Publication date:
January 2025

Author:
Fernando Montenegro

The State of Workforce Security: Key Insights for IT and Security Leaders

OMDIA

paloalto NETWORKS

Contents

Summary

Organizations' growing reliance on changing technologies means a growth in the importance of cybersecurity. That said, any cybersecurity initiative must be practical and tailored to meet the organization's actual needs. This study, commissioned by Palo Alto Networks, explores how these needs have been changing and how security has fared, and it considers possible paths for evolution.

The modern workplace has undergone significant transformation, characterized by at least three major shifts. First, there has been an increase in remote work adoption, even if there is some post-pandemic pushback. Secondly, numerous organizations have adopted a mixture of managed and unmanaged devices, like bring your own device (BYOD), in their environments, which brings challenges for security compliance. Finally, there has been a dramatic rise in the use of software-as-a-service (SaaS) consumption, with some organizations reporting thousands and tens of thousands of applications being used. A key factor in the use of these applications is that they're often accessed via browsers—the study finds that, in some cases, browser-based usage corresponds to over 80% of daily work.

This study also highlights some of the challenges facing security programs. First, responses indicate that traditional security controls are unevenly deployed, with very few organizations reporting widespread coverage across their IT estates. This results in potential gaps in visibility and protection. At the same time, there is constant pressure to deploy security controls in a way that does not affect worker productivity. Then, responses indicate that even when the controls are being widely deployed, the prevalence of security incidents remains high, with incidents such as ransomware, phishing, and browser-based attacks reported by over 90% of respondents.

Two technologies are worth considering when looking at possible ways to move forward: secure access service edge (SASE) and secure browsers. SASE offers a way to optimize the delivery of security and networking functionality across the enterprise network from a cloud-delivered perspective. Secure browsers, on the other hand, can deploy several security controls close to the user without disrupting their productivity.

As organizations consider the multiple moving parts of their security programs—everything from business alignment, optimizing the use of resources, maintaining security systems to operate efficiently, supporting user productivity, and more—the use of technologies such as SASE and secure browsers can play a critical role.

Introduction

Change, constant change: if there is one aspect of cybersecurity that professionals can count on, it is, ironically, the continual change to which teams must respond.

Organizations are embracing increasingly complex supply chains that involve both physical and digital partners. These partnerships—with the organization sometimes as a supplier, sometimes as a consumer, often as both—come with an increasingly complex technological footprint. These collaborations result in changes to the organization's workforce—for example, with the increasing number of contractors and hybrid workers—as well as changes to how the organization deploys technology.

Change is also attributed to the effects of cybersecurity's heightened demands, both from the perspective of being more deeply integrated into the organization—in security functionality and user experience—as well as dealing with a shifting threat environment. Security teams are also more commonly understaffed, and are continuously asked to "do more with less," seeking assistance in the form of tech solutions that help enable them to do so.

This paper provides insights from Omdia's research, commissioned by Palo Alto Networks, to examine these changes. It explores modern work processes, how cybersecurity has been deployed, what kind of threats are present, and more. It also highlights the necessity of using stronger, more secure browsers as a valuable component in this environment.

The data for this research comes primarily from two end-user surveys conducted in early and mid-2024. Please refer to the appendix for further information on methodology, sample sizes, and general demographic and firmographic information.

Embracing the SaaS-driven future of work

Build a resilient, hybrid workforce

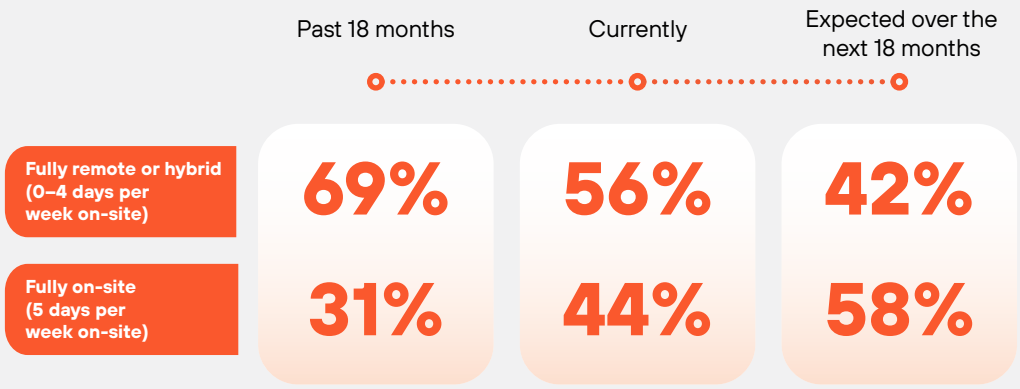
For most organizations, "digital transformation" was already a catalyst for change. The 2019 pandemic accelerated those efforts around digital transformation trends in multiple ways. It emphasized the importance of increasingly complex supply chains and displaced significant portions of the workforce. While some of that displacement appears to be receding (see **Figure 1**), it has altered the very makeup of the modern organization: the workplace is now hybrid, with a combination of fully remote, fully on-site, and hybrid workers.

Currently, the average workforce consists of 31% hybrid workers and 25% fully remote workers; even if many are expected to be back on-site in the next 18 months, 42% of employees will be remote in some way.

EVEN IF MANY ARE EXPECTED TO BE BACK ON-SITE IN THE NEXT 18 MONTHS, **42%** OF EMPLOYEES WILL BE REMOTE IN SOME WAY.

Figure 1: The shifting nature of the workforce

What proportion of your total workforce (employees and contractors) is estimated as... (average)



Notes: N=514 IT/security decision makers

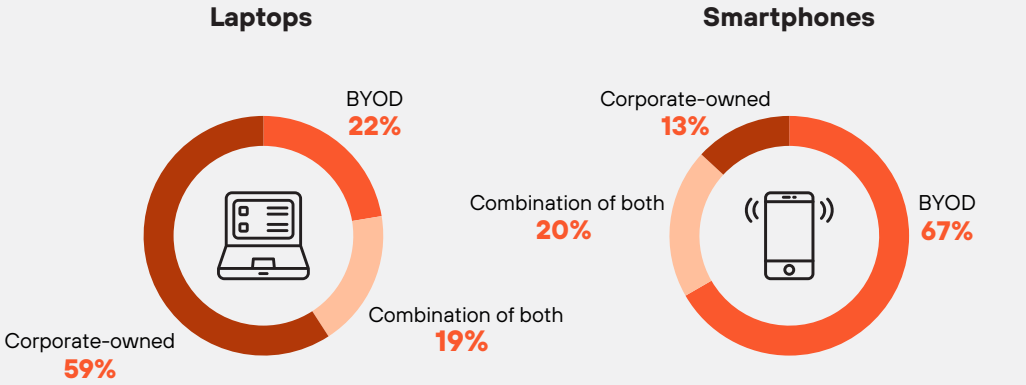
Source: Omdia

Address the prevalence of BYOD in your IT environment

Omdia's *2024 Employee Collaboration and Productivity Survey* includes relevant details that point to most organizations having a hybrid IT estate when it comes to ownership of laptops and mobile devices (see **Figure 2**).

