Hindsight Is 2020 — The Pandemic Provides A Wake-Up Call

Integrated Solutions Future-Proof Organizations

FORRESTER®

Table Of Contents

Project Director:
Sarah Brinks,
Senior Market Impact Consultant

Contributing Research:
Forrester's Infrastructure &
Operations research group
and Forrester's Security & Risk
research group

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

FORRESTER®

Executive Summary

The impacts of the COVID-19 pandemic are far-reaching and ongoing. Nearly a year ago this month, companies across the globe had to quickly pivot and provide entire workforces with the necessary support to begin working from home successfully. And as is to be expected with such rapid transformation, enterprises subsequently experienced significant challenges with increased security risks, subpar digital experiences for their employees, and complexity created by siloed and disparate toolsets. Now with remote work becoming the new long-term reality, enterprises must move with intention toward a more holistic remote work strategy that equally balances management, security, and productivity.

An integrated workforce solution is needed to enable enterprises to embrace a distributed work strategy. This must be done through a secure, scalable, and unified digital infrastructure. Implementing a solution that improves security across users, devices, networks, clouds, and apps, simplifies device and network management, and better supports remote workers to overcome challenges that are impacting employee experiences.

VMware commissioned Forrester Consulting to evaluate the impact of a more remote workforce on security, employee and customer experiences, and operations. To explore this topic, Forrester conducted an online survey with 526 global future-of-work decision-makers who have responsibility for strategy and security at their organizations. We found that the impacts of the pandemic have been a mix of bad and good. Enterprises face a lot of challenges, but the shared adversity has seen some relationships being improved across organizations.

80% of enterprises had to accelerate their remote workforce strategy because of the pandemic.

IT teams control the majority of the budget for remote-work initiatives and technology investments.

KEY FINDINGS

› **The pandemic has had varying effects on EX across organizations.** The majority of firms in our survey have seen the size of their remote workforces increase due to the pandemic. For some firms, this number has grown by as much as twenty times compared to what it was two years ago. This shift has impacted the employee experiences of our respondents differently. Nearly 30% of employees said their experience has improved since the start of the pandemic; however, 38% have seen a decline. Global decision-makers are prioritizing the adoption of integrated workforce solutions that offer exceptional employee experiences to avoid employee burnout and mass departures.

› **Shared adversity has improved relationships between IT and security teams.** Prior to the pandemic, relationships between IT and security teams at all levels were predominantly negative. But ever since talk of the new normal and regional lockdowns began, teams have been forced to collaborate, communicate, and align to support their remote workforce. As a result, many of these key relationships have been improved — this improvement extends to HR, workplace resources, and office and facilities teams.

› **Security is top of mind.** Data, endpoint, and network protection and identity/access management are top security use cases for the coming year. Enterprises are focusing on future-proofing their organization and improving their security posture. As security threats change and evolve, security leaders must quickly adapt and ensure their remote workforce is secure from external threats.

FORRESTER®

The Pandemic Has Positive And Negative Impacts

Enterprise leadership has had to make a lot of big changes fast as a result of the COVID-19 pandemic. Eighty percent of enterprises have had to accelerate their remote workforce strategy as a result. These changes have sent ripples throughout entire organizations, driving increases in personal device usage, help desk tickets, and internal siloes. In surveying 526 global future-of-work decision-makers, we found that:
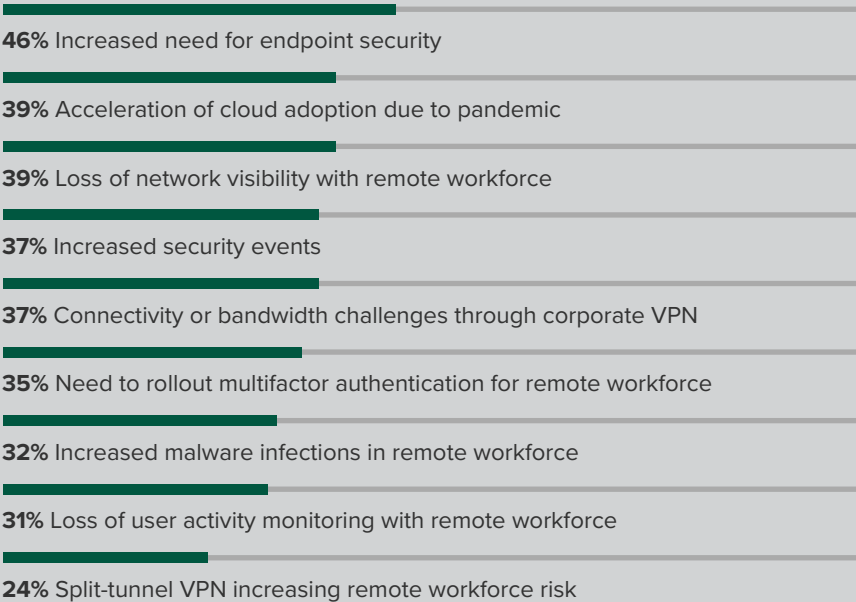
› **An increased remote workforce has impacted the entirety of organizations.** Nearly 40% of respondents have seen a decline in employee experience since the start of the pandemic. Workforces have become increasingly siloed since going remote, impacting both employee productivity and collaboration. Networking challenges, specifically with VPN infrastructure, have added to the negative experience of employees. Technology challenges, with personal and work devices, have increased the number of help desk tickets and overall need for support. Additionally, onboarding new employees or employees to a new role has become more difficult.

