TANIUM

PSB Insights Study

IT Leads the Way: How the Pandemic Empowered IT

Industry Insights for Thriving in 2021

Insights Into IT Challenges and Empowerment in 2021

Early in 2020, as the pandemic struck, businesses around the world found themselves emptying their offices and shifting to a remote workforce. The transition caught most IT organizations by surprise. Suddenly, nearly all employees were working remotely, outside the protected networks and monitored systems of the IT organization.

But IT organizations did their best, and their best got the job done. Productivity resumed and in some companies even improved. Security teams worked hard to keep attacks at bay.

The pivot to working from home (WFH) proved that enterprise IT organizations could do the unimaginable – and do it quickly and well. Once you realize you can move all your users to WFH in days instead of years, you start to wonder what else you can do quickly.

What digital transformation projects, long considered a moonshot, might turn out to require far more down-to-earth efforts? What new projects become more feasible? Now the organization is more distributed, mobile, less reliant on legacy, on-premises servers, and more agile thanks to the adoption of cloud applications and services.

If massive changes are possible, how should IT organizations budget for 2021 and 2022?

Tanium partnered with PSB Insights, a global custom research and analytics consultancy, to answer those questions and more. PSB Insights surveyed IT decision-makers (ITDMs) at 500 enterprises. Half were in the U.S. and half in the U.K., distributed across a variety of industries, including financial services, healthcare, manufacturing, and retail. More than half of the respondents are C-level decision-makers.

In this report, we'll share highlights from their survey and offer suggestions for IT decision-makers as they accelerate digital transformation in 2021 and beyond.

“At the beginning, it was about survival. Security, which never takes a back seat, took a back seat out of necessity. Very quickly we had to shift back from simply keeping the lights on to security being our main focus.

We quickly pivoted to how do we keep the business running more safely, what are the specific tools we need to do that. It's honestly given us the opportunity to focus on security initiatives that we weren't able to before, like securing the edge.”

Mitch Teichman
Sr. Manager, Client Engineering,
VITAS Healthcare

The organization faced new risks.

Since the pandemic, IT decision-makers (ITDMs) have observed risky behavior from employees ranging from:

41%
storing sensitive data

38%
clicking on phishing emails

37%
inappropriate admin access

37%
leaking confidential data

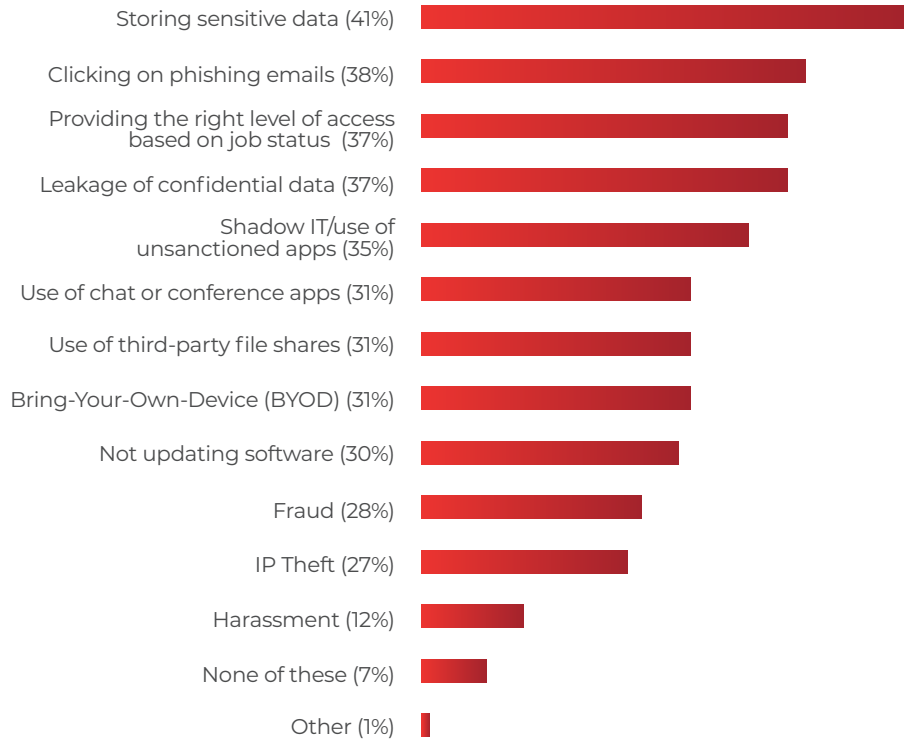
35%
a rise in risky behaviors around the use of ShadowIT/unsanctioned apps

A Rude Awakening: Shifting to a Remote Workforce

In early 2020, 88% of companies felt some level of confidence in their ability to fully and securely support remote work. Yet 61% of organizations had difficulty switching to WFH.