Figure 2: Use of BYOD for laptops and smartphones

What is your organization's approach to providing employees with mobile devices?



Source: Omdia

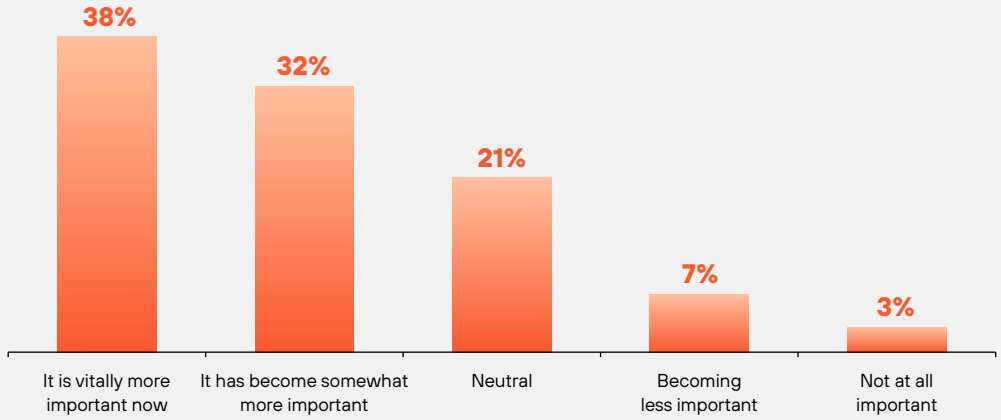
It's important to note that the use of BYOD devices for smartphones is significantly larger than for laptops.

Support for mobile devices is also seen as a critical component of employee productivity. According to the same survey, almost 70% of respondents indicated that the use of mobile devices has increased in importance over the past two years (see **Figure 3**). Currently, organizations are mostly handling the security of these BYOD devices by completely blocking access to corporate resources: 70% of respondents say that at least 50% of their BYOD mobile devices do not have any access to corporate resources.

97% OF ORGANIZATIONS BLOCK ACCESS TO CORPORATE RESOURCES ON SOME PROPORTION OF BYOD MOBILE DEVICES.

Figure 3: The importance of mobile collaboration

How has the importance of enabling your employees to communicate and collaborate via mobile devices (not just PCs) changed over the past two years?



Notes: N=514 IT/security decision makers

Source: Omdia

Key takeaway

Hybrid work will remain prevalent, with 42% of employees expected to work remotely in some capacity, emphasizing the need for organizations to adapt to a permanently hybrid workforce using a combination of laptops and mobile devices. While this need for collaboration increases, organizations inversely block access—preventing the very collaboration they're trying to emphasize.

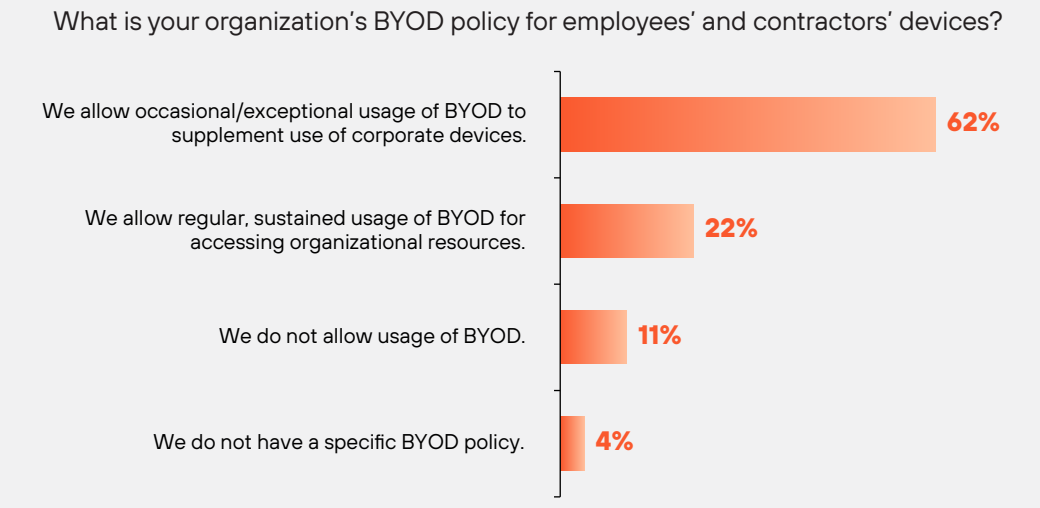
Secure access for a diverse, dynamic workforce

Another change is that work and careers today are much more dynamic—this includes employees' tendency to have shorter tenures, an increase in those working as independent contractors, and more. This means, for example, that organizations have a larger proportion of temporary or contract staff: respondents indicate that nearly 30% of their organization's workforce, on average, is made up of contract or temporary staff. Whether it is a personal device owned by a contractor or a managed device owned by a third-party firm, all of these external employees often require access to internal applications and data.

Adding to this scenario of a diverse workforce, organizations now also support the use of mobile devices (e.g., smartphones and tablets), and increasingly support BYOD general-purpose computers. These options usually extend to both regular employees as well as contractors. Only a small fraction of respondents, 11%, indicated that they explicitly do not support BYOD (see **Figure 4**).

98% OF ORGANIZATIONS REPORT SOME LEVEL OF BYOD POLICY VIOLATION AMONG THEIR EMPLOYEES.

Figure 4: BYOD policy for employees and contractors



Notes: N=514 IT/security decision makers
Source: Omdia

This number varies by industry, size, and other factors; for example, more regulated industries, such as financial services or government, tend to be more likely to block BYOD. Still, it is common to have organizations allowing some sort of access to corporate data from BYOD endpoints. A prudent security design will take into account that, even if a policy exists, there is a non-negligible chance of access to corporate resources from BYOD devices, be they personal devices or those from contractors.

