



WHITE PAPER

TRENDS AND SOLUTIONS FOR A MORE SECURE PERIMETER

CONNECTIVITY, NETWORKING AND SECURITY

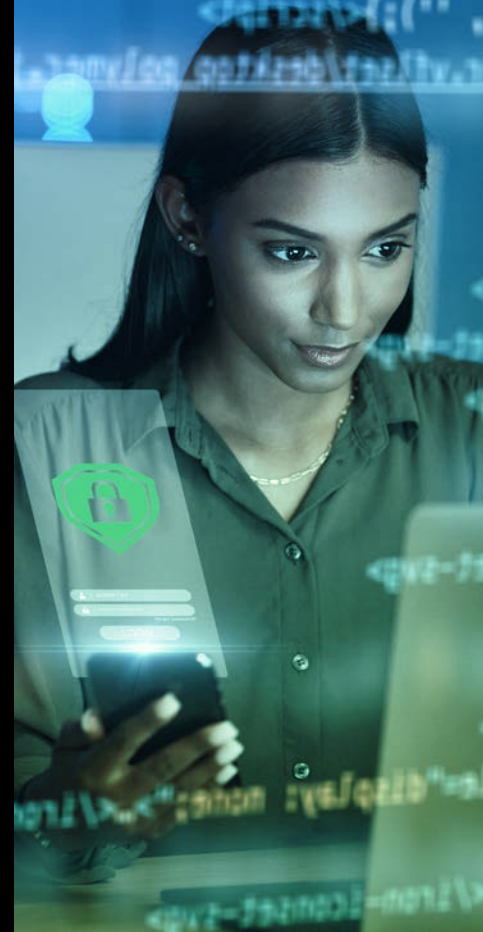
GTT

A White Paper Based on Data
Gathered by Hanover Research

INTRODUCTION

It's been more than three years since the terms Secure Access Service Edge (SASE) and Security Service Edge (SSE) have become part of the language of advanced security and adoption of both is growing.

GTT commissioned Hanover Research, a leading provider of research and analytics for organizations worldwide, to gain insight into how businesses are adopting and using SASE and SSE.



Hanover's survey data and our analysis in this paper provide executives with current information and context, enabling them to lead the discussion in their organizations on the benefits of advanced security and integrated networking.

In Hanover's survey, respondents were divided into two groups: those that favored SASE and those that favored SSE. In the survey, 81% of SASE respondents said they will deploy a SASE framework within the next 12 months, while 77% of the respondents that do NOT plan to deploy SASE will move forward with SSE solutions in the same time period.

Therefore, it's not too bold to say it's only a matter of time before these security postures are adopted across all enterprises and become table stakes. The data shows we can expect an adoption rate similar to that of SD-WAN, which began a decade ago and provides the building blocks for the SASE framework.

All of the respondents in the study are decision makers on SD-WAN, SSE or SASE purchase/usage for their company; work in the US, UK or Europe; are employed full time as managers or higher in IT, Infrastructure, Networking, Security, Finance or Operations in sectors such as Business Services, Retail, Hospitality/Accommodation, Manufacturing, Food & Beverage, Healthcare, Financial Services, or Technology industries; and possess five or more sites; and achieve annual revenues of at least \$200 million.

IN HANOVER'S SURVEY

81%

of respondents say they will deploy SASE in the next 12 months

77%

plan to deploy SSE within the next 12 months

TOP LINE NUMBERS

Most Enterprises Have Deployed or Are in the Process of Deploying SD-WAN, SSE, SASE and Other Network Security Solutions

According to the research, while nearly half (45%) of companies with SD-WAN solutions have them deployed at scale, just 35% are now using a SASE solution. Looking ahead, 34% plan to deploy one in the next 1-6 months, 44% plan to in the next 7-12 months and 19% are at least a year away. A mere 3% currently do not plan to deploy a SASE solution at all.

Companies with SD-WAN, SSE and SASE solutions entrust both their security and networking teams (68%, 59% and 60%, respectively) to jointly manage each solution. They also either co-manage with a third-party managed service provider (MSP) or task an MSP to fully manage their SD-WAN (85%), SSE (84%) and SASE solutions (82%). These figures demonstrate the need for an MSP to help manage modern, complex networking and security frameworks.

What Cyberthreats Are a Major Concern for Enterprises?

Their greatest cyberthreat concerns include:

46%

Undetected vulnerabilities

45%

Ransomware / hostage situations

44%

Data theft

43%

Network interruptions

The top drivers of enterprise security strategies include:

46%

Increasing security controls

37%

Updating security architecture for remote / hybrid workforces

36%

Consolidating security products for simpler architecture



By contrasting the above stats with the top deployment challenges — synchronizing security policies between security components (34%) and managing complex security policies (33%) — one can detect a gap between security needs and implementation capabilities that must be overcome.

Satisfaction Levels and the Evolution of Security and Network Capabilities

While most enterprises are satisfied with their cybersecurity implementation experience, 67% of respondents reported that they were not “completely satisfied.” Managed service providers have an opportunity before them to build value in their partnerships with clients and improve the transparency and simplicity of the implementation process. The evidence shows that respondents are interested in the evolution of cybersecurity solutions and want to understand more about how MSPs can help them deploy better-performing technology.

In fact, in a related survey conducted by Hanover Research on behalf of GTT, 75% of respondents stated that dedicated customer support would be a reason to adopt a new SD-WAN solution through an MSP if it could offer improvements that their current SD-WAN solution could not match.

Currently, the most preferred (43%) type of cybersecurity technology is an internally managed best-of-breed security solution integrated with SD-WAN. When asked about the future, the preference for this type of solution drops to 29%, and the choice of an integrated SD-WAN security solution managed by a service provider becomes the most preferred at 32%.

Taking this shift into account, along with the fact that more than 70% of companies using SD-WAN on its own or as part of a SASE solution are considering further integration, one can appreciate that leaders are moving toward a more holistic and managed approach to network cybersecurity.

THE BIG TAKEAWAY

97%

of respondents say integration is the logical next step of organizations with SSE and SD-WAN solutions

A solid majority of cybersecurity and networking teams (88%) are fully integrated or regularly work together. Of those who have integrated their teams, respondents say it has resulted in stronger security (57%) and faster decision making (53%).

Respondents that are not working as integrated teams also report faster decision making (59%), but only on components within their individual purview. This is because teams that work in silos lack big-picture visibility and the opportunity to collaborate, slowing down decision making and implementation.

Also, nearly half (49%) of respondents in the non-integrated group say that lack of coordination or clarity in team responsibilities is an issue, which helps make the case for integration and transparent communication.

To enable integration, respondents say their organizations have increased their investments over the last year in multiple network areas, particularly in integrated SD-WAN/Security solutions (67%) and cloud connectivity (67%). Respondents also state that their organizations plan to further increase their investment over the next year, chiefly in integrated SD-WAN/Security solutions (57%) and cloud connectivity (56%).

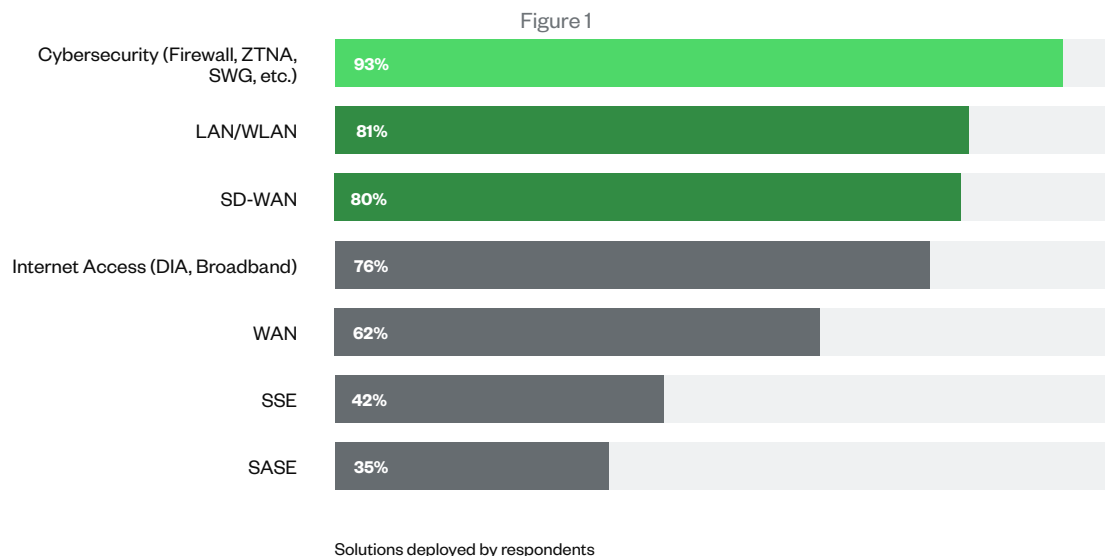
DEPLOYMENT

SD-WAN, SSE AND SASE

What Enterprise Network Security Solutions Do Respondents Use?

