

Insights from 2020 – New Workforce Priorities Shift the IT Landscape





In 2020, 80% of organizations had to accelerate their remote workforce strategy, and 65% had to rapidly piece one together.

To better understand the impacts of the COVID-19 pandemic on organizations, VMware commissioned Forrester Consulting to survey 526 decision-makers with responsibility for strategy and security from various industries globally on how the challenges of suddenly shifting to a remote workforce affected their company and what they perceive as the future of remote work.¹

The pandemic illuminated and exacerbated preexisting issues regarding security, technology and employee experience. Organizations confronted these challenges while shifting to a distributed workforce environment:

- Increased security risks
- A subpar digital employee experience
- The complexity created by siloed, disparate toolsets and inefficient technology

Security is top of mind. Over 35 percent of organizations experienced an increase in security events since their workforce went more remote, exacerbated by a lack of resources and insufficient staffing. The staff in place found themselves spending too much time addressing day-to-day tasks. Enterprises are now focusing on future-proofing their organization and improving their security posture in terms of safeguarding endpoints, protecting data, and managing access.

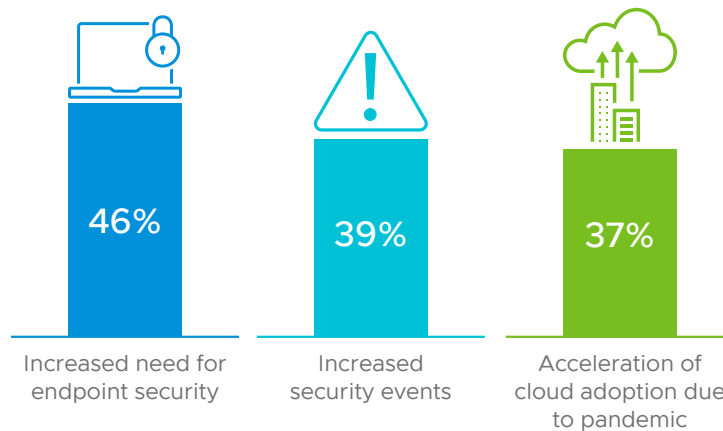


FIGURE 1: Security Impacts of an Increased Remote Workforce Due to the COVID-19 Pandemic

1. Forrester Research, Inc. "Hindsight Is 2020 — The Pandemic Provides A Wake-Up Call: Integrated Solutions Future-Proof Organizations." Sarah Brinks. January 2021.



66% of respondents indicated that the challenge of “**Employees burning out and leaving our company**” had become more significant since the COVID-19 pandemic started.

Employee productivity and collaboration have suffered due to the workforce becoming more siloed. Networking challenges, specifically with VPN infrastructure, have added to employees’ negative experience. It was difficult to deploy devices to users with minimal budget for process improvement. The necessary openness to a bring-your-own-device (BYOD) strategy heavily relied on IT teams for connectivity, support and security on myriad devices and systems, increasing frustration and the number of help desk tickets.

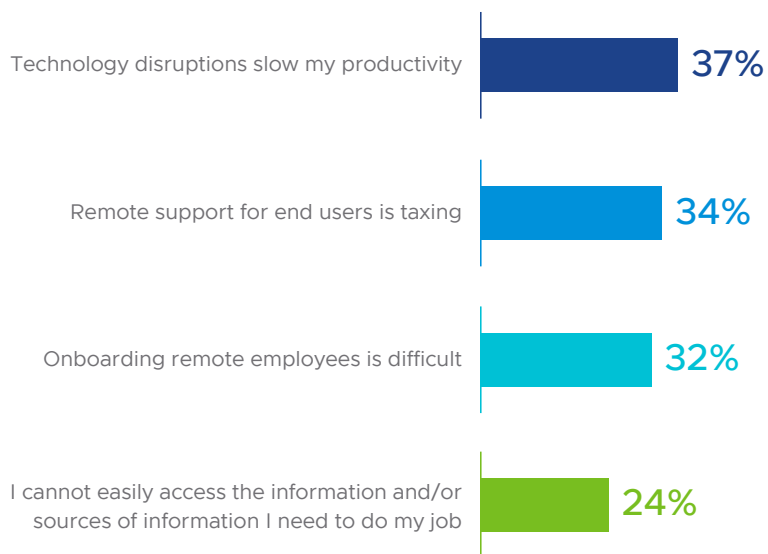
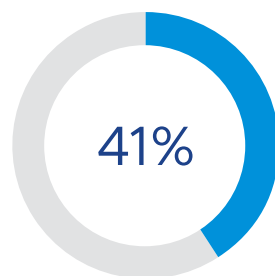
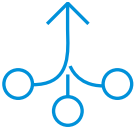


FIGURE 2: The top technology challenges today are disruptions that slow productivity, and remote support that is taxing for end users.