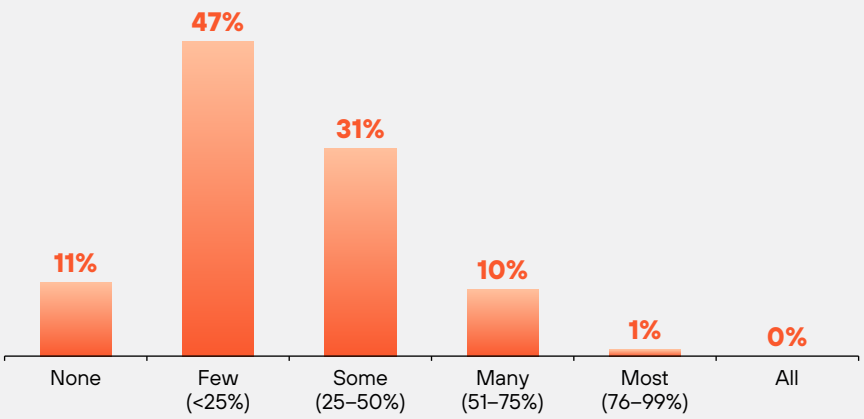
Looking at it from a different perspective—the proportion of individuals accessing corporate applications from personal devices—it is common for organizations to allow access (see **Figure 5**). The vast majority of organizations allow access to corporate applications and data from mobile devices and tablets, but they do so while enforcing some controls on large swaths of their user population. According to respondents, approximately 70% of organizations block some access to 50% or more of their user population.

This creates a potential issue as some controls may impede productivity.

APPROXIMATELY **90%** OF ORGANIZATIONS ARE ENABLING ACCESS TO CORPORATE DATA FROM PERSONAL DEVICES.

Figure 5: Access to corporate data from personal devices

What proportion of employees or contractors working remotely regularly access corporate applications and data from their personal devices?



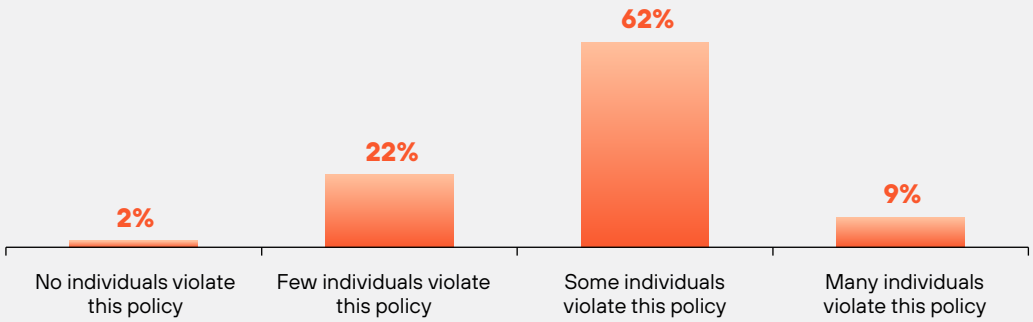
Notes: N=514 IT/security decision makers

Source: Omdia

Anticipating a significant latent security issue, the research indicated that there are astoundingly high levels of policy non-compliance. Of those who reported that they do not allow the use of BYOD, 98% of respondents indicated that there is some level of policy violation in using BYOD devices (see **Figure 6**).

Figure 6: BYOD policy violation

Which of the following best describes your employees' and contractors' behavior related to not being allowed to use personally-owned devices for remote work?



Notes: N=58 respondents from organizations who do not allow usage of BYOD

Source: Omdia

Interestingly, the respondents' general perception is that providing access to corporate resources from these devices may get worse in the future, as many report that they expect to have increased the number of devices accessing corporate resources. 58% of respondents indicated that they feel that unmanaged devices introduce more rather than less risk to the organization.

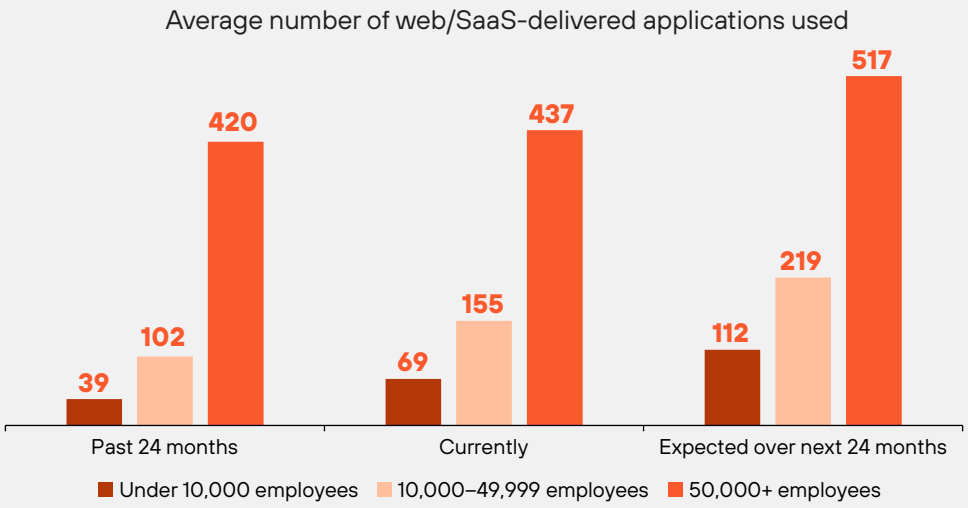
Key takeaway

Organizations increasingly rely on a flexible workforce and BYOD access, but this shift brings significant security risks due to the prevalence of both policy violations (98%) and unmanaged devices, emphasizing the need for robust security strategies.

Strengthen security as SaaS application use grows

And what applications are these users accessing? Over the years, the answer has shifted to a large proportion of SaaS application delivery models. It's important to note that most of these applications are browser-based, leading to a surge in browser usage. The incredible ease of procuring, deploying, and maintaining these external applications has made them ubiquitous. Across the pool of respondents (which includes organizations from 2,500 employees and up), the consensus is that there is significant growth in the number of applications used (see **Figure 7**).

Figure 7: Number of web/SaaS applications used



Notes: Q16: How many different web/SaaS-delivered applications does your organization use in the following time periods?
N=514 IT/security decision makers

Source: Omdia

For larger organizations (50,000 employees and more), the growth factor is less, but the number of applications is significantly higher—an average of 437 now, expected to grow to nearly 520 in the next 24 months.

SaaS applications are utilized across multiple areas of organizations, from workforce productivity (Microsoft365 and Google Workplace Suite are the two most popular options), to communications (Teams, Slack, Zoom, and others), sales and marketing (Salesforce, Hubspot, and more), software development "(GitHub, GitLab, and others), and numerous other categories.

