TATA COMMUNICATIONS

OMDIA

OMDIA.COM

How Businesses are Engaging in Secure Network Transformation

From upgrading the legacy to new innovation, networks underpin digital transformation

Brian Washburn

January 2021

Table of Contents

List of Figures

List of Tables

COVID-19 speeds ICT and network transformation

Enterprises had the rug pulled out from under them when COVID-19 came along in early 2020. As offices were shut and workers were sent home, organizations immediately needed to reprioritize investments, to add platforms and services necessary to keep workers connected and businesses operational.

But the initial impact of COVID-19 on enterprises also depended on factors such as the industry, country, digital practices, and partner flexibility. Enterprises have managed costs by cutting headcounts, reducing budgets, and revisiting contracts. Enterprises are now stepping up investments in critical strategic areas that support ways their operations and revenue streams need to change. As the pandemic takes its course, Omdia recommends enterprises keep in mind the following factors:

Volatility will stay. There is uncertainty over the speed of economic recovery, exacerbated in some cases by government policy and trade disputes. This market uncertainty affects IT projects, budgets, contract terms, and new supplier selection.

Government and industry remote working mandates. Most businesses that could, sent their workers home. These remote workers need broadband internet and secure access into corporate networks and cloud resources. Next steps include network optimization to all connection points: remote workers, internet VPN gateways, and applications hosted in data centers or in the cloud.

IT is accelerating some key projects, re-thinking others. Enterprises had an initial scramble to keep operations active during the pandemic. As we move into the next stage, enterprise IT is expediting digital projects that optimize the business for this "next normal." Enterprise IT departments will re-evaluate suppliers to align with flexible, engaged partners. They will part ways with partners that enforced static contracts and did not help the business pivot.

Network has a central role. Remote access requires strong network security; collaboration requires reliable network performance. Digital applications need networks that are secure, flexible, high-performing, and resilient. These requirements are met by transformational platforms and services: SD-WAN, hybrid networking, cloud connect, and dynamic bandwidth.

Security is a part of transformation. In its enterprise surveys, Omdia sees time and again that IT cannot adopt new solutions and services until security is addressed. Omdia finds virtually all enterprises undergoing network transformation engage with service partners at one or more points along the way. Managed services partners bridge in-house gaps in expertise, starting with security.

Secure network transformation for businesses

The state of the industry

Across industries, businesses currently face many of the same pressures. They need to become more flexible, increase reliance on automation and become more efficient. New solutions addressing these needs fall under digital applications and digital transformation. Digital applications are about gathering new data and uncovering business intelligence insights that help companies make the right decisions at the right time. Digital applications also bring new and more intelligent ways to work with customers and manage partner relationships; and make securing and consuming supplies, and delivering goods and services, more efficient.