› **A larger remote workforce drives endpoint and network security priorities.** An increased need for endpoint security is the top security impact due to the pandemic (see Figure 1). More remote endpoints mean security teams struggle to address both network and end-device security. Connectivity and visibility into the network are other pivotal pandemic impacts. Since the workforce has gone remote, security teams have had to regain visibility into their networks and address connectivity or bandwidth challenges through the corporate VPN.

65% of enterprises had to piece together a remote workforce strategy.

Figure 1

"How has an increased remote workforce (due to the COVID-19 pandemic) impacted security at your organization?"

46% Increased need for endpoint security

39% Acceleration of cloud adoption due to pandemic

39% Loss of network visibility with remote workforce

37% Increased security events

37% Connectivity or bandwidth challenges through corporate VPN

35% Need to rollout multifactor authentication for remote workforce

32% Increased malware infections in remote workforce

31% Loss of user activity monitoring with remote workforce

24% Split-tunnel VPN increasing remote workforce risk

Base: 526 global future-of-work decision-makers with responsibility for strategy and security
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, January 2021

FORRESTER®

Security use cases are given top priority for the next year as enterprises focus on data, endpoint, and network protection and identity/access management. Decision-makers are motivated to prioritize these use cases to future-proof their organizations and improve their security postures.

› **IT's role is critical and changing.** From the pandemic's outset, the role of IT has been continuously evolving into an increasingly complex IT environment. Our study found that IT teams control the majority of the budget for remote work initiatives and technology investments (see Figure 2). IT teams have been asked to change the way they support the workforce. Additionally, the pandemic has accelerated cloud adoption for the dependability and flexibility that cloud infrastructure offers. Three-quarters of respondents have accelerated their cloud migration plans. Enterprises are more open to bring-your-own-device (BYOD) strategies, relying on IT teams for connectivity, support, and security of these devices. The use of VPN is also changing: 11% of firms no longer use VPNs, and 16% have dropped VPNs for an alternative technology.

When the pandemic started, 65% of survey respondents claim that their enterprises had to piece together a remote workforce strategy. This includes purchasing ad hoc technology solutions like collaboration tools (65%), cloud-based virtual desktops (59%), additional hardware devices (48%), and remote access Zero Trust Network Access (ZTNA) to support the remote workforce and replace VPNs. In fact, the most common approach to technology purchases to support remote workers has been to purchase multiple point solutions from different vendors and integrate them together to create a remote working solution (see Figure 3). A quarter of enterprises have purchased a point solution to fill gaps in their existing systems. These strategies act as a Band-Aid, briefly stemming the flow of challenges, but they are not enough to be a long-term solution.

› **Relationships across the organization have improved through shared hardships.** The shared experience and hardship of the pandemic has had a positive impact on forcing collaboration and communication across enterprises. Prior to the pandemic the relationships across IT and security teams were considered to be more negative than positive (see Figure 4). However, some teams have seen significant improvements to these relationships. For example:

- The relationship between IT leadership and IT practitioners went from 33% positive pre-pandemic to 53% positive today.

- The relationship between security and IT practitioners went from 33% positive pre-pandemic to 52% positive today.