Cybersecurity solutions such as FWaaS (Firewall as a Service), ZTNA (Zero Trust Network Access), SWG (Secure Web Gateway), CASB (Cloud Access Security Broker) and Managed Detection and Response (MDR) make up the top of the field at 93%, as shown in Figure 1.

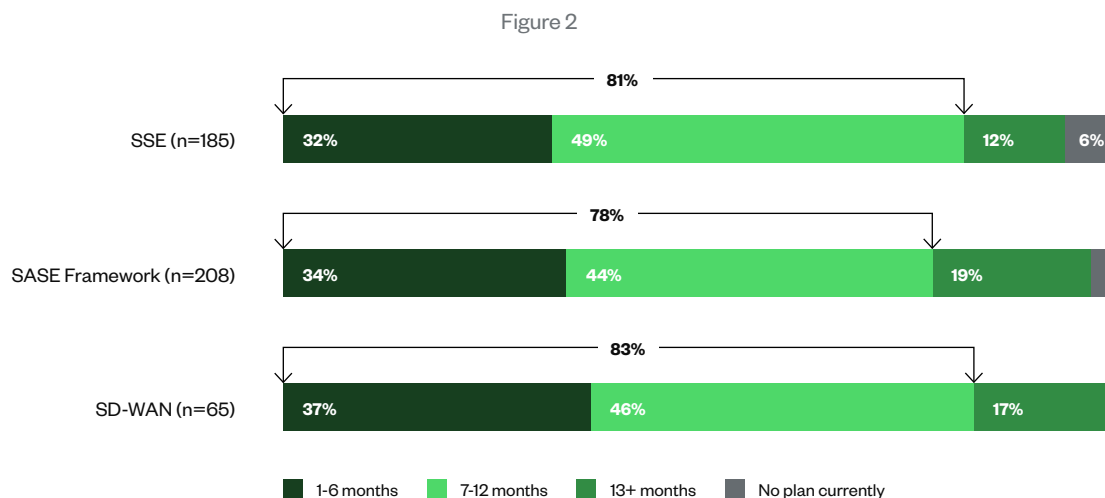
Considering that SASE solutions require the deployment of SD-WAN and 35% of respondents currently use SASE, as shown in the chart below, one can conclude that approximately 1/3 of respondents have already integrated security and SD-WAN. However, most organizations still lack integrated SSE and SASE deployments. That absence is captured in Figure 2 on the following page, as these two frameworks, along with SD-WAN, are at the top of many to-do lists.



What Do Respondents Without These Solutions Plan to Deploy, and When?

When asked about their future deployments of SSE, SASE and SD-WAN, most respondents acknowledged that such activities would occur within the next seven to 12 months, as shown in the chart on the next page, with fewer stating that they would deploy within the next six months. Significantly fewer respondents say their company plans to take longer than one year to deploy and fewer still acknowledged that they had no such plans.

Given these responses, most companies recognize the importance of cybersecurity as a critical part of their networking portfolio and are taking steps to ensure deployment.



What Do Respondents Plan to Deploy?

Firewalls (60%) and Secure Remote Access (45%) will be the first solutions to be deployed in the next six months, as illustrated in Figure 3 on the following page. Not surprisingly, Distributed Denial of Service (DDoS) Mitigation tools (71%) are the most common solution to be deployed among all respondents as the frequency of DDoS attacks and their costs continues to rise.

According to a recent report from [Corero](#), “Denial of Service (DDoS) attacks are not an expensive outlay for cybercriminals. A mid-sized attack that lasts for a whole day can be bought for around \$250 on the dark web. This amount of money is insignificant to the cybercriminal in comparison to the damage to the targeted businesses and its customers when the service they are expected to deliver or receive becomes unavailable.”

In Verizon’s 2024 Data Breach Investigations Report (an analysis of attacks occurring between November 1, 2022 and October 31, 2023), DDoS attacks were “responsible for more than 50% of incidents analyzed this year.”

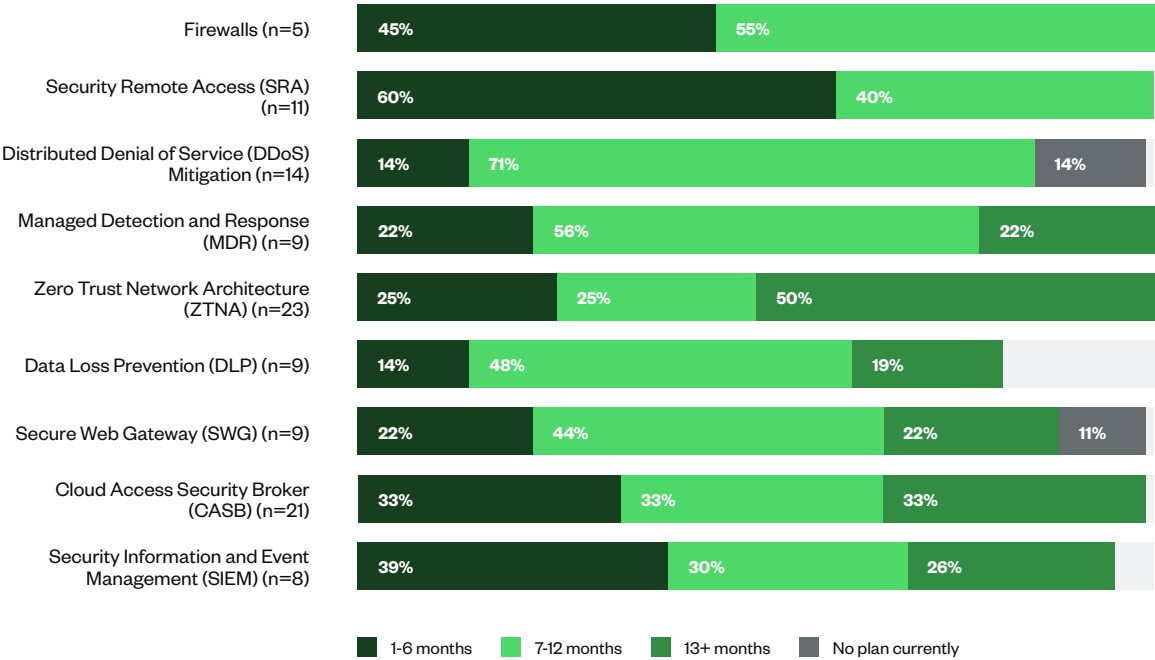
DDoS attacks are not the only threat of course. Security misconfiguration and other breaches are expensive and frequent— and largely avoidable.

In terms of costs, according to IBM’s 2024 annual Cost of a Data Breach Report, conducted independently by Ponemon Institute, the average cost of a data breach rose from \$4.45 million in 2023 to \$4.88 million. These figures reflect the costs of more than 600 organizations impacted by data breaches between March 2023 and February 2024 and were the highest increase since the pandemic. The same report states that more than half of breached organizations face high levels of security staffing shortages, representing a 26.2% increase from the previous year.

In another report sponsored by IBM, 84% of critical infrastructure incidents could have been mitigated by implementing best practices and security fundamentals, such as asset and patch management, credential hardening and the principle of least privilege. The report also revealed that the most observed web application risk was security misconfigurations, including allowing concurrent user sessions that could weaken multifactor authentication (MFA).

Figure 3

New Network Security Solution Deployment Times



What About Their Scale of Deployment?

Less than half of respondents have deployed SD-WAN solutions at scale, showing there is a significant need for those companies to catch up with those that have more evolved network and security postures. In regard to their stage of SASE framework integration, those that have taken this path appear to be taking their investment more quickly from proof of concept or limited deployment to deploying at scale, as seen in Figures 4 and 5.

