Navigating Disruption

An ePlus Special Report on the technology impact of COVID-19 and how IT organizations can be more prepared for the future

Where Technology Means More®

Introduction

Disruption is common in today's marketplace. But not even the most forward-thinking professionals in the industry were quite prepared for the massive disruption caused by COVID-19.

Almost overnight, business leaders faced a new challenge. Their priorities shifted from increasing operational efficiency and improving customer experience to only one thing: survival. Adapting to new conditions and keeping their businesses alive and operational while protecting the safety and health of their employees became the singular focus of nearly every senior executive.

Technology leaders were pressed to find solutions, fast. Workers were going home—for how long, no one knew—but they needed to maintain productivity if business operations were to continue. For some organizations, this required massive changes to business processes, technology infrastructure, and application and data security.

As organizations worked through the early phase of the crisis, we wanted to know more about their experience in an effort to help support them during this unprecedented time. We recently surveyed 135 technology professionals, with titles ranging from CIO and IT Director to CISO, and representing organizations spanning every industry, to understand the most significant technology challenges they had to overcome.

Going forward, the future is still unclear, especially for those in technology leadership roles. Our hope is that you can use this information to assess your own experience during this time against that of your peers. We are confident that the insights and recommendations presented will help you focus your efforts on preparing for whatever comes next.

At a Glance

As you might expect, not every company struggled with the same technology challenges during the early months of the pandemic or in the subsequent months since. Despite each organization's unique challenges, the findings from the survey did highlight several common themes:

Many organizations struggled with data center capacity challenges for a variety of reasons, but business needs didn't slow down, which resulted in an increase in spending on cloud services.

As employees sheltered at home, technology leaders were inundated with requests for remote access to applications and data so that remote workers could remain productive in their day-to-day jobs.

Workers had to learn to operate in a virtual world where communication and collaboration can be challenging both for internal teams and for those interacting with customers.

The accelerated adoption of cloud services and allowing remote users to access sensitive data left many organizations concerned over security risks and vulnerabilities.

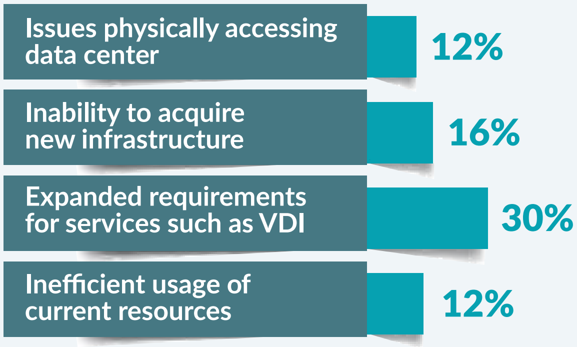
Data Center Capacity and Cloud Spend

Response to the pandemic—and the subsequent CAPEX spending freezes, inability to physically access the facilities, and supply chain issues—had a significant impact on the data center. As technology leaders rushed to find solutions to address the disruption, over half **(58%) of those surveyed said they experienced capacity challenges in their data centers.**

Several issues contributed to the strain on capacity. The need for expanded services to address remote work, such as virtual desktop infrastructure (VDI), accounted for almost one-third (30%) of the problems. Another 16% struggled with the inability to acquire new infrastructure.

But infrastructure and services were needed quickly. With capacity challenges in the data center, many organizations expanded their use of the cloud. Over the first 90 days of the pandemic, one quarter (25%) of organizations saw an increase in their cloud spending. And almost one in ten (9.9%) saw their cloud spend jump by more than 20%.

Data Center Capacity Challenges:



25%

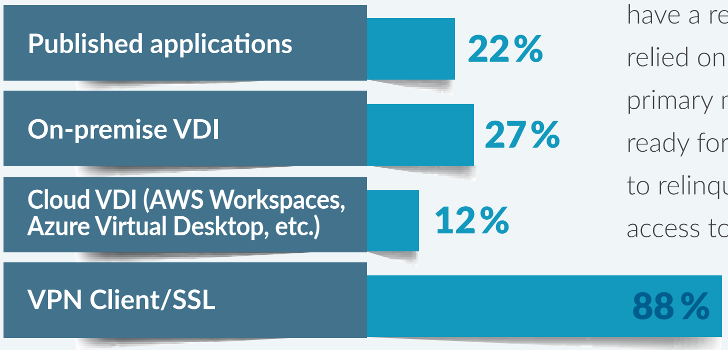
Of organizations experienced increase in cloud spending.

