



# When the World Stayed Home

*Cyberattacks increased as Global IT leaders transitioned to a distributed workforce*





## Executive Summary

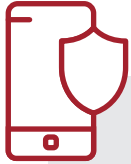
COVID-19 is a global shock unlike anything that has come before. A two-in-one combination of economic and health crisis, it has far-reaching implications for many businesses, not just in terms of the direct financial impact, but also how they are operationally structured. Across the planet, employers responded to government mandates by enforcing strict work-from-home (WFH) orders for staff, creating a distributed workforce on an unprecedented scale. Some estimates suggest that as many as two-fifths of employees will continue remote working even after the pandemic has receded.

Before the virus emerged, IT leaders were already concerned about several challenges. Endpoint visibility gaps were so acute that 71 percent told us they find previously unknown IT assets on a weekly basis. Tool sprawl, shadow IT, siloed IT teams and legacy tech were also cited as key challenges. Most (53 percent) IT chiefs were concerned that these gaps could expose them to cyber-attacks, as well as damage the brand, lead to non-compliance fines and negatively impact customer churn.

In order to discover the extent to which the crisis has exacerbated such challenges, and how organizations are preparing for what comes next, Tanium commissioned this global study.

The report was compiled from interviews with 1,004 CXOs (CEOs, CIOs, CTOs) and VPs in the United States, United Kingdom, France and Germany. All of their organizations shifted to a distributed workforce during the global COVID-19 pandemic and employ 1000+ people.

## What We Found



### **CXOs and VPs were caught out by remote working security challenges:**

85 percent of respondents felt prepared,<sup>1</sup> when carrying out the swift transition to a distributed workforce during the COVID-19 pandemic, but 98 percent subsequently faced security challenges. This was despite the fact that 74 percent benefited from increased IT spend in order to transition to a distributed workforce when compared to the same period in 2019.



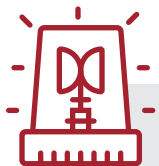
### **Organizations stored problems up for later:**

43 percent had experienced difficulty patching personal devices which has opened up their organisation to risk, and 93 percent delayed or cancelled other security priorities in order to accommodate the transition to a distributed workforce. The projects included identity and access management (IAM), and security strategy work.



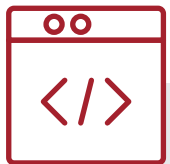
### **COVID-19 exposed enterprise security gaps:**

90 percent reported an increase in the frequency of attacks. Visibility of new devices, overwhelmed IT capacity due to VPN requirements and increased security risks from video conferencing were the top three security challenges.



### **This is the new normal:**

Most (85 percent) respondents believe the pandemic's negative impact will be felt by their organizations for months. In fact, a majority (70 percent) of respondents say that successfully implementing home IT long-term will be difficult for multiple reasons, including: compliance regulations (26 percent), managing cybersecurity risks (25 percent) and balancing cyber risk with employee privacy (19 percent).



### **Visibility and control will play a central role in the new reality:**

Almost half (48 percent) of respondents plan to invest in endpoint management that enhances visibility of IT assets as employees return to work on-site and a similar number (47 percent) to improve patch management process.

<sup>1</sup> Combining responses of "Very well prepared" & "Adequately prepared"

## From perception to hard reality

Most (85 percent) CXOs and VPs thought they were ready for the shift to remote working. A majority (74 percent) even benefited from increased IT spend in order to transition to a distributed workforce when compared to the same period in 2019. Thirty-eight percent of respondents claimed spending increases of 51 percent or more. But many underestimated the impact of the crisis on cybersecurity, with 98 percent admitting they faced security challenges in transitioning to a distributed workforce model due to COVID-19.

Patching was one of the key areas where organizations appear to have been caught off guard. Eighty eight percent of respondents had trouble in this crucial area. In fact, 43 percent of respondents experienced difficulties patching remote workers' personal devices, which has opened up their organisation to risk. Forty five percent also claimed they were able to scan and patch but not track how many devices had been fixed and patched.

## Storing up problems for later

In some cases, the impact on security was dramatic, potentially exposing organizations to severe risks further down the road.

For a quarter (26 percent) of CXOs and VPs, vulnerability management, such as patching or vulnerability scanning, has been less of a priority since the pandemic started. Respondents deprioritized vulnerability management as a result of overloaded VPNs and lack of visibility into endpoints during this period. This decision coincided with a period of several months when Microsoft issued some of its heaviest Patch Tuesday updates, including the largest in its history. During this time, multiple reports warned of cyber-criminals probing for vulnerabilities in VPNs and other remote working tools.

Ninety-three percent of respondents said they also had to cancel or delay security priorities to accommodate the transition to remote working. Identity and access management (39%) and security strategy work (40%) were cited most frequently as being hit by delays or cancelled.

## COVID-19 exposed enterprise security gaps

At the same time, organizations were experiencing a major surge in cyber-attacks from opportunistic cyber-criminals and nation states looking for gaps in security posture. Ninety percent told us they witnessed an increase in frequency of attacks<sup>2</sup> due to the pandemic, reporting 30 percent more threats than usual. The most common of these were attacks involving data exposure (38 percent), followed by business email compromise or transaction fraud (37 percent) and phishing attacks (35 percent).