Figure 4

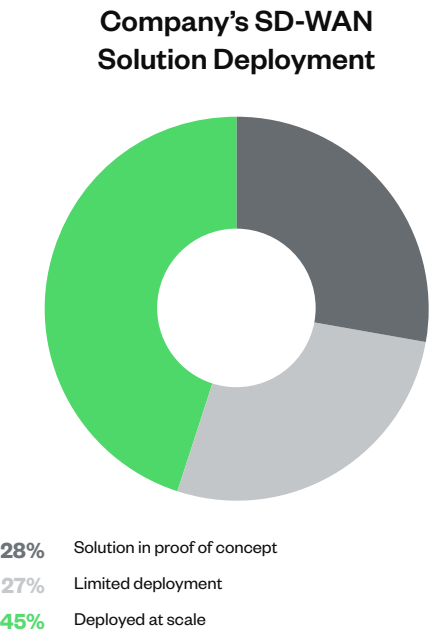
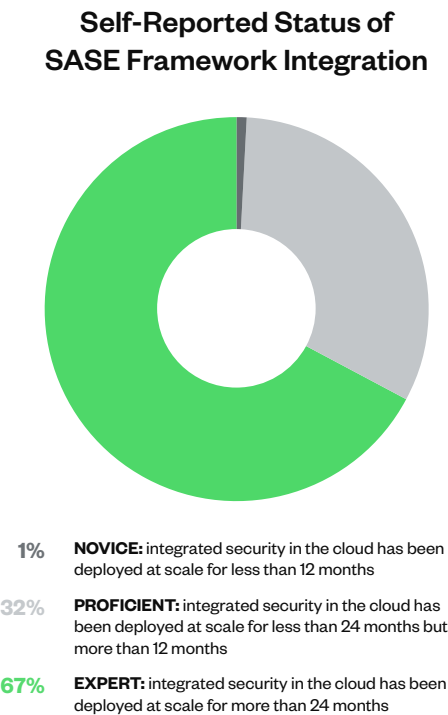


Figure 5



What Some Companies Are Getting Right About Integration

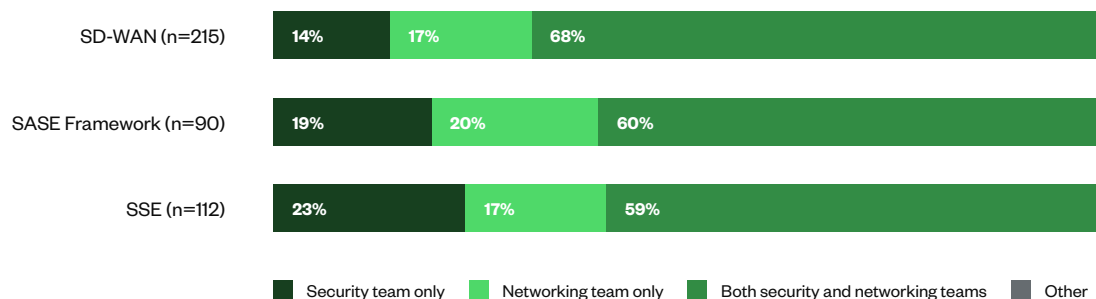
In reviewing the data for SD-WAN deployment and SASE framework integration, the mission-critical nature of these enterprise security solutions becomes undeniable. Furthermore, mature companies that have deployed SD-WAN at scale and have integrated SASE frameworks at scale have done so for at least two years. This points the way forward for those companies that have not yet taken an at-scale approach to their cybersecurity needs.

As an experienced managed service provider, GTT will work with you to create and deploy the ideal managed at-scale SD-WAN and SASE solution for your business. In addition to benefiting from the high quality of our SD-WAN and SASE providers, and our ability to aggregate all the necessary components, your business will receive an on-time, on-budget, scalable, integrated SD-WAN and SASE solution that reduces risk and capital costs.

Integrated Security and Networking Teams Most Common for SD-WAN, SASE and SSE

The need for integration between security and networking appears to be high when it comes to managing SD-WAN, SASE and SSE solutions. This is reflected in Figure 6, which examines the division of labor between networking and security teams on multiple solutions, and Figure 7 on the following page, which looks at co-management.

Figure 6



GTT is helping us by providing a fully managed service and continuously improving the safety measures to ensure that our network traffic is isolated properly and secured.

—GERTJAN MINKELS
SOLUTION ARCHITECT, CLOETTA

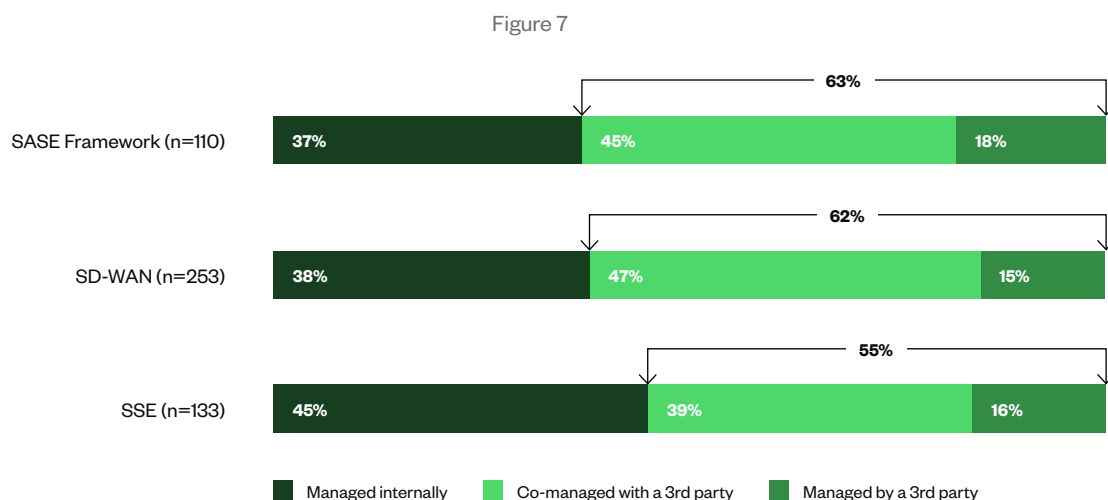




Co-Managed SASE and SD-WAN Is the Most Common Arrangement

Most respondents indicated that their organization currently must have control over some or all their SASE Framework (82%), SD-WAN (85%) and SSE (84%) solutions. This level of control may be based on working with legacy technologies and may not completely reflect the rapid changes occurring in networking and security management, co-management and fully managed services.

While fewer companies so far are willing to hand off their solutions entirely to a third party, the shift toward reliance on a third party is increasing as more organizations realize how complex it is to secure their network as they move along on their journey. This is revealed by the number of respondents that are co-managing their SASE Framework and SD-WAN solutions with a third party rather than managing them solely in house, as seen in Figure 7.

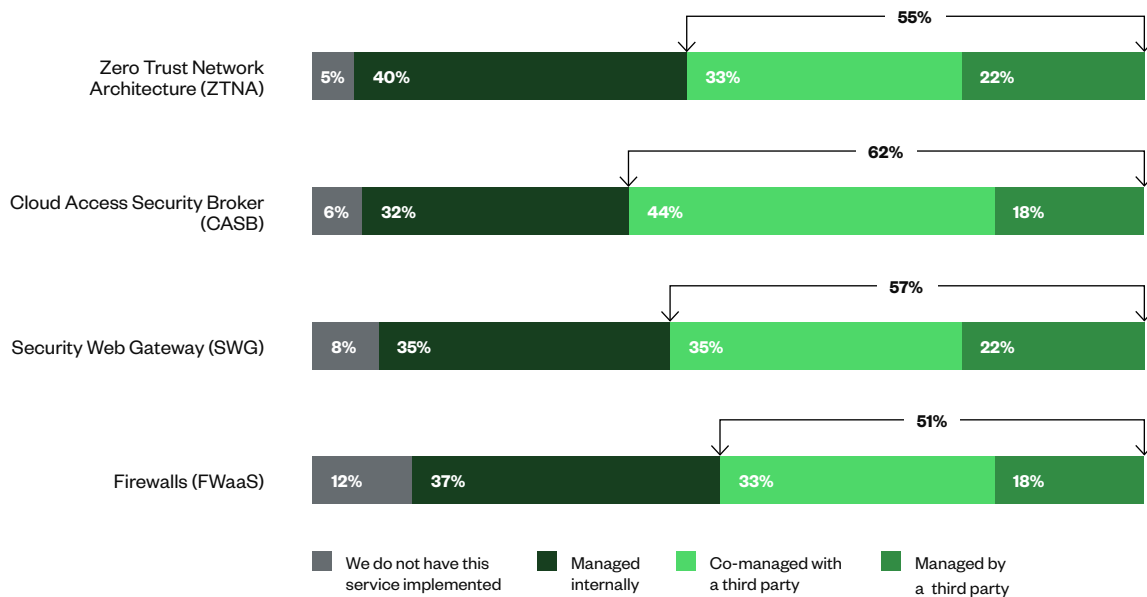


Internally Managed or Co-Managed Most Common for Most SASE Services

Similar to the responses above for SASE Framework, SD-WAN and SSE solutions, most respondents stated that their company needs control over some or all their SASE services. However, while 18% was the highest percentage for third party managed solutions such as SASE Frameworks, SD-WAN and SSE, 18% is the lowest percentage for third party managed SSE services, as shown in Figure 8 on the next page.

We also see that many companies desire a hybrid solution that enables them to co-manage their technology with a 3rd party. It is entirely possible that as these services become more complex and more integrated, many enterprises are likely to completely outsource them to an MSP with a contact at the customer site. For some this may be a permanent arrangement, while for others it may provide a transition period that enables the company's internal IT team to learn and increase their expertise.

