Creating a Unified Approach for Secure Enterprise Networking

Contents

Executive Summary **3**

IT and Technology Need to Deliver Better User Experience (UX) and Cyber Protection **4**

Customer Experience (CX) and Workflow Transformation are Top Strategic Business Priorities *4*

Understanding Customers and Cyber Security are Top Business Challenges *6*

Maturity of the Digital Infrastructure to Adapt to Business Needs **8**

Common Shortcomings *9*

The Case for Network and Security Transformation **11**

Future Outlook & Conclusion **12**

About GlobalData **14**

Contact Us **15**

Executive Summary

Businesses are looking to be more agile in their operating models to balance the myriad of strategic priorities against business challenges which are constantly in a state of flux. GlobalData's research shows that the top business priorities are improving customer experience (CX) and using new technologies, such as cloud and Artificial Intelligence (AI), to automate workflows. The top challenge is the ability to improve customer insights across all segments, traditional and digital channels, and touchpoints. Further to this, protecting against the threat of cyber security attacks is also a major challenge for nearly two-thirds of business leaders surveyed worldwide.

This comes at a time of a major platform change. Businesses have moved away from traditional fixed networking where traffic connected to users, applications, and devices, at central locations, such as an enterprise data centre, campus, or branch, to a model that also supports widespread remote working. Users rely on multiple access technologies, use a myriad of devices, and require a new approach for delivering secure networking in a cloud-centric world. With the genie out of the bottle, network protocols and security policies are converging. Thus, businesses require digital infrastructure that provides secure access to data and applications for the hybrid workforce.

Platforms are like ecosystems. When they change, everything else must adapt. Unlike perimeter-based security approaches that inspected traffic through firewall devices and manual look-ups, this new architecture, often referred to as Secure Access Service Edge (SASE), promotes a best of breed approach with elements such as a secure web gateway (SWG), zero-trust network access (ZTNA), and cloud access security broker (CASB) to ensure a consistent and secure access to web, cloud, and/or private applications for users on both sides of the proverbial firewall. This report is based on the research conducted by GlobalData, independent research and advisory firm.[1] The study finds that IT leaders need to plan for the following:

- **Dramatic Shifts in Usage Behaviour:** Some 68% of businesses are seeing more corporate traffic being generated from outside the traditional firewalls. Likewise, nearly 80% of the enterprises surveyed are directing this corporate traffic primarily to the cloud. Within the next 18 months, nearly all traffic will come from outside the office and directed to the cloud, bypassing the branch and campus environments. Most enterprises use the Internet to carry over 50% of their network traffic via secured tunnels, instead of private networking.

[1] The study surveyed nearly 160 C-level executives covering many Fortune 500 companies who are responsible for networking and security services across the USA, Europe (France and Switzerland) and Asia (Hong Kong and Singapore). Respondents surveyed represented first-hand viewpoints from 17 industries.

- **Increases in Network and Cloud Investments:** Given these trends, the locations of clouds will determine infrastructure strategy and investment. More notably, 86% of business and IT leaders are increasing their investments into network and security with 23% are planning an investment more than 10% greater than the previous year.

