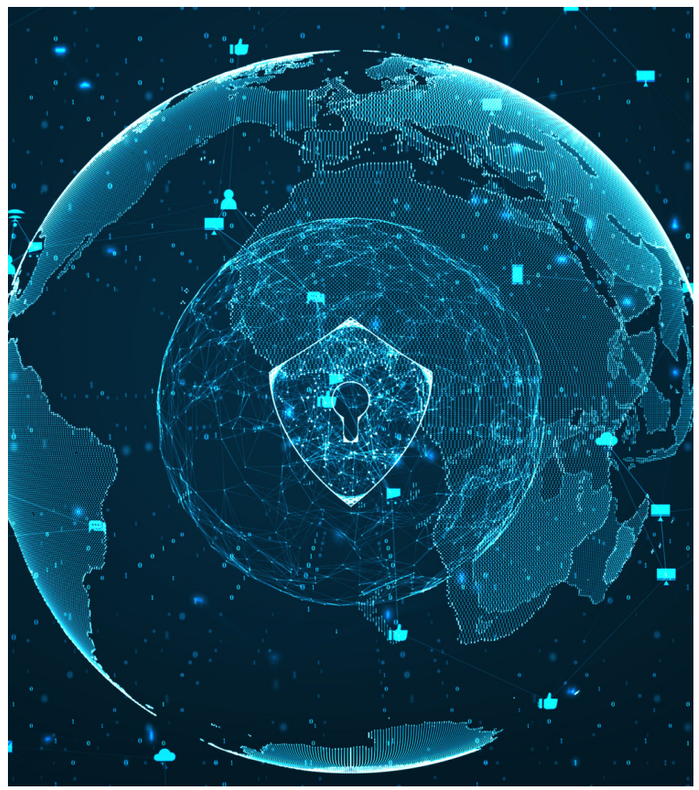
By Kelly Jackson Higgins for Dark Reading

IT security teams face new threats and incidents every day, but the sudden, forced transformation of enterprise IT and business operations to a work-from-home model in the wake of the COVID-19 pandemic has shaken the core of the security operations center (SOC). Practically overnight, IT security teams were tasked with securing the devices of employees now working from makeshift home offices after organizations shuttered most of their brick-and-mortar offices amid stay-at-home orders worldwide.

The attack surface has become bigger and more distributed, with millions of workers logging in from their home networks that also host inherently insecure consumer devices like smart TVs and virtual assistants. IT security teams, with less visibility into those environments, must ensure these at-home users practice proper security and privacy measures while using corporate applications and conducting online meetings. The already-challenging patch management process now comes with a new twist of a heavy volume of remote devices in addition to regular server updates. Typical enterprise patching tools aren't optimized for remediating endpoints via remote links and virtual private network connections, so security pros may need to automate more of their software patching and updates and also rethink how they triage and prioritize which patches to apply and when.

Meanwhile, some members of the SOC team also are working from home full-time now, changing the dynamic of the physical SOC to that of a more distributed operation. These already-slim security staffs could face cuts, too. Amid the pandemic-fueled financial crisis hitting businesses worldwide, they likely will be doing even more with less.

Security monitoring tools and controls are more critical than ever, including remote network monitoring, mobile



device management, behavioral detection, VPN clients, zero-trust-based remote access, and identity management.

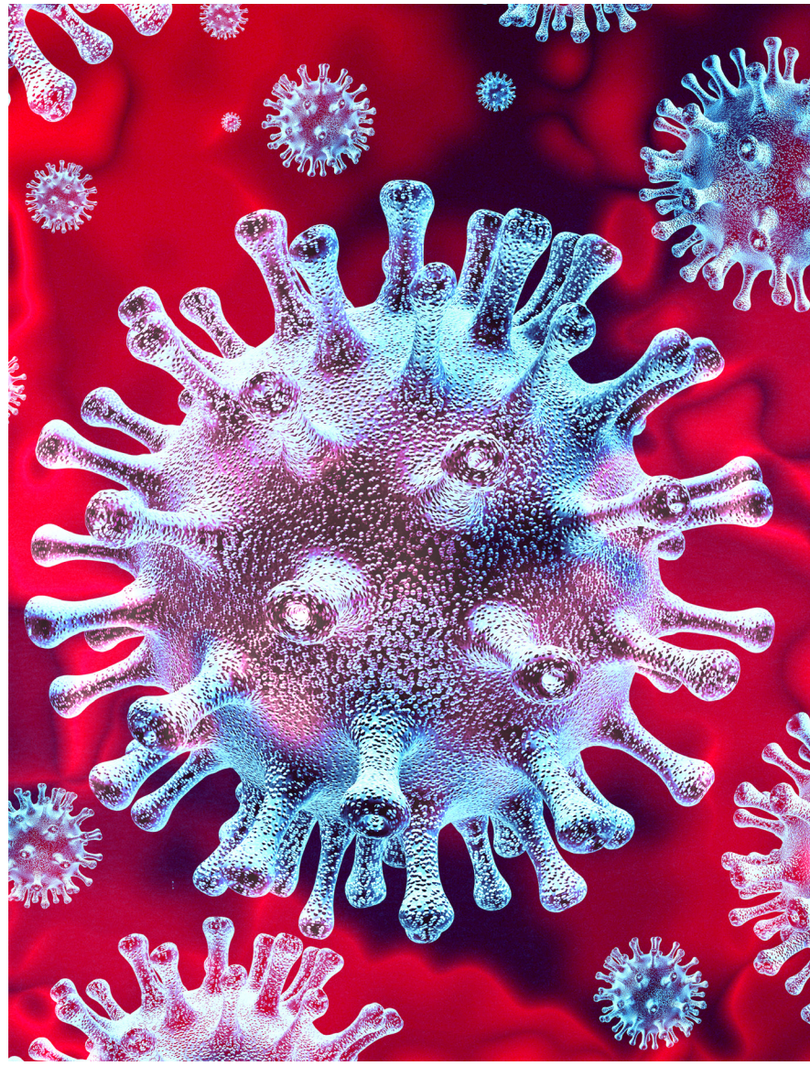
And as always, cybercriminals and nation-state attackers know opportunity when they see it: These groups are preying on worries and interest in COVID-19 with phishing emails and domains that use the virus as a lure. The uptick in COVID-19-themed attacks was immediate: AT&T Cybersecurity reported a 2,000% increase from February to March of COVID-related indicators of compromise (IOCs) shared by security experts to its open threat intelligence exchange, for instance.

The fallout from the rush to get users up and running at home often resulted in poorly tested remote access configurations, opening the door for attacks. Attackers have been taking advantage, pushing malware-laden VPN installers, malicious mobile apps, COVID-19 infection trackers on malicious websites, and campaigns posing as World Health Organization tools that drop keyloggers and Trojans onto victim devices.

Sadly, hospitals, overwhelmed with more COVID-19 patients than ICU beds and respirators, have been a popular target for ransomware and other cybercrime. A grassroots effort by hundreds of security experts from different companies recently formed a Justice League, of sorts, to help hospitals and healthcare organizations protect themselves from attackers. The group, which includes threat intelligence and incident response experts from Microsoft and Okta, is working to identify and alert healthcare facilities that are vulnerable or exposed to the latest attack campaigns – and offering assistance if they do suffer a cyberattack.

In the end, the COVID-19 crisis ultimately will shape the direction of security technology as we know it. Some tools and features will become more critical in this new enterprise network model, while others – including vendors – will potentially fade away as new ones emerge. Still, it's unclear just how much enterprises will be able to afford to invest in security amid a global financial crisis, even at this time when they are more at risk of cyberattacks.

All of these issues, and many others, are among the topics covered in this special report, "Computing's New Normal," compiled by the enterprise IT news organizations at Informa Tech. With news coverage and feature stories from InformationWeek, ITPro Today, Dark Reading, Data Center Knowledge, and Network Computing – as well as Omdia, Informa's IT research organization – this special report provides a unique set of perspectives on the effects of the pandemic from all sides of the IT organization.



Attack Surface, Vulnerabilities Increase as Orgs Respond to COVID-19 Crisis

In typical fashion, attackers are gearing up to take advantage of the surge in teleworking prompted by the pandemic.

By Jai Vijayan for Dark Reading

The speed at which organizations are being forced to respond to the unfolding COVID-19 health crisis could be leaving many of them vulnerable to attack by threat actors rushing to exploit the situation.

Over the past few weeks, security vendors and researchers have reported an increasing number of malicious activities tied to COVID-19 that they say are elevating risks for organizations across sectors, especially healthcare and law enforcement.

Predictably, a lot of the activity has involved phishing and social-engineering campaigns where COVID-19 has been used as a thematic lure to get people to click on malicious attachments and links in emails or to download malware on mobile and other devices. There have also been reports about account takeover and business email compromise activity, a growth in domains serving up drive-by malware, and attempts to exploit virtual private networks (VPNs) and other re-

mote access tools.