Figure 8



We appreciate the level of professionalism GTT has brought, as well as the benefits that come from working with a global managed network and security services provider. GTT's team supported us through the change from MPLS to SD-WAN, and we leverage their technical knowledge to enhance our own skills so we can support our users in a more informed way. We are very happy with GTT's responsiveness and level of service, and we know that our business is supported by a fast, resilient network.

—MARIO PARICIO
 IT CTO MANAGER, HMY GROUP

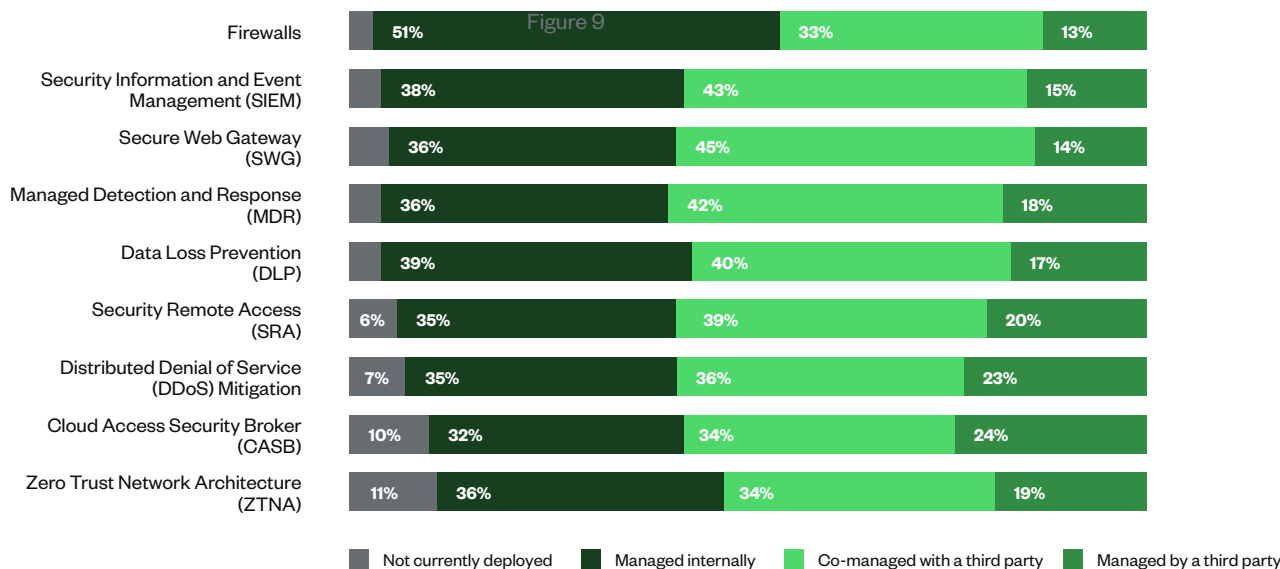
The responses in Figures 7 and 8 on the preceding two pages reveal an interesting insight. They show that for most companies there is a need for managed service providers to help overcome skills gaps and share expertise around complex design and deployment with in-house technology teams who have a profound understanding of the needs of the individual business. The combined knowledge sets lead to improved deployments.

In this way a hybrid solution that is co-managed with a third party provides the level of confidence companies need, furnishes the right mix of solutions and services, and offers knowledge and expertise that supports customer deficiencies, allowing the customer to focus on their core business.

This hybrid management process fosters deep relationships between in-house technology teams and their managed service providers and enables the two-way transfer of knowledge. We expect this hybrid process to evolve for different companies in different ways. Some are likely to offload more management responsibilities and the technology infrastructure to their MSP, so that their internal IT staff can concentrate on handling revenue-generating activities that run on that infrastructure. Others may use the hybrid process to upskill their internal IT staff, allowing them to become experts in a wide range of SASE services and take on more day-to-day management chores.

Network Security Solutions for Companies That Have Not Deployed SASE

Figure 9 shows that most organizations manage firewalls internally. This is not surprising as firewall technology is the most mature and comparatively simple to deploy and manage versus more complex and newer cybersecurity solutions that require hands-on expertise from a qualified managed service provider. Network security solutions will increase in sophistication as traffic growth increases, along with the wider distribution of users and applications, spreading the attack surface over greater areas. All these factors require the deployment and management of more tools to thwart bad actors, leading to a greater reliance on external expert MSPs.



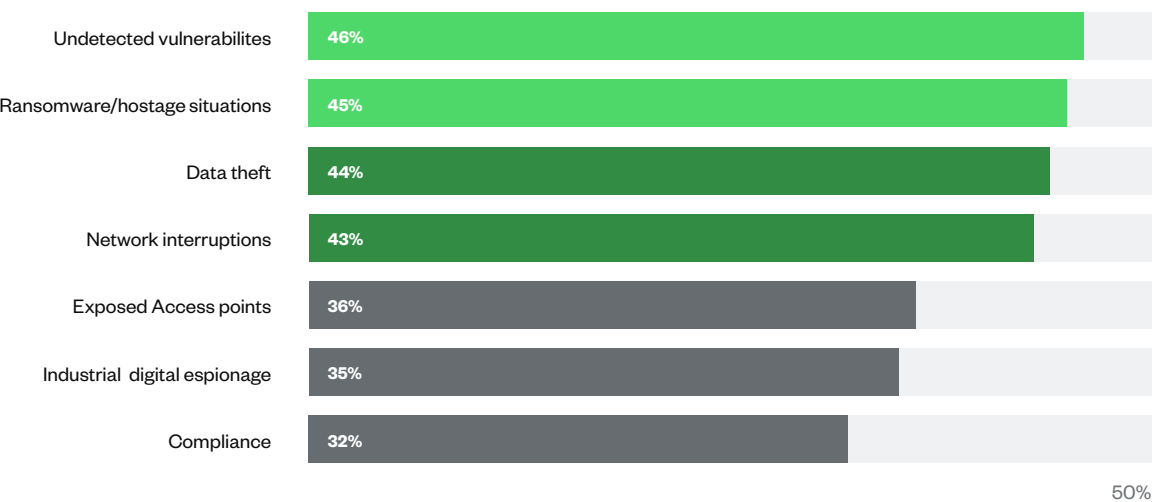
WHAT CYBERTHREAT CONCERNS ARE THE MOST PRESSING?

Undetected Vulnerabilities and Ransomware Top the List

As mentioned earlier in the top line numbers section of this white paper, respondents ranked their greatest cyberthreat concerns. The most common threats are undetected vulnerabilities (46%), ransomware/hostage situations (45%), data theft (44%) and network interruptions (43%). These are followed by exposed access points (36%), industrial digital espionage (35%) and compliance (32%).

The greatest threats tend to be those that are unknown, as the monster you cannot see is much more frightening than the monster you can. Undetected vulnerabilities sap the business in terms of energy and costs, with the average time to detection being between 10 and 200 or more days. Most companies (75%) cannot respond to a security incident the same day. Furthermore, 53% of breaches are discovered outside of the business.

Figure 10



At GTT, we’ve found that blind spots leading to undetected vulnerabilities present the greatest challenge to many IT departments. To overcome blind spots, a Managed Detection and Response (MDR) solution offers a critical service that constantly monitors the network using technology and security professionals. The result is a reduction in risk and faster response.



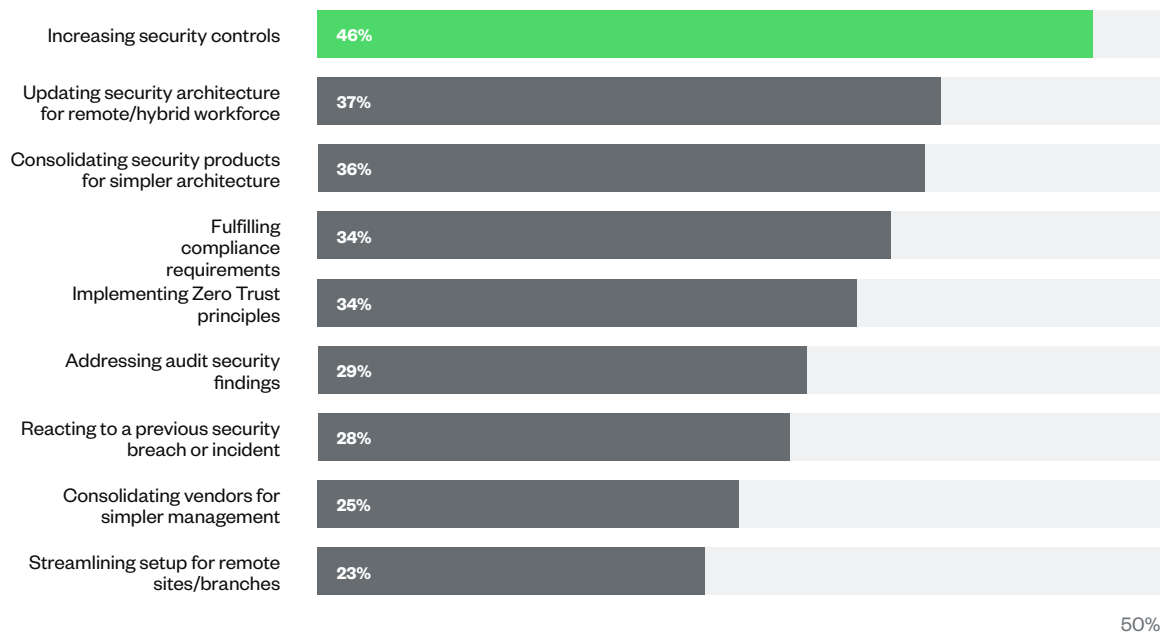
WHAT'S DRIVING ENTERPRISE SECURITY STRATEGIES AND CREATING THE GREATEST CHALLENGES?