- And while the relationships between IT audit and both security and IT teams still need improvement, they have improved at least slightly since the start of the pandemic.

Similar relationship improvement can be seen between HR and workplace resources teams, with teams being 36% positive pre-pandemic to 47% positive today. Office and facilities teams have managed to go from 38% positive pre-pandemic to 50% positive today. The support and management of staff and facilities during a time of relative disruption when the majority of the workforce has gone remote helps to build alliances and unanimity across teams.

Figure 2

"Using your best estimate, how much of the budget for remote work initiatives and technology investments is controlled by the following departments/teams?"
(Midpoint averages)
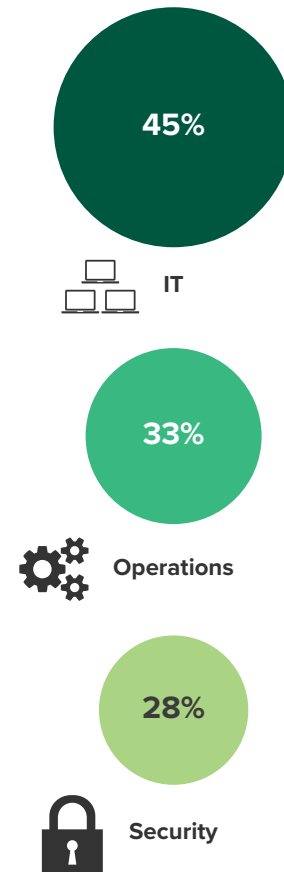
45%

IT

33%

Operations

28%

Security

Base: 526 global future-of-work decision-makers with responsibility for strategy and security
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, January 2021
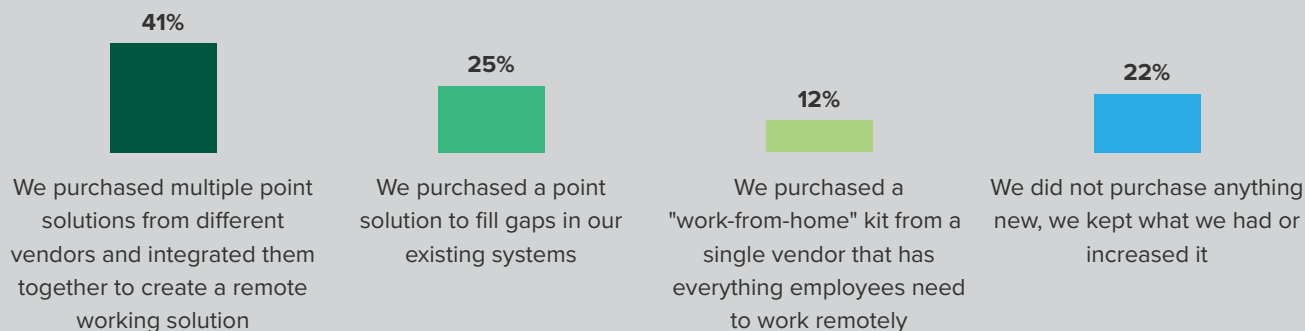
FORRESTER®

There is a great deal to learn from in both the positive and negative impacts of the pandemic. Enterprises can take advantage of the improved relationships between IT and security teams to find integrated solutions that will support the day-to-day experiences of their newly remote workforces. Positive relationships between teams can break down silos and create cross-function buy-in for engagement in integrated solutions. The need for EX improvements is rooted in the overall business strategy. Organizations that want to grow through new products, channels, or markets cannot progress without considering the implications of how employees relate to one another, to leadership, and to the customer. EX leaders should work with the top business executives to understand any changes in the growth strategy.[1]