Since late 2022, there has also been an explosion in the number of options for SaaS offerings with support for generative AI (GenAI). While OpenAI's ChatGPT has taken mindshare, numerous other options exist from large and small vendors alike. Across all these SaaS options for GenAI, there is a common concern that using these applications may leak sensitive corporate information, not to mention concerns about output accuracy and fairness.

SaaS apps are great for efficiency, but the very nature of their efficiency introduces potential issues. Users focused on their work are often not attuned to specific technical details and may fall prey to those exploiting these distractions: an attacker may, for example, use phishing-like features such as similar site or domain names (often referred to as "typosquatting") to lure users to malicious content. Furthermore, numerous SaaS applications use security features such as certificate pinning that make inspection by corporate security teams harder or, in some cases, impossible without significant disruption to user experience.

SAAS APP ADOPTION CONTINUES TO RISE IN DOUBLE DIGITS ACROSS LARGE AND SMALL ORGANIZATIONS.

Key takeaway

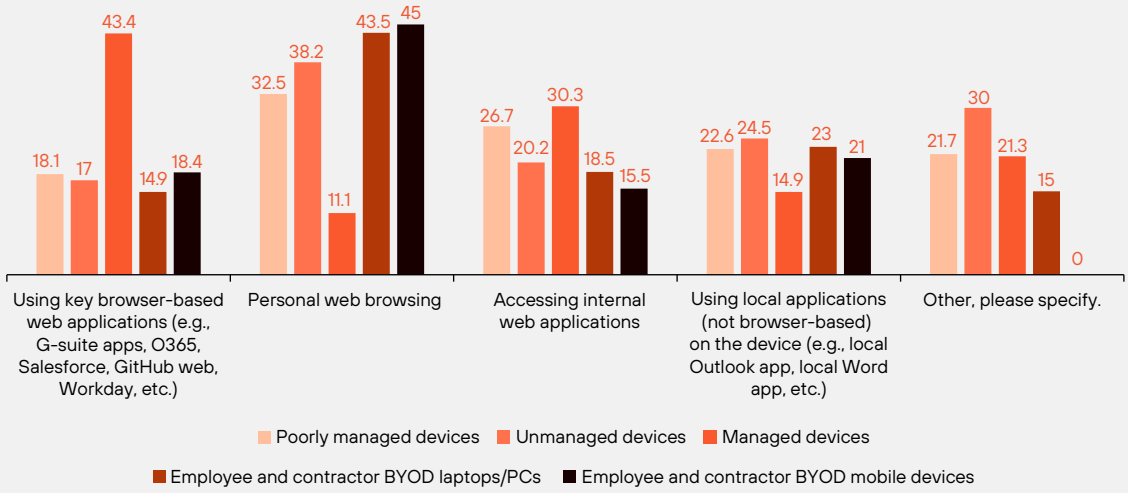
The rise of SaaS applications boosts productivity but also increases the chance of security risks such as data leaks, phishing attacks, and limited oversight, posing challenges to protecting sensitive information.

Optimize security for extensive browser usage

Closely aligned to the focus of this research, modern organizations have reported that the use of browser-based applications has grown and that their staff spend a significant portion of their days using browser-based applications. **Figure 8** shows the proportion of different application usage and device types.

APPROXIMATELY **85%** OF THE WORKDAY IS SPENT ON BROWSER-RELATED ACTIVITIES ON MANAGED DEVICES.

Figure 8: Usage of applications by device type



Notes: N=514 IT/security decision makers
Source: Omdia

It's notable that respondents estimate their typical users spend, in some cases, upward of 80% of their workday on browser-related activities. While estimated usage differs between managed and unmanaged devices, the aggregate view points to significant browser usage.

NO ORGANIZATIONS HAD EVERY SECURITY CONTROL ON ALL DEVICES. EVEN ORGANIZATIONS WHO REPORTED

100%

COVERAGE BY A SECURITY CONTROL STILL EXPERIENCED A SECURITY INCIDENT.

Key takeaway

Employees spend over 80% of their workday on browser-based applications, highlighting the need for strong security measures around browser usage, especially as usage patterns vary between managed and unmanaged devices.

Security teams work hard to catch up, with mixed results

Cybersecurity continues to be an area with significant innovation. The changes to the broader IT environment highlighted earlier—digital transformation, the rise of SaaS, BYOD, AI, and more—have resulted in significant investments in numerous types of security controls. Importantly, though, the research has shown that those investments don't result in complete coverage. Across all 16 security controls surveyed, even organizations that reported 100% of their devices were covered by any one specific control still experienced one or more security incidents.

The security controls surveyed included:

Scope	Controls
For all IT assets	Firewall/network security and inspection
	Network data loss prevention (DLP)
For laptops/desktops/ servers/VMs	Endpoint DLP
	Endpoint security (EPP and/or EDR)
	Local network security protection (host firewall)
For mobile devices	Mobile device management
	Endpoint DLP
	Mobile threat defense
	VPN
For user activity (threat protection)	Secure web gateway
	Use of sandbox for malware analysis
	DNS security protections
	Security for user SaaS activity via CASB/SSPM
	Use of virtual desktops (VDI/DaaS)
	Use of remote browser isolation (RBI)
	Zero trust network access (ZTNA)

Across the set of respondents, there were none (0%) that reported having all controls widely deployed across all devices. Only a small percentage (8%) indicated they had all security controls deployed on at least 50% of their devices. Further, no organizations were immune to security incidents—even those who reported 100% coverage by a security control.

Key takeaway

Despite significant investments in security controls, no organization achieved full coverage across all devices, and even those with 100% coverage in specific areas still experienced security incidents, underscoring gaps and the need for continuous cybersecurity innovation.

Tackle persistent security challenges head-on

So, organizations have evolved, and they have deployed numerous security controls, although for most organizations, these controls may not be deployed across the entire estate. What have been the results?

The research revealed respondents' awareness of significant issues, including a high incidence of multiple security incidents, across many organizations.

Broadly speaking, respondent concerns are grouped into four areas:

- A visibility gap – Organizations are concerned about not having enough visibility into the state of their systems, how their users are behaving, and more. This lack of visibility can affect how the organization responds to security incidents.
- The threat of all potential security incidents – From that visibility gap, these are the concerns about possible negative security outcomes that may occur. These can include a variety of scenarios including data leakage and malware infections, followed by outcomes such as lateral movement, privilege escalation, and others, ultimately resulting in data loss, outages, and more.
- Navigating actual security incidents – Despite having security controls deployed, most organizations had to handle security incidents, including the high prevalence of phishing and browser-based incidents.
- The productivity impact – How can organizations deploy adequate security controls without affecting user productivity?