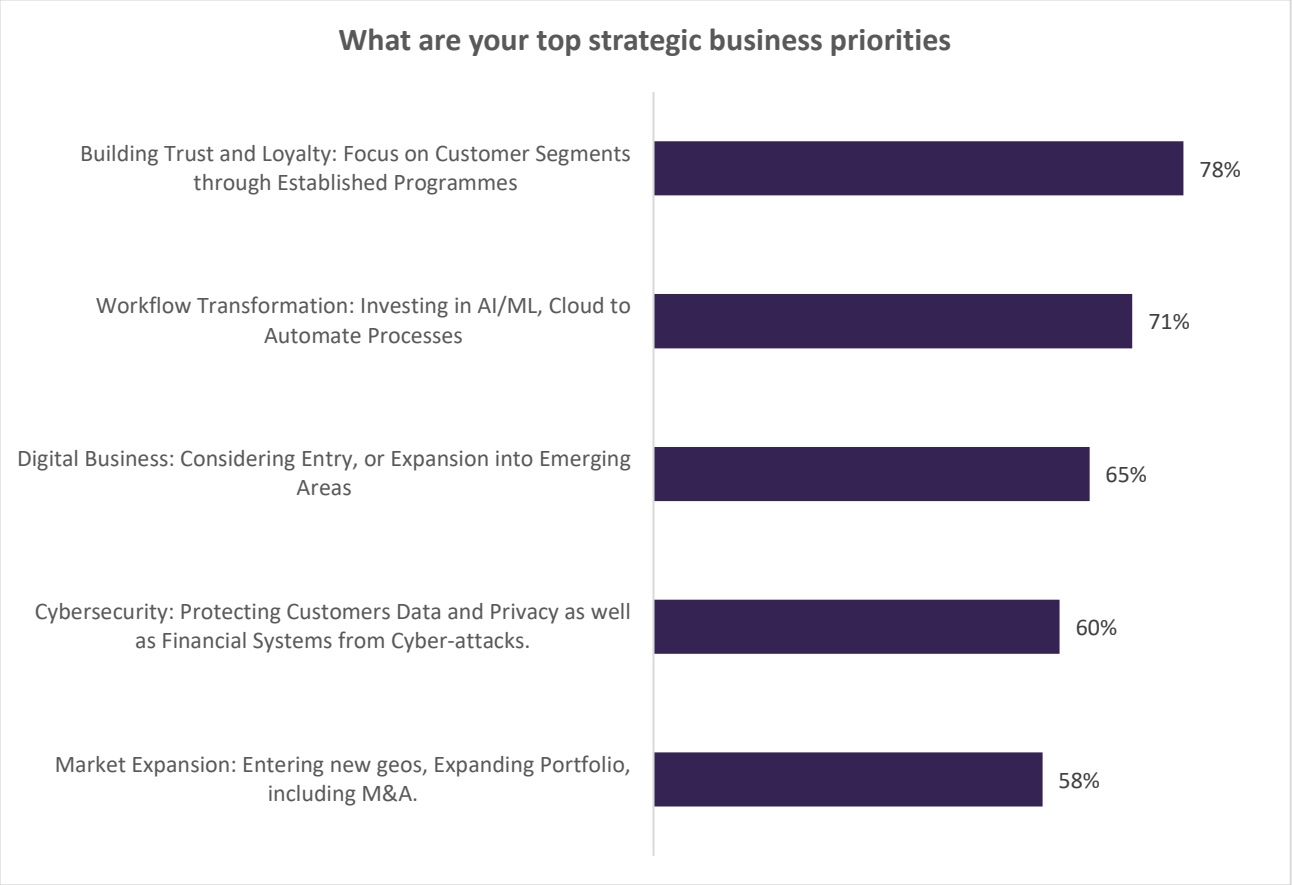
- **Proactive Strategy:** With multiple strategic priorities and strategies in play influenced by digital infrastructure, 36% of the ICT budgets are being driven outside traditional IT Departments and by the lines of business directly. Nearly one-third of the budgets are being allocated to projects that set out to transform business and challenge the status quo.

- **Convergence of Network and Security Posture:** While SASE frameworks are well-known, there is considerably more work to be done to align network and security vendors. Despite convergence, survey respondents are using more security than network vendors. And in over one-third of the cases, the vendors are not the same and aligned.

IT and Technology Need to Deliver Better User Experience (UX) and Cyber Protection

Customer Experience (CX) and Workflow Transformation are Top Strategic Business Priorities

The transformation of businesses using digital solutions is now in full swing. This is becoming a necessity for survival, especially for business-to-consumer firms. Based on GlobalData's research, the top strategic business priority is customer-focused: 78% of respondents indicate their priority is to build trust and loyalty among customer segments through established programs and improve CX. Technologies now play a key role in enhancing customer interaction, allowing customers to engage brands through different channels based on their preference. Customer expectations are also changing, and they now demand faster response, as well as the ability to reach businesses through a range of methods such as mobile apps, email, contact centres, website, SMS, and chat apps (e.g., WhatsApp). This makes it imperative for businesses to gather information about their customers and engage across different channels and touch points (e.g., in-store interactions, online sales, outbound marketing, and customer service).