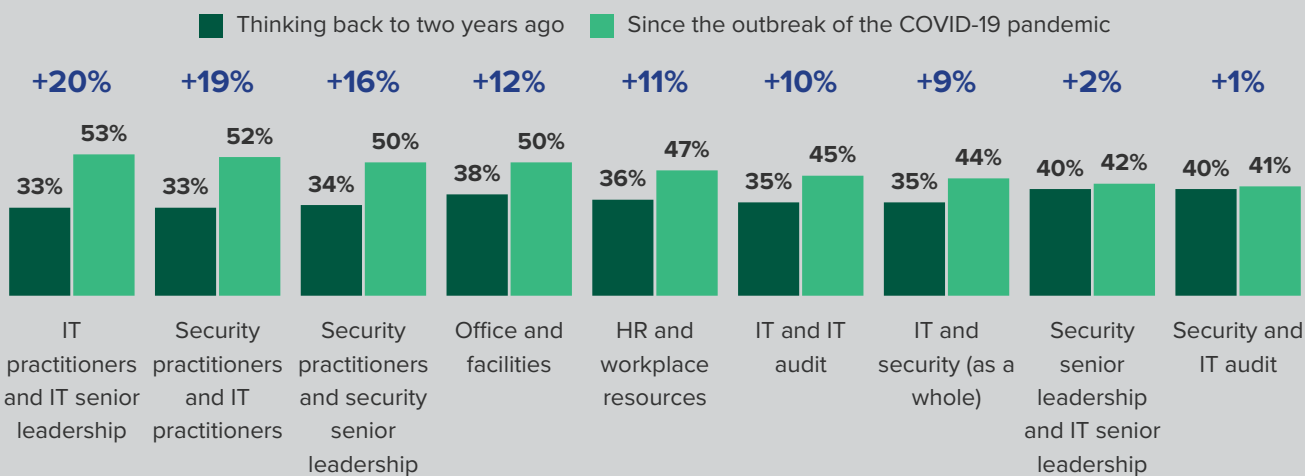**25% of enterprises purchased a point solution to fill gaps in their existing systems.**

Figure 3

"Since the impact of the pandemic, what has been your organization's approach to purchase technology to support remote working?"

41%	25%	12%	22%
We purchased multiple point solutions from different vendors and integrated them together to create a remote working solution	We purchased a point solution to fill gaps in our existing systems	We purchased a "work-from-home" kit from a single vendor that has everything employees need to work remotely	We did not purchase anything new, we kept what we had or increased it

Base: 526 global future-of-work decision-makers with responsibility for strategy and security
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, January 2021

Figure 4

"Which of the following characteristics best describe the relationships between the following teams?" (Percent positive)

■ Thinking back to two years ago   ■ Since the outbreak of the COVID-19 pandemic

	+20%	+19%	+16%	+12%	+11%	+10%	+9%	+2%	+1%
Thinking back to two years ago	33%	33%	34%	38%	36%	35%	35%	40%	40%
Since the outbreak of the COVID-19 pandemic	53%	52%	50%	50%	47%	45%	44%	42%	41%
	IT practitioners and IT senior leadership	Security practitioners and IT practitioners	Security practitioners and security senior leadership	Office and facilities	HR and workplace resources	IT and IT audit	IT and security (as a whole)	Security senior leadership and IT senior leadership	Security and IT audit

Base: 526 global future-of-work decision-makers with responsibility for strategy and security
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, January 2021

FORRESTER®

# Key Challenges Are Brought To Light Due To The Pandemic's Disruption

The pandemic has shown enterprises' key challenges in stark relief. Our study revealed that most of these challenges have not only preexisted the pandemic, but that they have also been made more challenging as a result of its impact. This study segmented challenges across four categories: security, technology, process, and people (see Figure 5). We found:

› **Evolving security threats are the top security challenge.** Security teams struggle to keep up with the changing and evolving nature of both internal and external threats while trying to keep their remote workforce secure. A lack of resources and insufficient staffing/leadership is exacerbated by a lack of budget. The staff that is in place find themselves spending too much time addressing day-to-day tasks.

› **Inefficient technology slows the enterprise.** Since the start of the pandemic, remote workers have had to confront technology disruptions that slow down productivity; a lack of network automation adds to these inefficiency challenges. As IT teams step up in increased ways to support end users, 60% of respondents say that remote support is taxing. Additionally, and likely contributing to the taxing nature of end user support is an ongoing struggle for 55% of enterprises with break/fix issues related to end-user support in increasing difficulty since the start of the pandemic and as more firms open up to a BYOD strategy.

› **Device deployment and burdensome processes hold up progress.** Since the pandemic began, IT teams have been struggling to deploy devices to end users. Budget for process improvement has also become more challenging to secure, especially as employees struggle with security policies put in place by their organization that end up hindering their productivity. There are also tasks that need to be completed which are harder to do from home. While technology and process support can help ease some of this burden, there are simply some things that are easier to do in the office.

