SPONSORED CONTENT

IDG

Shifting Cybersecurity to Support the Expanded Remote Workforce

Survey points to growing need for managed security services

COMCAST BUSINESS

IDG Communications, Inc.

THE REMOTE WORKFORCE HAS EXPANDED DRAMATICALLY DURING THE COVID-19 PANDEMIC, likely causing long-lasting shifts in work patterns, physical office requirements, and demands on IT teams. Organizations are adjusting to support these changes, including reevaluation by IT organizations of how their current and future cybersecurity technology and policies will ensure their ability to secure the work environment.

A recent survey of IT decision-makers indicates that, on average, the number of remote workers will increase by almost a third this year and into 2021. The survey, conducted by IDG and Comcast Business, indicates that growth in the number of remote workers is causing most organizations to invest more in remote IT operations to support them and in cybersecurity to address the challenges of protecting against a growing threat profile.

The increase in remote work has also dramatically impacted cybersecurity policies and practices. More than half of the survey respondents indicated that they are reevaluating wide-area network (WAN) infrastructure and investments, accelerating deployment of new security technology, and adopting new approaches such as implementing "zero trust" policies.

"In early 2020, the initial challenge for IT was how to increase remote access capacity to support everyone working from home," says Shena Seneca Tharnish, VP of Cybersecurity Products for Comcast Business. "Once they got through those challenges, security became top-of-mind in order to protect data if employees are not on a virtual private network or using company-issued devices to access sensitive applications and data."

Enterprises indicated that they have a wide array of needed functions and services they expect from advanced cybersecurity solutions. Foremost is data loss protection (DLP), particularly for larger enterprises, followed by protection from denial-of-service and distributed-denial-of-service attacks.

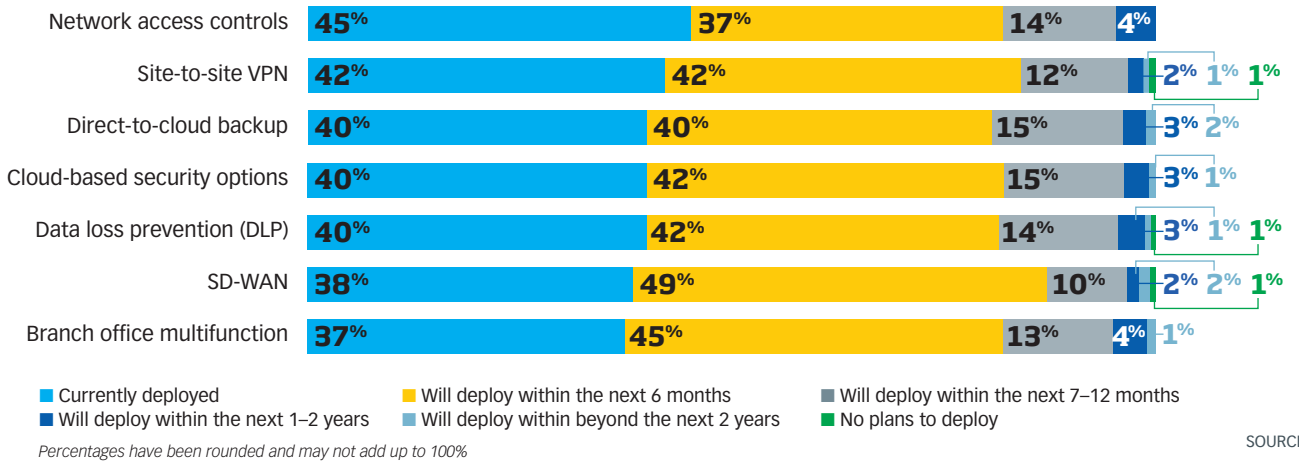
Those that are supporting a greater share of workers remotely are much more likely to have already deployed advanced WAN solutions such as DLP, network access controls, direct-to-cloud backup, and software-defined WAN (SD-WAN), among others. Most of those with fewer remote workers plan to deploy these within the next year.