The danger posed by these threats has been exacerbated by new requirements for "social distancing" and the resulting push by many organizations to widen or implement telework capabilities for their workforce. The sudden COVID-19-related surge in the use of videoconferencing, remote access, and VPN services — especially at organizations that have not used them before — is giving attackers more targets to go after and defenders a lot more terrain to protect.

"Many companies did not have the infrastructure for this sort of work and had to deploy it quickly," says Omri Herscovici, security research team leader at Check Point.

This includes externalizing internal Web services and email access, desktop, and other internal resources. In some cases, internal services that may not have been previously accessible from outside the perimeter are now being hastily opened to allow employees to work from home.

Many are implementing new technologies for remote access without enough testing or without first ensuring secure configurations, Herscovici says. Companies are also likely struggling with managing and protecting a sudden rise in server loads and with issues like implementing proper authentication mechanisms and security auditing capabilities for their newly telecommuting workers, he notes.

"The attack surface for malicious actors has increased since some parts of an organization's infrastructure that were only used internally are now exposed to the Internet," Herscovici says.

VPN and Telework Risks

Attacks that seek to take advantage of user inexperience with respect to remote working are one major concern. "Tens of thousands of businesses are turning their workforce into a remote army, and they are urging staff to use VPNs for the first time," says Lior Rochberger, a security analyst with Cybereason's Nocturnus team and the co-author of a recent COVID-19 research report.

"Unsuspecting victims around the world are falling victim because they are being tricked into downloading and installing malware masquerading as legitimate VPN clients," Rochberger says.

One malicious website that Cybereason's team uncovered claimed to provide a range of legitimate VPN installers and installers for apps like Instagram and Facebook. However, those who attempt to download the VPN installer only get directed to a malware-hosting site. "There is a lot of danger because as anxiety sets in, people's minds are elsewhere and they trust these websites without double-checking that it is legitimate and trusted," Rochberger says.

Concerns over enterprise VPN security were high even before the COVID-19 crisis. Security researchers have reported on numerous critical remotely executable vulnerabilities in widely used VPN products in recent months that have prompted alerts from the US Department of Homeland Security (DHS) and others. Organizations that might have been close to addressing those issues are likely going to fall behind once again in the new rush to enable telecommuting at many organizations, says Pascal Geenens, security evangelist at Radware.

"VPNs have been the subject of targeted access over 2019," he says. "[Now] the opportunity and attack surface [have grown] with more organizations deploying remote access."

In a March 13 alert, the DHS's Cybersecurity and Infrastructure Security Agency (CISA) urged organizations that are implementing remote access capabilities for workers in response to COVID-19 to install the latest security patches and configurations on their VPNs.

It also advised the use of multifactor authentication on all VPN connections to increase security. "If MFA is not implemented, require teleworkers to use strong passwords," the CISA said.

Exploiting a Crisis

Meanwhile, threat actors, who have a penchant for exploiting a crisis situation, are launching a barrage of spam, phishing, and other malicious campaigns to get users to part with credentials and other sensitive data.

According to KnowBe4, there has been a virtual epidemic of COVID-19-themed phishing emails in recent weeks. Many of them have purported to be from the US Centers for Disease Control (CDC), the World Health Organization (WHO), the US Department of Health and Human Services (HHS), and enterprise HR departments. Recently, for instance, IBM reported on a new campaign where a previously known keylogger called HawkEye was being distributed in emails spoofing WHO's director general. While most of the phishing emails have spoofed government organizations, attackers have been spoofing private ones as well. One campaign that KnowBe4 tracked, for instance, involved a phishing email with a fake bill for COVID-19 insurance coverage from Cigna.

An interactive map from Johns Hopkins University tracking the spread of COVID-19 globally has been an especially popular spoofing target. Numerous attackers have begun hosting near-identical-looking trackers on malware-laden sites and are using phishing emails to lure people to these sites.

Some are using an app-version of the tracker to get users to load malware on mobile devices. Kristin Del Rosso, senior staff intelligence engineer at Lookout, says researchers from the company recently discovered a trojanized version of a functional COVID-19 tracking app being used to download surveillance software on mobile phones.

"We have seen other actors using the COVID-19 media coverage to deploy coronavirus-themed mobile ransomware and banking Trojans, as well as track a device's geolocation," Del Rosso says. With the order to shelter in place, organizations are quickly implementing work-from-home policies that have the potential to increase their mobile risk. "Ultimately, it comes down to educating the end users and continuing to follow best practices, even in times of crisis," she says.

7 WAYS VPNS CAN TURN FROM ALLY TO THREAT

1) Vulnerable Key-Handling Routines
Most VPNs are "black boxes." That opacity is why a vulnerability like a hard-coded key or keys stored insecurely can be so dangerous.

2) Weak Encryption
Avoid encryption algorithms that were once thought safe but are now known to be vulnerable, like DES, 3DES, SHA-1 and RSA (with small keys).

3) Authentication Bypass
Pay attention to vulnerabilities that allows a threat actor to access resources behind the VPN without going through the authentication process.

4) Weak Protocols
There are a few protocols used in most VPNs – PPTP, L2TP and IKEv2 are considered "damaged goods" by most experts, while OpenVPN is considered the best available.

5) Nosy VPNs
Be wary of free or cheap VPNs. Many turn their users into products by tracking their every online move; some even actively serve malware to their customers.

6) Single-Layer Protection
A VPN should mask the end user's IP address and provide blacklist URL protection, among other things. Be wary of third-party VPN services that don't provide the proper protection.

7) Weaponized HTTPS
HTTPS can hide malicious activity and act as a component in an attack. Monitor, patch and maintain a healthy skepticism concerning traffic from new and unusual sources.

By Curtis Franklin Jr.

Rochberger says Cybereason, too, has seen attackers creating malicious mobile applications posing as legitimate apps developed by the WHO purportedly to help people recover from COVID-19. “Instead, the application downloads the Cerberus Trojan to steal sensitive data,” she notes.

According to Check Point, more than 16,000 new coronavirus-related domains have been registered since January. More than 2,200 of them are suspicious and another 93 are being used to serve malware. Many malware authors appear to be viewing the pandemic as an opportunity to accelerate sales and are offering coronavirus specials and discounts to criminals and wannabe-criminals in Dark Web markets. Among the COVID-19 specials is a 15% discount on a Facebook account-hacking service.

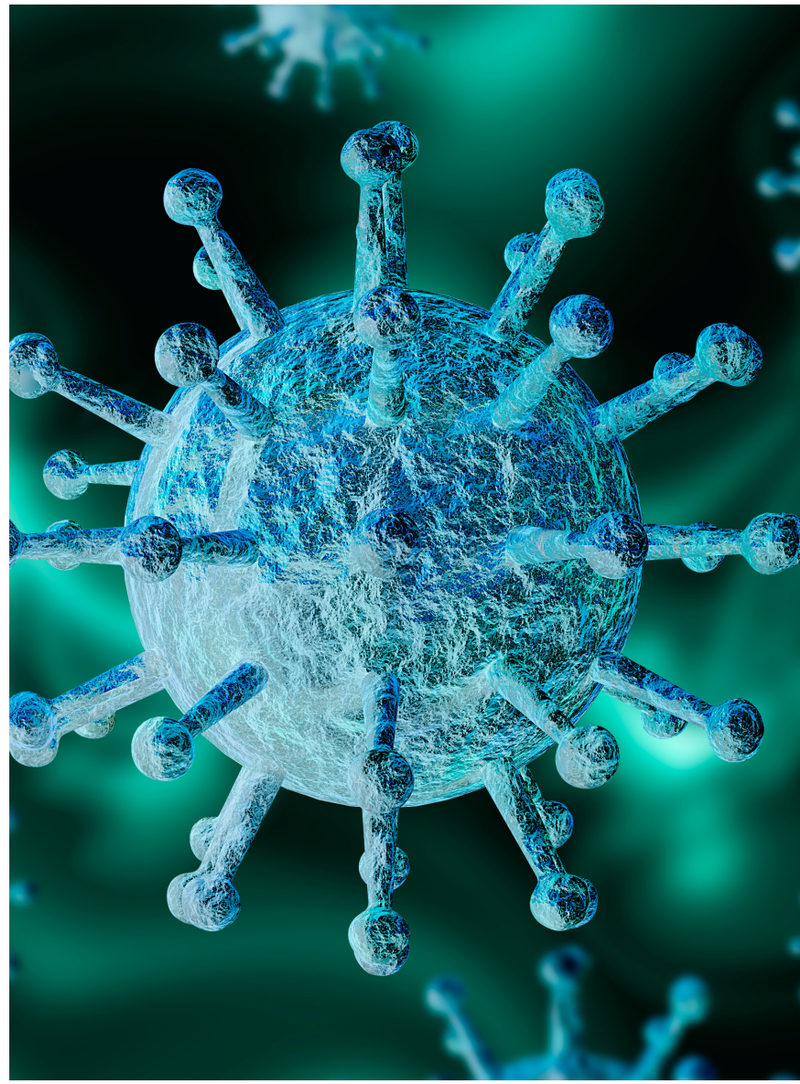
While many of the new and emerging COVID-19-related threats are targeted primarily at individuals, they impact organizations equally. So enterprises need to special attention to the security fundamentals, researchers say.

