Enterprise
Strategy Group™
by TechTarget

Improving Security Operations Through SASE and XDR

Keys to Optimize Security Modernization Initiatives

John Grady | Principal Analyst
ENTERPRISE STRATEGY GROUP

JUNE 2024

This Enterprise Strategy Group eBook was commissioned by Comcast and is distributed under license from TechTarget, Inc.

CONTENTS

> “IT transformation continues to accelerate, and **slowing business innovation is not an option**.”

John Grady | Senior Analyst
ENTERPRISE STRATEGY GROUP

IT Transformation Leads to Security Challenges

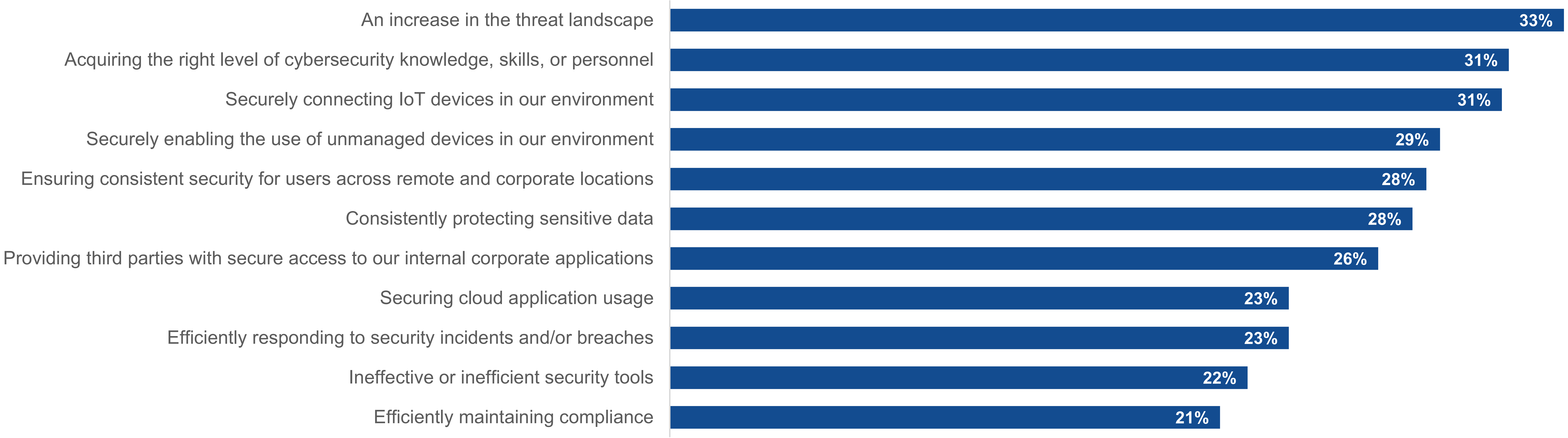
Security Teams Face a Variety of Challenges Due to Transformation

Businesses today move faster than ever before. IT transformation continues to accelerate, and slowing business innovation is not an option. These facts become issues when it comes to cybersecurity. When asked which cybersecurity challenges have been most impactful to their organization, security professionals unsurprisingly cited the threat landscape most often (33%).

Yet many of the other challenges cited are related to changes in enterprise environments and security teams simply trying to keep pace. The continuing proliferation of IoT devices (31%), use of unmanaged devices (29%), remote and hybrid work models (28%), third-party access (26%), and cloud adoption (23%) all highlight this trend.

Adding to the complexity, the skills shortage remains an issue, and nearly one-third (31%) say acquiring the right level of cybersecurity knowledge, skills, or personnel is a challenge. Security teams increasingly have to not only do more with less but also enable the business to move faster.

Cybersecurity challenges



Source: Enterprise Strategy Group Research Report, *Security Services Edge (SSE) Leads the Way to SASE*, November 2023.

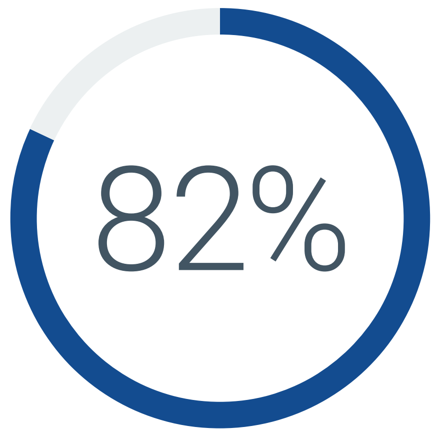
Security Operations Teams Struggle to Keep Pace

Cybersecurity is a broad category, and security operations is a particularly important component of it. Preventative measures are important, but how organizations identify, analyze, and respond to threats as quickly as possible is critical since attacks are inevitable. Unfortunately, nearly half (45%) say security operations are more challenging than two years ago.