1 in 10

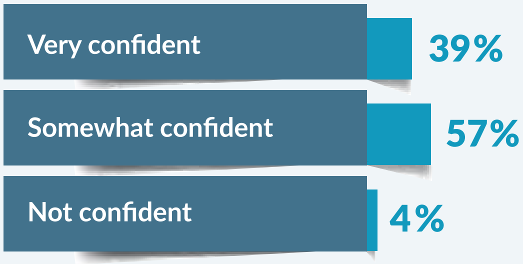
Increased cloud spend by 20% or more.

Remote User Access

Primary Method(s) for Remote Access



Confidence level in deployment and configuration of technical controls for detecting threats and protecting sensitive data:



Cost and Performance Concerns

9% *Facing both cost and performance issues*

12% *Find performance acceptable but cost is not sustainable for long term*

14% *Indicate cost is within budget but performance or other concerns are lacking*

The pandemic has forced IT organizations to change quickly and to adjust to new realities. While most organizations we surveyed did have a remote access strategy—in fact, 88% relied on virtual private network (VPN) as a primary method for remote access—few were ready for large-scale deployment. Many had to relinquish tight controls and expand remote access to systems and sensitive data to more users than ever before. Prior to the pandemic, virtual desktop infrastructure (VDI) was used by only 39% of organizations surveyed, but the sudden increase in the need for secure remote access drove VDI adoption to new heights over the past few months.

Lessening controls, while necessary in some instances, can create security vulnerabilities. But in a crisis, shortcuts are taken and full vetting of risk may be overlooked. As more remote users were added and access to sensitive data was allowed, **only 39% of the technology leaders we surveyed were very confident they had the technical controls in place to protect the organization against security threats.** Over half (57%) were somewhat confident, but were still concerned that more work needed to be done.

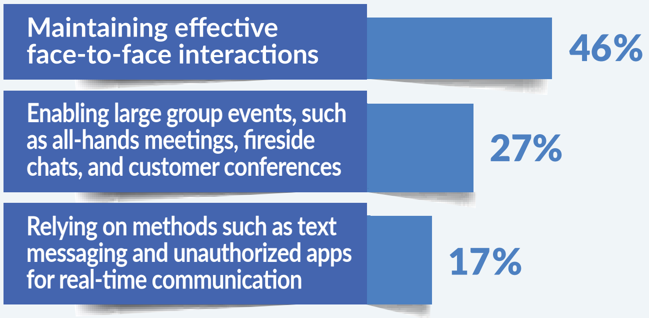
While all businesses have found a way to work remotely at this point, it has come at a price. **Thirty-five percent of respondents said they were facing cost issues with their remote access strategy and/or performance issues leading to poor end-user experience.**

Remote Collaboration

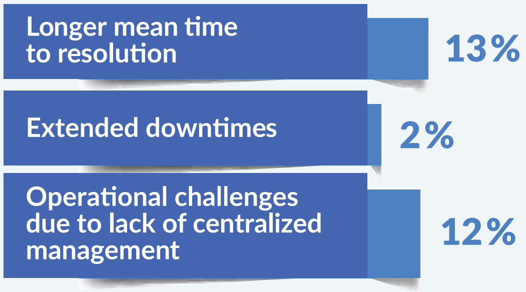
With so many people working away from the office, collaboration and productivity will decrease unless proper tools and processes are provided. The survey responses bear this out, as **46% of respondents reported having issues maintaining effective face-to-face interactions.** Nearly 17% began to experience shadow IT as employees began relying on text messaging and over a quarter (27%) said they struggled with large group events like all-hands meetings and customer conferences.

Remote working has affected more than just employee productivity. Those tasked with providing technical support—help desk operators, IT support resources, and support services managers—have found their jobs harder to do in a remote environment, which has led to slower response times and longer mean time to resolution (MTTR). **In fact, 26% indicated they were having management issues resulting in longer MTTR,** extended downtimes, and/or operational challenges due to a lack of centralized management.