This includes keeping software properly updated to prevent exposure to new threats, resetting and enforcing strong passwords for remote workers, and ensuring passwords are changed periodically, says Geenens from Radware, which recently published a set of recommendations on the topic.

VPNs are another way to secure data between remote workers and core systems, says Kevin Curran, IEEE senior member and professor of security at Ulster University. “In the ideal world, organizations would have a zero-trust network system deployed,” Curran says. But it can be difficult to implement purely in response to the unfolding health crisis, he admits.

Mobile device management capabilities are another fundamental requirement for organizations right now, Curran notes. “Even Windows 10 now enables devices to connect to a cloud-based Azure Active Directory, which bolsters the existing support in Windows for the traditional version of Active Directory,” he says. Organizations need to have control of mobile devices that access their environments and have capabilities such as remote wipe and configuration of enterprise data protection policies.

“Containerization is another option for companies to separate corporate and personal data on an employee’s device,” Curran says. “This involves separating out the corporate mobile apps and the data associated with these into ‘containers’ on the mobile device, creating a clear division as to what is subject to corporate security policies, such as wiping.”



Patching Poses Security Problems with Move to More Remote Work

Security teams were not ready for the wholesale move to remote work and the sudden expansion of the attack surface area, experts say.

By Robert Lemos for Dark Reading

A growing body of survey data suggests that the move to remote work has caused a growing number of headaches for security teams, especially regarding securing remote systems and maintaining up-to-date software through patching.

In mid-March, 45% of companies encouraged workers to move to remote working, up from only 13% of companies in 2018, according to IT community Spiceworks. Yet security teams consider their company's capability to patch remote systems to be inadequate, according to a recent study released by Automox, a cyber-hygiene tools provider. While 48% of security teams patch on-premises desktops and laptops in the first three days, that declines to 42% for remote desktops and laptops, according to the firm.

"Remote desktops usually play second fiddle in terms of patching and prioritization — it's usually more difficult to manage them," says Chris Hass, director of information security and research for Automox. "Most teams have a good idea of what is going on with the corporate machines, but they often don't have any visibility into remote workers' systems, so there absolutely has been a large increase in the attack surface because of remote work."

A major impact on businesses from the coronavirus pandemic is the speed with which companies have moved to remote working, changing the way that employees access business applications and increasing the potential attack surface area — a particular headache for IT security.

Most companies were not prepared for such a

broad-based move to working remotely. While, on the whole, anywhere from 56% to 62% of employees could work from home, according to remote work analyst Global Workplace Analytics, only about 15% of respondents said their disaster recovery plans do not require any changes at all, according to a survey by Spiceworks of IT professionals. Because companies were taken by surprise, most are not prepared to patch and attest to the security of remote systems, says AJ Singh, co-founder and vice president of product management for remote management services firm NinjaRMM.

"Remote work has absolutely increased the complexity and scale of patch management in organizations," he says. "Now, in addition to maintaining and patching servers and devices on-prem, IT professionals must also manage the devices used by remote workers, making sure they are secure before accessing a business's data."

Patching is already an expensive proposition, with hundreds and thousands of vulnerabilities affecting a business's software and systems, says Sumedh Thakar, president and chief product officer at Qualys. The only way for most companies to deal with the issue is to prioritize the vulnerabilities based on the criticality of the assets affected by the issues. For example, companies should only focus on the BlueKeep vulnerability if they have Remote Desktop Protocol (RDP) services in place, for example.

However, the move to remote work has changed the calculus of prioritization for many companies and reduced their visibility, he says.

"It is becoming immediately clear that traditional enterprise security solutions deployed inside the organization's network are completely ineffective in patching [and] remediating these remote endpoints due to the pressure they would put on VPN concentrators, bandwidth for deploying patches or sheer amount of time they would put to tweak these solutions," Thakar says, adding: "Now, prioritization based on risk becomes interesting because vulnerabilities critical for these remote endpoints are probably different than those posing risk to traditional server farms."

Automation is another critical tool for better handling the patching of remote workers' systems. To get patching under control, businesses need to have the right tools in place to automate large parts of the patching process, says NinjaRMM's Singh.

"Ultimately, companies need to accept the fact that patch management is a constant chore regardless of remote work or working in an office," he says. "For the foreseeable future, however, it will be more important than ever to make sure end users' machines are tightly secured to avoid any loss or breach of sensitive data."

For vendors, the move to extensive remote working may result in significant business. While 44% of companies had already committed to spending more on IT in 2020, now 39% have further increased their budgets, according to Spiceworks.

And remote working is the area most in need of improvement, the survey found. Almost all — 92% — of IT professionals are concerned about the security of company-owned devices used from home and connecting to a home network.

REMOTE WORK SENTIMENT

80% of employees want to work from home at least some of the time

35% of employees would change jobs for opportunity to work remotely full time

➔ Flexibility is one of the highest ranked benefits by Millennials, even higher than student loan or tuition reimbursement

➔ More than a third of workers would take a pay cut of up to 5% in exchange for the option to work remotely at least some of the time

Source: Global Workplace Analytics, March 2020

Coronavirus Plan: How IT Can Enable Remote Work

Is your organization prepared to implement widespread remote work to protect employees against coronavirus? Here's what you need to do.

By Jessica Davis for InformationWeek

Is your enterprise IT organization smelling a little more like hand sanitizer these days? It's going around. As organizations in the US and around the world prepare for the advance of the coronavirus, now known as COVID-19, plenty of unknowns remain about the virus that has killed thousands around the world. Several US metropolitan areas have reported cases of the illness, and the spread can be tracked by this dashboard and map from Johns Hopkins University.

Public health officials are also tracking the spread, and the corporate world is proceeding with caution.

"When you walk into an event like this, there's a lot of fear, uncertainty, and doubt," says Rick Barr, chief operating officer at OneLogin, an identity management and workforce access company that also helps customers with business continuity. That FUD is already changing how organizations do business.

Several companies, including Apple, Amazon, Cargill, EY, Salesforce, and Twitter, have curtailed all but essential business travel. A number of big industry events have also been canceled, including Mobile World Congress in Barcelona. Google Next is going digital only; Adobe Summit recently did. The Game Developer Conference (which is owned by Informa, the same company that owns InformationWeek) is postponed.

That's a lot of disruption for the technology industry and for most industries. Still, public health experts recommend keeping a "social distance" from other people

Credit: Xavier Laine/Getty Images

Previous Next

of 6 feet. That's hard to do if you are wedged into an airplane seat, a keynote auditorium seat, an open-office workstation, or even one of those old-fashioned cubicles. That's probably why many companies are also allowing or even encouraging employees to work from home. In some cases, the directive to work from home is just if the employee is sick. In other cases, such as Twitter, all employees are being encouraged to work from home.

Is your enterprise IT organization ready to support the entire workforce of your company working from home? Thanks to digital transformation and cloud computing, you probably have migrated a lot of work to the cloud already. You may also have collaboration tools in place such as chat software and video conferencing. Still, are you ready for the day your CEO tells everyone to work from home tomorrow?

If you haven't prepared at all for such an event, it's a good idea to start with a team of maybe eight employees and tell them all to work from home starting tomorrow. That's according to John O'Duinn, author of the book *Distributed Teams*. O'Duinn is also a longtime software development leader who worked for the US Digital Service under the Obama administration as well as for multinational organizations and nonprofits. He currently works as a senior strategist for CivicActions.

You want to make sure that this pioneering team has someone from the C-suite on it, so that there's someone who can override any bureaucratic bottlenecks to making it work, such as authorizing a software purchase.

That team works from home for one day with each person doing their normal work. They interact with co-workers, clients, and partners. Use all the systems the company has set up.

The next day, do an assessment. How did it go? Were there any hiccups? That's where you need to direct your attention. Troubleshoot the problems and then roll out the solutions to the team. It's only through practice that you will turn this new way of working into muscle memory, making it as natural as working at your desk at the office.

If you are the one who will be working from home for the first time, or for an indefinite amount of time, O'Duinn recommends that you test your VPN before you leave the office. To do that, first disconnect from that office network, then turn on your mobile phone's Wi-Fi hotspot, and connect to the corporate network that way. Make sure you can connect via VPN or gain entrance through whatever security measures your enterprise has in place. Do this while you are at the office so that you can enlist the help of IT workers while you are there. Make sure you can access your email, your chat, your video conferencing, and any other essential tools this way.

Look at your physical desk. Are there any physical files you need to take with you? Do you need the phone number of the help desk in case you can't get access to the network from home? Bring it with you, along with your laptop and your mobile phone. (Don't forget chargers.)If you'll be using your mobile phone and videoconferencing, you will also want to make sure you have a headset and maybe an external webcam, according to O'Duinn. These can be a step up from the webcams built into your laptop, allowing you to position them to show you at a more flattering angle.