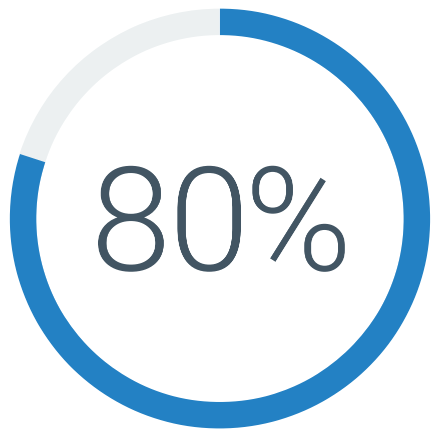
There are a variety of reasons for this. Again, the skills shortage comes into play, with 79% agreeing that it has affected security operations. There is also strong agreement that disconnected tools (82%) and manual processes (80%) present challenges. Unfortunately, as the environment expands and new threat vectors are identified, the default response is to add new tools. Over time, this often results in diminishing returns. Part of the issue here is that, even when tools uncover anomalous behavior, it is not always malicious. Three-quarters (75%) agreed that it is difficult to keep up with security alerts.

This lack of efficacy, coupled with the need to manually stitch together tools and data to draw meaningful conclusions, ultimately hinders efficiency and means that security teams are less likely to quickly identify legitimate issues.

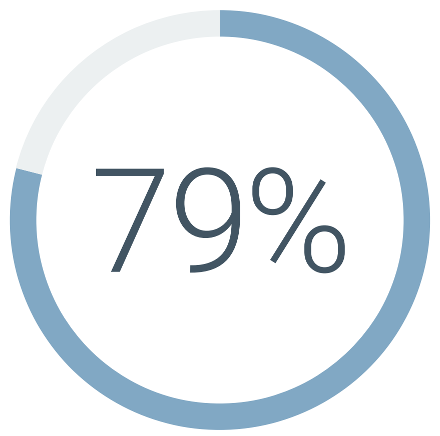
Security operations challenges



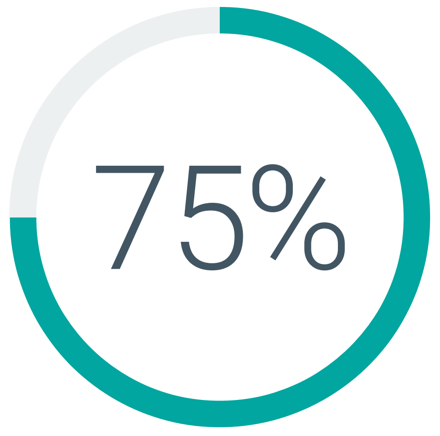
Security operations are still dependent upon numerous **disconnected analytics engines and point tools**



Security operations are still dependent upon **numerous manual processes**



The cybersecurity **skills shortage has impacted** security operations at my organization



It is difficult for my organization to keep up with the volume and variety of security alerts generated byour security analytics tools

Source: Enterprise Strategy Group Complete Survey Results, *2024 XDR and SOC Modernization Trends*, May 2024.