Suddenly, most work is being performed outside the network perimeter. Employees are on their own, possibly using their own devices, on Wi-Fi networks they might share with family, neighbors, and friends. They're working and – as we all know too well – many of them are distracted, sharing home offices with spouses and children, many of whom are still trying to attend school over video networks. The odds of an employee making a security mistake go up exponentially. The odds of the IT organization detecting that mistake plummet.

What has been the highest-risk behavior you observed among end-users from the beginning of the pandemic through today?



The IT Realities of Remote Work

In early 2020, how confident were you that you could fully and securely support your employees working remotely?

39%
Very confident

10%
Not very confident

49%
Somewhat confident

2%
Not confident at all

How difficult was the process of shifting employees to remote work?

11%
Very difficult

31%
Not very difficult

50%
Somewhat difficult

8%
Not difficult at all

> “While the transition to WFH has spurred admirable innovation on the part of IT organizations, it has also increased new risks for security and operations. Now, more than ever, teams need to focus on building a strong foundation for asset visibility and control to have a clear picture of risk.”

Payal Mehrotra
Senior Director of Risk, Tanium

IT Facing New Challenges and Increased Complexity

Once the pandemic struck, most organizations faced new security challenges and more complexity.

Here’s what the survey found. As a result of the pandemic:

73%
of respondents say they are facing new IT security challenges

69%
of respondents say they are facing new IT operations challenges

52%
of respondents say IT security challenges have become more complex

56%
of respondents say IT operations challenges have become more complex

The survey results are understandable, given that the rapid shift to a WFH model wrenched existing security and operations models apart.

More devices and new applications mean less control and new opportunities for cyber attackers. Let’s take a look at how IT leaders are reacting to this new world.

Security Challenges Resulting from a Perimeter-Less Enterprise

PSB Insights surveyed IT leaders at various management levels and operational roles. Concern about new IT security challenges resulting from the transition to a WFH strategy was seen in the vast majority of respondents.

The decision-makers who have an influence on the following areas were most likely to have identified new IT security challenges:

73%
Network security

72%
IT operations

73%
Cloud Security

70%
Web protection

72%
Data center operations

It's perhaps unsurprising that network security features at the top of the list. Moving employees to remote networks to enable home working has a direct effect on network security. The company firewall used to be the primary bulwark between employees and attackers, and now much of what the firewall protected has moved outside it.

The Transition from Perimeter Security to Edge Security

Without the firewall, companies are forced to assess endpoints individually. Defense moves from the network perimeter – the firewall – to the network edge. Each endpoint must be managed, regardless of whatever network the endpoint connects to.

Managing endpoints requires improved visibility and reporting. (Many IT monitoring products overlook 10-20% of endpoints altogether. You can't secure what you can't see.) It also ensures those endpoints are configured with the latest security software and patches.

The decision-makers who have an influence on the following areas were most likely to have identified new IT security complexity:

1. Network security (51%)
2. Web protection (51%)
3. Data center operations (51%)
4. Cloud security (50%)
5. IT operations (50%)

Security for websites and new cloud applications and services – the new IT environment for remote workers – ranked high as well.

IT Operations Transition to a Perimeter-Less World

The rapid switch to a remote workforce effectively ended the strategy of making a heavily guarded network perimeter the foundation for IT security.

- Prior to the pandemic, only a third of companies (35%) had a majority of remote employees and most companies (54%) had no plans to increase remote work in 2021.
- But because of the pandemic, 86% of companies now have some or most of their employees working remotely, with 65% saying they expect at least part of this increase to continue indefinitely.

New Operational Challenges

The decision-makers who have an influence on the following areas were most likely to have identified new IT operations challenges:

1. Network security (70%)
2. Cloud security (69%)
3. IT operations (68%)
4. Data center operations (67%)
5. Web protection (66%)

Now that employees access internal resources from consumer devices at unsecured locations, IT security teams have been forced to adjust their security models. They must bring security and management to whatever endpoint devices employees use regardless of location.