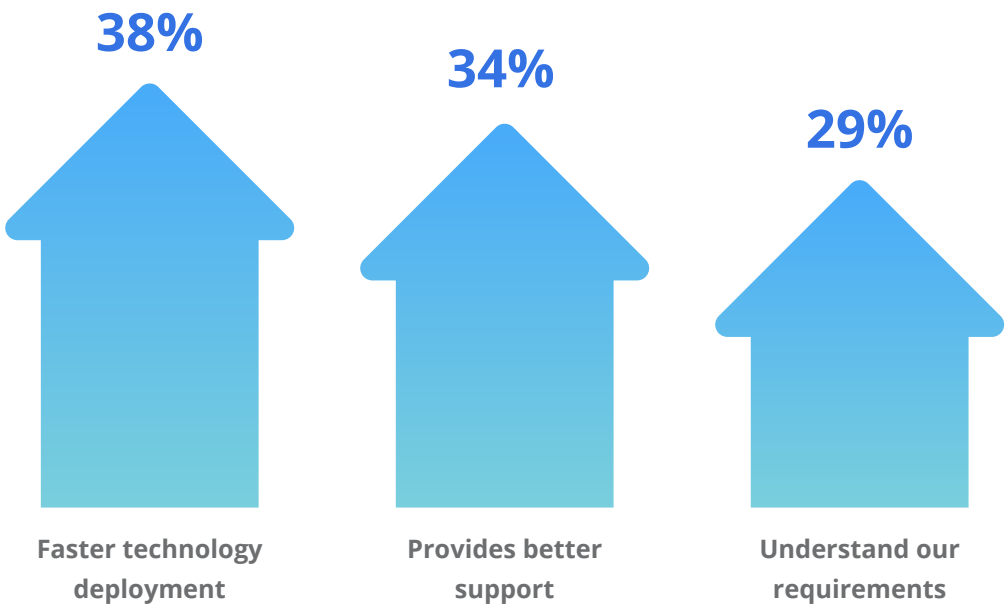
For many businesses, 2020 has been a very challenging year. Omdia enterprise survey research conducted after the global spread of COVID-19 shows that the average business is reducing its 2020-2021 IT budget by about 15% year-over-year in the wake of COVID. But more than half of enterprises surveyed by Omdia are accelerating network projects such as SD-WAN, hybrid networking, and cloud connect services adoption. This is because enterprise digital transformation first requires network transformation.

These new network services must be secure, ensuring the business is kept safe. Enterprises cannot risk having major IT systems compromised and core data stolen, held hostage, or destroyed. Companies large and small are under a constant barrage of attacks, with some businesses specifically targeted by bad actors. A serious security breach starts with compromised systems and lost revenues, followed by massive liability and settlement headaches, and finally long-term damage to the company's reputation.

The risks of a breach make security top-of-mind for enterprise IT executives, even as the business tightens IT budgets and requires efficiency improvements. Enterprise IT needs help. Omdia enterprise research shows that the top 3 factors IT executives currently want from partners are: to understand its business better, to move more quickly, and to improve support. (see Figure 1).

Figure 1: Enterprise IT values partners that offer speed and support

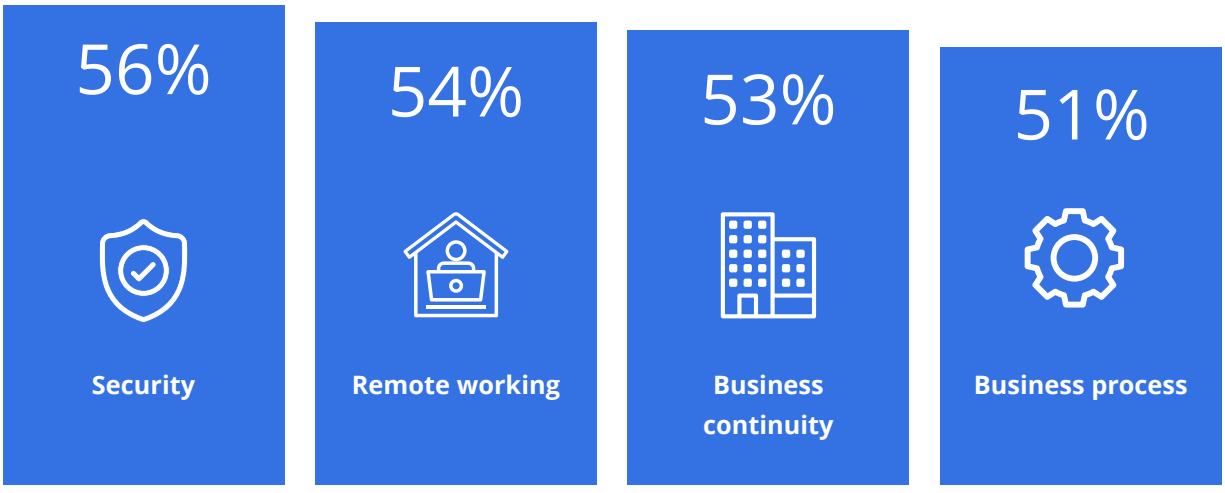
Enterprise IT priorities from services partners



Source Source Omdia COVID-19 enterprise ICT trends

While enterprises must tighten IT budgets, security remains their investment priority, joined by a need to support a newly remote workforce. Enterprises are also willing to step up investments to improve disaster recovery and business continuity, and to improve their business processes, whether through entirely new digital applications or more conventional applications modernization. More than half of enterprises continue to move budget into each of these areas to support the business (see Figure 2).