BACK TO CONTENTS

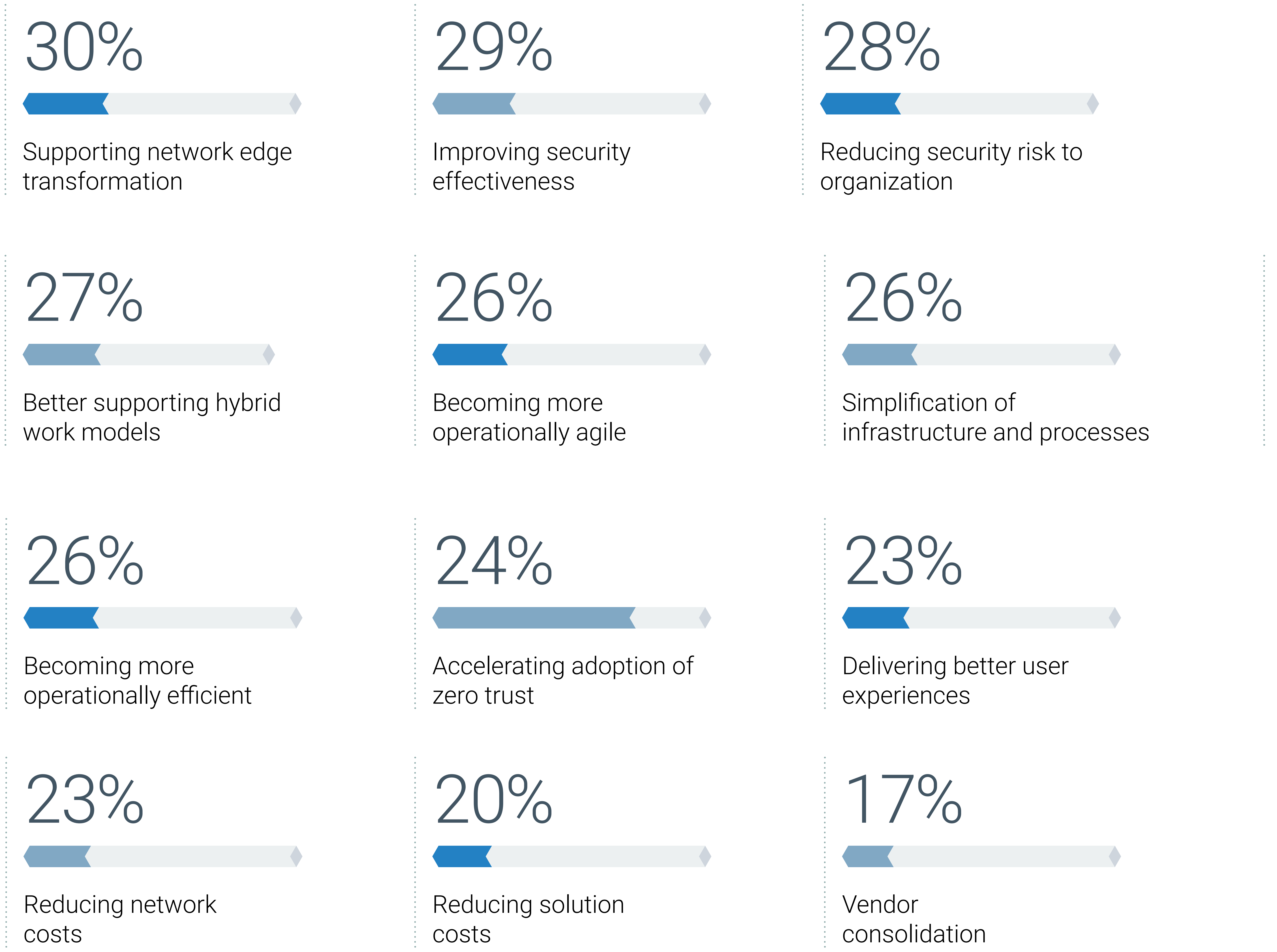
Modernization Initiatives Emphasize Consolidation for Efficiency and Effectiveness, but Gaps Remain

Security Teams Look to SASE to Address Cyber Challenges and Modernize Security

To address these issues, two overarching trends within cybersecurity have begun to see broad adoption: secure access service edge (SASE) and extended detection and response (XDR). To improve security, SASE converges previously disparate tooling across both security and networking in a more cloud-centric architecture, in some cases from a single vendor. On the network side, this includes SD-WAN, WAN optimization, and digital experience management, while the security side includes zero-trust network access, secure web gateway, cloud access security broker, and firewall, among other capabilities.

While improving security effectiveness rates highly as a reason to turn to SASE (29%), many organizations point to efficiency as a driver. Supporting network edge transformation (30%), becoming more operationally agile and efficient (26%), and simplifying infrastructure and processes (26%) were all commonly cited as drivers for SASE.

SASE drivers



Source: Enterprise Strategy Group Research Report, *Security Services Edge (SSE) Leads the Way to SASE*, November 2023.