Source: GlobalData Survey 2024, n = 158

With customer engagements not limited to one business function, there are now various applications used across lines of business (LoB) for customer engagement, and data may be stored in various locations. To optimise CX, there is a need to connect systems, applications, and data across departments. Workflows also need to be streamlined and simplified, which can result in greater productivity.

The second highest strategic business priority (71% of respondents) is related to workflow transformation by investing in AI/ML, cloud, and other technology stacks to automate back-end processes (e.g., onboarding and compliance). AI-based chatbots are now commonplace and the continued advancement in AI technology will enable chatbots to become more effective in handling more customer complex requests and handing over the interaction to a human in session and context, when needed. AI-based assistants are also enabling employees (including contact centre agents) to become more productive. This can be in better ability to identify likely reasons for calling to support advanced routing, recommending next best actions, providing real-time sentiment analysis, and call summarisation.

As enterprises continue to pursue better CX, they see greater opportunities in developing a digital business. This is ranked third in the list of key strategic priorities (65% of respondents). Besides improving customer engagement, a digital business is also about leveraging data for insights, developing new business models, improving operational efficiency, and allowing for faster decision-making. Digital businesses tend to also operate at a lower cost, better able to reach wider audiences and improve time to market for new services. This often results in the greater use of cloud services, including SaaS, and PaaS to support many of the emerging business requirements.

While digital businesses are an aspiration by nearly two-thirds of respondents, there are also legacy core business systems closely linked to traditional processes. There are limitations of data that can be uploaded to the cloud due to reasons such as regulatory compliance, data protection, and cost of migration. This means that the IT environments are becoming more bifurcated. This can create added layers of complexity as employees accessing both traditional and/or new systems from more locations.

Other high priority areas include the need for cyber security and protecting customer data and privacy from cyber-attacks (60%); market and portfolio expansion including M&A (58%); attracting top talent (53%), ensuring financial resiliency and improving business continuity planning (47%). All of which are important for achieving corporate goals, allocating resources and managing performance.

Understanding Customers and Cyber Security are Top Business Challenges

The digitisation process involves adopting new technologies, modernising existing applications, and ensuring legacy environments interconnect, where needed, to support the customer buying journey and lifecycle. Enterprises face some common hurdles, such as organisational and technical challenges. The top business challenge for enterprise, among 70% of respondents, is their ability to improve customer insights and predicting buying behaviour. While data analytics tools have been widely available for some time and are getting more sophisticated, the challenge for businesses is the ability to connect disparate data repositories, often hosted in different environments, to deliver real-time capabilities and insights. Having full visibility into customer interactions provides better insights that help to predict customer buying behaviour and trigger personalised services to drive monetisation.

Source: GlobalData Survey 2024, n = 158

As businesses gather more customer data and mine for insights, cyber-attacks and data breaches are also a major concern. Data breaches can cause considerable damage to a business including financial losses, regulatory repercussions, and reputational damage. Losing customer data can also trigger other fraudulent activities downstream (e.g., identity theft). Data management including governance and visibility is therefore crucial especially when employees are accessing sensitive data (that can be residing in various environments). Having more granular identity and access policies using real-time data for users, devices, and applications, for example, will help to manage the risk of cyber-attacks, especially with remote working. Many of these newer security solutions promote zero-trust concepts and multi-factor authentication.

Moreover, while businesses aim to elevate CX by supporting different traditional and digital channels, they have found it challenging to deliver consistent UX. Some 60% of the respondents indicated this as a key business challenge. While businesses are going digital, they are also transforming their traditional channels. For example, brick and mortar stores are featuring more self-service kiosks, immersive experiences (e.g., AR/VR), offline to online integration of ICT systems (e.g., inventory management, POS, etc.), and are looking to improve visibility across the supply chain.