Figure 2: Security and remote working are top enterprise priorities



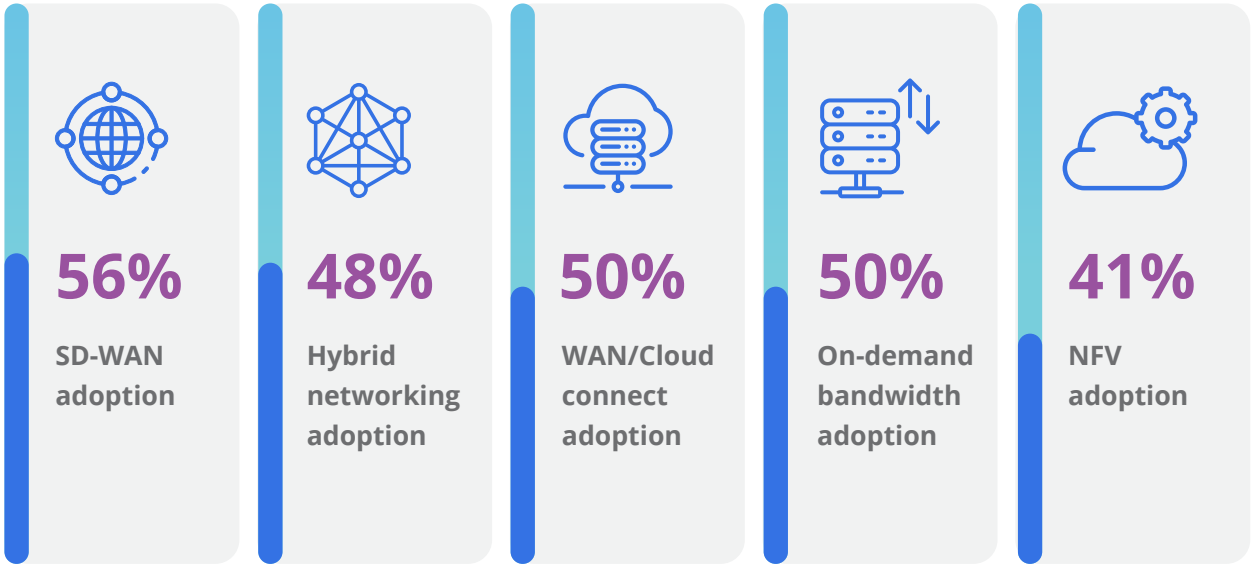
Source Omdia COVID-19 enterprise ICT trends

Security plays a key role in enterprise network solutions

Some industries have strict national regulatory and commercial compliance guidelines, which ensure they keep sensitive information private and secure. Public sector, finance, and healthcare industries have stringent safeguards for data privacy and protection of citizens and clients. Given that businesses across every industry process transactions, they must protect sensitive data, whether in retail, manufacturing, utilities, business services, logistics, education, or other businesses.

When industries transform their network, new services must either provide new security features or at least reinforce existing levels of security. For example, SD-WAN deployments, which have been deployed by more than half (56%) of large enterprises, add new features and analytics insights that enhance companies' existing security measures. Half of enterprises have adopted hybrid networking and WAN connectivity to cloud services, which can extend private network security to enterprise endpoints, data centers and cloud destinations (see Figure 3).