BACK TO CONTENTS

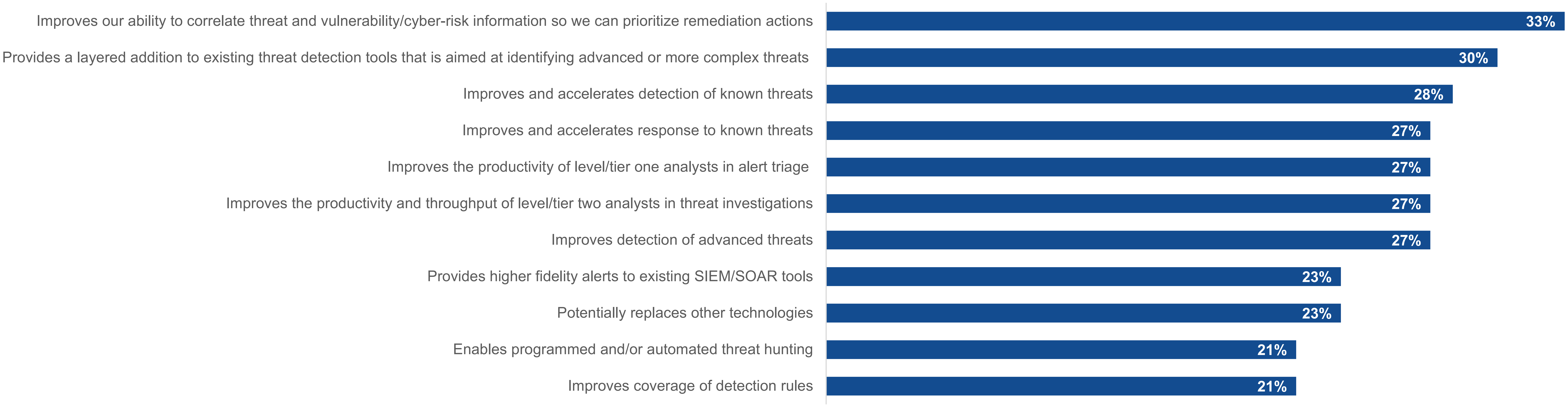
Security Teams Turn to XDR to Improve Efficiency and Modernize the SOC

As security operations teams have become dependent on a variety of disconnected data sources, it has become more difficult to accurately stitch information together. Large organizations have come to rely on security incident and event management (SIEM) as the aggregation point to alert on potentially malicious behavior, but the difficulty in writing detection rules and properly tuning and maintaining these systems can become incredibly burdensome.

To augment this process, many organizations have begun to look to XDR to better collect, normalize, analyze, and respond to security data. Many of the vendors providing XDR solutions position it as a platform or consolidation play.

Again, many use cases point to improving efficiency in the security operations center (SOC). One-third (33%) indicated improving threat and vulnerability or cyber-risk information to prioritize remediation actions was a priority use case. Improving tier 1 (27%) and tier 2 analyst productivity (27%) and improving the detection (28%) and response (27%) of known threats all rated highly.

XDR priorities



Source: Enterprise Strategy Group Complete Survey Results, *2024 XDR and SOC Modernization Trends*, May 2024.

BACK TO CONTENTS

Yet the Anticipated Consolidation Has Not Materialized

A majority (69%) of the organizations moving forward with XDR say they're actively consolidating or integrating tools as part of the initiative. However, the focus appears to mostly be on the integration front, considering how users define XDR. Only 26% identify XDR as a detection and response product suite from a single security technology vendor, while 52% believe it is an open, integrated security product architecture designed to interoperate and coordinate with threat prevention, detection, and response.

While an open architecture provides more flexibility with regard to the vendors being used, the opportunity to select best-of-breed capabilities across the stack, and help in avoiding vendor lock-in, success is dependent on the level of integration in the open ecosystem. Unfortunately, if those integrations are not fully built out, security teams may have significant work to do on their own to make the architecture work, which could limit expected efficiency gains.

XDR definitions

22% XDR is an **extension** of endpoint detection and response (EDR) technology

26% XDR is a detection and response **product suite** from a single security technology vendor

52% XDR is an **open integrated security product architecture** designed to interoperate and coordinate with threat prevention, detection, and response

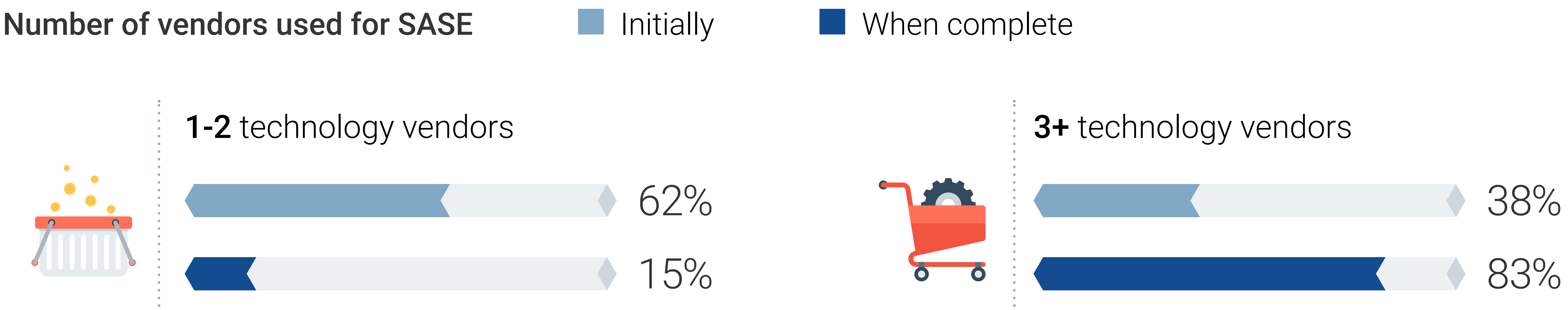
Source: Enterprise Strategy Group Complete Survey Results, *2024 XDR and SOC Modernization Trends*, May 2024.