For management, pull out those rules and procedures you wrote up to deal with emergencies and crises, according to Barr. Figure out the way that you will communicate directives with employees. Will instructions go out over an office email, a group text message, or a robocall? How will you communicate so that all employees get the message?

Now is the time to lay this foundation for how you will continue your business operations in the wake of an emergency like a viral outbreak. Barr says you should ask yourself, "What are the systems, communications, and processes I need to implement to continue on as an existing business entity serving customers and employees?"

Pitfalls to Avoid in the COVID-19 Rush to Work From Home

With so many workers setting up workstations at home, be mindful of these potential problems.

By Jessica Davis for InformationWeek

What happens when you suddenly have to move your entire workforce from their offices at headquarters or another facility to their many different individual homes? That's what many businesses and their IT departments have been finding out as businesses, governments, and other organizations adjust to extraordinary circumstances driven by the need to self-isolate to combat the spread of COVID-19.

Many workers have had to make the change almost overnight, packing up the contents of their desks, grabbing their laptops, and setting up at home offices the next day. It has been a disruption to how many people typically work and how many organizations typically work. That means it will bring a host of new issues.

"There's a second wave of support conversations that are going to pop up," says Christy Wyatt, CEO of Absolute, which provides technology to help companies manage their fleets of desktops and laptops. In the best of times, VPN software can get out of date and even road-warrior expert users need help. Add into the

Previous Next

mix all of these work-from-home newbies who have never used a VPN before, and IT support can expect to be busy.

"There's just going to be a lot of phone calls coming into the help desk about why can't I get my email, why can't I get online, why can't I seem to connect to the network?" Wyatt says.

Recently, too, there has been a rush to buy laptops.

"The demand has been insane," says Ben Niernberg, executive vice president at Chicago-area value added reseller and managed service provider MNJ Technologies. Customers are looking for laptops, webcams, keyboards, and mice, he says. Demand has been three to four times the normal run rate.

So far MNJ Technologies has been able to track down the inventory it needs for customers, but it's difficult to find, Niernberg says. Customers who have standardized on one vendor's PCs are finding themselves having to settle for another vendor's instead. However, so far pricing has held steady for MNJ customers, Niernberg says.

Still, some workers may be faced with the prospect of packing up those desktop PCs at their offices and setting them up in their home offices. However, Wyatt warned, "those devices were never equipped to operate off the network." They may not include Wi-Fi capabilities, for example. They may not be equipped with VPN software.

Addressing the issue of an entire workforce suddenly working from home must be approached with an element of calm.

"It's going to be a marathon, not a sprint," Wyatt says. "No one will have it together on day one. But make sure employees have what they are going to need when they leave the building."

For instance, you need something on workers' devices that lets IT fix them remotely. It's not like you can tell a user to swing by the help desk so you can fix it for them, Wyatt says. Operating as if you can't physically touch a machine is the new normal.

One more key piece of advice: Organizations and workers should also be extra vigilant when it comes to security right now because hackers also have some extra time on their hands, Wyatt warned. Plus, workers who are already distracted by their disrupted routines and new work environments may be more likely to click on email that seems like it's from the IT department, but it turns out to be a phishing attack.

"There's a disorientation that's happening to the enterprise," Wyatt says.

10 Tools for Providing 24/7 IT Support to Remote Workers

In a remote working environment, providing 24/7 IT support can be challenging, but there are plenty of tools available to help organizations support their users.

By Richard Hay for ITPro Today

Providing 24/7 IT support to enterprise users is not a new concept. IT pros and system administrators are often called upon at all hours of the day (and night) to assist end users with hardware and software problems. Over the last few weeks, as more companies are shifting their workforces into remote work due to the COVID-19 coronavirus pandemic, that support has become much more challenging.

Some of these companies will already have a robust toolbox to support those workers who are now working from home. Others have likely been scrambling to make sure their enterprise users can work effectively from their temporary home offices. As such, the enterprise demand for IT tools that support remote working has increased significantly.

The good news is that those tools for remote access and support already exist, so getting ramped up to support your remote workers can happen very quickly.

Credit: Michal Cizek/Getty Images

Previous Next

Both MacOS and Windows operating systems already have built-in remote desktop clients that can be used effectively to manage remote assistance. Windows 10 even has a feature called Quick Assist that provides very rudimentary features that give you remote control of another Windows 10 device, but the user must be in front of the screen to establish the remote connection.

While useful, the capabilities of these in-operating system tools are somewhat limited compared with many of the tools that are available on the market today.

While there are other free third-party remote IT support options, many of them are limited to home/personal use. Some of them can even lock you out if they detect you might be using the tools/service for work-related functions and support.

That's why an enterprise company tasked with providing 24/7 IT support to their remote workers will need to consider subscription-based services. This will help avoid any licensing issues plus give you a range of support options from the company providing those tools.

Here are 10 remote IT support tools to consider for your organization.

AnyDesk

Provided client computers are running the remote application, this remote desktop tool works on computers running Windows, MacOS, Linux and FreeBSD, as well as mobile devices running Android and iOS. The service offers an own-network option for remote employees who cannot or should not access a cloud for security purposes.

Beyond Trust Remote Support Software

This service allows IT help desk employees to see remote employees' screens and fully interact with the remote desktop – in other words, if someone needs help changing passwords or updating programs, the IT help desk employee can get the remote worker to download the client app, launch it and let the help desk tech take over and do the rest. Features supported include remote control and screen sharing, unattended access, annotations, file sharing and remote mobile device camera sharing.

TeamViewer Tensor

Aimed at organizations that have incorporated bring-your-own-device (BYOD) or choose-your-own-device (CYOD) policies into their machine management, this cloud-based service can establish secure connections to corporate networks and accounts. Thus, it is equipped for remote mobile device control.

Microsoft Endpoint Manager (MEM)

MEM was announced at Microsoft Ignite last year and utilizes analytics and intelligent actions in a new dashboard interface utilizing Intune and Configuration Manager data. IT pros can manage Windows, Apple and Android devices, including operating system, security and firmware updates. This service directly supports Windows Autopilot, the next 24/7 IT support service on our list.

Windows Autopilot

This software and service targets your need to set up and preconfigure hardware heading out to your remote workforce. Using either available hardware inventory or new purchases from partner OEMs, you can decide on the full configuration of software and group policies for a remote worker's device without having to install any software on the device itself. The device is shipped to your end user and, upon receipt, they log in with proper credentials to trigger the cloud-based configuration process. You can even perform remote resets, repurposing and recovery of devices using Windows Autopilot.

RescueAssist

Formerly known as GoToAssist, this remote IT support software and service can be used not only to support PCs and Macs but also Android and iOS mobile devices across your company. The 24/7 IT support services allow for remote control of the end user's hardware, can provide remote diagnostics and can allow for unattended access without a user being present. The software can handle multiple remote sessions – up to 10 – at the same time to help with productivity. A built-in chat feature can help triage problems to help with managing urgency around support issues.

SolarWinds TakeControl

This service has similar features to RescueAssist including attended and unattended support options, the ability to support iOS and Android mobile devices, fast chat and file transfers, deep diagnostics for troubleshooting end user devices and the ability to record remote support sessions. These features are included in the basic subscription package for the service. Additional features such as batch scripting, registry editing and real-time session monitoring require a higher-level subscription.

Zoho Assist

This service offers a three-tiered subscription (Standard, Professional and Enterprise) for remote IT support plus an additional two options to get unattended access capabilities. Among the features you will find at the entry-level subscription are file transfers, reboot and reconnect, screen capture and the ability to run two simultaneous sessions. To gain other remote assistance features like mobile support, session recording or more simultaneous sessions, you will need to bump up to higher subscription levels.

ConnectWise Control

There are two variations of this IT support service – Support and Access. ConnectWise Control Support provides complete remote-control abilities for your help desk personnel so they can perform on-demand remote support and problem solving 24/7. This includes support for Windows, Mac and Linux plus the ability to remotely view the screens of ChromeOS, Android and iOS-based devices. ConnectWise Control Access brings to bear unattended remote access to your work-from-home users. Remote monitoring of machines helps you to identify and resolve problems without causing any disruption for your remote workforce.

MSP360 Remote Assistant

This is another renamed service; it used to be known as Cloudberry Lab. According to the product website, this software is "absolutely free," although a registration form needs to be filled out to gain access to the download. The feature list for this IT support software is robust and comparable to many of the previously mentioned services in this list. Among the key abilities, you will find remote and unattended access, a quick support client, file transfers, and support for Windows, MacOS and mobile devices running iOS and Android. In addition to those features, there is also voice and text chat plus a meeting option with unlimited participants.

This software could fill in multiple remote workforce capabilities for many smaller companies.

There are no doubt other tools and services available to help enterprise IT pros provide the 24/7 IT support their end users need in this unexpected work-from-home environment.

Whether a company is refining its remote support tools or creating a new plan to encompass all those needs, there are plenty of options available.

Slack vs. Teams: Comparing Their New Features and Approaches

Two of the biggest names in collaborative tools unveiled new features recently – and what they chose to work on says a lot about where collaborative tools are planning to go.