Employee and customer communications challenges:

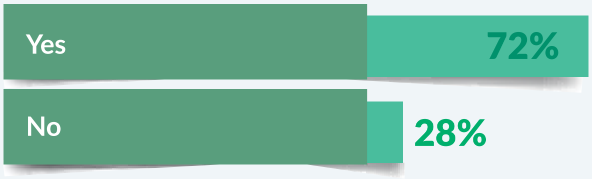


Business impact of remotely-distributed IT support teams:

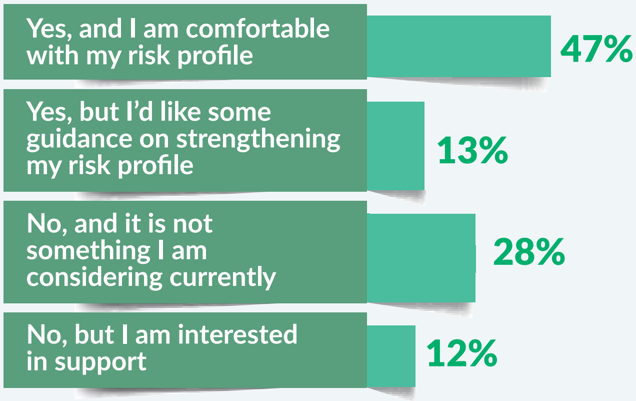


Security Risk and Vulnerability

Are you using multi-factor authentication (MFA) for remote users?



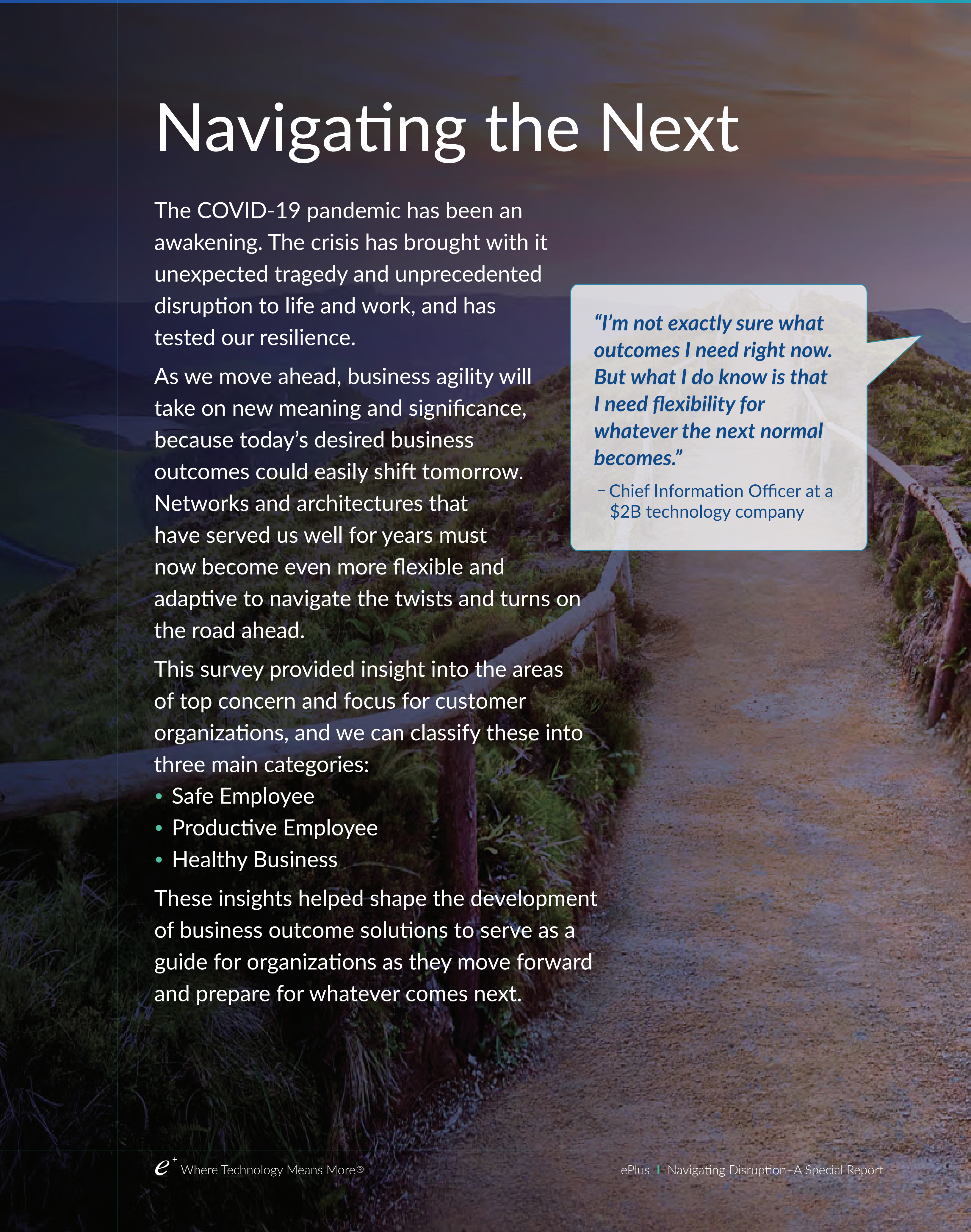
Have you reassessed your compliance and risk profile (including the profile of key partners/suppliers) after enacting your COVID response plan?