BACK TO CONTENTS

Consolidation via SASE Is Also in Question, but Often a Question of Timing

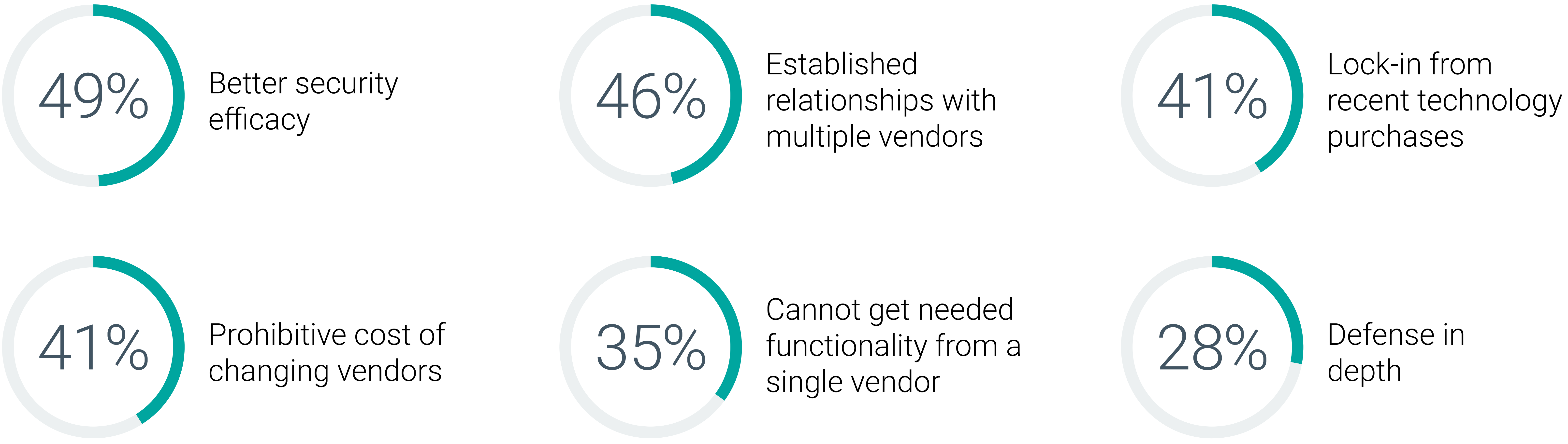
With regard to SASE, the single-vendor concept is gaining momentum. Yet many organizations seem to have trouble believing that one or even two vendors will be able to meet their needs over the course of a SASE implementation. This is likely due to the sheer number of point products and vendors organizations currently use for network and user security.

But this perception is likely to change over time. In fact, many of the reasons given for the expected use of multiple SASE vendors comes down to current contracts, relationships, and the prohibitive cost of changing vendors. While this provides more clarity in the long term, it means that organizations will need help implementing and integrating disparate tools in the short term.



Number of vendors used for SASE

Reasons to use more than one vendor for SASE



Source: Enterprise Strategy Group Research Report, *Security Services Edge (SSE) Leads the Way to SASE*, November 2023.