Figure 3: Enterprises embrace network transformation services



Source Omdia Enterprise Network Services Insights 2020

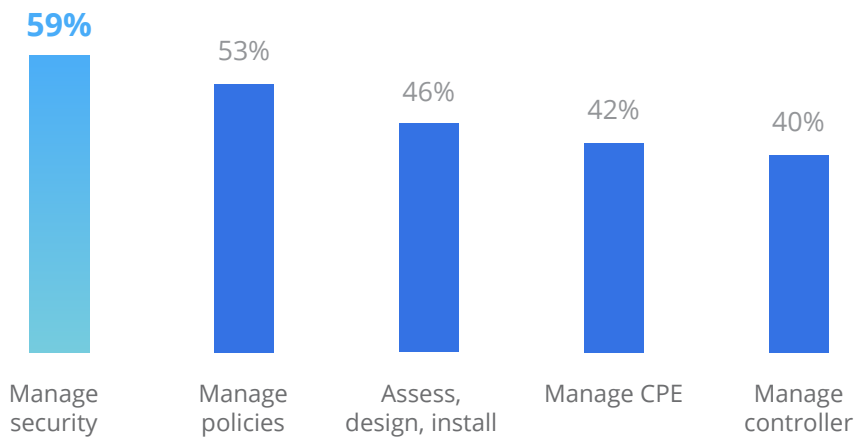
SD-WAN's role in secure network transformation

While more than half of enterprises now have some experience with SD-WAN, there is wide variability on deployments. A little more than one-third of enterprises using SD-WAN are still at pilot or early adoption stages. About 10% of SD-WAN adopters have mature deployments that reach throughout their organization. The remainder of enterprises are some place in between.

When it comes to new services such as SD-WAN, enterprises rely heavily on managed services to help with assessment, deployment and day-to-day operations (see Figure 4). In its surveys, Omdia finds virtually every large enterprise gets outside help for SD-WAN at one or more steps along the way. Enterprises most frequently seek help securing SD-WAN, but need help across the board: help setting up the new platform, hosting and maintaining controller software, supporting premises hardware, or managing SD-WAN policies.

Figure 4: Service providers help enterprises with SD-WAN expertise

Enterprise turn to provider partners in SD-WAN



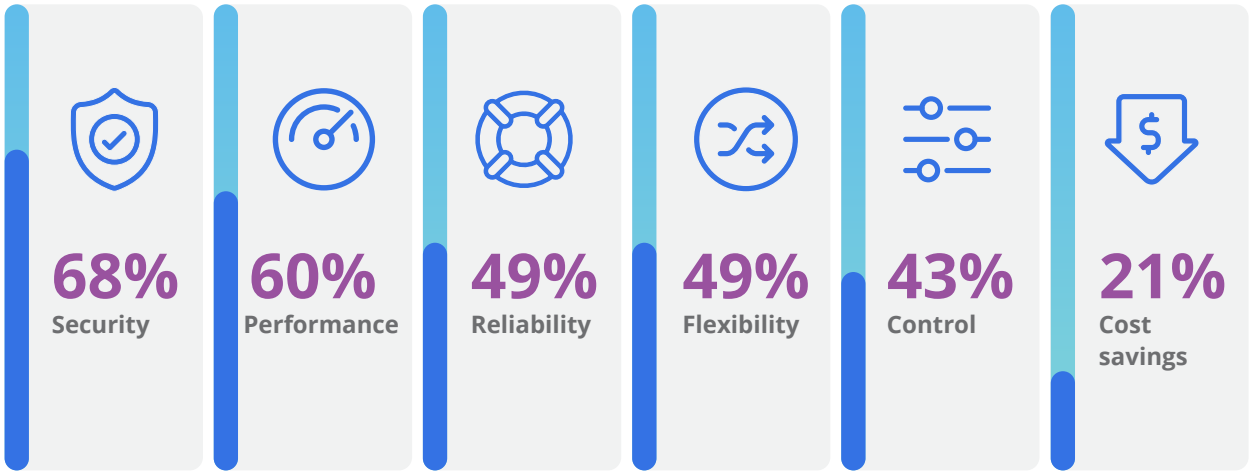
Source: Omdia Enterprise Network Services Insights 2020

Even though many enterprise SD-WAN deployments are still works in progress, more than 90% of adopters already report net positive returns. These companies estimate a 44% increase on average in returned value from deployments. Enterprises realize SD-WAN value in ways including direct cost savings; indirect cost savings such as improved efficiency and uptime; and net gains through new features and improvements, such as improved security and better operational analytics.