Cloud security becomes a pressing issue, too, as employees turn to the cloud for everything from next-generation business applications to collaboration tools such as Slack and Zoom.

Increased Operational Complexity

Working with a perimeter-less infrastructure, IT teams found themselves having to select and deploy new solutions for monitoring, managing, and securing endpoints, cloud applications, and other IT assets. The decision-makers who have an influence on the following areas were most likely to have identified new IT operations complexity:

1. Cloud security (69%)
2. IT operations (68%)
3. Data center operations (67%)
4. Web protection (53%)
5. Network security (52%)

Accelerated Investments

With these new challenges and increased complexity in mind, IT decision-makers are prioritizing initiatives differently this year.

In response to the open-ended question “As you plan for 2021, what are your company’s top three initiatives for IT?”, survey respondents shared:

- ✓ Better IT infrastructure
- ✓ Exploring edge computing and 5G technologies
- ✓ Cloud infrastructure and moving more to the cloud
- ✓ Risk management
- ✓ Focusing on ROI for new technologies

Businesses Are Primed for Digital Transformation

In 2020, a lot of companies discovered they could do what they'd estimated to be two years of work in just two months. Now they're re-evaluating what else is possible and what is required.

For example, how can recent advances in AI and cloud services be applied? What legacy applications should be retired next and replaced with something cloud-based, more user-friendly, and mobile-centric?

In the PSB Survey, we found customers accelerating their investments in a range of technologies. Some technologies, such as augmented reality, are probably intended to enrich interactions among remote employees. Others, such as data and information security, are intended to keep a company's rapidly evolving IT infrastructure secure and compliant.

Whatever security and operational risks companies face, the answers that IT organizations provide must continue to support rapid innovation and digital transformation.

Everything is moving faster now: business units, threats, and the daily work of IT to manage it all.

Compared to their plans before the pandemic, companies are accelerating their investments in these seven areas:

1. Cloud infrastructure (66%)
2. Data and information security (63%)
3. Security and compliance software and services (59%)
4. Artificial intelligence and machine learning (45%)
5. Asset discovery and inventory (41%)
6. Zero Trust technology for securing endpoints and accounts (38%)
7. Augmented reality and virtual reality (36%)

The interest in Zero Trust makes sense since it's a security model that assumes no login attempt or software installation should be trusted without authentication. It's a sensible model for organizations interested in increasing the endpoint security of a workforce operating remotely and outside what was the network perimeter.

"As many of our customers launch toward the new digital transformation era in a post-COVID world, we've found that things have not just accelerated, they've leapfrogged.