BACK TO CONTENTS

How a Managed Approach Can Help With Modernization Initiatives

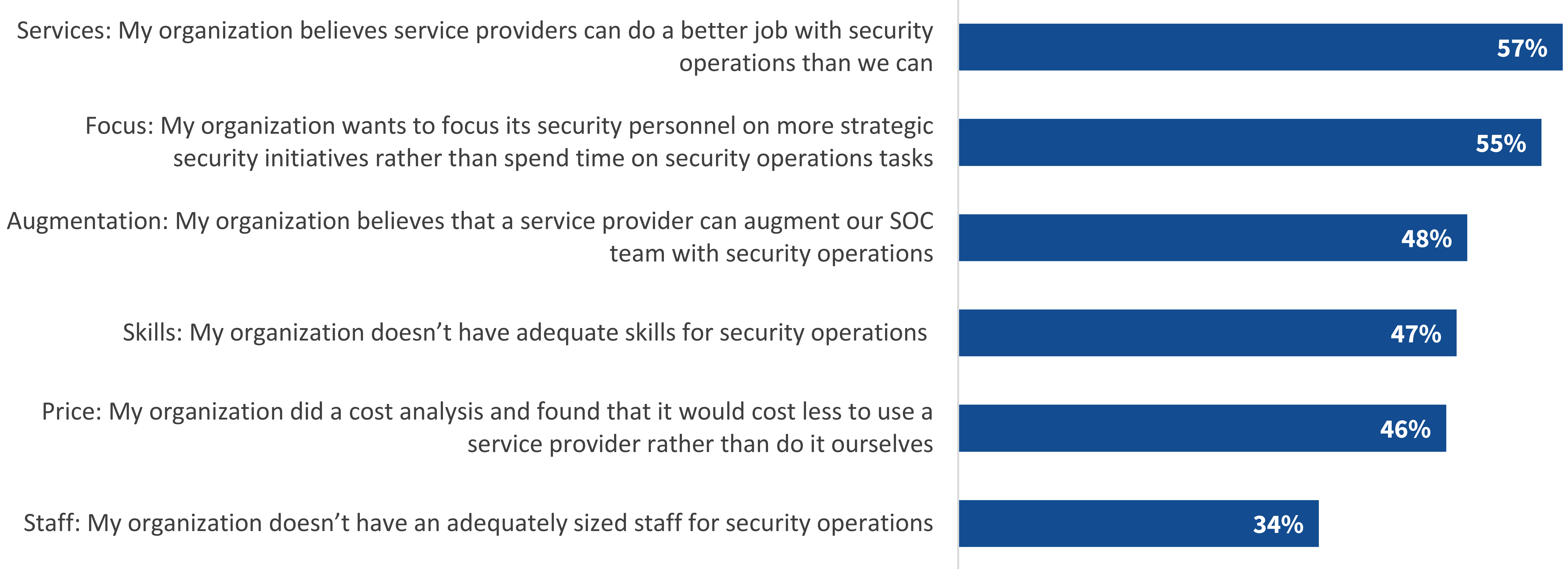
Organizations Turn to Managed Services for a Variety of Reasons

The use of managed services is nothing new in IT generally or cybersecurity specifically. However, given all the challenges highlighted previously that security teams face, there is clear value in engaging with managed security services providers (MSSPs).

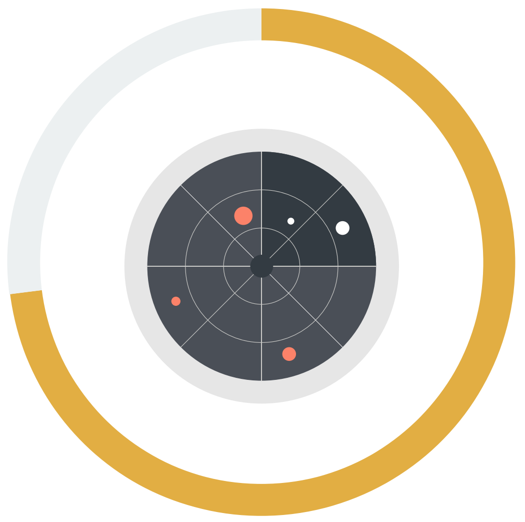
There are a variety of reasons security teams may decide to work with an MSSP. Simply filling in gaps with regard to skills (47%) or staff sizing (34%) and augmenting existing SOC teams (48%) are common reasons. The expectation that service providers can do a better job with security operations (57%) or that engaging service providers will be more cost-effective (46%) were also frequently cited. Finally, simply aligning in-house personnel on more strategic tasks was noted by more than half (55%) of respondents.

Considering the implementation and management challenges associated with both SASE and XDR, these all become relevant reasons to explore how a services-led approach can deliver the efficiency gains sought through these modernization initiatives. That is likely why 73% associate XDR and 66% associate SASE closely with managed detection and response services.