By Lisa Schmeiser for ITPro Today

In late March – at a time when legions of white-collar employees learned how to adjust to a new work-at-home paradigm and shift their communications to collaborative workspaces – two of the biggest players in collaborative software released new designs or features for their products.

Their approaches were revealing: Slack's subtle tweaks were meant to amplify features that users might not have known about and to encourage prolonged engagement in the Slack workspace. By contrast, Microsoft's announcements for Teams enhancements that will be available later in 2020 are not about boosting engagement so much as they are about expanding the prospective user base for their overall suite of tools. Let's compare the approaches the two companies are taking in the hopes of gaining prominence in the collaborative tools space.

See the sidebar on page 18 for details on Microsoft Teams' planned features.

The notable traits among Teams' new features: They're designed to work in environments where desk work isn't the norm, and they're creating a virtual workspace where individual interaction with calendaring or communication

Previous Next

can be tightly proscribed by management.

Essentially, Microsoft's moving out of the office and into service and manufacturing workflows. In the battle between the two tools, that could be a differentiator. For example, Microsoft's product announcement states, "The Bookings app offers a simple way to schedule and conduct appointments with external participants via Microsoft Teams, such as job candidate interviews, client meetings, healthcare virtual visits, virtual financial consultations, customer service appointments in retail and more."

The real tell, however, is in a new headset collaboration. Again, from the announcement: "RealWear, industry leader in head-mounted, ruggedized solutions, is partnering with Microsoft Teams to support digital transformation in manufacturing and other industrial environments. … This partnership brings together RealWear devices and Microsoft Teams to empower first-line workers while keeping their hands free. Teams on RealWear devices will be available later this year."

Microsoft has been working on Teams for three years now, while Slack has been working on its primary product for nearly seven years. Slack's latest redesign is positioned as "a simpler, more organized experience for our users" and offers the following tweaks and improvements:

The ability to move across channels and search across an organization's Slack workspace with a new navigation bar.

The ability to search for key conversations, files, apps and more at the top of the app's sidebar.

The ability to start a message from anywhere with a handy new compose button.

Increased control over the user interface with the ability to organize channels, messages and apps into custom, collapsible sections.

The ability to access different tasks in different applications via shortcuts – thus reducing a user's need to move out of Slack to complete a task such as checking a spreadsheet or editing a document.

Unlike the Microsoft announcement – which is meant to position Teams as part of a wider technological infrastructure across industries – the Slack announcement leans into the idea that productive workers never need to leave its collaborative workspace. The company rolled out its Workflow Builder last year; the in-workspace WYSIWYG tool allows IT pros and end users (who have sufficient permission) to automate

PLANNED FEATURES FOR MICROSOFT TEAMS:

- Offline support for Teams.
- Teams support for low-bandwidth connections.
- The addition of the customer scheduling and appointment managing Bookings application within Teams; this app is usually available to Microsoft 365 and Office 365 customers.
- Upgrades to the worker shift-scheduling management tool Shifts within Teams.
- A "your shifts" view for frontline workers who are not managers.
- A new push-to-talk experience in Teams that enables clear voice communication over the cloud, turning employee- or company-owned smartphones and tablets into walkie-talkies.
- Integration within Teams for Kronos Workforce Central v.8.1.
- Real-time noise suppression to address background noise on Teams connections.
- A "raise hand" feature for Teams video meeting attendees.

workplace-specific tasks that depend on retrieving and acting on information. Examples Slack offered include onboarding new workers, collecting and collating incident reports in real time, or requesting time off from HR. Now, the company is anticipating workflows such as starting a meeting with Cisco Webex Meetings or creating a customer support ticket with Freshdesk.

For a lot of end users, Slack may have initially defined the user experience for what collaborative workspaces should be like – the emojis and reaction GIFs, the ability to easily drop and retrieve files, and the ability to narrow or broaden a conversation's focus or narrow or broaden the intended participants in the conversation. And – most crucially – Slack was early to the idea that the collaborative workspace should be extensible, so users can integrate other data-reliant task flows into their communal workspace. The redesign makes sense for Slack 2019.

However, in early 2020, enterprises and the end users they serve are now grappling with multiple options in the collaborative tools space beyond Slack vs. Teams: Webex, Zoom and Google Hangouts, to name a few. Whether Slack's new features are enough to keep enterprises as engaged as Slack hopes workers will be is now an open question.

How Zoom, Netflix, and Dropbox Are Staying Online During the Pandemic

Inside the efforts to keep the quarantined world's popular Internet services running smoothly.

By Yevgeniy Sverdlik for Data Center Knowledge

To fight the COVID-19 pandemic, huge swaths of humanity have transformed their daily routines. Offices and schools are closed, city streets are empty, and most people are trying to substitute as many of their normal activities as they can with Internet-powered alternatives.

But cloud platforms of some of the most popular Internet services the quarantined world is now heavily leaning on for work, socializing, and entertainment – Zoom, Dropbox, and Netflix – have so far had no major trouble absorbing the massive surge in usage. That's according to infrastructure leads for each of the three companies, who spoke as candidly as they could about the situation in a recent webinar. Conducted over Zoom, the virtual event was organized by Kentik, developer of network monitoring tools, which some of the speakers' companies use.

That their infrastructure has been able to handle the surge and, importantly, a shift in traffic patterns doesn't mean there isn't a ton of work taking place to ensure things stay this way. "It's been all hands on deck," said Alex Guerrero, senior manager of SaaS operations at Zoom. It's also important to avoid overconfidence in the ability of the massive collection of independent networks that make up what we call "the Internet" to handle what may come in the future, as more cities around the world go on lockdown, as more employees get sick, and as infrastructure operators start feeling the impact of disrupted supply chains more acutely.

Credit: Chesnot/Getty Images

Network intelligence company ThousandEyes has been tracking network outages of ISPs, public cloud providers, unified communications, and edge services globally and has noted an upward trend in the outages since mid-February.

Zoom Scales Up

To date, Guerrero's team at Zoom has been focusing primarily on scaling up bandwidth in various places on its network. That has meant peering with more carriers and ISPs, ordering more transit, and increasing bandwidth on existing inter-

connections, with a particular focus on peering closer to end users.

"That's mainly what I'm looking at: bandwidth and being as close to the customer as possible," Guerrero said. "Our product can handle a lot of latency, but still, the closer you are to the eyeballs, the better performance."

Zoom traditionally keeps about 50 percent more capacity on its network than its maximum actual usage, he said, and the team has been busy in recent weeks maintaining that cushion.

Being an Equinix customer has helped Zoom increase its network's bandwidth, Guerrero said. The company has been using Equinix's Cloud Exchange Fabric, the software-defined network interconnection platform, to a great extent to boost capacity, he said.

Zoom today is in 19 data centers around the world, and each facility is connected to the biggest exchange in the market it's in, Guerrero explained. Now, however, its network engineers are looking at second-biggest and, in some cases, third-biggest exchanges in those markets to bring its network closer to more end users.

As usage goes up, the platform is designed to scale both network and compute automatically, "with very little human intervention," he said.

Zoom uses a combination of its own data centers and public cloud (by Amazon Web Services) for its compute infrastructure. While it has had some challenges quickly scaling compute in its own data centers due to the lock-down-related "supply chain issues" (details of which Guerrero did not disclose), scaling compute in the cloud hasn't been a problem.

Netflix Is Careful Not to Scramble

While Netflix runs mostly on AWS, its platform is also a hybrid because it operates its own content delivery network (CDN). Like Zoom, it has had no trouble scaling cloud capacity, but it did hit a recent snag when trying to get more servers into the ISP locations to increase the capacity of its CDN.

"We have had multiple fires at this point with our supply chain," said Dave Temkin, VP of network and systems infrastructure at Netflix, during the webinar.

Netflix's primary server manufacturer (who Temkin did not name) is in Santa Clara, California. When six Bay Area counties, including Santa Clara, issued a shelter-in-place order, Temkin's team had 24 hours "to get as many boxes out of there as we could."

Those issues have since been resolved by switching to a different manufacturing location, he said. Otherwise, the part of Netflix's infrastructure that delivers content to users has been scaling up as designed. Temkin's team has effectively "pulled forward" its growth plans for the coming holiday season, he said.

Things are different for the part of the company's infrastructure that's used to make content. Most content production is shut down around the globe," he said.

Besides the problem social distancing presents for shooting movie scenes, other big parts of the production process, such as post-processing, visual effects, and animation, are things you can't simply do at home because they require a lot of network and compute power. Temkin and his colleagues have been searching for solutions to make some of those things possible for creators to do remotely. "The Internet itself seems to be scaling pretty well," Temkin said. While there has been some strain – in some cases on interconnects, in others on last-mile networks – "generally nothing is absolutely melting down."

Netflix has worked to ease the strain, he said. It was unclear whether he was referring to scaling of bandwidth and compute on Netflix's network or the company's decision to reduce its video bit rates in Europe to ease congestion.