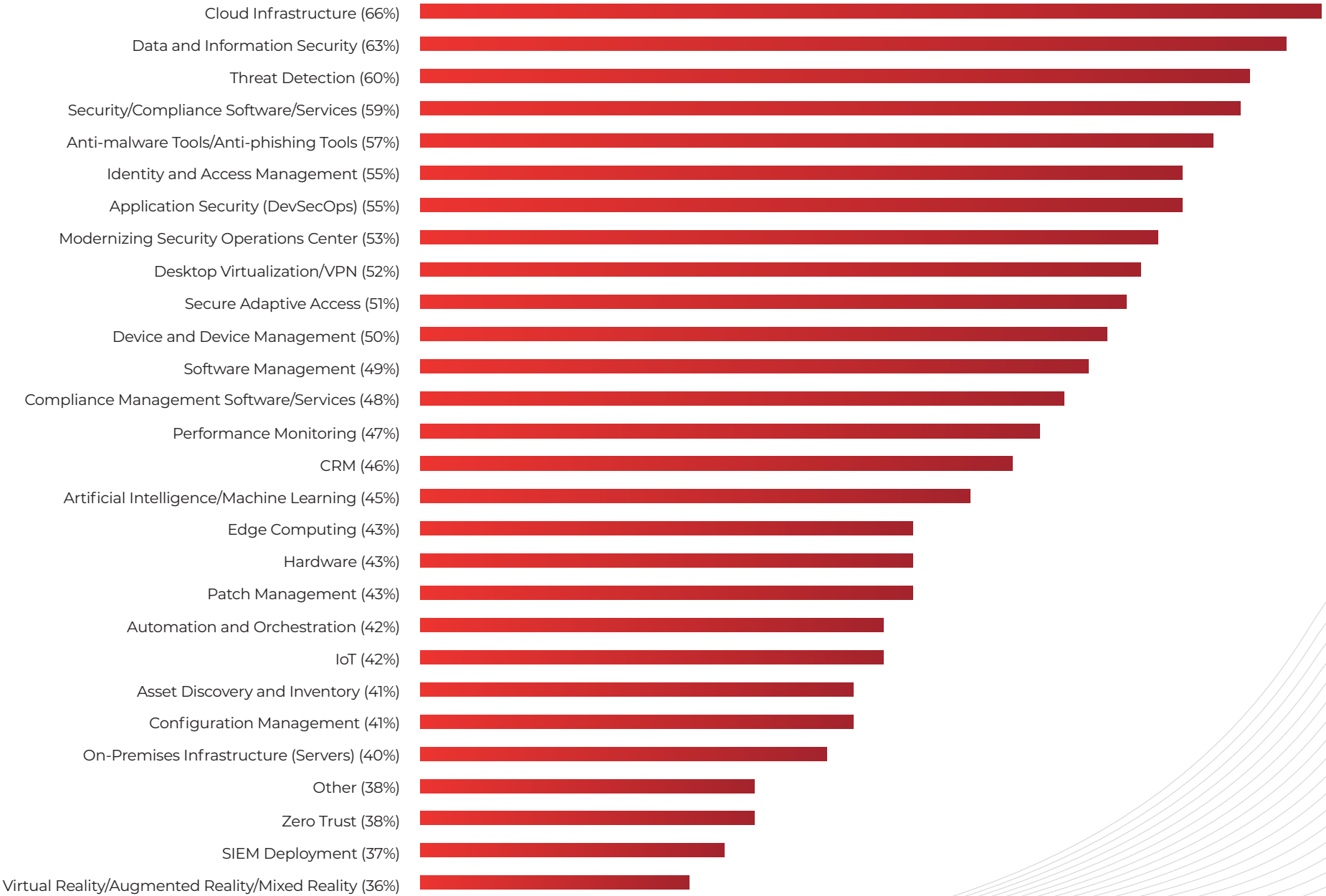
Things that would have taken years to get seeded and get to an outcome are now taking months if not weeks."

Sunil Potti
Vice President and General Manager,
Google Cloud Security

"Digital transformation has been a topic for years, but it took a global pandemic to push organizations to make it a reality. Nearly overnight, we've had to support thousands of distributed employees, shift to cloud or SaaS-based technologies, and reimagine how we engage with our customers, partners, and employees in a remote-work environment. In 2021, companies will lean in even further by giving employees the freedom to live and work from anywhere, which will make endpoint visibility and control an IT imperative."

Thomas Stanley
Chief Revenue Officer, Tanium

Compared to your original plan prior to COVID-19, for 2021 are you going to invest in the following sooner?



IT Organizations Have New Reputations – And New Expectations

The pandemic shifted the perception of many IT organizations from the land of "slow and no" to being fast and agile. A large number of organizations shifted to WFH within a week; some shifted in just a day or two. Employees across the organization noticed.

The survey included a few open-ended questions. One of those questions was "How has the pandemic shifted the perception of your IT team and their abilities to respond/react quickly?"

The answers show IT teams realized they needed to act fast. They did, and business units noticed their achievements:

- "Perception of the IT team has become one of the most important in the business."
- "Impressed with our team. We needed to react quickly to get everyone up and running from home and it was a major task, but the IT department was able to rise to the occasion."
- "It made us better and more prepared for what might happen."
- "The pandemic has made us all more united and work for the betterment of the company thus increasing profits."
- "We realized we have to be more proactive and respond to threats faster."
- "Had to quickly shift priorities, upper management was impressed."
- "Gained a great deal of respect and recognition."

In 2020, IT organizations surpassed previous expectations. Now, of course, those expectations have risen.

Going into 2021, IT organizations need to ensure they can meet business units' goals for agility and effectiveness. The pace for digital transformation – jolted into a higher gear with the pivot to WFH – isn't going to slow down.