› **Enterprises must beware of employee burnout.** Employees feel unsteady these days as they struggle to balance their work and personal lives. The fear and uncertainty associated with the pandemic frequently changes the expectations of both the workers themselves and their organizations' leaders. Employee burnout increases with the loss of perceived control and higher workloads. Isolation can also contribute to poor EX. Since the pandemic began, and most of the workforce went remote, naturally occurring silos and barriers have ended up slowing communication. This is a significant burden to onboarding new employees or employees changing roles.

Losing talent is bad for business. Employees are not loyal to underwhelming work experiences, and when they leave, their replacement is costly: between 150% and 200% of their annual salary, on average. This lost value includes investment in onboarding and training for new hires and indirect costs like productivity loss, morale damage, and, in certain cases, decreased workplace safety.[2]

37% of enterprises experience an increase in security events since their workforce went remote due to the pandemic.
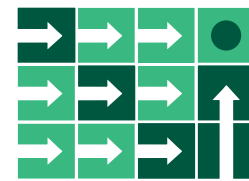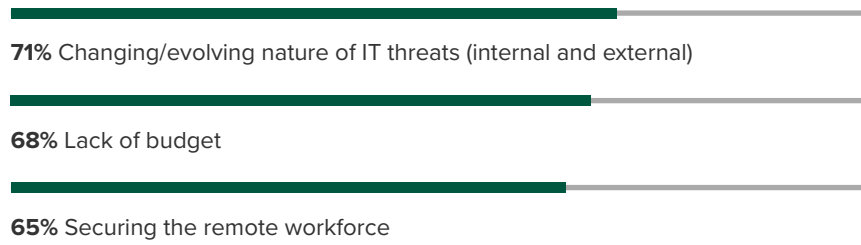
37% of enterprises said their priorities have shifted to supporting only revenue-impacting initaitives since the pandemic started.
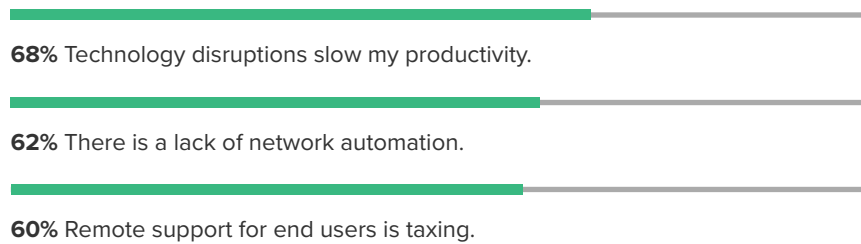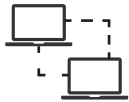
FORRESTER®

Figure 5

"Thinking about the security, technology, process, and people challenges you are facing, have they become more or less challenging since the COVID-19 pandemic started?" (Responses showing significantly/somewhat more challenging)
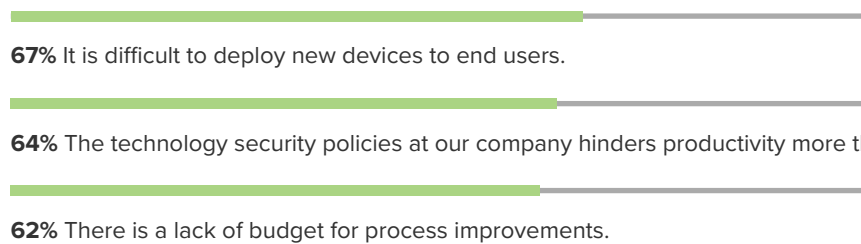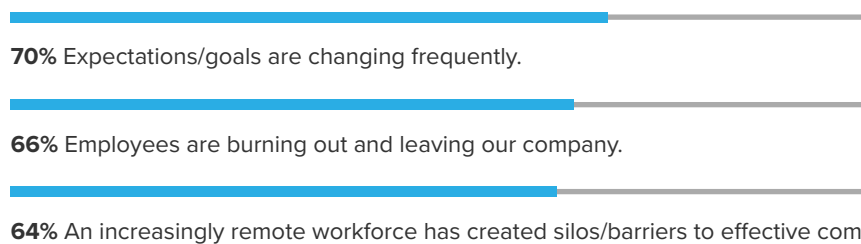
Top 3 Security Challenges

71% Changing/evolving nature of IT threats (internal and external)

68% Lack of budget

65% Securing the remote workforce

Top 3 Technology Challenges

68% Technology disruptions slow my productivity.