Overall, Temkin's philosophy has been to avoid scrambling for resources to ensure other, more essential services can get them if they need – services

like healthcare, e-learning, and videoconferencing.

Dropbox Is Seeking Peers

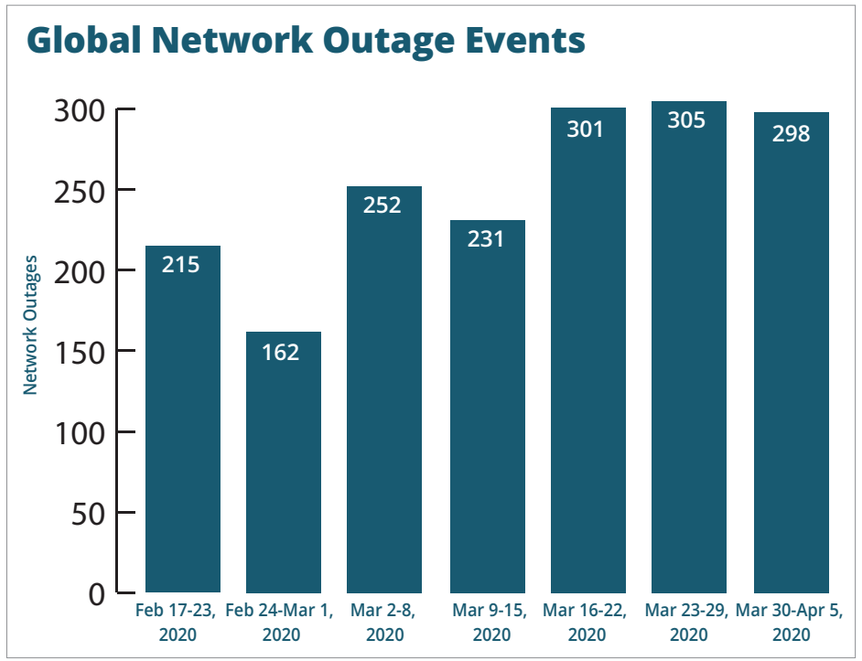
Unlike Zoom and Netflix, Dropbox runs mostly out of its own data centers. The company moved its platform from AWS to its own computing facilities in 2015. However, the company continues to rely on AWS for unanticipated bursts in capacity and for some capabilities it wouldn't make sense for Dropbox to build in-house.

The value of a hybrid cloud platform is "you can always utilize public cloud capabilities and public cloud scale," said Dzmitry Markovich, senior director of engineering at Dropbox.

Like Zoom and Netflix, the cloud storage and collaboration company's platform has successfully relied on automation to scale along with the recent surge in demand. But there have been some operational challenges with "restricted access" by some vendors around the world, Markovich said. Another challenge for Dropbox has been the shift of Internet traffic from being highly concentrated in big hubs to a more distributed pattern, he said. Instead of having a lot of traffic coming from 1,000 accounts in a university, for example, Dropbox is now seeing all of those accounts access its platform from many places, through many networks. To address this, Markovich's team has been analyzing its last-mile connectivity strategy and actively looking for more last-mile ISPs to peer with. Dropbox already peers "heavily," but it's now investing in even more.

Accelerated Scaling Plans

Markovich, Temkin, and Guerrero all declined to specify by how much the shift to working from home has increased network traffic. Cloudflare, provider of CDN and other Internet infrastructure services, said as of mid-March it has seen roughly a 10 percent decrease in traffic in office areas, a 20 percent increase in residential areas, and a 5 percent decrease for campuses over the prior month.



Source: ThousandEyes

Bill Long, senior VP of core product management at Equinix, who also participated in the webinar, said his company was seeing increases in traffic on its infrastructure ranging from 10 percent to 40 percent starting in December.

Equinix is the world's largest operator of data centers of the kind where much of the interconnection that enables the Internet takes place. "The good thing is all that core infrastructure is actually scaling pretty well," Long said.

Luckily, the pandemic started just as many companies, including Equinix, had been upgrading their networks from 10-Gigabit links to 100-Gigabit links, and that tenfold increase in capacity has been partly responsible for things running as smoothly as they have, he explained.

Because they can quickly provision multiple 100G links and scale their bandwidth in an automated fashion, many companies are in a good position to absorb massive increases in traffic. The technical capabilities to scale network capacity were there, and many Equinix customers had been planning to scale anyway – just not as quickly, Long said.

Stress Test: Data Center Operators and the Pandemic

Enterprise data center teams, data center providers, and cloud platforms meet the biggest crisis of their lifetimes.

By Yevgeniy Sverdlik for Data Center Knowledge

It has not been an easy few months for the data center industry.

In-house corporate data center teams rushed to build out their ability to support more remote workers than ever before. Commercial data center providers tightened access to their facilities around the world and dusted off their pandemic contingency binders – if they had them. Some data centers had to be disinfected after having coronavirus-positive visitors.

Data center operators scrambled to decide and formalize which of their staff were essential to keep on-site and which to send home, and also make sure that among those sent home were people who could take over for those remaining on-site in case the latter get sick.

Data center providers have put most construction projects on hold. Facebook, for example, has suspended data center construction in Huntsville, Ala., and in Clonee, Ireland.

As work and school shifts to bedrooms, living rooms, and kitchen tables, people are leaning on Internet services more than they ever have. Besides trying to keep their own

families' lives in balance, infrastructure teams responsible for making sure those services stay online have been busy expanding bandwidth on their networks and computing muscle in their data centers.

Microsoft Azure reported a massive surge in use of its cloud services in some regions in March, which caused problems when customers were trying to spin up some cloud compute resources. The company, however, said it hadn't seen any "significant" service disruptions. It is now "expediting the addition of significant new capacity that will be available in the weeks ahead."

The Internet Is Doing OK, Mostly

The Internet as a whole has been handling record spikes in traffic – and shifts in when people access the Internet and from where – without major meltdowns. However, ThousandEyes, which monitors global network health, has noted an upward trend in network outages in various parts of the world.

People in charge of infrastructure for several popular online services said the problems have been mainly at the "last mile" – the networks that deliver Internet content to end users in homes and offices. Some of those networks aren't architected to support the levels of traffic they are now seeing.

That's the reason big content services like Netflix and YouTube have been reducing video bitrate in some parts of the world. They want to relieve some of the strain on the last-mile ISPs whose networks weren't ready for all of their customers to get online at the same time, said John Graham-Cumming, CTO of Cloudflare, operator of one of the world's largest content delivery and DDoS protection networks.

Data Center Access Restrictions

Equinix, the world's largest data center operator by revenue, cut off nearly all customer and vendor access to its facilities in France, Germany, Italy, Spain, and the United Kingdom in March, allowing people in only for "critical and essential work."

Equinix has not done this in New York and Santa Clara, Calif., both major data center markets heavily hit by the pandemic. A company spokesperson did not respond to a request for explanation in time for publication.

Out of the big providers, Equinix's measures in Europe have been the most drastic. Its largest rival, Digital Realty Trust, has reduced critical on-site staff to a minimum in areas of the world where US health regulators have said the virus was spreading aggressively (Level 1 or higher). The company has been taking visitors' temperature before granting access to its facilities in Singapore and Hong Kong.

CyrusOne, which operates data centers in the US and Germany, continues to provide customer access to all of its facilities, "subject to certain prescreening questions," Andrea Munoz, CyrusOne's VP of operations and customer success, told DCK via email.

Its tenants in Germany are hyperscale cloud platform operators that use their own on-site teams, and "suspending all customer access has the potential to compromise their ability to maintain critical services," she said in response to a question about why CyrusOne hasn't taken the same measures Equinix has in that country.

Ramping Up Remote Work

The most frequently sited bottleneck the crisis has created for enterprise IT teams has been enabling a larger remote workforce than ever before. Many companies' networks hadn't been set up to give most of their employees private, secure network access to corporate networks from their homes.

One large US transportation company, for example, could support VPN access to its network for a single-digit percentage of its workforce (in the thousands) before the crisis hit, a senior IT and data center leader at the company

who asked not to be named told DCK. But the company's management decided to have everyone work from home in the beginning of March, and the team in the company's two data centers undertook "emergency deployments to increase capacity and capability for remote workers."

While social-distancing requirements caused some segments that drive business for the company to grind to a halt (automotive manufacturing, for instance), other segments have been busy "with spot business," where things like medical supplies need to be moved in an emergency fashion, he said.

The VPN capacity ramp had to be quick, but the team had been mostly prepared for it. Conversations about readying the infrastructure to respond to the crisis had been taking place in February, and a "war room" had been established. Still, "we all underestimated the velocity of this thing coming up," the data center leader said. "Who knew it would come this quickly?"