Increasing Security Controls Tops the List of Drivers, While Challenges Around Synchronizing Security Policies Must Be Overcome

The top drivers of enterprise security strategies were also included in the top line numbers section of this white paper. They are increasing security controls (46%), followed by updating security architecture for remote/hybrid workforces (37%) and consolidating security products for simpler architecture (36%). The chart below indexes these and the additional drivers.

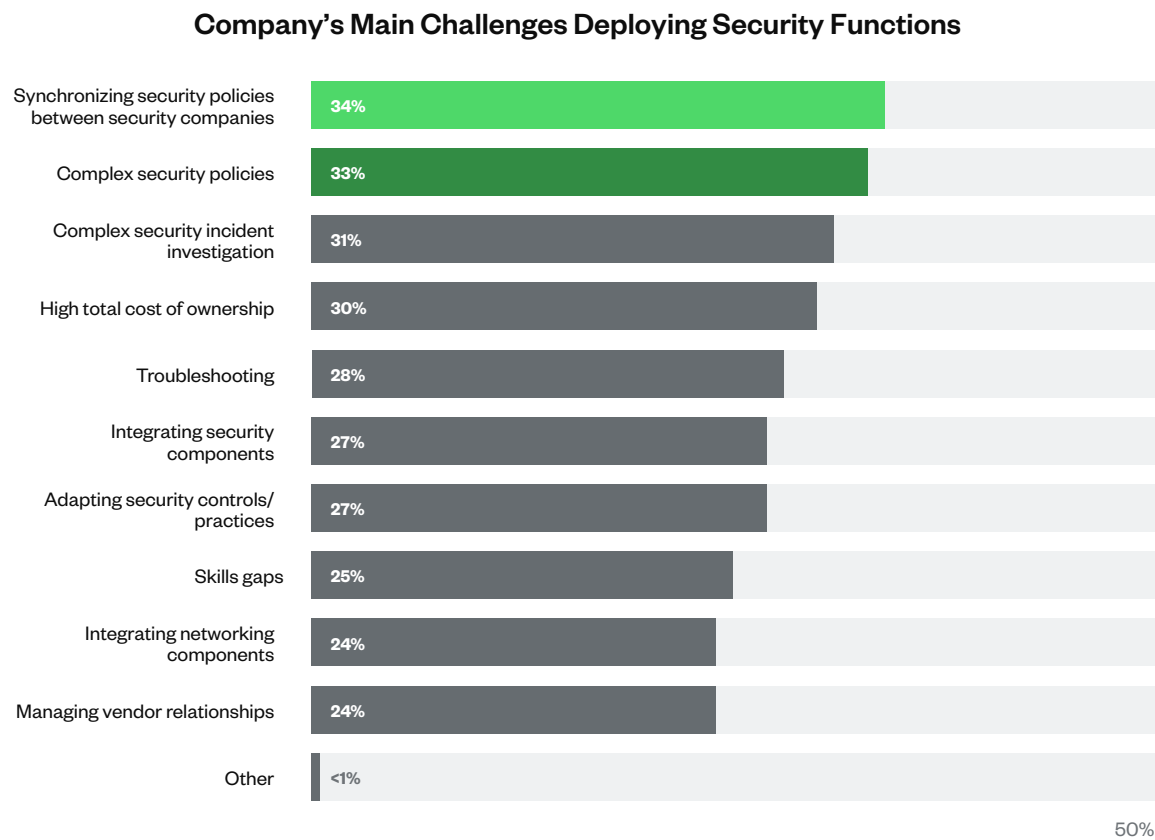
Figure 11

Company's Main Security Drivers



The next chart contains the top deployment challenges. The top two are synchronizing security policies between security components (34%) and managing complex security policies (33%), which indicates a gap between security needs and implementation capabilities. Additional challenges are listed below.

Figure 12



The data in these charts shows that focusing on developing the best security strategies is not enough. Organizations must acquire the right security team or expertise to overcome challenges in deploying their strategies, ensuring that their plan succeeds.



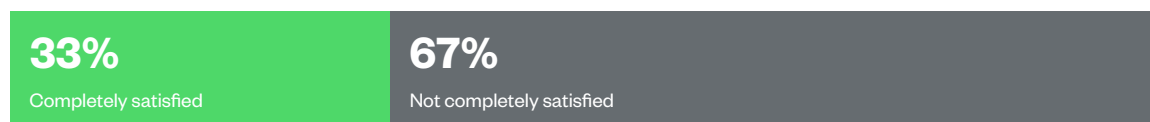
SATISFACTION WITH CYBERSECURITY IMPLEMENTATIONS

Nearly All Respondents Are Satisfied, Yet There Is Room for Improvement

More than half of respondents (67%) stated they were not “completely satisfied” with their cybersecurity implementation. This provides a significant opportunity for MSPs to emphasize the implementation phase of these deployments and add value and gain trust with excellent customer service.

Figure 13

Company’s Satisfaction with Cybersecurity Implementation



Our SD-WAN, connectivity and security services from GTT help us manage our growing cloud usage and enable quick execution of any changes we need, such as new SaaS services or spinning up new sites anywhere in the world. GTT supports a flexible and hybrid work environment wherever we go.

—STEPHEN AITKEN

CORPORATE INFRASTRUCTURE ARCHITECT, ELOPAK



The data around satisfaction of cybersecurity implementation provides insight into how the industry is not doing enough to service customers and meet expectations.

To ensure we do right by our customers, GTT focuses on providing industry-leading solutions and support. In this way, our security solutions include professional and managed services and support teams in local markets worldwide. Through our consultative approach, we guide, design, evolve and optimize your network. Moreover, we provide fully managed or co-managed options to match the specific support your network needs.

In fact, GTT is a 2023 Customer Experience Innovation Award Winner for its SD-WAN, according to TMC's CUSTOMER magazine. GTT was also recognized in 2024 by ISG for Managed SD-WAN Leadership and as a Rising Star for SASE managed services. The awards recognize best-in-class companies setting the standard in delivering exceptional customer experiences.

100%

of GTT customers surveyed who have Technical Management engaged in their deployment recommend GTT's Technical Management function.

>91%

of GTT customers surveyed stated that they would recommend GTT's Service Management offering to a friend or colleague.

MOST COMMON CYBERSECURITY SOURCE: CURRENT AND FUTURE STATE

The Shift to an Integrated SD-WAN/Security Solution Provided as a Managed Service is Expected to Top the List

Respondents indicated that a best-of-breed security solution integrated with SD-WAN describes their current or planned cybersecurity solution. However, organizations appear to be opting for the advantages of this type of integrated solution provided as a managed service for their future needs.

As far as the need for integration is concerned, an article in Forbes entitled, "Why Companies Are Struggling with Cybersecurity: Big Players in Bad Situations" describes the problem this way. "It is particularly frustrating when the cybersecurity landscape is flooded with tools and solutions targeting specific threats ... However ... (instead) of an integrated and comprehensive approach, we end up with a disjointed and compartmentalized strategy that hackers exploit. ... Throwing money at the problem without a holistic approach to the solution is ineffective."

This desire for an integrated solution as a managed service is indicated by the respondents, as shown in Figures 14 and 15.