62% There is a lack of network automation.

60% Remote support for end users is taxing.

Top 3 Process Challenges

67% It is difficult to deploy new devices to end users.

64% The technology security policies at our company hinders productivity more than they should.

62% There is a lack of budget for process improvements.

Top 3 People Challenges

70% Expectations/goals are changing frequently.

66% Employees are burning out and leaving our company.

64% An increasingly remote workforce has created silos/barriers to effective communication.

Base: 526 global future-of-work decision-makers with responsibility for strategy and security
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, January 2021

Integrated Workforce Solutions Ease Pandemic Burdens

How do you overcome difficult technology challenges that impact your organization? Start by embracing a solution that not only supports your remote workforce but one that also provides both end-to-end security and network and device management via automation and analytics. Seventy-three percent of decision-makers feel an integrated workforce solution is a high or critical priority for their organization, and they have high expectations for its benefits (see Figure 6). An integrated solution provides critical benefits:

> **End-to-end Zero Trust security supports the enterprise.** Forrester's Zero Trust (ZT) framework is about transitioning away from traditional perimeter-based security approaches and embracing a workload-first, data-driven, and identity-aware security model.[3] Top drivers for adopting an integrated solution are: improving the organizations security posture (46%) and achieving a more holistic view through endpoint security and network security collaboration (see Figure 7). End-to-end ZT offers security controls for users, devices, networks, clouds, and apps. ZT provides visibility: 1) across networks and devices for compliance; 2) into current blind spots of employee activity and security; and 3) of the specific users who are accessing data and their access methods.
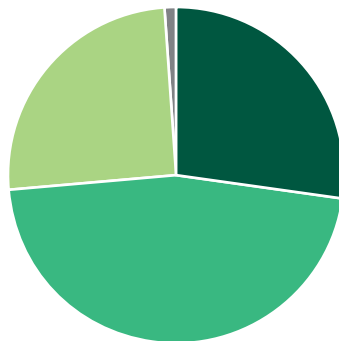
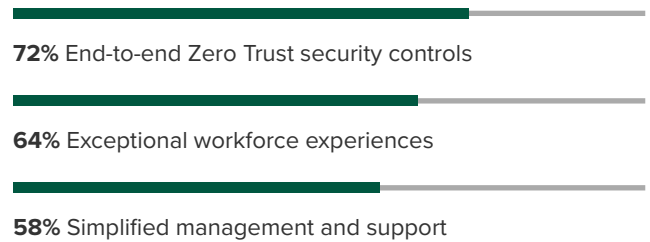**71% of enterprises sited a reduction in complexity as a top benefit of end-to-end security.**

Figure 6

"How would you describe your organization's need for an integrated workforce solution?"

- **27%** Critical priority
- **46%** High priority
- **25%** Low priority
- **1%** Not on our agenda

"What benefits would you expect for your organization from an integrated solution?"

72% End-to-end Zero Trust security controls

64% Exceptional workforce experiences

58% Simplified management and support

Base: 526 global future-of-work decision-makers with responsibility for strategy and security
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, January 2021

Figure 7

"Which of the following are driving the need for an integrated solution?"

46% Improvement to security posture

42% Increase in remote workforces' effectiveness

40% More holistic view through endpoint security and network security collaboration

38% Better employee experience

38% Increase security for remote workforces

38% Cost savings

35% Improve management of people, tools, and resources

33% Better security and management of devices

32% Easier training and onboarding

28% Optimization of and access to the network

28% Increase visibility

26% Improve collaboration across the organization

26% Reduce complexity

Base: 517 global future of work decision makers with responsibility for strategy and security that are prioritizing an integrated workforce solution
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, January 2021

› **Exceptional workforce experiences.** Enterprises need to provide exceptional technology experience wherever the workforce resides. And an integrated solution can be vital in this attempt to provide seamless access to applications and improved support. Removing technology barriers that impede employee productivity will improve EX through optimized access to the network. This will improve the scale of secure access to applications and data and contribute to fewer technology disruptions. Integrated workforce solutions break down silos and improve collaboration across the organization for easier training and onboarding of employees.