Some Cloud Security Challenges

Cloud services have played a large role in enabling the rapid expansion of remote work. Companies that support a larger remote workforce are hosting a significantly greater proportion of their applications in the cloud—73% of those with a greater number of remote workers said that more than half of the applications are cloud-hosted, compared to 38% of those with fewer remote workers.

Reliance on the cloud does come with new security challenges, however, with 98% saying that securing applications, data, and infrastructure in the cloud is very or somewhat challenging. Almost all organizations (95%) feel that their current security infrastructure impedes their ability to protect data as it moves to and from the cloud. However, confidence in how secure cloud infrastructure, data, and applications are is split almost evenly among those who are confident (51%) and those only somewhat confident (44%).

FIGURE 1: **HAVE YOU DEPLOYED OR ARE YOU PLANNING TO DEPLOY ANY OF THE FOLLOWING AS PART OF YOUR WAN STRATEGY?**



Percentages have been rounded and may not add up to 100%

SOURCE: IDG

With growth in remote work enabled by and dependent on greater utilization of cloud resources, IT teams are investing in multiple ways to architect their cybersecurity stance.

Organizations in the survey have a broad spectrum of concerns regarding cloud-based security. Topping the list are data theft (36%), lack of staff skilled to manage security for cloud applications (36%), and fear that cloud application providers could face advanced threats (35%). Tharnish says those concerns could point to the need for unified threat management (UTM) solutions, both on premises and in the cloud.

Securing the Changing Workforce

Dozens of organizations have already indicated that remote work is a long-term, if not permanent, proposition. With growth in remote work enabled by and dependent on greater utilization of cloud resources, IT teams are investing in multiple ways to architect their cybersecurity stance as they continue to build up WAN infrastructure while accommodating larger numbers of remote workers. To achieve flexibility, agility, and redundancy, most companies are adopting multicloud or hybrid cloud environments, and their networking and security architectures must evolve accordingly.

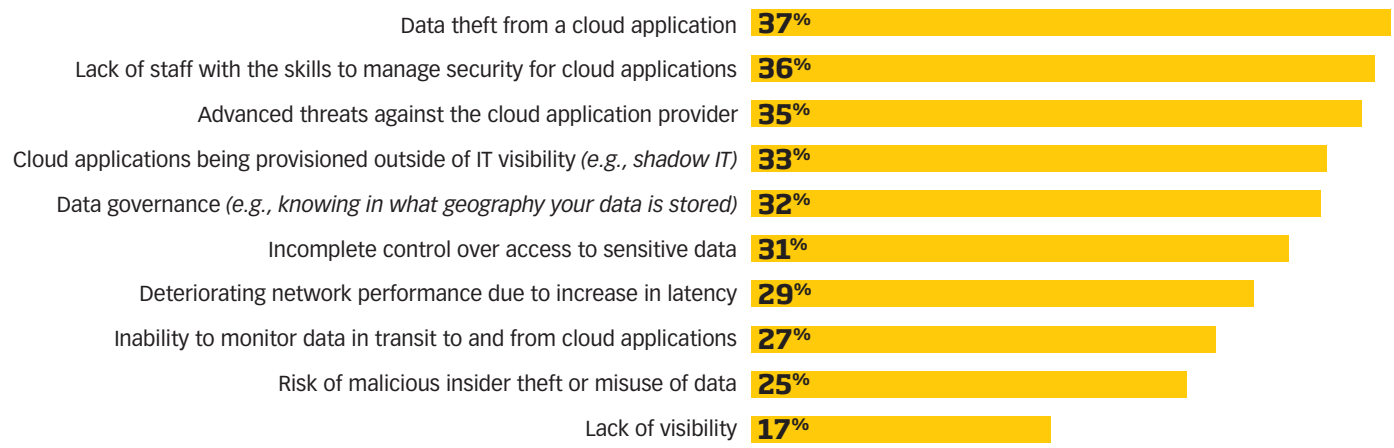
As a first priority, companies need to protect access to the network and deliver secure transport. Secure gateways are by far the most commonly utilized network security solution, in use at 72% of the organizations that participated in the survey. Site-to-site VPNs are in use by 52%, and fewer are using application-aware firewalls (37%), network access controls (37%), and other solutions.