The top three greatest security challenges for CXOs and VPs in transitioning to a distributed workforce were:

- **Identifying new personal computing devices in the network** (27 percent) – confirming the persistent problem of visibility gaps. Forty-five percent of respondents said that their organizations will return to normal by prohibiting personal devices on the corporate network in order to reduce risks on-site
- **Overwhelmed IT capacity due to VPN requirements** (22 percent) – failing VPNs can make patching problematic and force IT teams to abandon routing employee traffic through corporate security controls
- **Increased security risk from video conferencing** (20 percent) – hastily adopted tools may not be fit for enterprise use. Two critical flaws were found in one popular platform at the height of the pandemic

Security concerns are now rated by CXOs and VPs as the biggest challenge in accommodating a distributed workforce and associated digital transformation — more important than budget, support from the board of directors and talent/expertise. If left unmanaged they could represent a major financial and reputational risk to organizations, assuming most office work in the near and longer-term is carried out remotely.

---

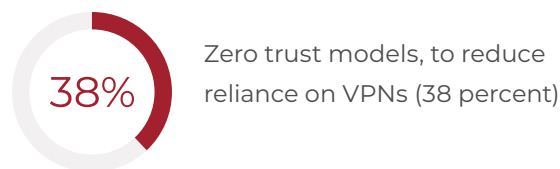
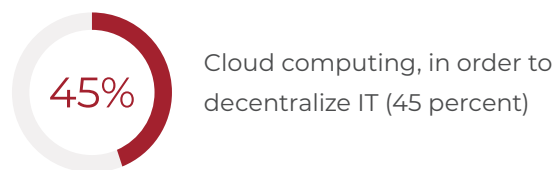
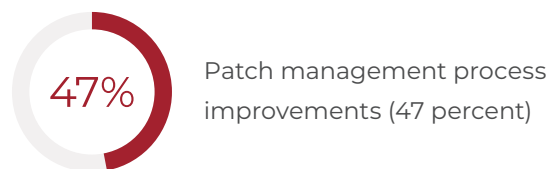
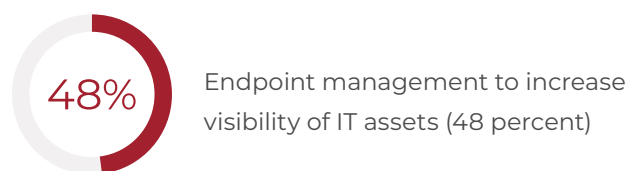
<sup>2</sup> Respondents were shown the following list of attacks; data exposure, business email compromise/transaction fraud, phishing, distributed/denial-of-service attack, password compromise, ransomware attack, other malware attack.

## What Happens Next?

Most (85 percent) CXOs and VPs believe the negative impact of operating during the pandemic's negative effects will last for more than at least three more months, and nearly one-third (33 percent) predict it will last for 6 to 12 months. It is therefore increasingly important that organizations urgently tackle their most serious remote working challenges.

The good news is that most plan to do exactly this. Seventy percent of CXOs and VPs said they'll make cybersecurity the number one priority for remote work, by meeting compliance requirements (26 percent), managing cyber risk (25 percent), and balancing cyber risk with employee privacy (19 percent).

Nearly all of these respondents (96 percent) said they plan to make changes to reduce risk as employees return to offices. They'll do this primarily by investing in:



## Visibility and control will play a central role in the new reality

Today, IT and business leaders find themselves at a unique moment. Most organizations adapted remarkably well to the unprecedented challenges placed before them at the start of 2020. But supporting employee productivity alone is not enough. Unless they pay due care and attention to continuous cyber-risk mitigation in a new work-from-anywhere era, those same organizations may find themselves exposed to serious financial and reputational damage.

Many CXOs and VPs may originally have under-estimated the scale of these challenges. But they are in a better position now. They know where IT security and operations problems are most pronounced—in patching, VPNs and in endpoint visibility. And they know that supporting mass remote working will for many of them represent a new normal.

The key will be to deal with the potential powder keg of unpatched vulnerabilities many are now sitting on, and mitigate risk going forward across a greatly expanded corporate attack surface. The best way to do this, as many have realized, is by improving IT endpoint visibility and control across on-premises and cloud-based environments. This will not only enable a push towards more productive, flexible modes of working, decentralized cloud computing models, and more agile zero trust approaches to security—it also means organizations can get delayed security projects back on track.

What emerges from a destructive global crisis could be a new resolve to enhance IT in support of the business, by putting unified endpoint management and security at its heart.


*This research was conducted by Censurwide on behalf of Tanium, polling 1,004 CXOs and VPs (CEOs, CIOs, CTOs) in companies with 1,000+ employees in total in the US, UK, France and Germany between May 29, 2020 through June 6, 2020. Censurwide abide by and employ members of the Market Research Society which is based on the ESOMAR principles.*





Tanium is a unified endpoint management and security platform proven in the world's most technically demanding organizations. Providing unparalleled speed, visibility, and scale, we serve half of the Fortune 100, top retailers and financial institutions, and four branches of the US Armed Forces, which rely on Tanium to make confident decisions, operate efficiently, and reduce risk. Tanium recently ranked 7th on the Forbes list of "Top 100 Private Companies In Cloud Computing For 2019," 10th on FORTUNE's list of the "100 Best Medium Workplaces" in the U.S., and 18th on the UK's Best Workplaces list. Visit us at [www.tanium.com](http://www.tanium.com) or follow us on LinkedIn and Twitter.


---

 [tanium.com](http://tanium.com)

---

 [@Tanium](https://twitter.com/Tanium)

---

 [info@tanium.com](mailto:info@tanium.com)

---