FORRESTER®

> **Simplified management and support.** Another top driver for adopting an integrated solution is modernizing device management, which improves the support experience for IT. For example, an integrated cloud-based device management solution can allow IT administrators to see in a single console: if all employee devices are patched correctly (regardless of location); if network access tools have the right configurations for information access; and if any employee technology is experiencing any type of breakdown. A simplified modern management approach can also increase speed so that organizations are able to better equip their employees with devices, apps, and faster connectivity than in the past.

INTEGRATED WOKFORCE SOLUTIONS BENEFIT INDIVIDUAL EMPLOYEES AS WELL AS THE ORGANIZATON

An integrated solution would increase the individual contributor's visibility into the organization, allowing them greater opportunities to make a difference. Acquiring cross-functional skills through integrated solutions improves the possibility of promotion. It also offers employees the ability to take greater responsibility across the organization as well as more access to leadership.

Key Recommendations

IT teams are still adjusting to their evolving role of supporting remote workforces in the new normal of the COVID-19 pandemic. To win in increasingly complex IT environments, enterprises need to balance security, employee, and infrastructure needs to win, serve, and retain customers.

Forrester's in-depth survey of 526 global decision-makers with responsibility for strategy and security for the future-of-work strategies yielded several important recommendations:

Implement an integrated solution. In order to win now and into the future, enterprises must implement a solution to fully enable distributed workforces and promote cross-functional engagement. Solutions must provide end-to-end Zero Trust security controls, create exceptional workforce experiences, and simplify the management of device and networks.

Embrace Zero Trust to secure the remote workforce. The top reason enterprises say they want to embrace an integrated solution is to improve the security posture. Organizations need to migrate away from VPN point solutions and embrace integrated access solutions. The solutions adopt Zero Trust principles of authentication and authorization prior to the network access and enforcement of least privilege access.

Infuse security throughout the remote workforce access path. It is not possible for any sufficiently large organization to secure the home environment of their remote workforce; each household can have dozens of unknown devices and unauthorized users like roommates and family members. Therefore, the employee's work devices or BYOD platforms must be made as secure as possible with endpoint protection and detection and response capabilities. This will allow IT teams to protect, detect, and mitigate security issues in the remote environment.

Make employee experience a priority from the top of the business down. In a competitive talent market with ubiquitous access to work environments and culture, a remote work option is no longer nice to have. A fully fledged remote work program is now a strategic advantage in recruiting and maintaining a highly engaged and productive workforce. This involves several key elements: a systematic approach to gathering and using employee insights to maximize return on EX investments; a focus on tailoring EX to individual employee needs rather than a one-size-fits-all approach; and a long-term commitment to continuous EX improvement, even if you can't easily measure the benefits. For potential new hires, the question is no longer, "Does your company offer a flexible work program?", but rather, "How good is the flexible work program at your company?".

Don't rely too heavily on technology — understand the human behind the technology, too. Identify which employee experiences are most important to improve. One-size-fits-all approaches to EX lead to lackluster experiences for everyone, just as they do in customer experience (CX) scenarios. So, use employee journey mapping to understand the daily journeys of all employees and identify the challenges they face. While there are key aspects of the employee experience — like onboarding, performance reviews, and promotions — that affect all employees that you must get right, you need to get more specific to deliver competitive EX.[4] To do this, develop a set of five to six employee personas to get started, and then layer in additional personalization via self-service, BYOD options, qualitative feedback mechanisms, and the use of AI.
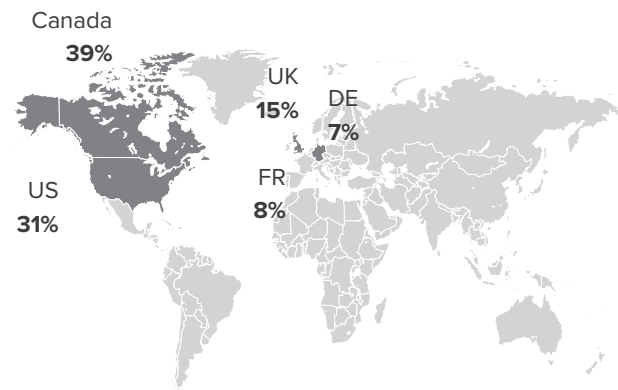
Embrace cross-functional cooperation as the role of IT evolves. Since the start of the pandemic, IT has become increasingly critical to the success of businesses and navigating the new normal. The shared adversity brought on by the pandemic has helped repair and improve cross-functional relationships. Take this momentum and drive forward cross-functional initiatives and demand collaboration across your organization. Focus on use cases that are important to business stakeholders to encourage engagement and buy-in.
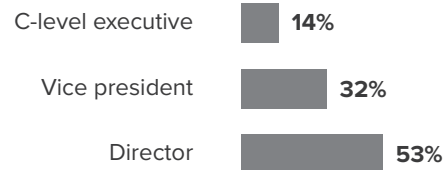
FORRESTER®