When it comes to new features, efficiency gains and direct savings, what aspects of SD-WAN are most important to enterprises? The top driver is security, followed by performance (see Figure 5). SD-WAN offers standard security tools such as firewalls, enhanced by new capabilities such as applications policies and path route restrictions, plus intelligence and management analytics that can be added to a centralized controller. Enterprises also value the greater performance, flexibility, and reliability that SD-WAN offers.

Figure 5: Enterprises value SD-WAN security and performance

How enterprise prioritize benefits of SD-WAN



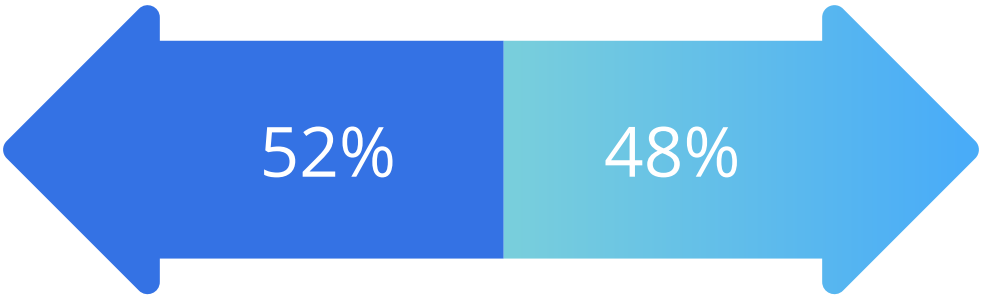
Source: Omdia Enterprise Network Services Insights 2020

Hybrid networks unify WAN and internet safely

In an effort to reduce their costs, enterprises increasingly turn their eyes on the high cost of operating dual private MPLS VPNs with full redundancy across all their sites. Dedicated internet and broadband internet services tend to be more flexible to deploy and offer more capacity at a lower price. These benefits drive enterprise IT to build hybrid networks for at least some of their sites, mixing private WAN together with secure internet VPNs.

When enterprises adopt hybrid networks, they turn to service provider partners for help. Enterprises most frequently (60% of the time) seek out partners for security assistance. Many hybrid network adopters also bring in partners to consolidate network access providers (56%), and to manage on-site hardware (50%). Some 42% of enterprises combine hybrid networks with partner-managed firewalls and hosted secure gateways. This adoption rate splits almost in half between site security managed at the CPE firewall, and internet traffic that is managed further upstream through network-hosted firewall gateways (see Figure 6).

Figure 6: Enterprises are split over centralized vs. distributed security



Of hybrid networking adopters separate and break out internet traffic locally, through on-premise firewalls

Of hybrid networking adopters aggregate internet traffic for processing through centralized, secure firewall/gateways

Source: Omdia global enterprise WAN services survey 2019

The top benefit that enterprises want from their hybrid networks is improved control (61%) using centralized management. Other important benefits include cost savings (56%), followed by improved network performance (53%) from using public internet connections alongside private WAN. Security is also important, ranking as a top benefit for 45% of enterprises. Companies tend to want their hybrid networks to maintain their existing levels of security and practices. Improving security is less frequently a main adoption driver for hybrid networking.

We have deployed a SD-WAN managed solution with internet and retired MPLS circuits. With SD-WAN, we were able to add local internet breakout, to take traffic directly onto the internet rather than tunneling over the enterprise network. Along with local internet breakout, we had to implement security tools to handle authentication. We also had to implement new cloud-based firewalls. These were factors that came with SD-WAN.

