SPONSORED CONTENT

IDG

As Enterprises Transform, So Does Edge Security

Balancing risk and security keeps IT teams on alert as they speed adoption of zero trust and SD-WAN and lean on service providers to aid integration and visibility.

COMCAST BUSINESS

IDG Communications, Inc.

BUSINESSES THAT HAVE UNDERGONE RAPID DIGITAL TRANSFORMATION IN THE PAST 12 TO 18 MONTHS ARE RETHINKING THEIR SECURITY STRATEGIES.

Data increasingly resides outside of the traditional data center and IT is under pressure to provide ready access to business users who are often working outside of traditional office space. That's causing substantial reprioritization of cybersecurity approaches and technology solutions.

A recent IDG and Comcast Business survey of 131 IT leaders in IDG's TechTalk Community indicates that more than half of midsize and large enterprises recognize that traditional security postures are not a good fit for the demands of a widely connected, cloud-focused organization. The increased need for connected business solutions has prompted growing dissatisfaction with a patchwork of existing network security components that do not align well with cloud components.

Increasingly connected and feeling vulnerable

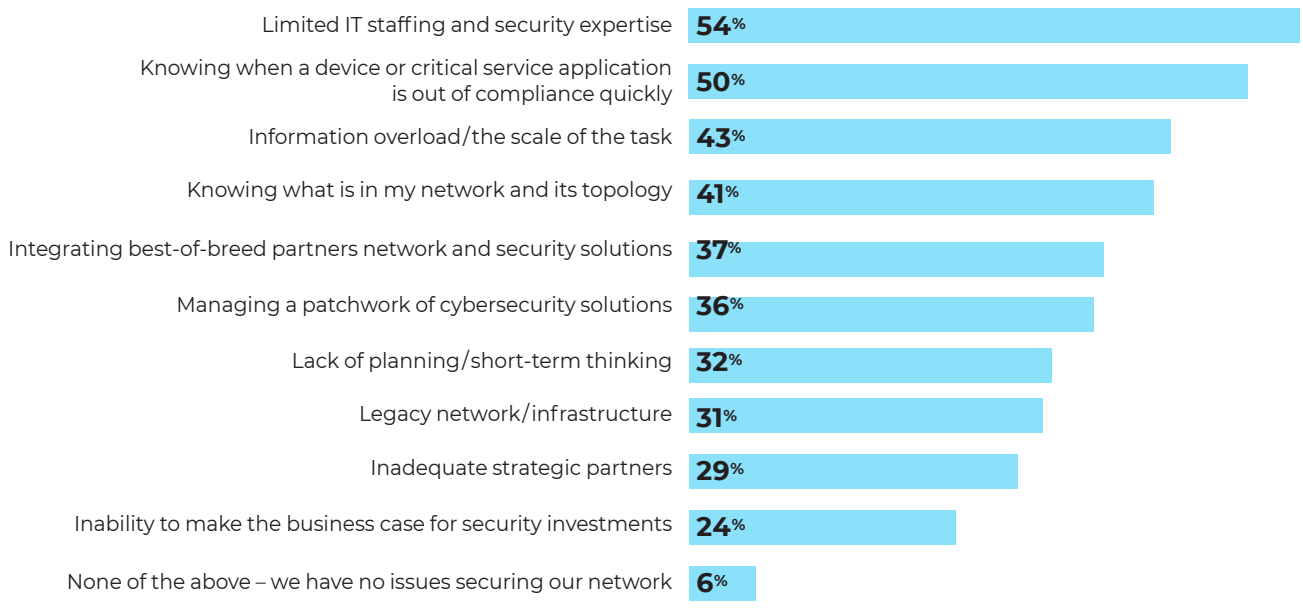
Many organizations are still grappling with how the COVID-19 pandemic has impacted demands on IT. More than a third of the surveyed organizations said that the acceleration of digital adoption over the past 12 months has gone hand in hand with the increased prioritization of security. Among that group, the top factor driving that heightened priority, cited by 48%, is enabling a remote or hybrid workforce.

Not surprisingly, the familiar woes of limited IT staffing and security expertise were cited as the leading impediment to ensuring that on-premises and cloud networks are secure. Related to that, information overload and the scale of the task are issues for 43% of those surveyed.

Given the frequency with which skill sets and expertise show up in IT security surveys, that may be a prime area for reevaluating traditional approaches, according to some industry experts. "We're not going to solve this problem by throwing bodies at it," says Pete Lindstrom, vice president of research for Enterprise and NextGen Security with analyst firm IDC. Instead, he says, organizations and the industry need to take advantage of automation and scalability being applied across other areas of IT.