Appendix A: Methodology

In this study, Forrester conducted an online survey of 526 global decision-makers who have responsibility for strategy and security in North America and Europe to evaluate future-of-work strategies. Survey participants included decision-makers in director+ roles. Questions provided to the participants asked about pandemic-related challenges, solutions needed to overcome challenges, and how their situation has changed compared to two years ago. The study began in December 2020 and was completed in January 2021.
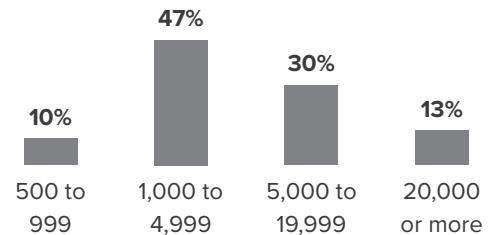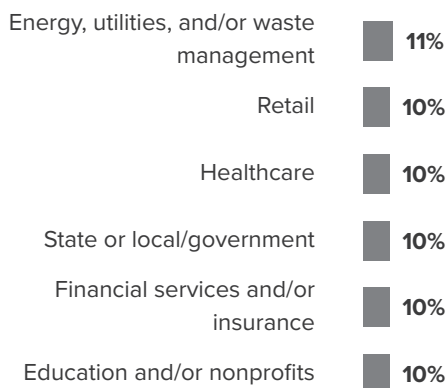
Appendix B: Demographics

Canada
39%
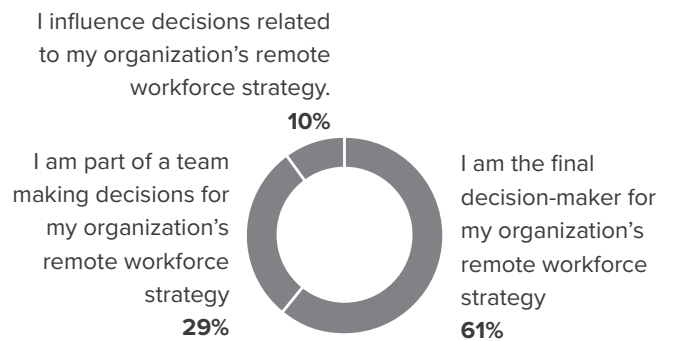
UK
15%

DE
7%

US
31%

FR
8%

INDUSTRY (TOP 6 SHOWN)

Energy, utilities, and/or waste management	**11%**
Retail	**10%**
Healthcare	**10%**
State or local/government	**10%**
Financial services and/or insurance	**10%**
Education and/or nonprofits	**10%**

RESPONDENT LEVEL

C-level executive	**14%**
Vice president	**32%**
Director	**53%**

COMPANY SIZE (NUMBER OF EMPLOYEES)

500 to 999	1,000 to 4,999	5,000 to 19,999	20,000 or more
10%	**47%**	**30%**	**13%**

RESPONDENT RESPONSIBILITY

I influence decisions related to my organization's remote workforce strategy.
10%

I am part of a team making decisions for my organization's remote workforce strategy
29%

I am the final decision-maker for my organization's remote workforce strategy
61%

Base: 526 global future-of-work decision-makers with responsibility for strategy and security
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, January 2021

Appendix C: Endnotes

[1] Source: "Now Tech: Employee Experience Consulting Practices, Q3 2020," Forrester Research, Inc., September 2, 2020.

[2] Source: "Understand Employees' Experiences," Forrester Research, Inc., December 8, 2020.

[3] Source: "Enhance EX With Zero Trust," Forrester Research, Inc., July 13, 2020.

[4] Source: "Understand Employees' Experiences," Forrester Research, Inc., December 8, 2020.

FORRESTER®