Head of IT
healthcare manufacturing firm headquartered in US

To make sure that all your transactions work properly, you need an accelerated WAN strategy. There is a modern retail business formula: The factors include operational technology, information technology, enterprise resource planning and back-end systems, regulation, and network-to-cloud strategy. You need to add these factors together to build an automation-driven business strategy. That is the modern enterprise retail success formula.

CIO
retailer headquartered in Middle East

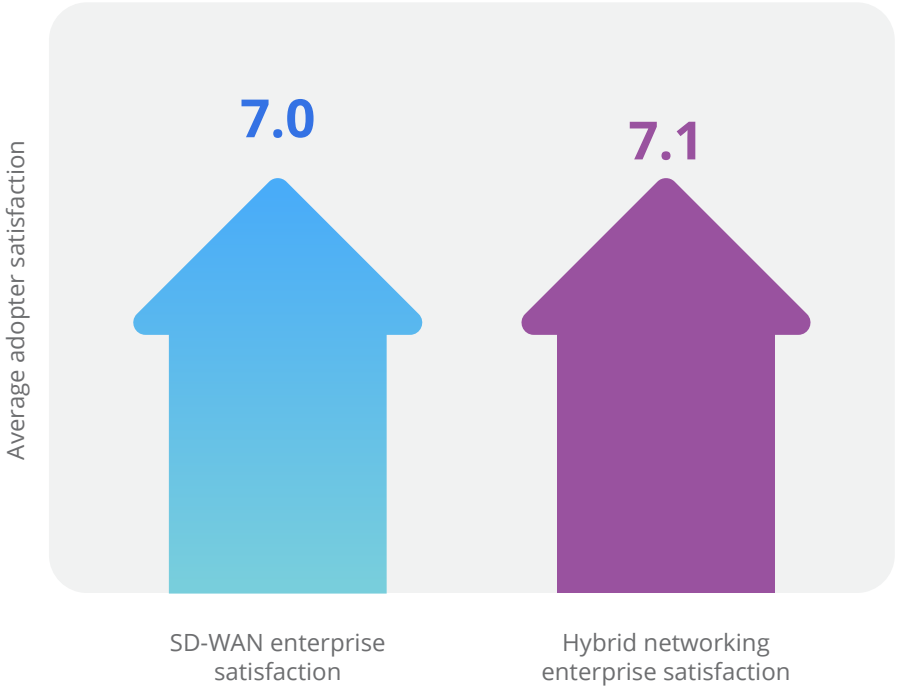
Value of network providers as enterprise partners

Network providers vie for lead partner role for enterprise networking projects, squaring off against other providers including integrators, vendors, cloud providers, and managed services specialists. Network providers are the lead partner for enterprise SD-WAN projects about 41% of the time; for enterprise hybrid networking projects about 35% of the time. If they are not lead partner, network providers still are active participants that help enterprises with their network transformation projects.

Overall, enterprises that adopt SD-WAN and hybrid networking are very happy they did. The enterprise success rate and satisfaction with these solutions is very high (see Figure 7).

Figure 7: Hybrid networking, SD-WAN adopters are highly satisfied

Enterprise adopters are highly satisfied with network transformation



Source: Omdia Enterprise Network Services Insights 2020

Enterprise Recommendations

SD-WAN helps build secure networks: In early days, vendors presented SD-WAN as a way to lower costs; IT executives were concerned about platform security. That model has flipped: SD-WAN's security features are now widely recognized and valued. Most enterprises (68%) adopt SD-WAN for security, while cost savings is much lower in importance.

Hybrid networks a solid choice for cost savings: Enterprises see improved network control (preferred by 61% of adopters) as a top driver to adopt hybrid networking, closely followed by cost savings (56%). Enterprises report hybrid networking is a dependable way to deliver returns: 96% of enterprise adopters say they have realized benefits from the move.