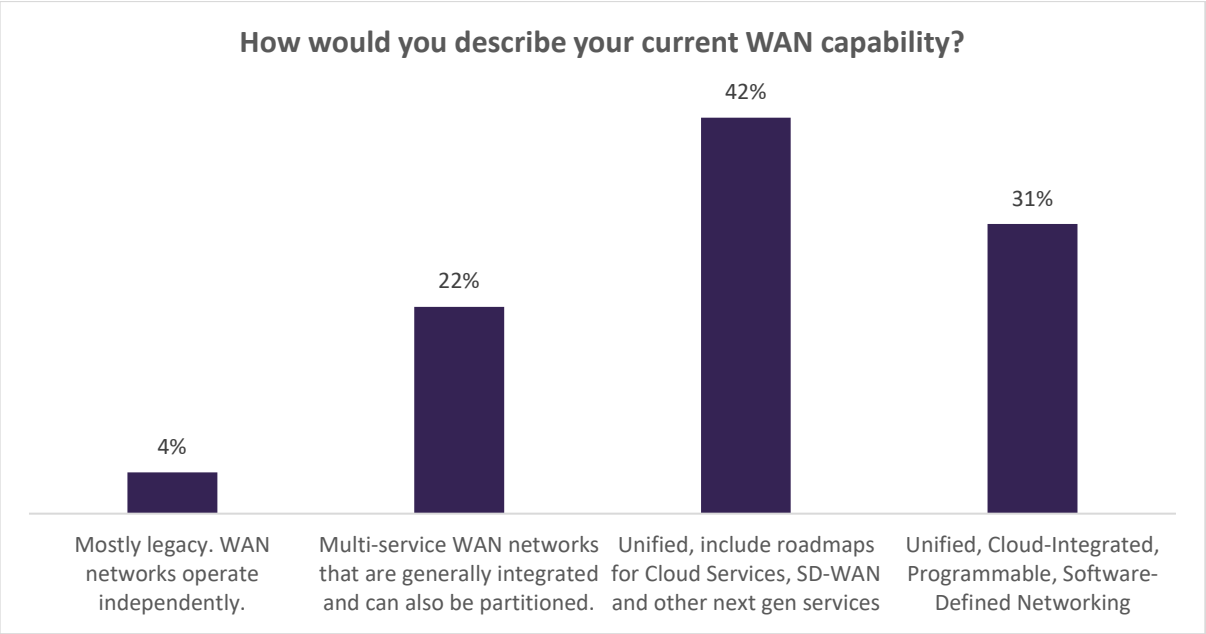
Some enterprises such as banks have also been reducing their branch footprint and pivot to online presence, mobile apps, pop-up locations, and digital kiosks.

While there have been a lot of interests and excitement with the use of AI and data analytics to enhance CX, there are now greater emphasis on getting the infrastructure right to deliver the desired outcomes. There is a need for greater agility in connecting their IT systems as well as securing them. Other concerns have been around the ability to support customer expectations such as speed, immediacy, and convenience (56%). In general, businesses have found that compliance requirements (52%) are also increasing. Global businesses with multi-jurisdictional requirements are looking for ways to better automate these processes.

Maturity of the Digital Infrastructure to Adapt to Business Needs

The wide area network (WAN) is vital in supporting business operations in a hyperconnected world. Technologies now form part of business processes, connecting supply chains, business partners, customers, and even machines. Over the years, the WAN has also evolved and less than 5% of enterprises in this study rely mostly on legacy WAN solutions. Enterprises have taken steps to consolidate their WAN while leveraging software-defined networking (SDN) technology to achieve greater flexibility. SD-WAN has become mainstream as companies use the technology together with Internet access to connect branch sites more effectively and reduce the need for costly private connectivity (e.g., MPLS-based networks).

However, only 30% of enterprises are more advanced in adopting a platform approach for their networking requirements. The WAN is no longer just connecting offices, branch sites, and data centres. It needs to connect to IT systems and applications residing in third-party data centres and in multiple public clouds. It equally needs to connect to different sites where data is generated including retail stores, edge computing systems supporting campus automation (e.g., warehouses, factory facilities, and distribution centres), and remote/mobile workers. More importantly, the WAN needs to become more agile and programmable to adjust dynamically to the changing IT requirements. With a unified platform, some enterprises can dynamically configure their WAN to achieve the performance required by business applications (e.g., network latency and jitter), gain visibility into the network security and automate compliance. Some capabilities can also support the ability to connect to different public clouds in a cost-effective matter and flexibility in connecting to other systems through APIs. There are also advantages in automation and orchestration.