During the early phase of the pandemic, business survival was paramount. Workloads were moved to the cloud. Users were given remote access and rights to data as needed to keep operations going, perhaps in some cases at the expense of normal security protocols.

Results from the survey showed that 72% of the organizations use multi-factor authentication (MFA) to guard against unauthorized access to data. But even with MFA, over half of the organizations (57%) were only somewhat confident that the security controls they had in place could protect them.

This lack of confidence has led many companies to step back and reassess their security profile in light of the many changes brought on by COVID-19. But not all of them. In fact, 40% of organizations indicated they had not reassessed their risk profile. And of those, 25% did not feel they had the skills in-house to do it themselves and would likely seek assistance from a qualified security consulting firm.



Navigating the Next

The COVID-19 pandemic has been an awakening. The crisis has brought with it unexpected tragedy and unprecedented disruption to life and work, and has tested our resilience.

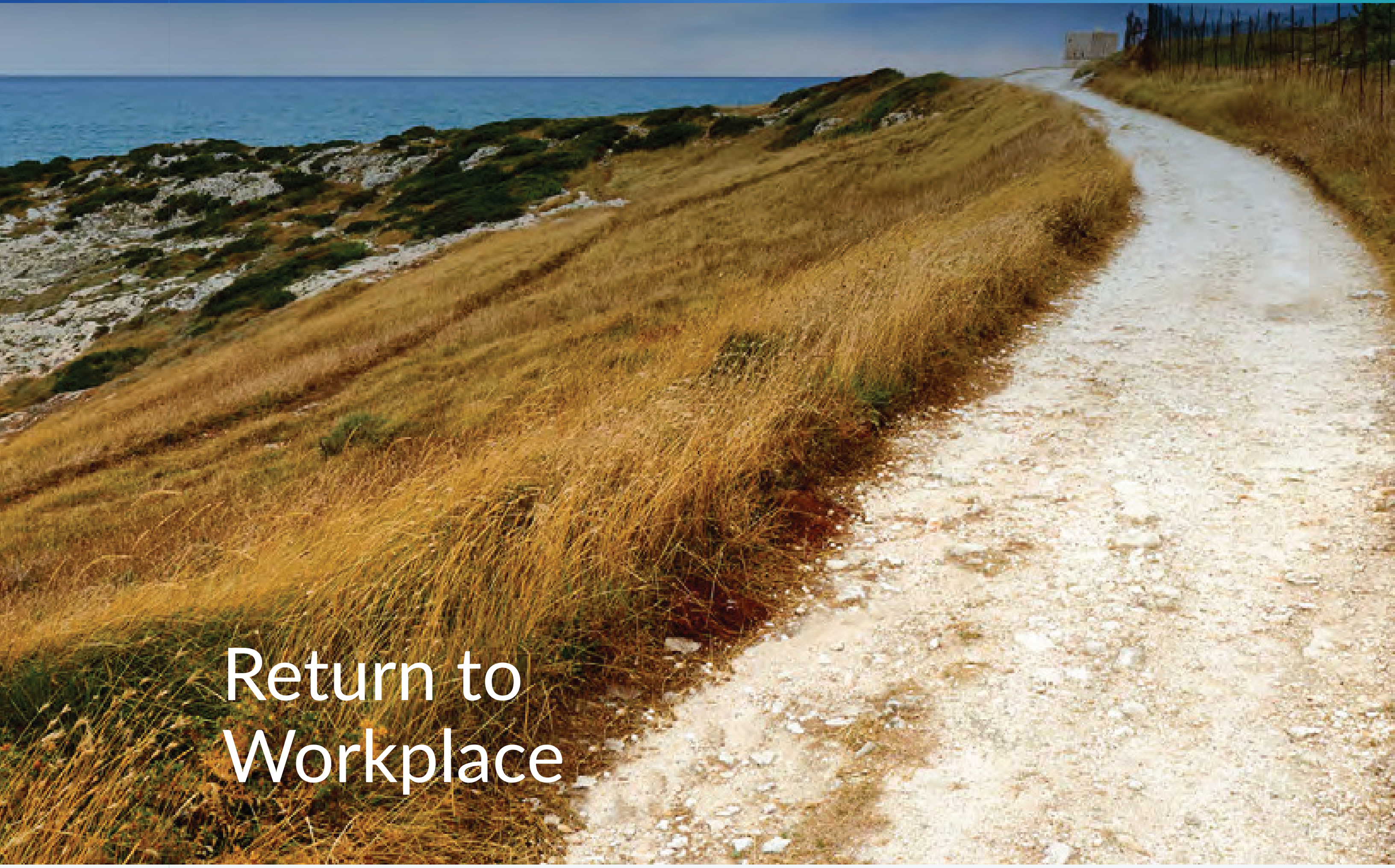
As we move ahead, business agility will take on new meaning and significance, because today's desired business outcomes could easily shift tomorrow. Networks and architectures that have served us well for years must now become even more flexible and adaptive to navigate the twists and turns on the road ahead.

> *"I'm not exactly sure what outcomes I need right now. But what I do know is that I need flexibility for whatever the next normal becomes."*
>
> – Chief Information Officer at a $2B technology company

This survey provided insight into the areas of top concern and focus for customer organizations, and we can classify these into three main categories:

- Safe Employee
- Productive Employee
- Healthy Business

