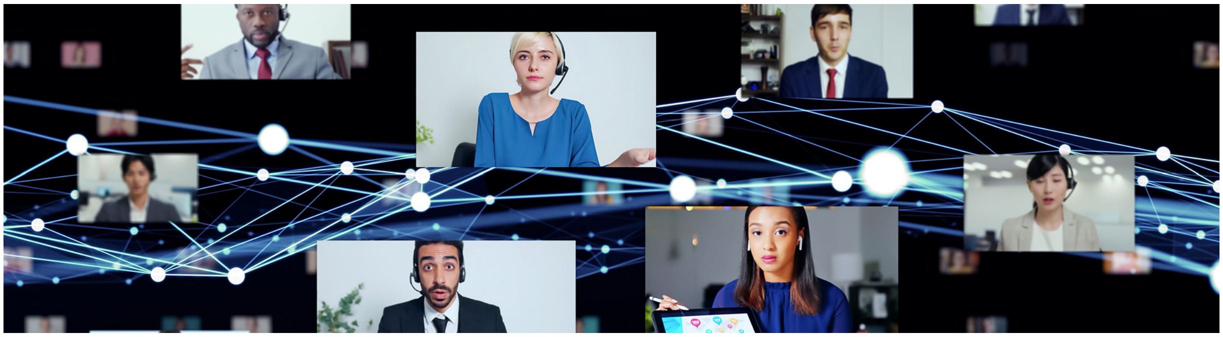
SPONSORED CONTENT | WHITE PAPER

Market Pulse

With Hybrid Work Here to Stay, It's Time to Optimize for the New Workplace



IMPLEMENTED UNDER GREAT PRESSURE IN THE EARLY DAYS OF THE PANDEMIC, remote work has become a seemingly permanent fixture. In an October 2022 Foundry MarketPulse Survey for Verizon: Supporting a Remote/Hybrid Workforce of over 100 US IT decision-makers, 92% said a hybrid work environment is now standard at their organizations.

IT priorities with respect to supporting remote workers

62%	Effectively integrating collaboration tools (chat, messaging, file sharing, web conferencing)
62%	Enabling seamless data and application access
58%	Providing reliable connectivity
56%	Securing business data/ transactions (e.g., endpoint security, device authentication on the corporate network)

Source: Foundry

The challenge for IT is supporting a hybrid workforce with technology that fits each diverse role in an organization. In matters ranging from security to reliable network connectivity to managing the software and hardware that makes remote work possible, IT leaders told us one size definitely does not fit all.

Two years after the pandemic outbreak, a majority of U.S. employees still had the option of working from home for all or part of the week, according to McKinsey.[1] In the Foundry survey, 91% of respondents said offering remote work has become critical to attracting and retaining talent.

But for remote work to succeed on a permanent basis, organizations must have the right technologies in place for protecting company assets and supporting people anywhere, whether they're logging in from home, attending a conference, or on the road meeting with clients. IT leaders in the Foundry survey identified the most critical capabilities as:

1. Providing seamless access to collaboration tools and data (62%)
2. Providing reliable connectivity (58%)
3. Ensuring strong security (56%)

CIO

SPONSORED BY

verizon

Fulfilling role-based needs

The initial rush to pivot to remote work meant many organizations lacked experience supporting a scattered workforce and time to understand the role-specific needs of individual employees. Over the past two years, IT leaders have gained more nuanced insights. An overwhelming majority of the Verizon-Foundry survey respondents agreed that to help employees perform their best, IT needs to deploy technology suited to their roles. Here's a breakdown of their recommendations:

ROLE	PRIORITIES & TOOLS
Executives	C-suite and other leaders need to stay connected to the organization and have little time for hands-on technology management. They are also high-priority targets for cybercriminals. They require dedicated internet connectivity and strong malware protection. Fully managed, 24/7 tech support, including deployment, set-up, and hardware life cycle management is also critical.
Knowledge workers	Knowledge workers need built-in network security, malware protection, and dedicated internet connectivity.
Customer service representatives	Formerly stationed in call centers, these customer-facing workers now need tech support for newly virtual environments, relying on IT to troubleshoot problems and protect against malware and other threats.
"Road warriors"	Sales representatives and other employees who travel frequently must have built-in network security, dedicated internet connectivity, and malware protection everywhere they go.
IT managers	Like C-level executives, IT managers are major targets for cyberthieves. Built-in network security is the top priority, with malware protection and dedicated internet access not far behind.

The cybersecurity challenge

One overarching theme the survey uncovered is the need for better cybersecurity. The multiplicity of connections increases the attack surface, and 70% of respondents said remote work makes it difficult for them to keep the corporate network and data secure. Among their specific concerns are the potential for an increase in data breaches (59%), malware attacks (55%), threat volume (45%), and end-user errors (45%).

IT security risks due to remote work

59%	Data breaches related to user access / authentication
55%	Malware attacks as a result of shared/unsecure connections with home networks
45%	Increased threats due to the volume of data generated by end-user devices
45%	End-user error and/or lack of security awareness

Source: Foundry

IT and infosec teams have already put important protections in place to improve security for remote workers, including VPNs (60%), malware protection (60%), and identity and access management systems (58%). Over the next 12 months, the security technologies they are most likely to deploy are:

- ➜ Multi-factor authentication (29%)
- ➜ Security and event management (27%)
- ➜ Endpoint detection and response (26%)

These protections should go a long way toward safeguarding data and systems accessed from afar.

Managing a more complex network

Another big challenge is network management. Seventy-one percent of respondents said remote work increases the complexity of managing the network and troubleshooting technical issues. Maintaining reliable connectivity is also a significant concern, cited by 58%.

Resolving these issues will likely require changes to the way networks are supervised. No matter how dedicated and hardworking an IT staff is, supporting 200 workers in one office building is simply not the same as supporting them across 200 different locations. Using one vendor to provide and manage all services could relieve some of the burdens imposed by a much broader technology estate, giving IT staff more time to work on higher-level tasks.

Improving the remote work experience

As IT teams work to optimize technology for today's distributed workforce, developments just around the corner could revolutionize the remote work experience, offering innovative and immersive ways for employees to consume information and learn new skills.

Respondents to the Foundry survey said 5G is the technology they are most eager to deploy to improve work experiences over the next 12 to 24 months. As 5G becomes more available, it can increase access to fast, reliable internet at a reasonable cost.

5G can also facilitate the incorporation of groundbreaking technologies, including Artificial intelligence (AI), which 63% of respondents said they would like to adopt within the next couple of years. Nearly half of respondents are interested in deploying virtual reality (VR) in that timeframe, and 39% have their eyes set on augmented reality (AR). AR and VR tools, backed by AI analytics informing the content they display, can allow employers to deliver information in powerful new formats, engaging workers through their senses as well as their minds.

Preparing the remote workplace of the future

The Foundry survey makes it clear that remote work is here to stay. To optimize support for a distributed workforce, IT leaders must move away from the one-size-fits-all technology deployments of the past and tailor role-specific solutions. Remote environments also call for increased cybersecurity protections and reliable internet connectivity. Organizations able to meet these needs will foster a more efficient and secure remote workplace, and help position themselves for an innovative future.

To learn more tips about how to boost your company's success with remote work, **click here**.

[1] www.mckinsey.com/industries/real-estate/our-insights/americans-are-embracing-flexible-work-and-they-want-more-of-it