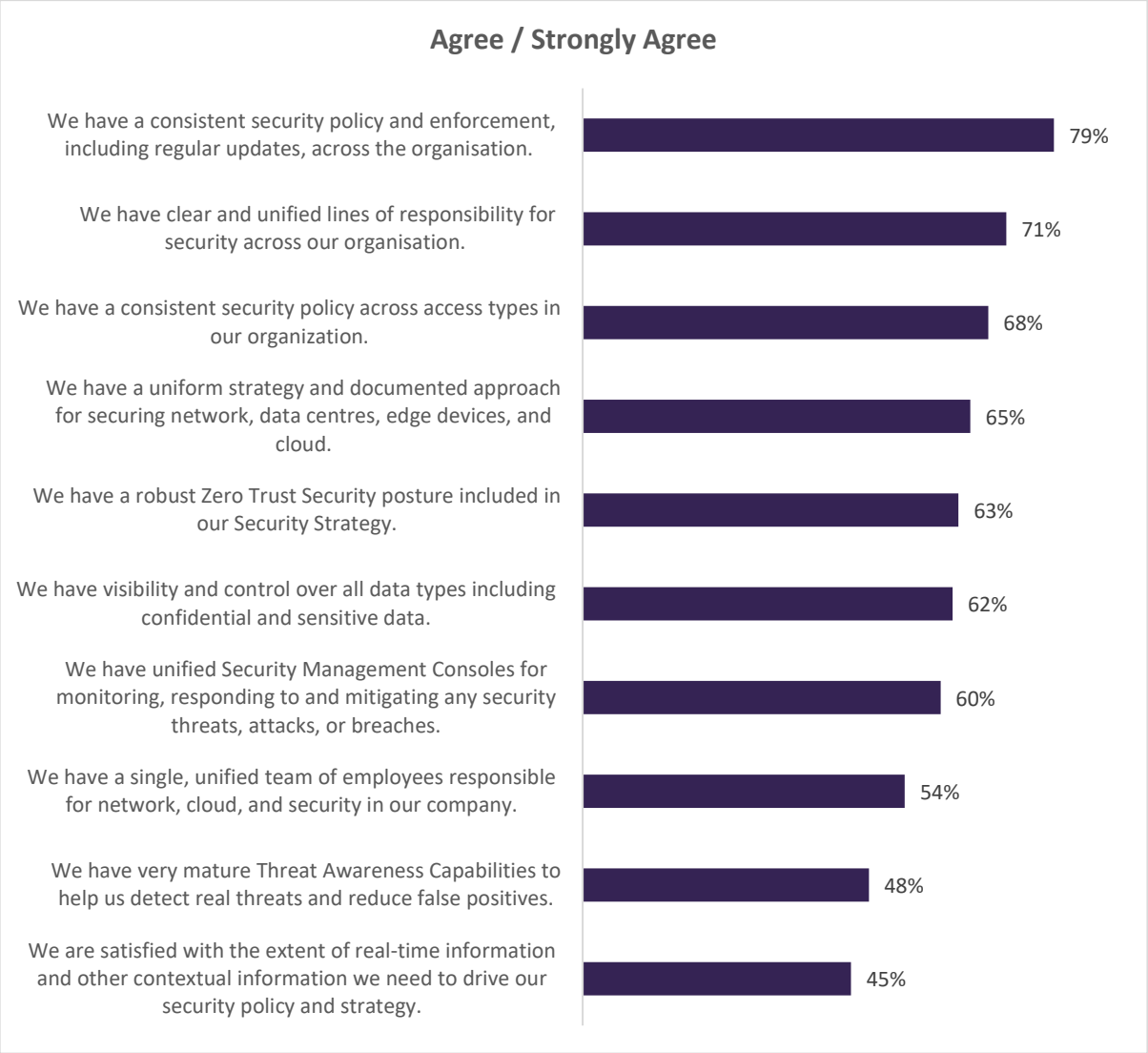
Source: GlobalData Survey 2024, n = 158

Common Shortcomings

Most of the enterprises today do not have end-to-end visibility to understand usage and performance. Many enterprises are relying on traditional approaches to perform troubleshooting which can take time while end-user experience is compromised. A platform that is equipped with full-stack observability (FSO) provides faster insights into the network and can help pinpoint issues more rapidly through the use of telemetry. There is also ongoing development around predictive analytics to ensure that network resources are configured correctly to prevent any issues from surfacing. Enterprises are also facing challenges in aligning network and application performance as they rely more on the public Internet for connectivity, which can be unstable without an underlay strategy. Some mission-critical applications have stringent latency requirements while other applications (e.g., video for collaboration) require higher bandwidth. The ability for the network to be adaptive and adjust to business intent is therefore crucial for ensuring performance and maintaining user experience.

Similarly, in the cybersecurity domain, most of the businesses surveyed have a consistent policy and enforcement, including regular updates across the organisation. Cybersecurity has always been a key priority for IT departments, but it has in recent years been discussed in the board room as more high-profile cyber breach incidents have been reported, detrimental to the businesses and customers impacted.

This has driven organisations to boost their IT security. However, there are still gaps as the cyber-threat environment continues to evolve. Enterprises are not confident that they have mature threat awareness capabilities and information (real-time and contextual) to guide them on security policy and strategy.



Source: GlobalData Survey 2024, n = 158

The Case for Network and Security Transformation

Network and security solutions are converging and there is a need for the two domains to evolve to meet the changes in IT workloads. The study conducted by GlobalData highlights the shift in traffic patterns that will drive network and security transformation:

- **User Traffic:** Over two-thirds (68%) of enterprises already see more user traffic generated outside the traditional firewall. Another 30% of enterprises believe that will be the case over the next 12 to 18 months. This points to the need to extend security beyond the traditional corporate network perimeters.