The role of IT has strained to continuously evolve. The pandemic has accelerated cloud adoption because of the infrastructure’s dependability and flexibility. A majority of enterprises had to piece together a remote workforce strategy, purchasing ad hoc technology solutions like collaboration tools and cloud-based virtual desktops. A quarter of enterprises purchased a point solution to fill gaps in their existing systems. These strategies have acted as a temporary fix, briefly stemming the flow of challenges but not enough to be a long-term solution.



41% of organizations purchased multiple point solutions from different vendors and integrated them to create an ad hoc remote working solution.



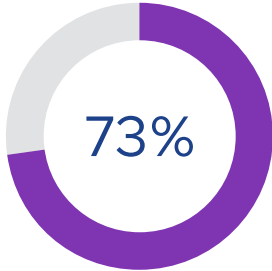
71% of enterprises cited a reduction in complexity as a top benefit of end-to-end security.

Addressing Pandemic Challenges

The survey revealed that the **shared adversity and problem-solving demands have had a positive impact by forcing collaboration and communication among teams.** For example, cross-functional relationships between IT and security teams and HR and workplace resources teams have improved. Prior to the pandemic, relationships between IT and security teams at all levels were predominantly negative. Organizations can take advantage of these improved relationships to overcome challenges and find integrated solutions with cross-function buy-in to support remote, anywhere workforce experiences.

With remote work as the new long-term reality, organizations must move with intention toward a more holistic remote work strategy that balances security, productivity and management. **An integrated workforce solution eases pandemic burdens and benefits employees as well as the organization** by providing:

- **End-to-end Zero Trust security**, which moves away from outdated perimeter-based approaches to a model that monitors users, devices, networks, clouds and apps across the network. Zero Trust provides visibility into who accesses data and how they're accessing it.
- **Exceptional technology experiences** by bringing seamless access to apps, improved collaboration, and easier training and onboarding directly to employees, anywhere.
- **Simplified device management** that improves the support experience for IT and enables organizations to better equip employees with devices, apps and connectivity.



of decision-makers describe an integrated workforce solution as either a high or critical priority.

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



FIGURE 3: Decision-makers have high expectations for an integrated workforce solution, anticipating critical benefits.



Take the Next Step

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

Learn more about how integrated solutions can future-proof your organization in *Hindsight 2020 – The Pandemic Provides a Wake-Up Call*.

[DOWNLOAD](#)

Key Recommendations

Forrester’s in-depth survey regarding anywhere-work strategies yielded several important recommendations.

Implement an integrated solution to fully enable a distributed workforce and promote cross-functional engagement. The solution must provide end-to-end Zero Trust security controls, create exceptional workforce experiences, and simplify the management of devices and networks.

Embrace Zero Trust to secure the remote workforce. To improve the security posture, organizations need to migrate away from VPN point solutions and adopt integrated access solutions based on authentication and authorization prior to network access.

Infuse security throughout the remote workforce access path, including the home environment. A household can have dozens of unknown devices and unauthorized users. Therefore, an employee’s work devices and BYOD platforms must be made as secure as possible with endpoint protection, endpoint detection and response capabilities to let IT protect, detect, and mitigate security issues.

Make employee experience a priority to maintain and recruit a highly engaged and productive workforce. A fully fledged remote work program is no longer a nice-to-have but a strategic advantage. Focus on tailoring and continuously improving employee experience to individual employee needs rather than a one-size-fits-all approach.

Understand the human behind the technology, and identify the challenges that employees face in their daily journeys. Pinpoint which employee experiences are most important to improve, and address specific roles to deliver a more tailored experience, for example, by developing five or six employee personas and then layering in personalization via self-service, BYOD options, qualitative feedback mechanisms, and the use of AI.

Embrace cross-functional cooperation as the role of IT evolves. The shared adversity brought on by the pandemic has helped repair and improve cross-functional relationships. Take this momentum to drive initiatives and foster collaboration across your organization. Focus on use cases that are important to business stakeholders to encourage engagement and buy-in.





vmware®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com Copyright © 2021 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at [vmware.com/go/patents](https://www.vmware.com/go/patents). VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. Item No: FY21-6223-VMW-FORRESTER-EXEC-SUMMARY-BRO-USLET-WEB-20210217 2/21