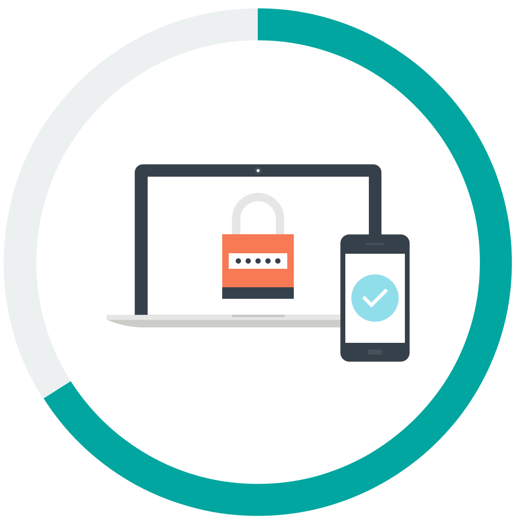
Reasons for using managed services



Association of security megatrends with MDR



73%
Extended detection and response (XDR)



66%
Secure service access edge (SASE)

Source: Enterprise Strategy Group Complete Survey Results, *Managed Detection and Response Trends*, May 2023.

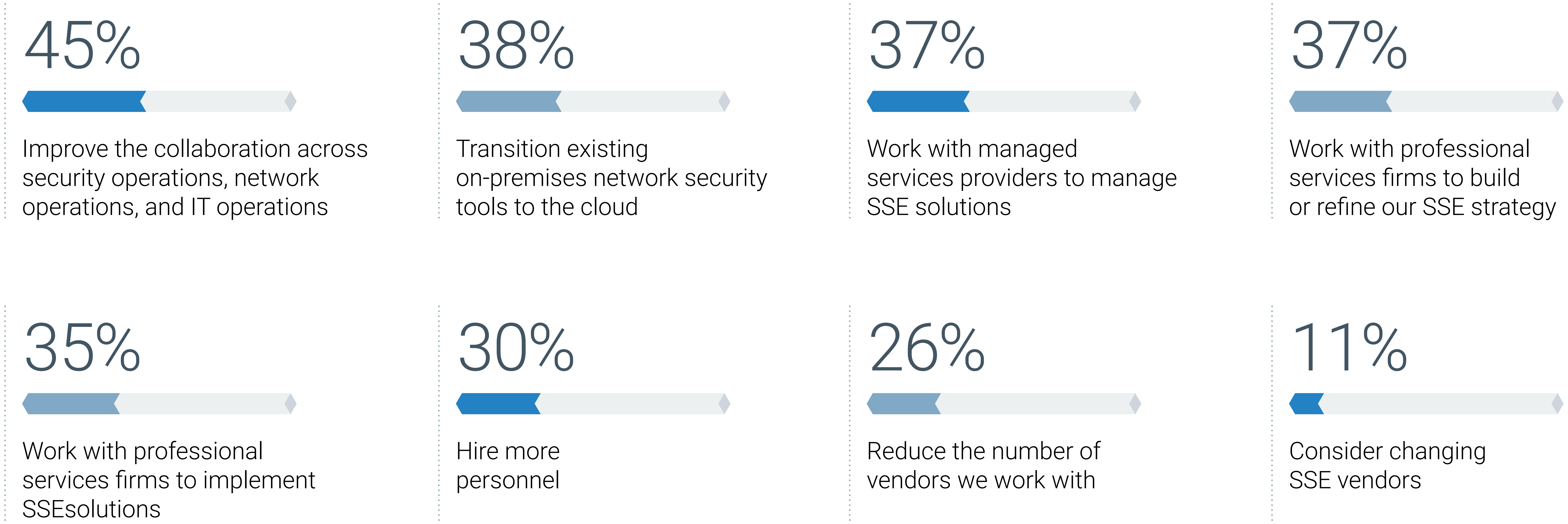
BACK TO CONTENTS

For SASE Specifically, Partnering With Service Providers Can Check Multiple Boxes

Further, leveraging MSSPs for SASE supports a lot of the actions organizations expect to prioritize for the initiative over the next 12-18 months. At the top of the list, improving collaboration across security operations, network operations, and IT operations was cited by 45% of respondents. While this should be a goal regardless of SASE, working with service providers does afford the opportunity to slow this process and make sure organizational changes are properly structured and implemented. More than one-third (37%) expect to work with MSSPs. But further, 37% expect to work with professional services firms for strategy, 35% expect to work with professional services firms for implementation, and 30% expect to hire more personnel. Each of these actions could arguably be similarly or better supported by working with an MSSP to support a SASE initiative.

> “At the top of the list, **improving collaboration** across security operations, network operations, and IT operations.”

Actions for SASE over the next 12-18 months



45%
Improve the collaboration across security operations, network operations, and IT operations

38%
Transition existing on-premises network security tools to the cloud

37%
Work with managed services providers to manage SSE solutions

37%
Work with professional services firms to build or refine our SSE strategy

35%
Work with professional services firms to implement SSEsolutions

30%
Hire more personnel

26%
Reduce the number of vendors we work with

11%
Consider changing SSE vendors

Source: Enterprise Strategy Group Research Report, *Security Services Edge (SSE) Leads the Way to SASE*, November 2023.