Connect network strategy to cloud strategy: Private network connectivity to cloud is another key network transformation component for enterprises. There are obvious security and performance benefits for a private, direct connection into cloud resources. Do note that the shift to cloud also changes traffic patterns. Nearly one-third (31%) of cloud connect adopters to date have redesigned their enterprise networks around cloud services.

We have a couple network provider partners right now… we have active-active links configured with BGP managed by network partners. We monitor device twins ourselves. If we find something wrong with a device or with a link first, we contact the managed network provider.

IT executive
retailer headquartered in Europe

Work with partners for secure, managed network transformation: Enterprises understand that network transformation is a process, and that improving security stance is among the desired outcomes. Enterprises realize they reduce risk when they bring in an expert security partner to augment their own skills. For this reason, for both SD-WAN and hybrid networking adoption security is the most common reason enterprises bring in an external service provider partner for assistance.

> **If I were to summarize my priorities, I want to take SD-WAN very quickly to all our sites, centralize LAN management, standardize our Wi-Fi for security, and virtualize our data centers.**
>
> **IT executive, electronics**
> manufacturing group headquartered in Asia

Conclusion

Network shifts require a security re-assessment

The global pandemic forced network changes nearly overnight. Large-scale remote working opened new threats in security perimeters already dealing with holes. Zero-trust network access – treating devices as untrusted whether they are inside or outside the corporate network – is an effective policy. But getting security alignment on zero trust across all assets is easier said than done.

Network transformation – which includes hybrid networking, SD-WAN and secure cloud connect – offers layers of protection to corporate assets for the perimeter and beyond the perimeter. However, security solutions need to be deployed and managed with the network, as part of an overall security strategy. Table 1 summarizes the sorts of managed security functions portfolio that enterprises need to consider, to help protect their assets as they migrate to new network models.

Table 1: A wide array of security functions protect enterprises against attack vectors

Security Function	Security Description
Firewall and next-generation firewall (NGFW)	Modern firewalls (which includes SD-WAN platform security) support deep packet inspection, complex analytics, and comprehensive reports. Traffic filtering handles features such as intrusion detection/prevention and virus/malware protection. These devices frequently also support internet VPN gateway functions.
Web application firewall	HTTP traffic analyzers are tuned to monitor specific web applications. They detect, protect, and report on security threats to individual applications.
Hosted secure gateway	Secure gateways connect public internet to private networks and other resources. They block unauthorized access and filter out unauthorized internet/web traffic. These gateways often aggregate large numbers of VPN tunnels from branch offices and remote workers.

Security Function	Security Description
Cloud access security broker (CASB)	Software designed to enforce security policies around SaaS, as well as other cloud services (IaaS and PaaS). CASB often includes analytics to detect and issue alerts for traffic anomalies. It often also supports data leakage prevention.
Identity access management (IAM)	Front-end authentication enables secure single sign-on for remote endpoints, allowing access to corporate resources. Access restrictions are based on each worker's/device's identity. IAM automates access provisioning to resources and handles identity lifecycle management.
DDoS mitigation	Detects high-volume attacks that threaten to block business traffic. Protects enterprise assets from being overwhelmed by fake traffic. There are ad hoc and always-on protection models. On-premises DDoS infrastructure may augment network-/cloud-based mitigation.
Security information and event management (SIEM)	Monitors, identifies, and warns against attacks on assets. SIEM is often paired with incident response (which is rapid, orchestrated, and/or automated) to neutralize attacks.
Threat protection	Collects and analyzes large volumes of internal monitoring data, and correlates with external data, to warn against and protect assets from emerging security threats.
Security professional services	Professional services compliment managed security portfolios. They handle non-recurring tasks such as vulnerability assessment, penetration testing, and compliance verification.
DNS Security	A collection of practices that preserve the availability, integrity and accuracy of domain name resolution services.
Browser Isolation	Executes web browsers inside virtual machines to prevent any browser exploits from getting direct access to users' operating systems, devices or data.