In addition to these concerns, which are mostly centered around technology, there are still human and process concerns.

Key takeaway

Despite significant investments in security controls, no organization achieved full coverage across all devices, and even those with 100% coverage in specific areas still experienced security incidents, underscoring gaps and the need for continuous cybersecurity innovation.

Bridge the visibility gap

The research results are quite clear in that organizations are reporting a significant gap in visibility of user activity and/or traffic. What are users doing across the multitude of SaaS applications being used, including the increased popularity of GenAI use cases? Just what kind of traffic is flowing across the network?

The topic also raises a question: Should this be called out as a concern, particularly at a time when organizations are already indicating that they are swamped with alerts, vulnerabilities, and more as it is? Shouldn't there be a focus on addressing those concerns first, then worry about additional visibility later?

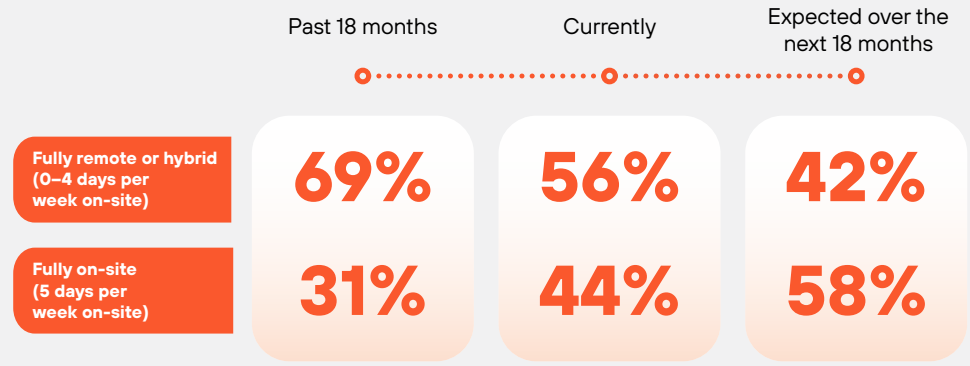
Visibility is essential so, no, a modern security program shouldn't ignore it. Rather, closing the visibility gap is an essential component of a modern security architecture, particularly in today's diverse and distributed modern organization. How can organizations reliably prioritize concerns when they don't even know all the concerns they are facing? Even as organizations attempt to implement "zero trust" programs, these initiatives ultimately also rely on granular application visibility and access control.

The next two figures illustrate one aspect of the visibility gap. Currently, only 13% of respondents have full visibility into data shared in AI tools; 58% have limited to no visibility into what data is shared. Another 65% have limited to no control over what data is shared in AI tools (see **Figure 9**). This lack of visibility and control exposes organizations to significant risks, including data breaches, regulatory non-compliance, and the potential misuse of sensitive information, ultimately undermining trust and operational integrity.

65%
OF ORGANIZATIONS HAVE LIMITED TO NO CONTROL OVER WHAT DATA IS SHARED IN AI TOOLS.

Figure 9: Level of current visibility into and control over data shared in AI tools

What proportion of your total workforce (employees and contractors) is estimated as... (average)



Notes: N=514 IT/security decision makers

Source: Omdia

This is an important trend, particularly as organizations look to better understand and control what kind of business data is shared with external services.

Another key visibility gap concerns encrypted traffic. Many organizations have reported significant gaps in their ability to decrypt network traffic for security purposes: on average, 64% of web traffic is left encrypted, and is therefore unavailable for security inspection.

Naturally, this gap comes with significant concerns. When asked about their main worries regarding the presence of encrypted traffic, respondents' top concerns were that it might be used for data exfiltration activities, command-and-control traffic, or as a conduit for malware to be delivered to the organization.

Visibility concerns also extend to how well organizations can monitor activities and traffic from BYOD or other unmanaged or poorly managed devices. 62% of respondents indicated that "increased visibility" was one of the benefits of being able to better secure work on unmanaged devices.

64% OF ENCRYPTED TRAFFIC IS NOT AVAILABLE FOR SECURITY INSPECTION.

Key takeaway

Organizations face significant visibility gaps in monitoring user activity, SaaS and GenAI data sharing, encrypted traffic, and BYOD usage, leaving them vulnerable to security risks. Addressing this gap is essential for prioritizing threats and enhancing overall security.

Reduce risk exposure

As mentioned before, organizations reported that security controls are often not deployed as comprehensively as desired. This scenario, alongside the prevalence of encrypted traffic, leads to a lack of visibility, be it on network traffic, SaaS applications, GenAI, and more. Organizations do not feel prepared to address security issues from unmanaged devices: 53% said they do not feel confident in their organization's ability to address security issues that arise from using these devices.

72% OF ORGANIZATIONS AGREE THAT UNSECURED DEVICES ACCESSING NETWORK DATA ARE EXPOSING THEIR ORGANIZATION TO RISK.

Respondents noted that this leads to a well-defined set of concerns, many of which affect the organization's data protection posture and its response capabilities during an incident. It can potentially impact downstream business considerations such as compliance with regulatory or contractual clauses.

As an example, organizations' most highly ranked concerns with the use of poorly managed or unmanaged devices included:

- Limited ongoing security monitoring
- The existence of shadow IT
- The need to dedicate more time and resources to investigating these devices
- Inconsistent data protection
- Unsanctioned sharing of devices/credentials (e.g., passwords) between individuals

Interestingly, nearly half (45%) of respondents who ranked shadow IT in their top three said it was their number one concern.

When considering security for SaaS applications in relation to unsafe devices, similar concerns surfaced:

- Respondents were significantly concerned with exposing corporate applications to threats from devices where they may not have enough visibility. Corporate applications often may not have as robust application security features as applications exposed to the public.
- The most popular concerns within the top three included:
    - Exposing applications with vulnerabilities
    - Accidental data leakage
    - Malware infections from insecure devices

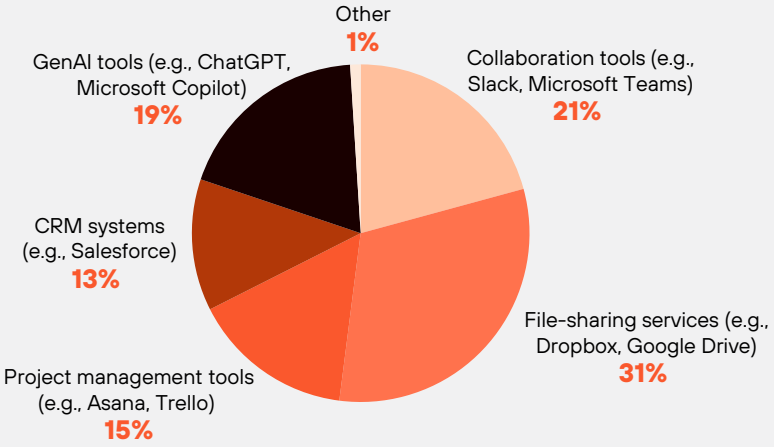
Lastly, in broad terms, when asked about top-level concerns for their organizations, respondents listed, in order of priority:

- Phishing
- Securing privileged users
- Securing BYOD

These concerns occur at a time when, as mentioned before, organizations have broadly adopted numerous SaaS applications, many of which require significant care to implement the proper security controls. Indeed, concerns about securing SaaS applications are pretty evenly distributed across different application types (see **Figure 10**).