Figure 14

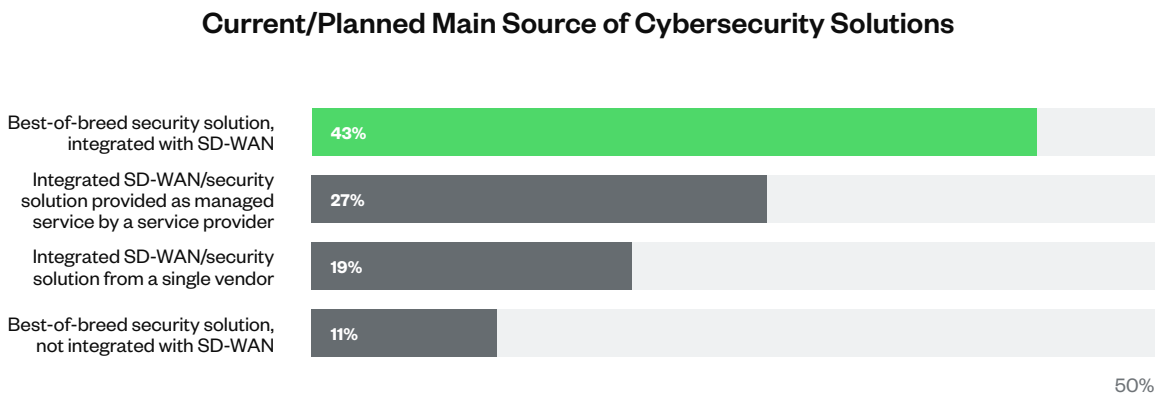
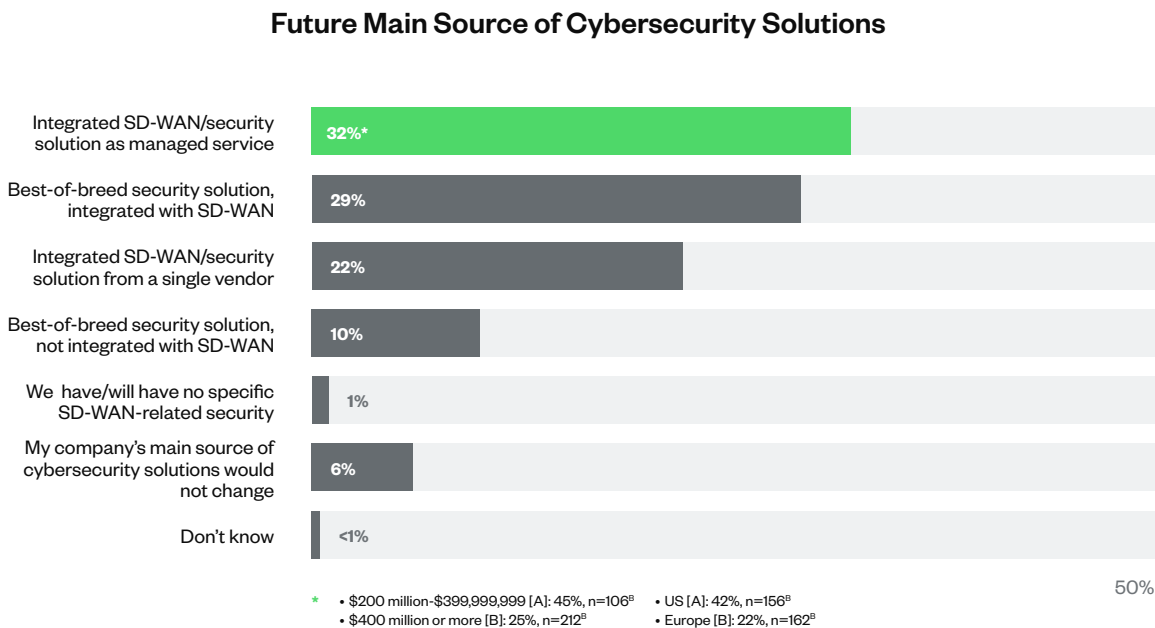


Figure 15



GTT delivers powerful and advanced SASE solutions with vendor-agnostic and client-bespoke implementations. We've awarded GTT this year's ISG Lens Rising Star for SASE (out of 84 companies reviewed with one awarded), as it is the challenger we see with the most momentum and trajectory for achieving a leadership position in this critical field of cybersecurity

—DR. KENN D. WALTERS
LEAD ANALYST, ISG

MOST COMPANIES USING SASE (71%) AND SD-WAN (72%) SOLUTIONS ARE CONSIDERING INTEGRATING MORE SERVICES

Overall Vendor Security Capabilities (50%) and Overall Vendor Network Engineering Capabilities (47%) Would Drive Companies to Consider a Single-Provider Solution for Both Network and Cybersecurity Services

Figures 16, 17 and 18 provide additional insight into the evolution of SASE and SD-WAN solutions, along with what factors are motivating companies to consider a single-provider solution. Principal among them is the realization that the complexity of today's security and networking solutions requires more integration, outside expertise and the convenience and responsiveness of a single-provider solution. A single strategic partner managing the entire program increases efficiency, provides a single point of contact that makes communication easy and simplifies billing.

Figure 16

Considered Evolution of Company's SASE Solution

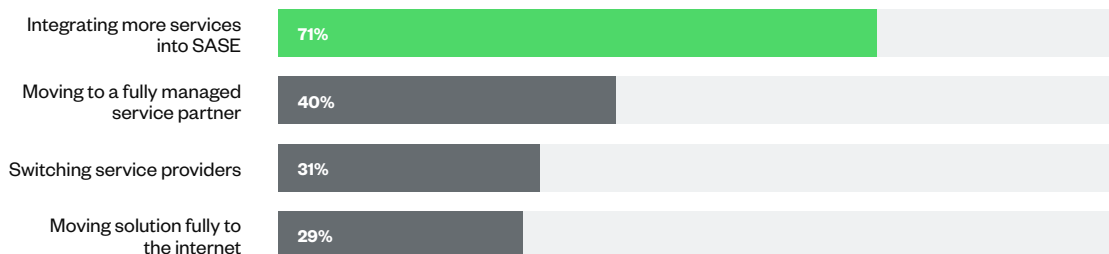


Figure 17

Considered Evolution of Company's SD-WAN Solution

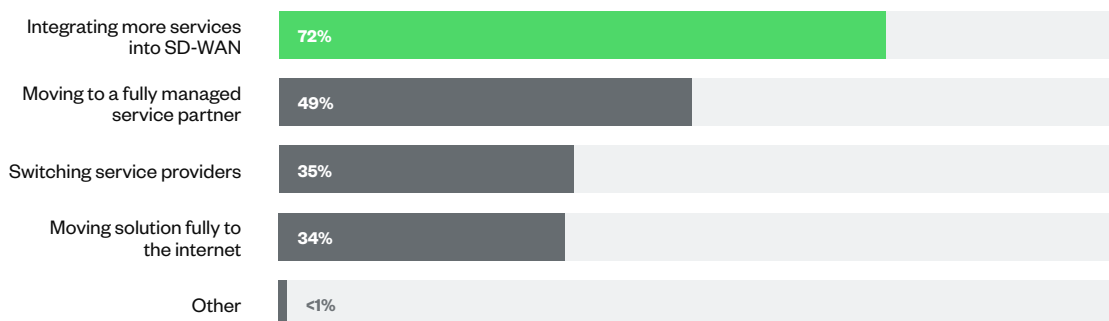
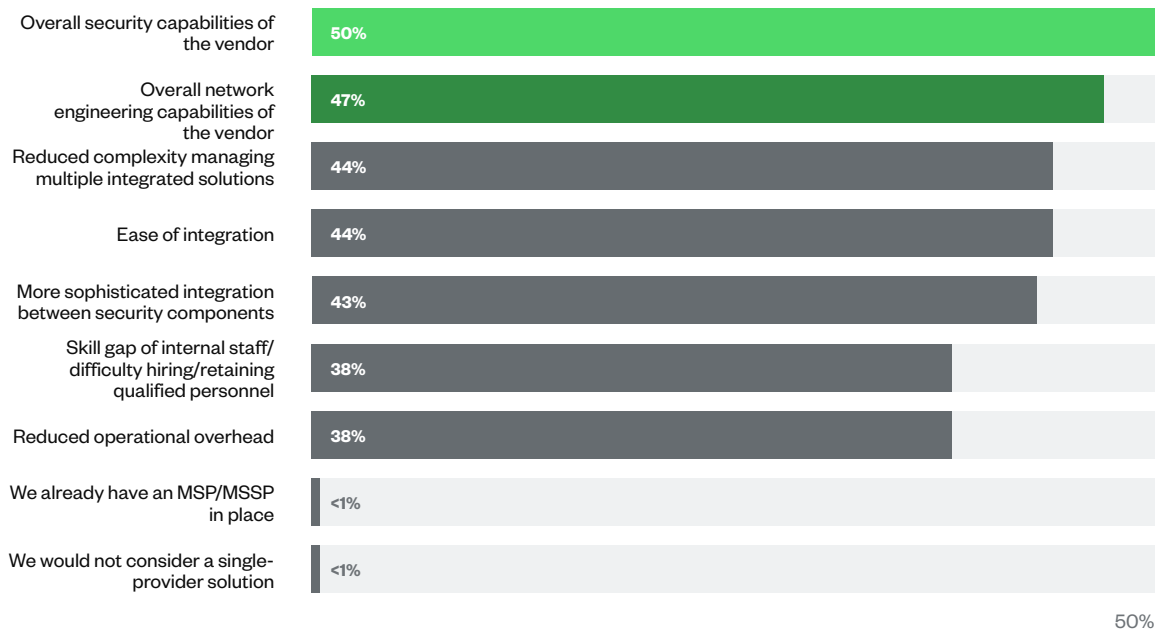


Figure 18

Driving Factors to Consider a Single-Provider Solution



50%

INTEGRATION OF SSE AND SD-WAN IS A LOGICAL NEXT STEP

Nearly All Companies (97%) Support Integration

Almost half of companies (47%) report that their cybersecurity and networking teams work separately but communicate and collaborate regularly, while 41% report that their cybersecurity and networking teams are fully integrated. Taken together, the data in Figures 19 and 20 on the next page shows the importance of integration in today's networking and security world.