FIGURE 1: **KNOWING THE NETWORK AND MANAGING POINT SOLUTIONS ARE KEY ISSUES THAT COMPOUND STAFFING/OVERLOAD AND COMPLIANCE ISSUES**

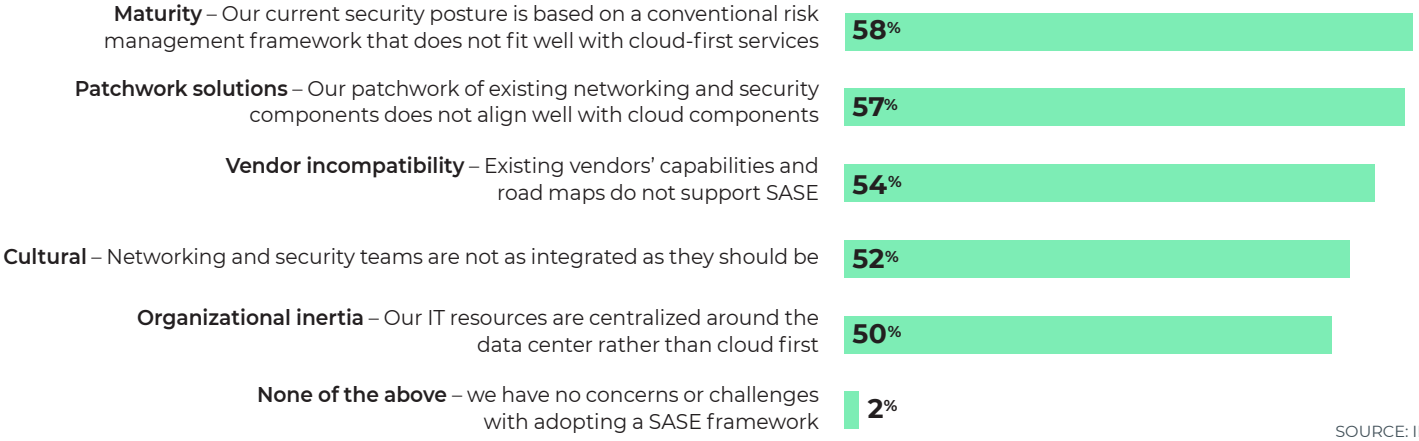
Challenges faced in securing the network



SOURCE: IDG

FIGURE 2: **ALL SASE-RELATED ISSUES ARE SHARED BY AT LEAST HALF OF ORGANIZATIONS**

Challenges to adopting SASE



SOURCE: IDG

Adapting to new challenges

IT organizations are rising to the challenges by investing in edge security solutions that help protect users and systems beyond the reach of traditional enterprise security, such as enhanced cloud security services and software-defined wide-area network (SD-WAN) services. They are increasingly adopting the "zero-trust" approach to network architecture, requiring verification of anything touching or trying to connect to systems from inside or outside the network, rather than assuming that they are trusted entities.

Most respondents have already deployed or plan to deploy key network security solutions such as SD-WAN, which 89% indicated has become a higher priority, 71% have already adopted, and 26% plan to adopt within six months. "Those are incredible adoption numbers," says Martin Capurro, vice president, Managed Services, with Comcast Business. "SD-WAN lets you do smarter things with traffic routing so critical business applications are available to customers and employees. The SD-WAN function and the security function go hand in hand."

Close on the heels of SD-WAN is data loss prevention services, which 67% of the respondents have already adopted and 31% plan to deploy within six months. Other network security services also gaining popularity are secure web gateways, endpoint detection and response, and cloud access security broker (CASB), among others. Those technologies are often tabbed as components in a loosely defined framework of cloud-based network security known as secure access service edge (SASE).

Survey respondents, however, are finding that conventional risk management frameworks and a patchwork of network and security components do not naturally fit with a cloud-oriented posture.

Midsize companies seem to be having a tougher time than larger enterprises in grappling with a patchwork of existing networking and security components that do not align well with cloud components.

"SASE is a viable concept to help protect the edge, but I also think it's a buzzword that is overused," says Shena Seneca Tharnish, vice president of Cybersecurity Products at Comcast Business. "A lot of the technologies within the SASE framework have been around for a long time, but IT teams are starting to evaluate how they can apply these to secure a business from end to end as more applications and users are shifted outside of the traditional perimeter."

As they adopt newer approaches embracing edge security and zero trust, organizations are also increasingly reliant on managed services providers (MSPs) to help them meet top security challenges as they expand their use of connected business solutions.

IT organizations are relying on MSPs to fill critical gaps, such as quickly spotting when a device or an application is out of compliance. Another critical visibility issue is simply knowing what is in the network and its topology.