BACK TO CONTENTS

Considerations for Selecting an MSSP

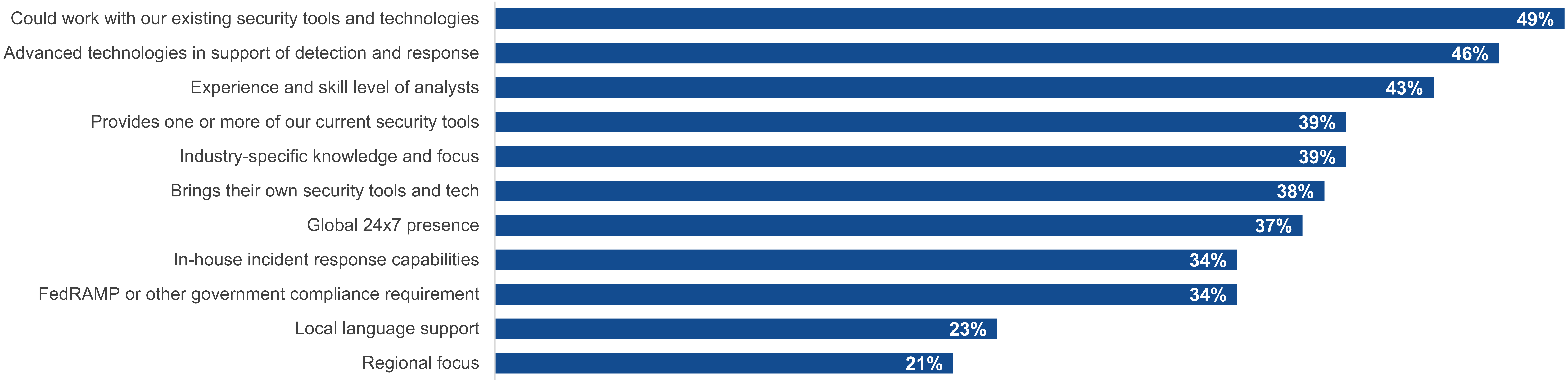
What attributes should organizations weigh when selecting an MSSP? There is a long list, but they can be grouped into three main categories: flexibility, expertise, and coverage.

Flexibility: The ability to work with existing tools was the most common response given, but at the same time, many organizations expect MSSPs to bring their own tools and technology to provide additional value. An organization's needs will often change over time, so the ability to support both of these points is critical.

Expertise: Obviously, the level of experience and skill of the analysts at the MSSP are paramount. In-house incident response (IR) resources are also a plus to bring management and response closer together. But industry-specific knowledge is increasingly relevant as the threat landscape shifts from broadly focused attacks to very specific campaigns targeted at verticals.

Coverage: Finally, many organizations prioritize coverage across regions. This is also relevant to support for different aspects of the security stack (i.e., both preventative and detection and response components).

Important considerations for managed providers



Source: Enterprise Strategy Group Complete Survey Results, *Managed Detection and Response Trends,* May 2023.

BACK TO CONTENTS

Conclusion

Make no mistake: Modernization initiatives such as SASE and XDR are critically important and well positioned to improve effectiveness as well as better address modern threat and enterprise environments. However, improving operational efficiency is a key priority for many IT organizations overall, especially with regard to cybersecurity. As an industry, what the journey to SASE and XDR will look like tends to be oversimplified, meaning that efficiency will be negatively impacted as security teams try to connect siloed tools and data sources. Managed services can bridge the gap, while technology improves and helps ensure organizations see tangible benefits from their SASE and XDR initiatives more quickly.

COMCAST
BUSINESS

Comcast Business is a leader in connectivity, global secure networking, and cybersecurity solutions. Backed by reliable connectivity, advanced secure networking solutions, and managed security services, Comcast Business' Cybersecurity Solutions are designed to meet the needs of customers of all sizes.

LEARN MORE

This Enterprise Strategy Group eBook was commissioned by Comcast and is distributed under license from TechTarget, Inc.

All product names, logos, brands, and trademarks are the property of their respective owners. Information contained in this publication has been obtained by sources TechTarget, Inc. considers to be reliable but is not warranted by TechTarget, Inc. This publication may contain opinions of TechTarget, Inc., which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget, Inc.'s assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget, Inc. makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

Enterprise Strategy Group™ by TechTarget

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.