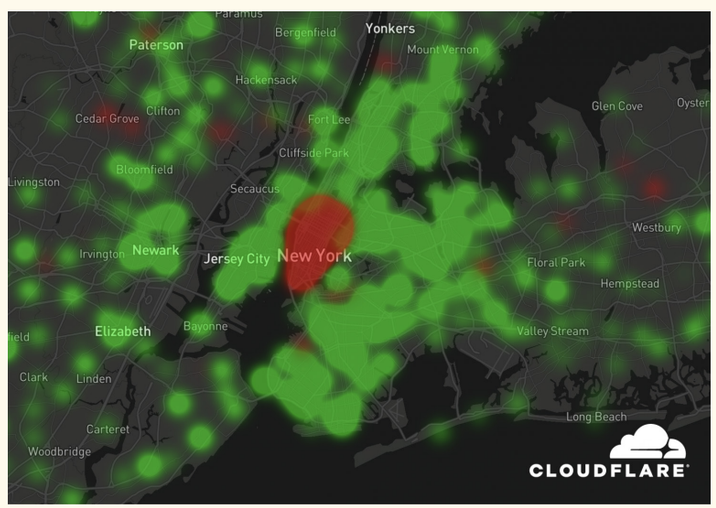
The team increased VPN capacity about tenfold in a "very short period of time," he said. The company had a bring-your-own-device (BYOD) strategy for remote workforce. As of the end of March, after ramping up, about half of the company's employees could access the company's network from their own machines at home through the VPN, he said.

They also expanded capacity for supporting remote application access via the Citrix thin client and created dashboards for business executives who now wanted visibility into the infrastructure. "A lot of dashboards were suddenly requested to track things" that were tracked before but not displayed in a way executive-level management could easily understand.

In the company's data centers, the team has been following advice such as the list of recommended pandemic-related steps by the Uptime Institute. "I hope we've done all of them," he said.

Among others, those steps include blocking vendor access for preventive maintenance, allowing them in only to fix problems; physically separating people that had been sharing office space; reducing the amount of staff per shift down to the most essential personnel; and

HOW INTERNET TRAFFIC HAS SHIFTED IN BIG METROS DURING THE LOCKDOWN



As schools and offices closed in recent weeks, and as activity all but died out in city centers, internet infrastructure operators have seen not only an increase in web traffic, but also changes in traffic patterns. Cloudflare's data team has found that traffic was down about 10 percent in office areas, up 20 percent up in residential areas, and down 5 percent on campuses. Marked in red in the image below of the New York metro region are areas where internet traffic substantially dropped from Feb. 19 to March 18, while areas marked in green are where traffic picked up. New York's most striking change is the red at the tip of Manhattan where Wall Street can be found.

rotating essential personnel ("three days on, two days off") to ensure there's backup available if a person with essential skills falls sick.

Essential Staff

Fred Dickerman, a senior VP at the Uptime Institute, said he and his colleagues had been in touch with their clients, including both enterprise data center operators and commercial data center providers, and the exercise of sorting through staff to identify who was essential to keep on-site and who wasn't had, predictably, been common across the industry these past weeks.

"We're seeing a lot of evaluation of who's essential, who's not essential," Dickerman told DCK. "The approach has been almost universally, 'OK, identify some of the essential people and send them home so they become the reserve, or split [them] up into teams and make sure the teams don't ever cross-contaminate.'"

In many cases, senior-level facility and site managers are being asked to work from home, he said. While they are essential, they have the knowledge and experience to step in for multiple types of lower-level employees, such as line engineers, technicians, or operations staff.

Dickerman said he expected that one of the broad industry changes to come out of this crisis will be organizations formally documenting which staff are essential to keep on-site during an epidemic, and who are their backups that should stay at home. Teams know who those people are today, but it's rarely documented, he said.

Can Data Centers Run Unmanned?

On March 23, Digital Realty Trust notified customers at three of its data centers in New York and New Jersey that the facilities had been visited by individuals who had tested positive for the coronavirus, Marc Musgrove, a company spokesperson, told DCK. (This was first reported by DCD.)

> "We're seeing a lot of evaluation of who's essential, who's not essential."
>
> — *Fred Dickerman, Senior VP, Uptime Institute*

One of the individuals entered the big New York City carrier hotels at 60 Hudson and 32 Avenue of the Americas on March 16, Musgrove confirmed. Another individual visited Digital Realty's data center at 2 Peekay Drive in Clifton, N.J., two days later.

In response, the operator had common areas in the affected facilities cleaned and disinfected, the spokesman said.

The company issued an update soon after, revealing more known instances of potential virus exposure in its facilities. A person who last worked at one of its facilities in Elk Grove, Ill. (outside Chicago), on March 24 tested COVID-19-positive, the company said. Customers were notified on March 27. Another person who last worked at a Digital Realty data center in Piscataway, N.J., on March 24 also tested positive. Customers were notified on March 28. A person who last worked at a Digital Realty facility in Atlanta on March 24 tested positive. Customers were notified on March 30.

The company said that in all three cases it "completed a full disinfection procedure for all common areas."

In a FAQ on its website, Digital Realty said it would evacuate a facility in case a person who visited it tested positive for 24 hours and conduct "a full building disinfection" in common areas and any areas operated by Digital. It's unclear whether the facilities in New York, New Jersey, Chicago, and Atlanta were evacuated.

If it does come to evacuation – of any data center – whether the facility can stay online without staff for the evacuation's duration depends to a great extent on its design, Uptime's Dickerman said. A facility with enough infrastructure redundancy to meet Uptime's Tier III or IV standards could run for 24 hours unmanaged, he said. But "it is a little bit like closing your eyes [and] driving your car on a straight stretch of highway. … You don't want to do it for too long."

A facility with a lower level of redundancy would be too risky to leave fully unmanned.

Also playing a role here is the organization's philosophy about remote data center management tools and security. There are two general camps, Dickerman explained. In one camp are organizations that have remote network operations centers and remote facilities monitoring, and provide technicians remote access through private network connections.

In the second camp are organizations that treat their data centers like "fortresses." They don't do any remote monitoring and don't allow any remote connections. In some cases, when a vendor must access a particular piece of equipment remotely, they'll have someone on-site physically plug into the network and unplug once the work is done.

While both approaches are valid, organizations in the first group are finding themselves better prepared for the current crisis than the ones in the second, Dickerman said.

Big Unknowns

Because planning and preparedness are in the data center industry's DNA, Dickerman said, citing a phrase by one of his colleagues, data center operators have mostly taken all of the necessary steps to minimize exposure to the virus while ensuring they can keep their facilities running.

But there are some big unknowns today that are concerning. One is the uncertainty about when the crisis is going to subside, he said. Should operators make plans to operate under the current conditions for the 18 months development of a vaccine for COVID-19 is expected to take?

Also unknown are plans governments could be making behind the scenes to escalate measures to fight the spread of the virus. They may not want to reveal those plans now "because they don't want to scare the bejesus out of people," Dickerman said.

Most operators he has been in touch with are making plans to get through spring and well into the summer, he said.

"Most authorities are saying there should be a shift in the environment by that time, but nobody knows that [for sure] … and people are thinking, OK, what if it does last a year?" he said.

Cloud Security Planning in the Time of Social Distancing

With organizations compelled to push work out to remote users and locations, cloud security becomes a very tangible matter.

By Joao-Pierre S. Ruth for Network Computing

The rapid move to remote work can raise security questions for organizations that must now lean heavily on their cloud resources. In some cases, teams may be relying on familiar systems and platforms that were established well in advance because of accelerated digital transformation and cloud migration. For other organizations, this may feel like a trial by fire. Security solutions company Optiv and enterprise software developer Atlassian offer some insight on what organizations should consider when it comes to cloud security concerns during the COVID-19 outbreak.

Adrian Ludwig, Atlassian's chief information security officer, says his company has employees around the world and the majority of the business is cloud-based. "With two exceptions, we don't run our own data centers," he says. Employee laptops make up the primary hardware used by Atlassian, Ludwig says, and in recent years the company put security measures in place to authenticate devices people use. Even with those steps, he says, the company still ran

into some recent hiccups when the entire team was directed to work from home. “The capacity we had for our VPN was nowhere near as large as it needed to be,” Ludwig says. “That was found out in a rolling cascade of failures.”

This led to changes in routing, he says, in order to restore secure access to services. Atlassian follows the zero-trust networking principle, with different corporate applications assigned varying levels of protection. “Our most sensitive applications are only accessible from a corporate device,” Ludwig says, with less-sensitive areas available through personal devices.

Security steps that he recommends organizations consider include categorizing applications to identify which ones are used daily and therefore will be needed remotely. Then organizations should consider the ways remote teams will tap into those resources, Ludwig says, and prioritize securing those connections. “Think about what that access looks like and how users will authenticate to that,” he says.

Joe Vadakkan, global cloud security leader at Optiv, says many enterprises already had some sort of remote plan or remote workforces to some degree. “From their perspective, it’s just about scaling it at a higher level,” he says. That includes increasing VPN access and virtual desktops, which can also mean higher risk.

The move to remote work, though, increases the need for security awareness training, Vadakkan says, as employees transition from operating within the controls of on-prem infrastructure. For example, an employee at home might use a personal laptop for the sake of convenience to download sensitive data or log into company email and other resources. “Those are some of the highest-risk areas from an end-user standpoint,” Vadakkan says.