"Zero trust is all about being aware of where the data is located and then looking not only at the network but also at the identities of the users at the end of these devices and systems and applications," says Tharnish. "I'm hearing from companies engaged in zero-trust journeys that one of the biggest challenges is they can't protect what they can't see. There also are many legacy devices and systems out there that don't have the modern capabilities to implement zero trust."

Knowing quickly when a device or a critical service application is out of compliance is the top driver among companies currently using MSPs or planning to use them for network security issues. Survey respondents want help managing the growing patchwork of cybersecurity point solutions, understanding what is on the network, and integrating the best network and security solutions.

Comcast's Capurro says enterprises want to consume enterprise security just like other cloud services, rather than owning and managing it themselves.

Milestones for achieving a new cybersecurity posture

Understanding the need for a new approach to cybersecurity is but one step on the road to achieving it. For most of those surveyed, for example, zero trust is more aspiration than reality. Just 2% said they are monitoring or maintaining a zero-trust architecture. Most are updating current architecture (59%) to integrate a zero-trust approach or are working on implementation plans (39%).

In many other areas, though, implementation of modern network security services is well under way across companies of all sizes. These services comprise foundational elements of SASE and other edge security protocols. Larger enterprises are significantly ahead in deployment as midsize companies try to catch up.

Larger companies are also substantially ahead in adoption of SD-WAN, a relatively new technology that, in comparison to what surveys in 2017 and 2019 revealed, has grown by leaps and bounds over the past four years. This likely reflects a shift from early do-it-yourself implementations toward greater reliance on managed SD-WAN services.

At the opposite end of the scale, perhaps surprisingly, similar percentages of midsize and larger enterprises, 39%, have adopted security information and event management (SIEM) solutions, a technology more typically associated with large enterprise networks. However, like so many other technologies, SIEM solutions have evolved into cloud-based software-as-a-service solutions that are easier to acquire and consume than more traditional on-premises versions.

Just 12% of those surveyed by IDG/Comcast Business said they self-manage SIEM or plan to do so within the next six months; 41% said they currently utilize fully managed solutions or are going to, and 47% do or will rely on comanaged SIEM.

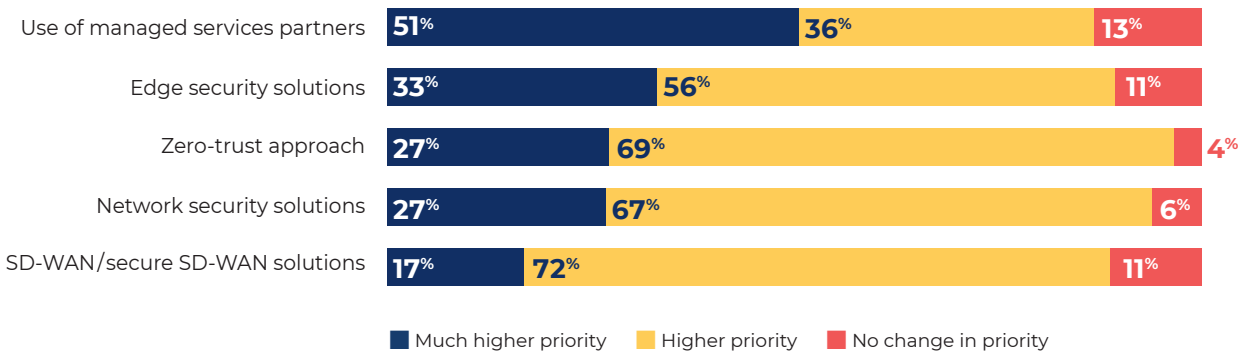
Overcoming challenges on the path forward

As hybrid work solidifies into a permanent reality and organizations rely on broader portfolios of cloud services, the convergence of networking and security solutions for the edge seems certain to dominate IT strategies for many years to come. Over the short term, survey respondents are inclined to seek bundled network and security solutions from trusted vendors.

It is also likely to take years of effort to overcome critical gaps in cybersecurity defenses spurred by the rapid transformation that enterprises experienced during the last two years. Part of the challenge is the effort involved in shifting from a data-center-oriented security perspective to that of a cloud-and-edge security perspective. After all, so much of business still revolves around data center constructs, even if they've been lifted-and-shifted to the cloud.