"We've been asked to do so many things that we never in a million years would have thought of, almost on a weekly or daily basis. I don't think anything is impossible anymore."

Mitch Teichman
Sr. Manager, Client Engineering, VITAS Healthcare

Cloud Migration Gains Speed

Cloud adoption correlates with readiness for a remote workforce. Replacing legacy on-premises applications with their cloud equivalents makes it easier for remote employees to connect to the applications they need from any location. In many ways, migrating to cloud applications simplifies support for a remote workforce.

But migrating business applications to the cloud creates new challenges in security, compliance, and operations. Are connections to cloud applications secure? Are employees accessing only authorized cloud applications? Are they leaking data through cloud applications? Organizations need to ensure that endpoints are continuously identified and monitored as they access cloud applications.

From the survey: there's a correlation between companies that were more than 50% remote before the pandemic and cloud adoption. Namely, 45% of companies with more than 50% of their staff remote before the pandemic said their company is well ahead of other organisations in adopting new technologies. In contrast, only 25% of decision-makers at companies that were less than 50% remote before the pandemic felt they were ahead of other organisations when it came to new technologies.

Incidentally, the U.S. is well ahead of the U.K. in its adoption of cloud services. Forty percent of U.S. IT decision-makers believe their company is well ahead of other companies in adopting new technologies such as cloud services, compared to only 24% of U.K. IT decision-makers feeling the same way. Almost no companies rated themselves as behind or well behind other companies. Responses varied by industry:

73%

of companies in healthcare rated themselves as ahead or well ahead

80%

of companies in manufacturing rated themselves as ahead or well ahead

78%

of companies in retail rated themselves as ahead or well ahead

92%

of companies in finance rated themselves as ahead or well ahead of their other companies in adopting new technologies

There are two possible interpretations of these results. The first is that our survey happened to select companies that are genuinely leading their industries in adoption of new technologies.

The second is that, buoyed by the recent success of IT initiatives like WFH, companies are feeling bullish about their own capabilities and foresight in adopting new technologies such as cloud platforms and new network security products. They don't have clear insight into the internal operations of competitors, so they've decided that they're well ahead of the pack.

Regardless of which interpretation is correct, clearly many companies in all these industries are interested in adopting new technologies and recognize the competitive advantage those technologies might deliver.

Which of the following best reflects how you would rate the cloud services adoption for your company compared to other companies?

	Overall	Finance	Retail	Healthcare	Manufacturing
My company is well ahead of other companies in adopting new technologies	32%	35%	28%	33%	27%
My company is ahead of other companies in adopting new technologies	46%	47%	50%	40%	53%
My company is about the same as other companies in adopting new technologies	19%	16%	20%	25%	16%
My company is behind other companies in adopting new technologies	2%	2%	2%	2%	1%
My company is well behind other companies in adopting new technologies	1%	0%	0%	0%	2%

A Closer Look at Four Key Industries

Finance

Before the pandemic struck, 93% of finance companies were somewhat confident or very confident they could secure remote employees if needed. Today, 60% of finance companies have significantly more remote employees than they did before the pandemic, and 18% have slightly more. But finance IT organizations recognize the security challenges in a remote workforce. The evidence: 67% are adopting threat detection sooner than they expected, and 44% are investing in asset discovery sooner than they expected.

Healthcare

In healthcare, 68% of companies reported more or significantly more of their employees were working remotely than previously planned. The pandemic has accelerated the widespread adoption of telehealth, enabling caregivers to consult with patients from any location. But IT organizations in healthcare companies know they need to protect Personally Identifiable Information (PII) regardless of where or how employees meet with patients. Now, 54% of healthcare companies are investing in threat detection earlier than they expected, and 46% are adopting Zero Trust security models sooner. (In a Zero Trust security model, every user is assumed untrusted until authorized.)

Retail

In the retail industry, 80% of companies have more or significantly more remote employees than they expected to before the pandemic. Endpoint vulnerabilities can lead attackers to ecommerce systems, so it makes sense that 58% of retailers are accelerating their investment in anti-malware tools.

Manufacturing

You might think that the nature of most manufacturing – building things in factories – would keep employees local, rather than remote, even during a pandemic. But 72% of manufacturers reported more or significantly more employees working remotely. As a result, 58% of manufacturers are accelerating their investment in threat detection, and 70% are increasing their investment in cloud computing, possibly to increase operational agility.