These insights helped shape the development of business outcome solutions to serve as a guide for organizations as they move forward and prepare for whatever comes next.



Return to Workplace

Organizations must develop a plan to safely return to shared workspaces, leveraging new technologies, protocols, and procedures. A well-developed plan will:

- Ensure employee and customer safety
- Comply with health guidelines
- Reinforce social distancing
- Monitor building usage and track occupancy
- Maintain a productive work environment

The technology required to implement a physical safety program has been in existence for some time, but is now being extended across verticals. It relies on cameras, Wi-Fi-based location services and Bluetooth low energy technology that work together to track and monitor movement within a defined workspace.

This flexible technology allows for the amount of detail collected to be customized – from collecting anonymous statistical counts to individually identifying people at a site – and provides both real-time and historical analysis tools for businesses that are partially or fully reopening their offices.

In many cases, organizations already have the foundational technology implemented and in place to make this outcome a reality; it simply requires reconfiguring an existing network and equipment to support the additional functionality.

Assessing Your Current Security State

Part of developing a safe return-to-work plan, including the physical workplace monitoring piece described in the previous section, requires reassessing security. The operating environment is different now. Workflows, processes, and behavior have changed. Only 57% of organizations in the survey felt somewhat confident in their current controls and architecture, and 40% have not reassessed their security profile since the pandemic began. Given the potential security exposures, this is not good.