FIGURE 3: **THE INCREASED NEED FOR CONNECTED BUSINESS SOLUTIONS MADE USING MSPs A MUCH HIGHER PRIORITY**

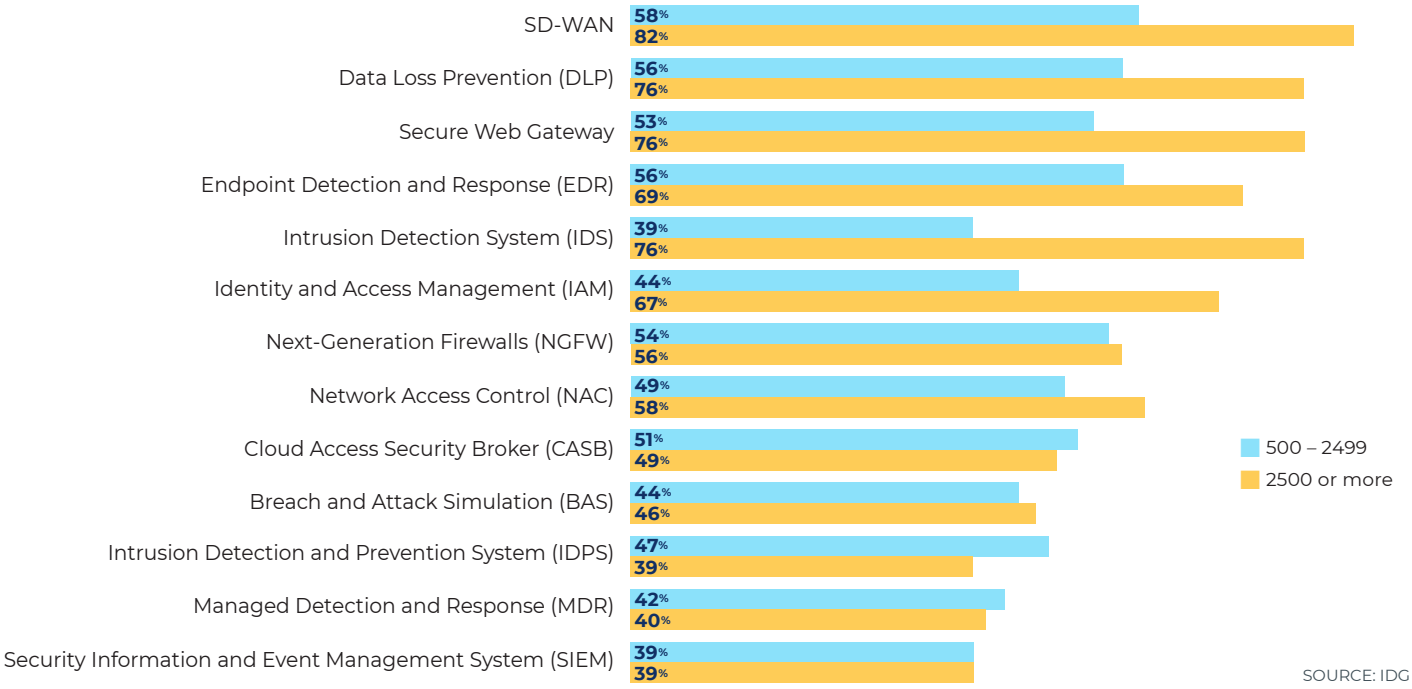
Organizations reprioritze their cybersecurity approach



SOURCE: IDG

FIGURE 4: **NOT SURPRISINGLY, LARGER ORGANIZATIONS ARE FURTHER ALONG THE ADOPTION CURVE FOR MANY SASE-RELATED SERVICES**

Currently deployed network security services (by company size)



SOURCE: IDG

That centralized perspective also pertains to traditional risk management strategies. "The big shift here is moving from a paradigm of compliance with a bunch of items in a checklist to a more structured approach to risk measurement," says IDC's Lindstrom. "Our technical architectures have changed. The approach should really be one of cybersecurity efficacy, where we're looking at runtime-based inline security as the preeminent driver for our risk levels rather than this traditional idea that if we could just get our policies, procedures, and processes just right, we'd be good to go."

Capurro of Comcast Business says that the experience of COVID-19 may be instrumental in accelerating a redefinition of acceptable risk. "Through the pandemic, we were all trying to manage risk and security, but we had to make some very real-world decisions in terms of what's the right balance between secure enough and productivity," he points out.

"It's not a question of 'Is it secure or is it not secure?'" Capurro adds. "It's what do you have to do to function in this new world and what is the right level of risk. We should always strive to do better, but it's not just an on-or-off issue — it's what is the right amount of security in the right place at the right time."

What is clear is that organizations have a growing repertoire of cloud-based network security tools on which to build a flexible, adaptive risk management security architecture for the future. The emergence of software-defined network elements, identity authentication technologies, microservices, and segmentation provides crucial building blocks for building a modern cybersecurity approach that can embrace hybrid work, myriad cloud services, and connected business solutions.

Learn about Comcast Business cybersecurity services.