Cross-Industry Trends

More than 50% of companies across these industries are investing more heavily in security and compliance than they planned to earlier.

Best Practices for Optimizing Endpoint Management and Operations in a Perimeter-Less World

Nearly 65% of companies expect some or all of their workforce to remain remote indefinitely.

What lessons should IT leaders learn from the past year and the results of our survey? Here are three lessons that stand out:

- **Expect the rapid pace of digital transformation to continue.** Businesses have discovered they can move quickly. Opportunities await those businesses that maintain this pace, building on success they achieved in 2020.

- **Remote is the new normal, so focus on endpoints, not firewalls — mobile users, not office.** The future is perimeter-less: The last shims holding traditional network perimeters in place have been discarded in last year's WFH scramble. Plan for a Zero Trust future with endpoints, as well as applications or data needed for work from anywhere. Security, monitoring, and control need to be available on any endpoint over any internet connection. You can't count on VPN access for security. Employees must be able to work with whatever software they need, wherever it resides: locally, in an internal data center, or in a public or private cloud. Manage users and endpoints, and you're ready for employees to work flexibly and safely.

- **Prioritize investments that deliver visibility and control for end users as well as IT.** Agility comes from three things: ready information about what can be done and how to do it, proven processes for executing decisions, and teams primed for acting on the latest information and delivering results quickly and reliably. For IT security and operations, agility requires improved visibility into endpoints, networks, and threats. IT platforms must help IT engineers act quickly. IT teams need a unifying platform to allow the organization to break down silos and work productively and securely.

"One of the lasting legacies of 2020 will be the distribution of workforces. Now that organizations and employees know that they can go remote, many will stay that way. Now that the shock of the transition has faded, CIOs in particular are starting to think about how you do IT when there are no corporate networks and when the need for remote access isn't limited to a select few employees.

2021 is going to be the year when CIOs really figure out how to take IT to the employee, empowering them with knowledge, tools and access that keep them connected and productive while limiting risk for the organization."

Chris Hodson
Global CISO, Tanium

Conclusion

Now is the time to invest in technologies that further unify teams, accelerating agility and digital transformation.

Orion Hindawi, co-founder and CEO of Tanium, recently raised an important question about data completeness or lack thereof. “A CRO would never settle for 85% complete revenue data,” he said. “Why should IT leaders settle for 85% complete data about endpoints or any other aspect of IT?”

To act quickly and effectively, IT organizations need improved visibility – 100% visibility — into all their operations. That means from legacy applications running in data centers and endpoints scattered across a remote workforce to new cloud applications and services adopted to better support a remote workforce. Whether the goal is improved security or digital transformation, IT organizations need improved visibility across their reconfigured, perimeter-less enterprise.

Next, IT organizations must adopt tools and platforms that empower them to act quickly and effectively, relying as much as possible on automation and minimizing the use of ad hoc, time-consuming manual processes that increase the risk of error.

Finally, they need IT teams ready to take advantage of improved visibility and an open platform to achieve amazing things.

As one survey respondent shared, IT organizations “gained a great deal of respect and recognition” for what they achieved in 2020. Some IT teams even surprised themselves with how resourceful and efficient they turned out to be.

Now it’s time for these remarkable teams to tackle the next challenges in security, operations, and digital transformation.

Study Methodology

Tanium partnered with PSB Insights to conduct an online survey among 500 IT decision-makers in the U.S. and U.K. (MoE ±4.33%) between November 19 and 24, 2020. These decision-makers represented a variety of industries, including financial services, healthcare, manufacturing, and retail.

About Tanium

Tanium offers endpoint management and security that is built for the world’s most demanding IT environments. Many of the world’s largest and most sophisticated organizations, including nearly half of the Fortune 100, top retailers and financial institutions, and multiple branches of the US Armed Forces rely on Tanium to make confident decisions, operate efficiently and effectively, and remain resilient against disruption. Tanium has been named to the Forbes Cloud 100 list of “Top 100 Private Companies in Cloud Computing” for five consecutive years and ranks 4th on FORTUNE’s list of the “Best Workplaces in Technology 2020.” Visit us at www.tanium.com and follow us on LinkedIn and Twitter.

tanium.com

@Tanium

sales@tanium.com