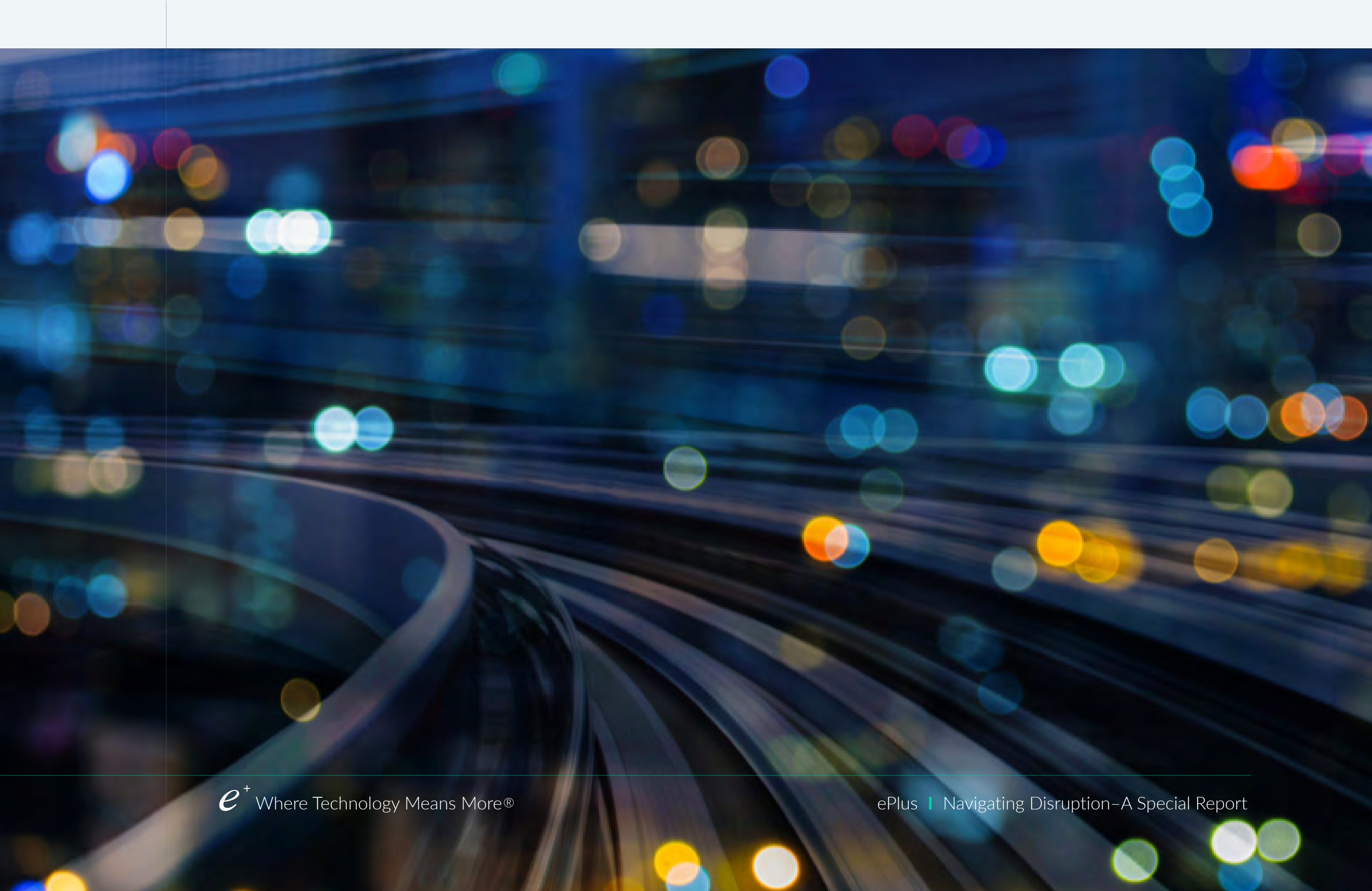
Risk profiles need to become continuous and adaptive. The pandemic brought with it a shift in risk—and risk will likely continue to fluctuate as we move forward. As a result, controls should be reviewed and adjusted, if necessary—and perhaps new controls should be added—to accommodate the new normal, which includes providing secure remote access for employees working from home or other locations.