- **Cloud:** Similarly, 78% of the enterprises surveyed have corporate traffic that is directed primarily to the cloud. This will increase to 98% in the next 12 to 18 months. As they consume more cloud services, the expectation is for the network to offer the same benefits, i.e., more adaptive, consumption-based, and can be provisioned on-demand.

- **Software-as-a-Service (SaaS) Consumption:** Some 64% of enterprises already consume more applications via the SaaS model. This will increase by 32% over the next 12 to 18 months. Application performance is an issue that needs to be addressed, especially for mission-critical, latency-sensitive applications.

- **Internet:** Most enterprises (59%) already use the Internet to carry greater than 50% of their network traffic via secured tunnels, instead of private networks such as MPLS-based IP VPN. Ensuring network performance and security using the public Internet must be addressed.

While the above areas are ongoing transition, there are other areas that are starting to ramp up:

- **Cloud On-ramps:** Today, only 38% of the enterprises develop their network strategy and investment by considering cloud locations and cloud on-ramps. However, 41% of them will consider cloud on-ramps in their network strategy going forward. To minimise network latency, the WAN must be able to route the traffic via the lowest level of router hops and cloud on-ramps facilitate faster access to cloud services.

- **Data Storage:** Today, 30% of the enterprises surveyed store sensitive data in the cloud and not in the enterprise data centre. This is expected to increase to 84% within 12 to 18 months. Security, data protection, and data sovereignty issues need to be addressed, which will be more complex for regulated industries. Enterprises also need to consider resiliency requirements since business operations are highly reliant on the availability of data.

- **Campus/Branch:** Today, 46% of enterprises see network traffic from the campus or branch location bypassing the traditional data centre and office locations and moving directly from the endpoint to cloud services. Within the next 12 to 18 months, this is expected to increase to 87%. Having direct access to cloud services is more efficient, allowing for better performance and reducing the WAN cost of transporting traffic back to data centres or office locations.