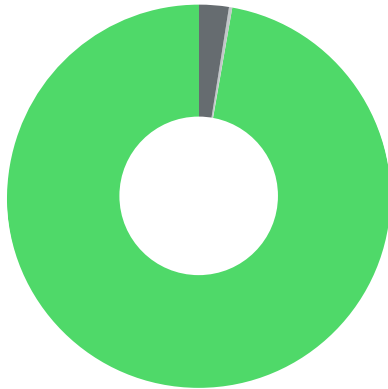


Through collaboration with GTT, we've designed and built a simplified, agile and efficient network to enable our cloud-first strategy, improving our global operation — from supply chain management to employee productivity. GTT offers us flexibility and a solid track record of delivering reliable global network solutions which makes GTT an ideal partner.

—STEVEN VANDAMME
CIO, BARRY CALLEBAUT

Figure 19

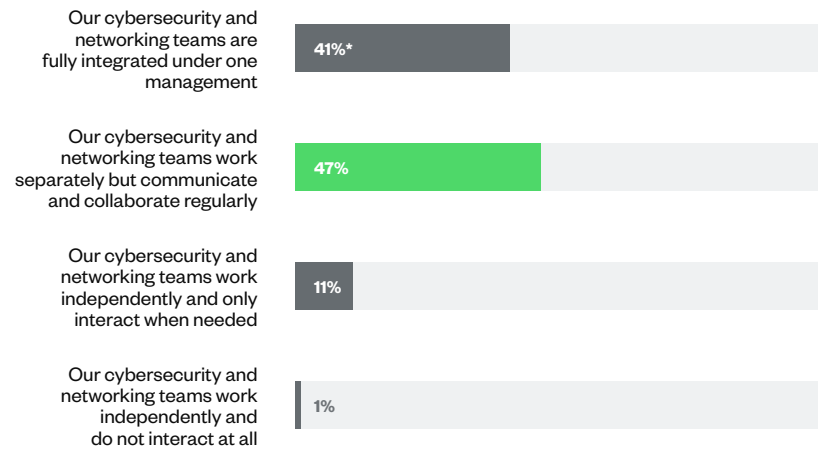
SSE and SD-WAN Integration a Logical Next Step



97% Yes
2.5% No
0.5% Unsure/I don't know

Figure 20

Company's Cybersecurity and Networking Teams' Integration



* • US [A]: 27%, n=156^a
 • Europe [B]: 55%, n=162^b

Integration, when properly performed, reduces the overall complexity of a network and leads to improved performance and other benefits. Examples include:

IMPROVING ONE'S SECURITY POSTURE

by gaining visibility into network traffic and security events by applying AI, machine learning and automation to rapidly detect and respond to threats.

ENHANCING SECURITY

for users, devices and applications by improving collaboration between teams and providing better oversight.

REDUCING LATENCY

by avoiding the routing of traffic through multiple network and security gateways.

INCREASING AGILITY

by enabling companies to quickly deploy new applications and services.

PROMOTING SIMPLICITY

by eliminating the need for multiple point products, which eases management and delivers a unified experience.

CUTTING IT COSTS

by simplifying operations while protecting existing technology investments.

Moreover, a thoughtfully implemented integration facilitates various digital transformation initiatives, including remote work capabilities, branch office modernization and cloud adoption strategies. Integrating SSE enables companies to enhance their security posture, simplify operations and support digital transformation initiatives while protecting against evolving cyberthreats.

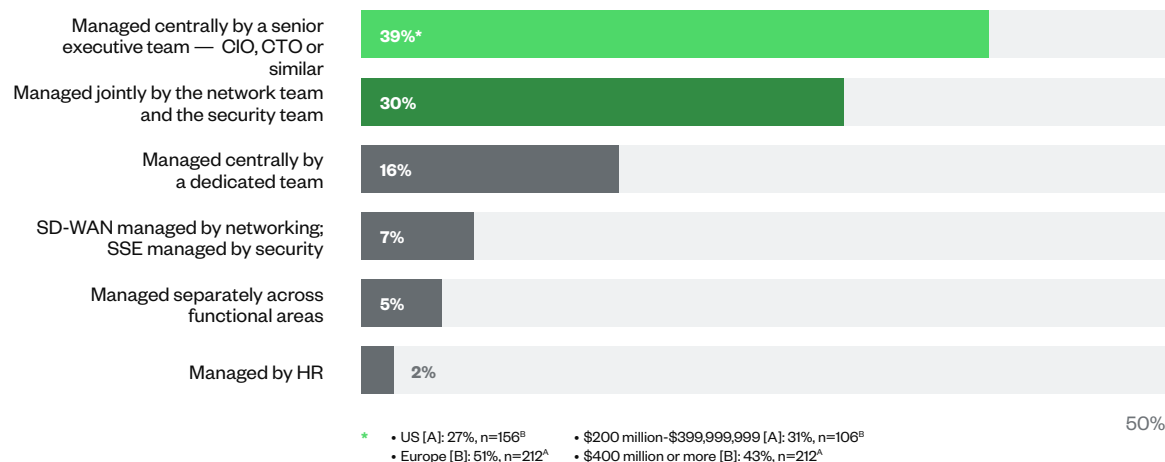
THE PROCESS OF SELECTING A CYBERSECURITY SOLUTION VENDOR

Senior Executives and Network and Security Teams Responsible

According to the respondents, organizations that place senior executives as responsible for making the selection are more likely to be European based (51%) than US based (27%). Revenue is another metric that correlates with senior executives selecting such solutions. Those that earn at least \$400 million in revenue (43%) are more likely to involve senior management than those that earn \$200 million to \$399,999,999 in revenue (31%).

Other data that emerged from the study is that network and security teams are jointly responsible for selecting cybersecurity solution vendors (30%), followed by dedicated teams and other selection processes.

Figure 21



THE EFFECT OF INTEGRATED VS. NON-INTEGRATED NETWORKING AND SECURITY TEAMS

The quality of security appears to be the greatest differentiator. In Figure 22, 57% of integrated teams selected stronger security as one of the top three results. In Figure 23, 38% of non-integrated teams selected network security as not as strong as it could be. This could be due to networking teams, which are not integrated with security teams, placing less value on security than those that are integrated and are more likely to recognize its value.

An interesting juxtaposition is that integrated teams chose faster decision making (53%) and more creative solutions to problems (42%), compared with non-integrated teams choosing faster decision making but only in their respective areas (59%) and lack of coordination or clarity in team responsibilities (49%). Taken together these responses suggest that the integration of Networking and Security teams produces better overall results from security to decision making.

WHY IT MATTERS

Positive business outcomes, faster problem resolution and clarity in responsibility result from the alignment and integration of the Security and Networking teams.

GTT provides distributed enterprises with holistic solutions that lead to reliable, resilient and protected applications, machines and data—anywhere in the world.