Many companies are eliminating a single point of failure, by spreading traffic, applications, and services over multiple clouds and SaaS services, which may make it more difficult to secure such environments. One way to skirt that issue is to segment different parts of the network and applications, based on their sensitivity and priority—that is, different infrastructures are used for compliance-related or mission-critical data and applications. Companies can thus effectively grant access to cloud resources without leaving themselves exposed.

To be able to segment networks and access, companies need a flexible network infrastructure based on SD-WAN. Current networking technologies connecting multiple clouds are struggling with the underlying transport's lack of awareness of different types of applications. SD-WAN provides application-aware networking to maximize the use of available resources, network conditions, and capacity; segment out and control unimportant traffic; gain visibility into traffic patterns into various clouds; and understand end user experience in order to deliver consistent performance for an organization's critical applications.

SD-WAN solutions also enable companies to move away from the "tyranny of the boxes." In the past, as new security capabilities and needs emerged, organizations typically installed new hardware-based appliances in offices and locations. At its best, this approach enables a buy-as-you-go approach to building a security architecture; at its worst, it results in a stovepiped array of hardware that is hard to integrate and requires specialized skills for each type.

FIGURE 2: **WHAT ARE YOUR BIGGEST CONCERNS ABOUT CLOUD-BASED SECURITY, IF ANY?**



SOURCE: IDG

SD-WAN platforms allow for the deployment of multiple virtualized functions on a single box. Thus, on-premises UTM solutions are becoming more manageable and cost-effective options with the emergence of universal customer premises equipment (uCPE) managed solutions. These appliances are able to run multiple security solutions as virtual network functions (VNFs), such as both a router and a next-generation firewall (NGFW) alongside an SD-WAN on the same device.

In addition to cutting down the number of devices and the effort required to manage provisioning and updating, uCPE solutions can be reconfigured so that organizations can swap out functions that aren't meeting their requirements and swap in new best-of-breed options. Provisioning of remote sites and branch offices can be centrally managed, with VNFs automatically pushed out to individual devices.

Bring Remote Workers into the Security Fold

With so many employees now working outside enterprise locations, on-premises security solutions will take on a different role and IT teams will need to rethink traditional security approaches.

One of the options IT teams have in securing the remote workforce is in shaping how those workers access cloud services. UTM can embrace workers who tunnel into hubs via VPNs and then access the applications securely as if they were on premises and within the network perimeter.

The spike in remote work has overwhelmed VPNs in some cases, with many companies struggling to add capacity and competing for services and equipment with many other companies that are facing the same hurdles. In some cases, IT may deem some applications not sufficiently critical to justify adding to VPN burdens. By allowing remote workers to go directly to less sensitive but secure cloud services without having to access VPNs, many organizations are able to alleviate that issue.

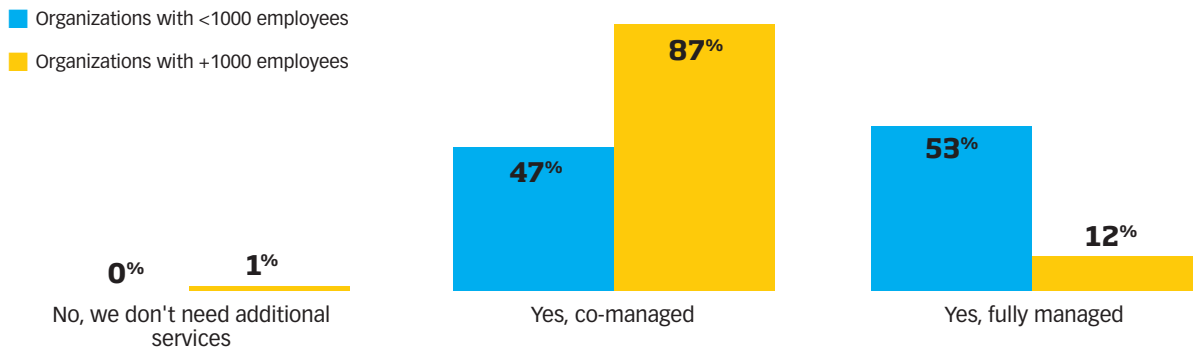
Multi-cloud deployments won't reach their full performance potential if networking and security are separated.