Future Outlook & Conclusion

There is a marked need to converge and align network and security vendors and strategy to keep pace with the realities on the ground. On the network side, only 31% believe that they are at an advanced stage with a platform that is fully unified, programmable, and software defined. The majority are more at an early stage of a SASE roadmap. Many end users continue to report pain points such as the lack of end-to-end visibility of usage statistics, advanced analytics, and performance. There are also other challenges related to the network overlay, particularly with the public Internet, which impact latency, speed, and throughput. Contracts also are too rigid and do not meet the needs of cloud-first requirements.

On the security side, some of the top pain points include the lack of real-time data and other contextual information we need to drive our security policy and strategy. This type of telemetry is particularly important for zero trust concepts which rely on multiple data sets (e.g., employee role, location, time, access point, and device type) to assign granular access policy control. The maturity of threat intelligence is another challenge as business and IT leaders need better solutions to detect real threats and reduce false positives. Fundamentally, as also seen in the survey, most companies do not have a single, unified team responsible for network, cloud, and security. The tendency is to have a central team for security with regional or local teams supporting network and cloud which creates interoperability challenges.

- **Importance of Underlay:** Network operators are unique in the underlay approach which focuses on the implementation of technologies, such as AI/ML, security, automation, and orchestration engines into the physical core network to deliver more value. This is often supported with cloud on-ramps, private peering, and management of third-party providers to deliver a better end-to-end performance. There are also varying levels of hardwired integration between the network and security (e.g., distributed denial of service [DDoS] protection). While there may be cost considerations in going with any public Internet provider via an OTT 'overlay', it creates more decoupling between network and security as well as overall performance.

- **Streamlining Vendors for Security and Performance:** As digital infrastructure requires the convergence between network and security domains, the survey respondents reported an average of seven security vendors and five networking ones. While 64% of respondents have broadly the same provider for security and network, 36% do not. This complicates the goals of SASE of offering network and security services into a single proposition. As users and workloads both become more distributed, it is important for network, security, and the cloud to work seamlessly, especially for layered security and high performance. One-off security designs and inefficient policies do not scale. The data shows a near ubiquitous expectation for secure and direct access to the cloud without the bottlenecks of the traditional WAN.

- **Choose Deployment Models Wisely:** As skill sets for network and security convergence can be scarce, depending on the company, most organisations have opted for co-managed (where the company maintains some level of direct day-to-day control and input) or fully managed services which are outsourced to a third-party. These two options are more popular for network and security management (with co-managed being the most popular across the board). DIY is the highest in security at 25% of deployments, compared to only 18% within the networking space. The use of AI will only increase adoption of the current deployment model and will unlikely cause users to switch between models. Therefore, businesses should weigh up the pros and cons carefully.

About GlobalData

GlobalData is a leading provider of data, analytics, and insights on the world's largest industries. In an increasingly fast-moving, complex, and uncertain world, it has never been harder for organizations and decision makers to predict and navigate the future. This is why GlobalData's mission is to help our clients to decode the future and profit from faster, more informed decisions. As a leading information services company, thousands of clients rely on GlobalData for trusted, timely, and actionable intelligence. Our solutions are designed to provide a daily edge to professionals within corporations, financial institutions, professional services, and government agencies.

Unique Data

We continuously update and enrich 50+ terabytes of unique data to provide an unbiased, authoritative view of the sectors, markets, and companies offering growth opportunities across the world's largest industries.

Expert Analysis

We leverage the collective expertise of over 2,000 in-house industry analysts, data scientists, and journalists, as well as a global community of industry professionals, to provide decision-makers with timely, actionable insight.

Innovative Solutions

We help you work smarter and faster by giving you access to powerful analytics and customizable workflow tools tailored to your role, alongside direct access to our expert community of analysts.

One Platform

We have a single taxonomy across all of our data assets and integrate our capabilities into a single platform – giving you easy access to a complete, dynamic, and comparable view of the world's largest industries.

Contact Us

If you have any more questions regarding our research, please contact us:

Dustin Kehoe <Dustin.Kehoe@globaldata.com>