Figure 10: Most challenging applications

Which type of SaaS applications or web applications are the most challenging for your organization to monitor and secure?



Notes: N=515 IT/security decision makers

Source: Omdia

Key takeaway

Limited security control deployment and the prevalence of unencrypted traffic creates visibility gaps, risking data protection, incident response, and compliance. Top concerns include securing unmanaged devices, SaaS applications, and addressing phishing, privileged access, and BYOD risks.

Confront recurrent security incidents

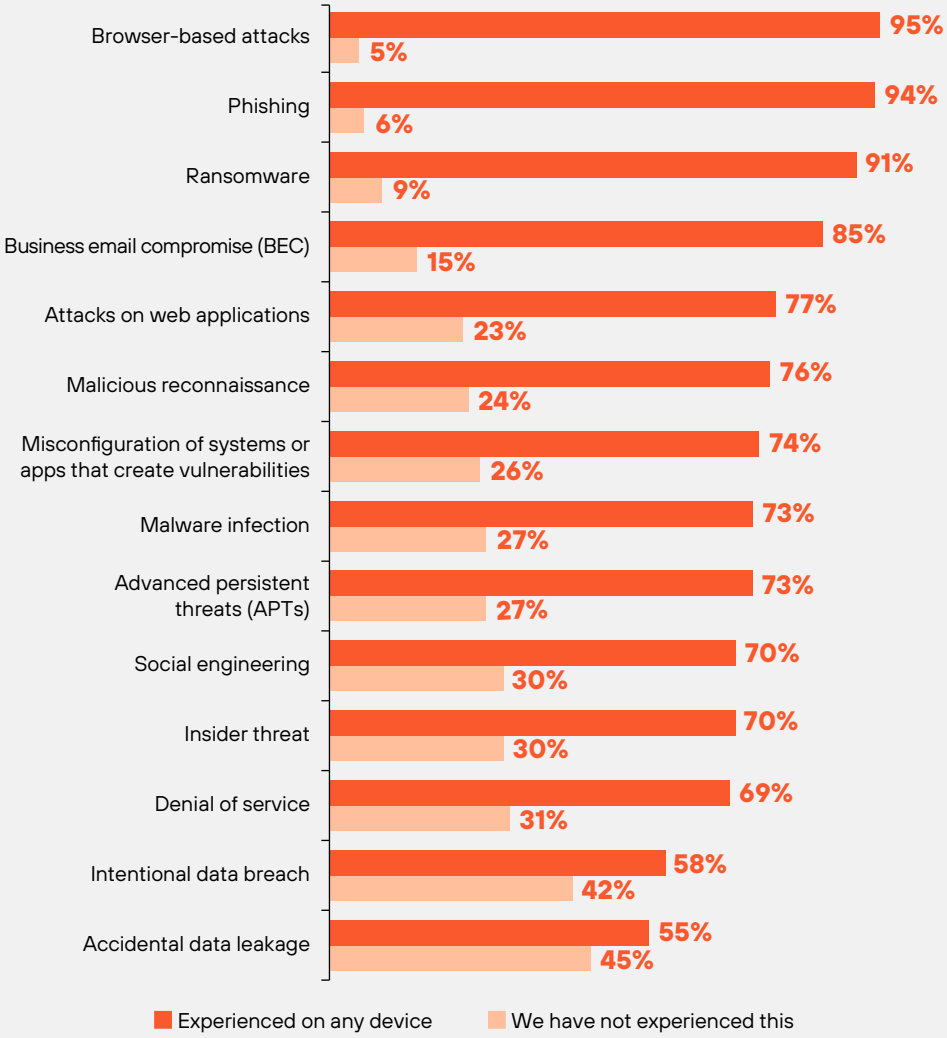
Finally, one key point of this research is that these concerns are not theoretical. Response data indicates that the combination of attacks' increased sophistication, broad expansion of IT footprints, and limited widespread deployment of security controls all appear to contribute to frequent security issues continuing to plague organizations, with no sign of letting go.

According to respondents, browser-based and phishing attacks are common. Every organization experienced at least one security incident in the past 12 months (see **Figure 11**).

95% OF ORGANIZATIONS HAVE EXPERIENCED A BROWSER-BASED ATTACK, AND 94% HAVE EXPERIENCED A PHISHING INCIDENT.

Figure 11: Security incidents in the past 12 months

Over the past 12 months, from where have each of the following security incidents originated?



Notes: N=514 IT/security decision makers

Source: Omdia

These incidents occur against a backdrop of numerous security controls already existing in the environment, even if imperfectly. Indeed, as we collected response data from organizations, one interesting statistic was that out of the respondents that reported having at least 50% coverage on all security controls—representing a mere 8% of total respondents—nearly 86% of them reported some security incident.

94% of organizations experienced a phishing incident originating from any device. The incidence of phishing was almost always in the 70–80% range, regardless of the security control deployed.

Key takeaway

Organizations continue to face frequent cyberattacks, with browser-based and phishing incidents being especially common. 95% of organizations indicate they experienced a browser-based attack originating from any device. Even among those with 50% control coverage, nearly 86% reported security incidents, highlighting the ongoing vulnerability of systems, even for those with extensive security controls.

Balance security with productivity

In addition to the concerns above, respondents were also clear that security by itself is not sufficient—it must be delivered in a way that does not impede productivity, including users bypassing security due to productivity impacts. As previously mentioned, nearly all organizations (97%) block access to corporate resources on some proportion of BYOD mobile devices. Blocking access to corporate resources can be detrimental to the productivity of those employees who prefer to utilize these devices for their work.