57%

Of organizations in the survey felt somewhat confident in their current controls and architecture.

40%

Have not reassessed their security profile since the pandemic began.



Secure Remote Access

Remote work has become an integral part of our new business operating model and will not go away when the pandemic is over. According to a recent Gartner poll, over 80% of company leaders plan to permit remote work after the pandemic and there will be a significant increase in remote workforce across all industries moving forward, with 48% of employees likely to continue working remotely at least part of the time after COVID-19*.

Faced with these ongoing challenges, every organization must adopt a platform that provides secure access to core business applications and data without incurring unnecessary organizational risk. With significant uncertainty around the future of returning to work, it is critical to develop an agile approach to secure remote access and not over-invest in technologies or skillsets in an area that can change overnight.

A strong remote-access strategy includes leveraging both data center and public cloud platforms to enable the ability to rapidly expand, or “burst,” to tap into additional capacity only as it is needed. Implementing this sort of hybrid solution approach provides a consistent end-user experience that is also optimized for cost and security efficiency. The ability to utilize and pay for only what you need is a critical piece to building an agile and secure remote access strategy.

80%

Of company leaders plan to permit remote work after the pandemic.

48%

Of employees likely to continue working remotely at least part of time after COVID-19.

*Gartner, July 2020 Poll: https://www.gartner.com/en/newsroom/press-releases/2020-07-14-gartner-survey-reveals-82-percent-of-company-leaders-plan-to-allow-employees-to-work-remotely-some-of-the-time

Collaboration

Operating in a remote environment can take a toll on productivity and effectiveness. According to our survey, **46% of organizations were experiencing challenges maintaining face-to-face interactions**.

Although they may be working from home, workers need to interact and collaborate with team members and business partners. Communication is essential to a productive work environment and a sense of team and community for employees. Organizations need a technology platform with persistent chat, expanded video services, and collaboration tools to help foster a remote work environment that serves the needs of their company and their people.

Cloud Costs and Security

Data center capacity challenges caused **an increase in cloud spending for 25% of organizations in our survey.** And the trend is expected to continue as more organizations seek increased flexibility and agility. Accelerated cloud adoption is not always responsible cloud adoption and frequently lacks a mature cost optimization strategy and cloud security posture.

Expanding the use of cloud services requires architecture planning to avoid wasting resources, overspending, and introduction of security vulnerabilities. To that end, organizations should adopt a combination of tools and internal practices to continuously review their cloud costs and security posture.

Expense Management

As organizations continue to deal with the pandemic, a strong focus has developed on finding immediate efficiencies and cost savings. Whether optimizing cloud and telecom costs, using staffing to fill needs during hiring freezes, or leveraging creative financing programs to maintain innovation via new technology, a hardened focus on management of expenses will be paramount.

How to find out more

Across the country and around the world, ePlus is partnering with our customers to tackle tough problems and address shifting needs across the IT landscape. Our customers span nearly every industry vertical and face diverse challenges. Whether expanding their networks and security protocols or making their cloud spend more efficient, our customers recognize our unique qualifications and rely on us to help them navigate the road ahead.

We are available and ready to provide leadership, guidance and expertise to any organization trying to figure out how to navigate their next – whether that be a Return to the Workplace, providing Secure Remote Access, Optimizing and Minimizing Wasted Cloud Spend or building an agile foundation to enable reliable Collaboration tools.

To learn more about how ePlus can help you Navigate the Next, please visit: https://discover.eplus.com/navigate-the-next/home/.

About ePlus

ePlus is a leading consultative technology solutions provider that helps customers imagine, implement, and achieve more from their technology. With the highest certifications from top technology partners and lifecycle services expertise across key areas including security, cloud, data center, collaboration, networking and emerging technologies, ePlus helps organizations transform IT into a business enabler. For more information, visit the ePlus website at www.eplus.com.

Where Technology Means More®

Corporate Headquarters
13595 Dulles Technology Drive
Herndon, VA 20171-3413
Nasdaq NGS: PLUS

888-482-1122
info@eplus.com
www.eplus.com