Security resources are available, he says, with services such as Amazon WorkSpaces and Microsoft’s Virtual Desktops that can be used with quick and minimal set up.

Controls and guardrails need to be established for observability and monitoring in the cloud as organizations make this shift to remote, Vadakkan says. Security hygiene must improve to keep up as risks escalate, he says. Lapses in human behavior could unwittingly create points of exposure that hackers might attempt to exploit. “During this time, people are going to be spinning up a lot of workloads without security controls,” he says. “That is bound to happen.”

Questions Vadakkan says organizations should discuss include capacity planning and matching rules to the increasing volume of remote work. “Traditionally, enterprises that are risk-averse have everything locked out,” he says. “Anything that’s not corporate IP is just shut down. Managing that at a higher scale is on the checklist.”

Companies may have continuity plans in place, and Vadakkan says it is important for those plans to include an understanding of data governance as people work from home. He suggests reviewing data loss prevention measures and discussing ramifications of business communications taking place over nonsecure, commercial versions of resources, such as Skype, Google Talk, or mobile texting.

As people operate outside of a corporate network, the chances increase that they might use a plethora of unsecured communication that may move faster or are simpler to access.

The problem is that using such conveniences may run the risk of exposing the company to bad actors who have been waiting for someone’s guard to come down. “We are already see massive phishing campaigns going on around COVID-19,” Vadakkan says.

Fighting the Spread of Coronavirus with Artificial Intelligence

From screening travelers, to analyzing news about the pandemic, to helping develop a cure, governments, researchers, and health organizations are putting AI to work.

By Keith Kirkpatrick for Omdia

While the spread of the coronavirus may have been inevitable, modern technology has certainly added to the challenge. For example, inexpensive air, vehicle, and rail travel has allowed infected people to spread the virus far beyond its genesis in Wuhan, China. The use of social media is allowing unfounded rumors around the cause, prevention techniques, and likely impact of the virus to flourish. And even the traditional news media's 24/7 coverage of the virus is, in some cases, adding to the hysteria surrounding the outbreak.

However, artificial intelligence (AI) technology, in particular, is being used to aid governments, researchers, and health organizations that wish to contain the spread of the virus. From early warning and detection algorithms, to big data-based analyses of patient travel histories, to the eventual creation and development of a coronavirus vaccine, AI likely will be a key enabling technology.

Previous Next

Detecting and Tracking the Virus

For example, reports surfaced that BlueDot, a Canada-based health monitoring platform, had actually identified and pinpointed the outbreak of coronavirus on December 31, five days prior to the official warning from the U.S. Centers for Disease Control and Prevention. BlueDot's algorithm uses natural language processing (NLP) and machine learning (ML) techniques to analyze news reports in 65 languages, along with airline flight data and reports of animal disease outbreaks. By sifting through these reports, the system was able to identify where and when infected residents were likely to travel, and it correctly predicted that the virus would jump from Wuhan to Bangkok, Seoul, Taipei, and Tokyo.

AI is also being deployed to help screen travelers for potential coronavirus exposure. The Malaysian e-government services firm MY EG Services Berhad, along with Chinese travel firm Phoenix Travel Worldwide, is deploying an AI-based coronavirus risk profiling solution that will be used on Chinese visitors to Malaysia and the Philippines. This solution is capable of incorporating historical geolocation and anomaly tracking. The ML algorithm is powered by a number of data points (previous known locations, heart rate, blood pressure, etc.) that can be cross-referenced with public transport ridership, as well as exposure to locations where there have been instances of infections, to determine whether they may have been exposed to or are at risk of having the coronavirus.

Developing a Treatment Plan

Beyond tracking the virus, AI is being used to help develop a vaccine or cure. Insilico Medicine is a Rockville, Md.-based company that is developing technology designed to inform doctors about molecules capable of fighting against the coronavirus. The technology uses ML to analyze the properties of specific molecules and how they may interact with the virus, and it is designed to provide feedback on those suited to counter the coronavirus.

Enabling Communications and Coordinated Responses: Smart Cities

Smart cities are also expected to be active in using AI to address not only the coronavirus outbreak, but also future pandemics or emergencies. The development of faster and more robust communications networks, such as 5G, is integral to the deployment and use of technology that can be used to monitor and treat virus outbreaks. Examples include active monitoring of and communication among patients who are being held under quarantine, as well as tracking the movement of people within a city or around the globe. AI can also be used to predict where demand for emergency teams are needed, and then automatically coordinate a response, taking into account labor schedules, material stockpiles, and expertise.

These types of coordinated responses are being enabled by the increasing use of AI within smart cities. While many of the technologies are in testing or limited deployment now, the successes of AI technology being used to track the coronavirus may help city governments underscore the demand for AI-driven systems. Such systems can often respond to situations more quickly and efficiently than solutions that solely rely on humans.

Omdia|Tractica discusses these issues in our Artificial Intelligence Applications for Smart Cities report, which provides a quantitative assessment of the market opportunity for smart city AI applications. The study includes analyses of 23 AI use cases distributed across six industry sectors: governance, safety and security, mobility and transportation, energy and resource management, infrastructure management, and healthcare.

Tech Companies Pitch in to Fight COVID-19

But they are not alone in donating time, energy, and money to combat this global menace.

By Bradley Shimmin for Omdia

Countries have been forced to shutter businesses and enforce social distancing practices among their citizens to slow the spread of COVID-19. In the middle of this global crisis, technology vendors and enterprise data practitioners are taking action by supporting remote working and facilitating research into the coronavirus itself.

Data and analytics practitioners need not settle for a temporary escape into video games, films, books, and the like, at least not 100% of the time. They can take direct, meaningful action. Even in the smallest measure, their participation could make a huge difference in terms of slowing the spread of COVID-19 and curbing future outbreaks.

Recent weeks have shown a tremendous willingness by the technology vendor community to commit valuable resources to the important task of supporting remote working. Communications vendors Cisco, Avaya, Zoom, Microsoft, and others have offered free collaborative services for workers forced to self-isolate. Technology firms are also putting their domain

expertise to good use, with Microsoft launching a COVID-19 tracker, Nvidia calling on its customers to donate graphical processing unit (GPU) cycles to the Folding@home project, and many corporations pledging and delivering significant funds to the World Health Organization's COVID-19 Fund appeal.

Corporations are not alone in donating time, energy, and money. Take the sudden transformation of data and analytics industry practitioners. On the popular data science competition website Kaggle, data scientists and data enthusiasts have been actively contributing predictive models for the virus. Interestingly, what started back in January as a purely intellectual exercise has quickly evolved into a more pressing effort, as evidenced on March 16 when the White House called on "Kagglers" to actively engage with scientists across the globe in answering some specific questions posted on Kaggle.

Many other similar opportunities are available for citizen data scientists and analysts to participate in combating this global menace. Omdia would like to call specific attention to the supportive effort put forward by graph database vendor TigerGraph, which is opening up free use of its database. This might not sound very impactful, but there's a lot of work needed beyond the text-mining operations going on at Kaggle.

First, scientists need to build a clear understanding of the way in which the virus spreads throughout a given group of people. This information could greatly assist government and community leaders in managing best practices for the crisis on a community-by-community basis. The best way to do this is to employ graph analysis, which looks directly at the relationship and distance between two or more data points, be they friends in a social network or COVID-19 sufferers in a given community.

> "Corporations are not alone in donating time, energy, and money."

TigerGraph hopes its users can help to identify clusters of virus infection, isolate super-spreading events, and define the shortest path to understanding the origin and overall impact of transmission within a particular area or community. To help with this work, the company has created an information and idea cleaning house on Discord, and it intends to deliver several TigerGraph Cloud Starter Kits specific to these questions to help both professionals and amateur practitioners get up to speed quickly.

We're also seeing analytics vendors pitching in, with data visualization and discovery leader Tableau opening a COVID-19 Data Resource Hub, a ready-to-use dashboard built on the JHU data stream. Tableau hopes that employers and other business entities can make use of this dashboard and data feed to check outbreaks against employee location data, track clinical supplies, and so on.

Why will this kind of analysis help? Unlike earthquakes and storms, pandemics work slowly. And given the nature of COVID-19, it is possible that we will find ourselves fighting outbreaks for some time to come. For that we'll need a means of tracing and isolating any flare-ups.

Of course, we're a long way from tackling long-term pandemic problems. For now, however, these efforts are important because they trumpet the extremely important message that we're in this together, and together we can rise to the challenge of protecting ourselves, our loved ones, and our 7.7 billion cohabitants who make up this pale blue dot known as Earth.

Previous

Network Defense as-a-Service (NDaaS)

CLOUD-BASED ADVANCED NETWORK SECURITY

CyGlass by NOMINET

PLAN

Learns and labels your network so you can focus on planning your network security efforts.

PRIORITIZE

Detects and scores anomalies so you can focus on the threats that matter.

PROTECT

Alerts on and blocks violations so you don't have to spend time on the small things.

GET YOUR FREE NETWORK THREAT ASSESSMENT TODAY!

sales@cyglass.com
www.cyglass.com