Figure 22

Results of Integrating Networking and Security Teams

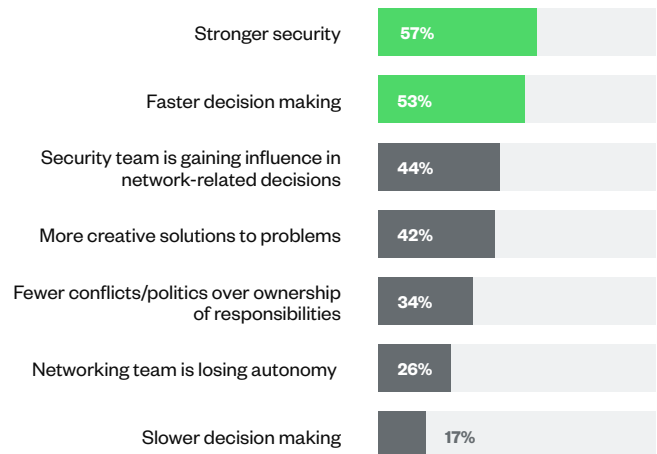


Figure 23

Results of Lack of Networking and Security Teams Integration

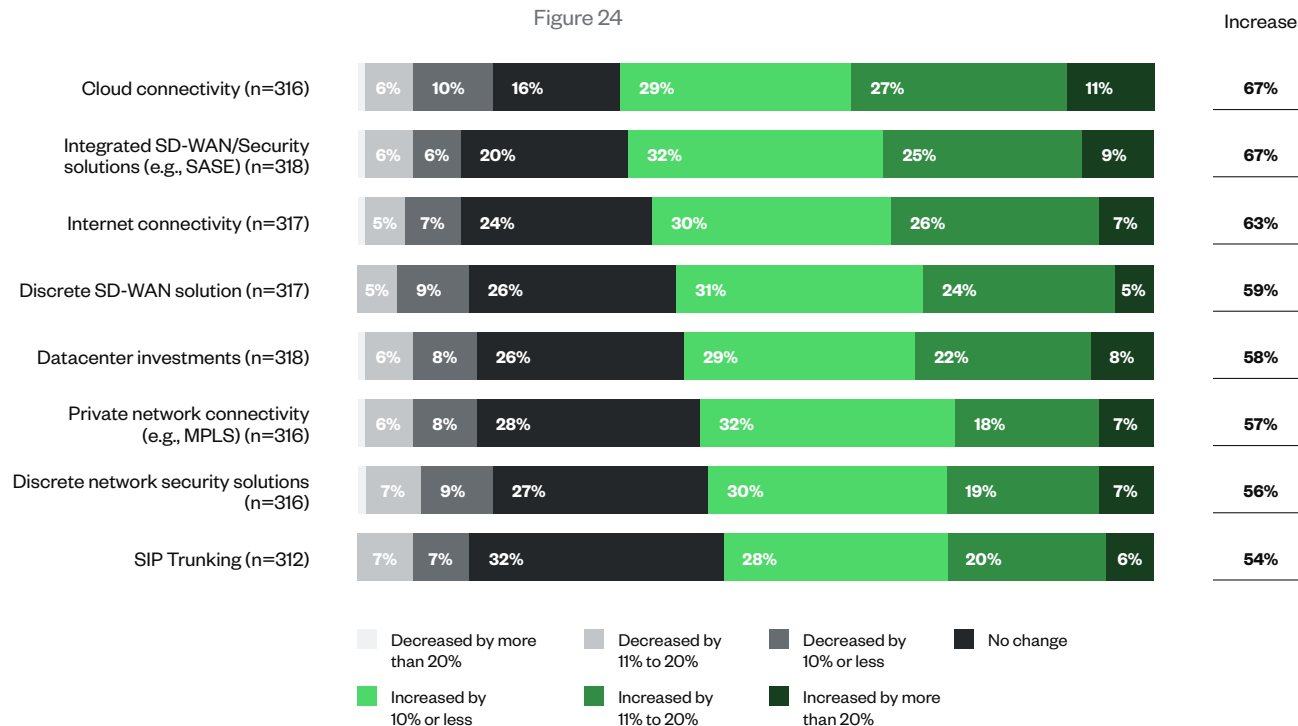


OVERALL INCREASE IN INVESTMENT SPENDING

More Than Half of Companies Increased Their Investments in All Network Areas Over the Last Year

According to respondents, companies are most likely to have increased investments in cloud connectivity (67%) and integrated SD-WAN/Security solutions (67%) over this time period.

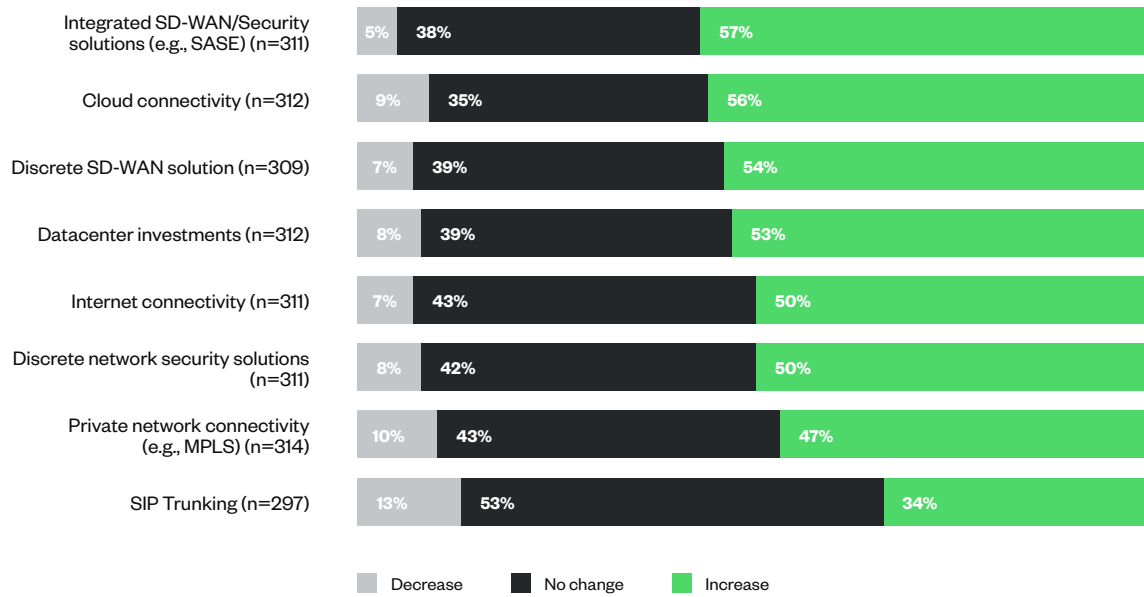
Figure 24



Most Companies Plan to Increase Their Investment in Most Network Areas Next Year

The overall increase in investments indicates that most companies see value in improving their protection against cyberthreats and outages and enhancing their cloud and digital operations. Only private network connectivity and SIP Trunking investments will not increase among fewer than 50% of companies in the study, according to respondents. This is because they increased their spending in these areas by more than 50% in the previous year.

Figure 25



GTT's flexibility and strength as an access-agnostic provider focused on getting our services up and running as fast as possible.

—IAIN BLAZEY
 HEAD OF IT, MITSUBISHI ELECTRIC



FINAL THOUGHTS

Companies with SSE and SD-WAN solutions realize that integrating and deploying SASE is the logical next step. They are also discovering that co-managing their technology with a third party managed service provider (MSP) offers a range of benefits that contribute to positive business outcomes. A co-managed solution ensures that the customer gains visibility and insights, while providing the customer with the choice of taking corrective action in-house or tasking the third party MSP to handle the issue. Moreover, integrating networking and security teams enables organizations to become more agile and efficient in their planning and execution.

For organizations that require control over some of their solutions, an experienced MSP brings expertise that the customer may lack, allowing the customer's IT team to focus on their strategy and core business. Other organizations view the co-managed option as a journey that allows them to build trust with their MSP. In this way the customer can authorize the MSP to manage more of their solutions as their comfort level increases. Lastly, there are also organizations that see the opportunity of engaging an experienced MSP to help train and empower their internal IT staff to learn how to handle more technology. Selecting the co-managed option, for either of these reasons, helps companies solve their challenges in ways that best fits their needs.

Other Papers from GT Created in Collaboration with Hanover Research

Learn about current and near-future use and adoption of SD-WAN, including what attributes to consider when selecting a Managed Service Provider (MSP) in the white paper [UNLOCKING THE POTENTIAL-Understanding Managed SD-WAN Adoption](#).

ABOUT GTT

GTT is changing the way you manage your enterprise network.

Simply and securely connecting people and machines to data and applications anywhere in the world. Providing one technology platform to connect, orchestrate, virtualize and automate your network. One digital experience to visualize, engage, consume and manage every element through a single partnership to support you whenever, wherever and however you need.

It's time to take back control. It's time to envision a new era of networking and security as a service. GTT Secure Connect converges managed SD-WAN and cloud-based security, delivering a SASE framework that consolidates multiple security point solutions — including Firewall as a Service (FWaaS), Secure Web Gateway (SWG), Cloud Access Security Broker (CASB) and Zero Trust Network Access (ZTNA) into an homogenous service offering that reduces network and security complexity.

The addition of FWA 5G connectivity and additional security enhancements to our Distributed Denial of Service (DDoS) and Managed Detection and Response (MDR) services presents a complete solution for our customers that provides secure multi-cloud access, reach to the edge and proactive protection from cybercriminals.

GTT can deploy on premise and support multiple functions, applications, priorities. GTT connects via wireless, satellite or wired technology and continues to evolve the technologies deployed on the GTT Envision platform. GTT connects, secures and simplifies complex technology challenges for the benefit of distributed enterprises.

To learn more about **Secure Connect**, **GTT's SASE framework solution** watch this short video: **GTT Secure Connect – A SASE Solution.**



GTT ENVISION

A single global technology platform to connect, orchestrate, virtualize and automate enterprise networks. GTT Envision enables enterprises to simply and securely connect people and machines to data and applications — anywhere in the world. This is a compelling means through which our customers can simplify their complex networking, security and cloud needs.

Learn more at [GTT.net](https://www.gtt.net).