Indeed, some of the highest levels of agreement (percentage of agree and strongly agree) from respondents were for the following statements:

- Improving user experience without sacrificing security measures is a key priority for my organization: 76%
- When performing a proof of concept (POC), a security tool that provides better user experience will get a higher score: 71%
- When performing a POC, a security tool that provides better productivity will get a higher score: 64%

Key takeaway

Organizations prioritize improving user experience alongside security, with most respondents agreeing that security tools that enhance productivity and user experience are favored during evaluations and proof-of-concept trials. Organizations must be careful not to unintentionally hinder productivity in the name of security by blocking access to devices designed to streamline work processes.

Securing modern workflows with SASE and browser security

The combination of technology usage evolution—particularly SaaS and web applications—and heterogeneous IT estates with managed and unmanaged devices that vary how security controls are implemented have placed significant demands on security teams.

According to our research, two interesting and complementary options exist for driving improvements in securing the modern workforce. From a service delivery perspective, the rise of SASE brings important efficiencies to delivering network security capabilities. Then, the rise of browser security options improves security close to the user.

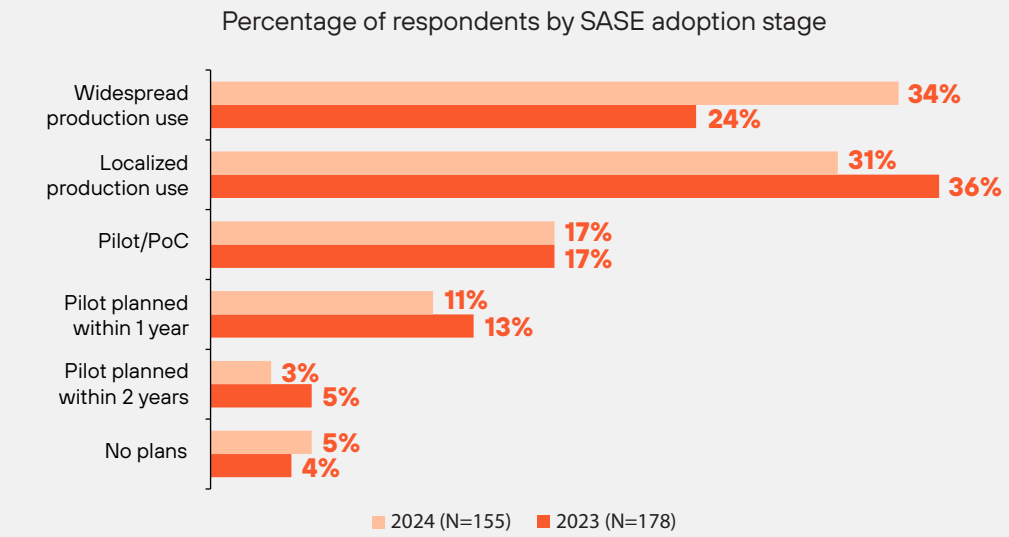
The role of SASE

In parallel to the control-specific questions asked of respondents, our research also incorporated additional research from Omdia. One of the areas of interest is the increased role that SASE seems to have in conversations about modern security architecture.

In essence, SASE refers to the packaged consumption of networking and security functionality "as a service," with significant benefits to the organization in terms of efficiency, user experience, and more. SASE capabilities typically include networking functionality (primarily software-defined WAN or SD-WAN) and security services including but not limited to firewall as a service (FwaaS), cloud access secure broker (CASB), secure web gateway (SWG), and zero-trust network access (ZTNA).

Respondents to Omdia's recent *Cybersecurity Decision Maker Survey* indicate that they have a strong appetite for SASE, with a significant jump in respondents indicating widespread production deployments of SASE (see **Figure 12**).

Figure 12: Percentage of respondents by SASE adoption stage



Notes: N=514 IT/security decision makers

Source: Omdia

Key takeaway

The growing complexity of technology usage, diverse IT environments, and varying security controls are straining security teams. To address this, secure access service edge (SASE) and browser security solutions are emerging as key strategies to improve network and user security efficiently.

The rise of browser security

While no individual security control or technology is a "silver bullet" to address security concerns, we have observed increased availability of browser security offerings that are playing an integral part in a broader security architecture. These offerings can help tackle several of the issues highlighted in this research:

- They support security controls and visibility for SaaS applications, including GenAI applications.
- They can be effective in tackling issues such as the consequences of users clicking through phishing attempts, or other browser-based attacks.
- They provide full visibility at the end-user side of application access, addressing some of the concerns with encrypted network traffic.
- These offerings can be deployed to managed and unmanaged devices, as well as mobile, enabling enhanced collaboration and productivity.
- They support a good user experience, reducing the use of VDI, RBI, or other latency-sensitive approaches.
- They natively integrate into broader organizational security initiatives such as SASE.

Browser security offerings are often referred to as "secure browsers," "enterprise browsers," and variations. The set of features and implementation options vary, but usually, secure browsers offer the following features:

- Centralized management of security features, including ties to corporate identity providers
- Malware protection via content inspection (e.g., sandboxing)
- DLP capabilities, including separation of personal and corporate browsing data, particularly "last mile" protection
- Enhanced visibility of user activities, with local, unencrypted access to browser session details
- Enhanced user experience

Secure browsers currently in the market can usually support different deployment models using a combination of components with different levels of efficacy, for example:

- Browser extensions compatible with key browsers such as Chrome, Edge, and others. Browser extensions may implement some—but not all—of the security features listed above. One of the benefits of extensions is that they may easily be added to BYOD/unmanaged devices as an initial step in improving browser security. They are usually considered an acceptable "first step" in the adoption of a more comprehensive secure browser deployment.
- A full secure browser application, usually implemented in addition to a common rendering engine such as Chromium, Firefox Gecko, WebKit, and so on. In this scenario, the secure browser is distributed as a full application, which gives it much greater visibility and control over the user session than just a browser extension. Importantly, a full browser application has visibility into the endpoint operating system environment and can implement functionality such as hardening.
- A secure browser may work particularly well alongside a SASE deployment, in the context that there are synergies between securing browser activities and using a SASE offering for enterprise-wide security capabilities.

A well-executed browser security program can significantly improve security for mission-critical web applications, regardless of whether they are accessed from managed, unmanaged, or mobile devices.

Key takeaway

The growing need for secure browsers is evident as they play a critical role in modern security architectures. These browsers provide enhanced visibility, support security for SaaS and GenAI applications, address key high-prevalence issues such as the impact of phishing and browser-based attacks, improve user experience, and integrate with initiatives like SASE, making them attractive for securing both managed and unmanaged devices.

Recommendations

Improving modern security architecture is a complex task, and organizations should consider several critical factors to do so effectively. No one piece of technology—including secure browsers—will automagically address all security concerns. As has often been said, effective cybersecurity requires a balance of people, processes, and technology.