"SD-WAN provides companies with the ability to control where traffic goes or to police traffic locally," Tharnish explains. "One of the key benefits of SD-WAN is that it can be implemented on top of any broadband or Ethernet connectivity. For IT managers, it's a more agile option than MPLS [multiprotocol label switching], because you can prioritize and shape traffic in a way that directs certain less vital data over less reliable connections so you can treat the most important traffic more sensitively."

In other cases, the data flow from the remote work location to the central hub, to the cloud, and back again may result in latency and application responsiveness issues. An improved user experience may justify a direct-to-cloud approach, and IT will have to adopt secure cloud environments based on the sensitivity of the data and applications at issue.

Naturally, there are fundamental differences in architecture between on-premises, hybrid cloud, and multicloud deployment models, and it's important for security to be integrated with the network layer. Multicloud deployments won't reach their full performance potential if networking and security are separated. If each layer uses different technologies from different vendors, it may make deployments more vulnerable to attacks. Network monitoring capabilities based on SD-WAN would provide for central oversight and coordinated response while maintaining segmentation of the network traffic flowing between applications and workloads across the multiple clouds.

FIGURE 3: **DOES YOUR ORGANIZATION NEED MANAGED CYBERSECURITY SERVICES TO MEET REMOTE WORK REQUIREMENTS IN THE NEXT 12-18 MONTHS?**



SOURCE: IDG

Advanced technologies are the top-ranked characteristic that respondents are looking for in managed cybersecurity solution providers.

Enabling Enterprise Bandwidth at Home

Whether focusing on VPN or cloud access, IT must also face the reality that some workers lack connectivity or sufficient bandwidth. With whole families at home during the pandemic, everyone trying to access online services at the same time can often result in a less-than-optimum connection.

Working with the right service providers, businesses can opt to provide workers with dedicated in-home, enterprise-grade connectivity that is separate from their residential network to increase productivity and flexibility while also offering cybersecurity solutions.

Weighing Your Managed Security Options

The IDG survey found that survey participants, on average, rely on 10 vendors for their cybersecurity needs. The greater the number of solution providers, the more time IT leaders will have to spend managing them and pinpointing gaps between vendors and sorting out finger-pointing when something goes wrong.

Integrated or bundled cybersecurity managed solutions will increasingly provide a simplified model for improved cybersecurity defenses., Among the survey respondents, 99% indicated that they will need managed cybersecurity services as they expand remote work capacity.

Managed security services can build out a security overlay enabling organizations to extend data protection across the changing remote workforce, but most of those surveyed indicated that they want a comanaged arrangement. That's particularly true of companies with more than 1,000 workers, whereas smaller companies are almost evenly split in their preference for fully managed (53%) and comanaged (47%).

"Larger companies want the flexibility and speed of being able to make one-time changes, such as temporarily changing a firewall to accommodate a partner, but they want a service provider to handle issues such as a global rollout," says Tharnish. "Smaller businesses that don't have the technology resources to make even small changes are more inclined to opt for a fully managed service."

One factor driving the need for managed cybersecurity services is the need for always-on expertise and support. Survey participants report a wide array of services they need from such service providers, with disaster recovery and business continuity rated highest, at 43%. Other areas that top their priority list are getting guidance from experts (40%) and managed detection and response (36%).

Advanced technologies are the top-ranked characteristic that respondents are looking for in managed cybersecurity solution providers. Second is an established vendor with a proven track record, although they aren't necessarily inclined to look for a trusted partner from previous engagements.

Ensuring reliability, security, and connectivity for remote work

The full extent and impacts of the rapid shift to remote work may not be known for years. But the blurring of lines between work and home has conclusively demonstrated the need to increase reliability, security, and connectivity for workers away from the traditional office.

Comcast Business' full suite of network solutions, expert engineers, and award-winning business tools and services are available to make sure businesses remain connected, secure, and agile as the remote work environment evolves.

Learn More About Comcast Business Solutions