That said, we recognize that secure browsers can play a significant role in helping organizations.

When evaluating the context in which to consider secure browser options, Omdia recommends that organizations:

- **Realistically acknowledge and address all device types.** The research has shown that unmanaged devices and/or poorly managed devices are inevitable and have the potential to introduce serious risk, even in the most careful of organizations. Even managed devices are not immune to vulnerabilities. Any device used by any user in an organization, whether it's classified as managed or unmanaged, requires strong, robust security controls. Ensure your cybersecurity strategy includes provisions and controls for multiple use cases, leveraging recommended approaches such as overlapping defenses, least-privilege, and zero trust principles.
- **Apply security controls at multiple levels, including network and endpoint.** Building on the previous point, as the workforce becomes more mobile, organizations must ensure that data remains secure regardless of where it is accessed or stored. Security controls should continue to be applied and monitored at both the device level and the network level. While network-level security measures can be an efficient source of information for a broad swath of devices, device-level security can tackle scenarios where network visibility is difficult or impossible. Importantly, pay attention to the browser as a new component of device-level security.
- **Treat the browser as a key environment for enforcing security.** The modern browser is a central mode for accessing cloud services, making it a prime candidate for security threats. Consider that while the browser may be a source of potential threats, it is also perfectly positioned to help protect against numerous threats, particularly if engineered to work with the rest of the organization's security architecture. Capabilities such as DLP, threat prevention, least privilege, support for zero trust, and enhanced visibility can help mitigate risk from threats such as phishing, malicious web apps, and so on, while enabling safe and efficient web use.
- **Utilize browser security in conjunction with other modernization efforts.** Browser security is at its strongest when it is utilized as a key element of a broader modernization initiative. Combining your browser security efforts with other frameworks, such as SASE, ensures a more unified threat defense is created across the entire ecosystem.
- **Balance security and user experience.** Implementing strong security controls should not come at the cost of a positive user experience. Overly strict measures can disrupt productivity and lead to workarounds that undermine security and increase risk, whereas secure browsers enable frictionless security by providing a native user experience that can be deployed quickly. Strike the right balance by ensuring that browser security initiatives have strong requirements for usability as well as security functionality.

Conclusions and next steps

Work environments have steadily become more complex, driven by the rise and evolution of SaaS applications, the proliferation of unmanaged devices, and increasing employee mobility. This shift has significantly expanded organizations' attack surfaces. While many have implemented various security controls with the best intentions, coverage often remains incomplete, leaving critical vulnerabilities exposed. The complexity of managing various devices and securing data across different access points results in coverage gaps that attackers are poised to exploit.

Adding meaningful security at the browser level presents a significant opportunity for organizations to address these gaps. Browser security measures, as part of a broader cybersecurity strategy, can help organizations protect against emerging threats and provide better visibility into the entire ecosystem. Explore how browser-based security solutions can complement your existing efforts and further strengthen your cybersecurity posture—ensuring your organization remains secure, resilient, and ready for what's next.

Appendix

Methodology

The majority of the data for this research comes from two separate surveys fielded by Omdia, using a web interface for capturing user responses. Both surveys targeted similar user populations and used extensive validation of results. Surveys were fielded online only, in a double-blind methodology to ensure respondents did not know they were partaking in Omdia/Palo Alto Networks research, and that Omdia did not receive any PII from respondents.

The first survey—undertaken in February 2024 —initially focused on how organizations deployed managed or unmanaged devices, including BYOD devices for employees or contractors. The survey had 514 respondents. The criteria for inclusion in the survey included:

- Specific countries (United States, United Kingdom, Canada, France, Germany)
- Minimum size of 2,500 employees worldwide (including both permanent and contractor staff)
- Management or senior management job role
- Key areas included IT Management, Cybersecurity or information security, and end-user compute
- Indicating some level of knowledge of how the organization was enabling security for remote employees

Geography	
North America (US, Canada)	75%
EMEA (France, Germany, UK)	25%

Company size (employees)	
2,500–4,999 employees	46%
5,000–9,999 employees	27%
10,000–24,999 employees	14%
25,000+ employees	15%

Respondent level	
C-level Executive	12%
Vice President	23%
Director	36%
Manager	30%

Respondent role	
IT Management	54%
Cybersecurity	17%
Information/data security	15%
End-user compute or digital workspace	14%

The second survey—fielded between July and August 2024—focused on additional questions related to technology deployments, use cases, and newer topics such as GenAI. The sample size was 515, using similar screening criteria for location, organization size, job level, and knowledge of technologies.

Geography	
North America (US, Canada)	73%
EMEA (France, Germany, UK)	27%

Company size (Employees)	
2,500–4,999 employees	39%
5,000–9,999 employees	27%
10,000–24,999 employees	18%
25,000+ employees	17%

Respondent level	
C-level Executive	13%
Vice President	23%
Director	35%
Manager	28%

Respondent role	
IT Management	53%
Cybersecurity	18%
Information/data security	15%
End-user compute or digital workspace	14%

In addition to the surveys listed above, this research also includes data points from Omdia's *Cybersecurity Decision Maker (CDM) Survey*, fielded in April 2024. Using a similar methodology to the two surveys above, the CDM survey obtained responses from approximately 960 respondents.

In comparison to the other surveys, CDM had a more global reach, and also included smaller organizations, as well as individual contributors as respondents.

Geography	
North America	20%
Europe	52%
APAC	29%

Company size (Employees)	
Less than 1,000	23%
1,000–2,499	22%
2,500–4,999 employees	23%
5,000–9,999 employees	22%
10,000+ employees	10%

Author

Fernando Montenegro

Senior Principal Analyst, Enterprise

askananalyst@omdia.com

Get in touch

www.omdia.com

askananalyst@omdia.com

Omdia consulting

Omdia is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision-makers thrive in the connected digital economy. Through our global base of analysts, we offer expert analysis and strategic insight across the IT, telecoms, and media industries.

We create business advantage for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalize on evolving business models.

Omdia is part of Informa TechTarget, a B2B information services business serving the technology, media, and telecoms sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help your company identify future trends and opportunities.

Copyright notice and disclaimer

The Omdia research, data and information referenced herein (the "Omdia Materials") are the copyrighted property of TechTarget, Inc. and its subsidiaries or affiliates (together "Informa TechTarget") or its third party data providers and represent data, research, opinions, or viewpoints published by Informa TechTarget, and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice and Informa TechTarget does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an "as-is" and "as-available" basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa TechTarget and its affiliates, officers, directors, employees, agents, and third party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa TechTarget will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.