Source: Omdia

Secure network transformation produces enterprise value

Transforming the network through SD-WAN, hybrid networking, and cloud connect services improves security and goes beyond. Network transformation underpins digital transformation. It has the potential to lower costs, improve performance, make the network more dynamic yet reliable, and provide a greater level of control over services. Enterprises as a whole see the value that SD-WAN, hybrid networking, and re-engineering the network around cloud services each bring to the business.

Omdia survey research finds that companies overwhelmingly describe their experience with these new solutions, services, and new ways of operating as positive. Those few enterprises with negative experiences understand their deployment setbacks are temporary, and still expect long-term benefits. These enterprises understand they need to make changes – reconfigure the network, change platforms or swap out partners – to correct course.

From its surveys and executive discussions, Omdia finds that enterprises recognize more value from network transformation when they combine and scale up services. SD-WAN and hybrid networking, for example, make for a natural combination. With flexible bandwidth and cloud connectivity in the mix, an enterprise can adopt a whole different way of thinking about networks, making it possible, for example, to shift bandwidth between locations and between services. Given the uncertain pace of global recovery, a network that is flexible to support personnel as they are brought back onto worksites – and reverse course if workers need to revert to remote – is valuable.

The role of network providers

Enterprises work closely with network providers for success in network transformation: 40% of enterprises work with a network provider as their top network transformation partner. Most enterprises have at least one network provider on their short lists to help reach network transformation goals. Omdia research finds that enterprises that partner with a large network provider as their top network transformation partner tend to be more satisfied compared to having other types of providers in the lead. This holds for SD-WAN solutions, hybrid networking, and re-designing enterprise networks around cloud services.

Enterprises will continue to explore further in the coming years how to transform the network to meet future needs, uncertainties, security requirements and budget limitations. Digital transformation, network transformation, and managed security are ongoing processes. These initiatives are not finished in one project. Enterprises should engage with partners that continue to evolve and grow their services, which can help augment enterprises' in-house IT with continuous external professional and managed services expertise, to help bring about secure network transformation.

TATA COMMUNICATIONS

Tata Communications Secure Network Transformation: Enabling enterprises on their network journey

Tata Communications can help businesses overcome challenges and deliver an efficient, scalable and secure experience for users and applications, leveraging private and public infrastructure.

CLOUD-FIRST, INTERNET-FIRST NETWORK ARCHITECTURE

Re-architect the network to hybrid with direct access from branch offices to clouds. Enable instant creation of cloud-to-cloud and cloud-to-edge connected solutions while improving latency and availability through:

- IZO SDWAN for intelligent routing, centralized management and advanced visibility
- IZO internet WAN for transition to the cloud by integrating internet with existing VPN network
- Broadband access for high speed internet
- NetFoundry for secure connectivity

CLOUD-TO-CLOUD CONNECTIVITY

Deploy cloud connect solutions that link data centers to multiple clouds via private connections and link users and branches to multi-cloud using internet, WAN and broadband, made possible by:

- IZO Internet WAN for network optimization integrated with private cloud solutions
- IZO Private Connect to link businesses to leading cloud services over MPLS or Ethernet
- NetFoundry for secure connectivity

MANAGING RISK FOR PERFORMANCE

Add on-premises, next-gen firewall together with cloud-based security through:

- Software-defined security with next-gen firewalls and DDoS protection
- Cloud-based security
- NetFoundry for application-based, zero-trust network access

RIGHT-SIZED AND OPTIMIZED NETWORK

Migrate to agile hybrid networks with MPLS and end-to-end, SLA-backed internet WAN with application-aware routing, and also carry out:

- Network architecture assessment to understand the current state
- IZO internet WAN as an alternative to MPLS links, and path selection among connections for security and flexibility with predictable network routing

Appendix

Methodology

Materials cited in this white paper are drawn from global quantitative enterprise research surveys conducted by Omdia both post- and pre-COVID; regular qualitative discussions that Omdia has with enterprise executives involved in networking and security topics, and with vendor and service provider communities.

Author

Brian Washburn
Research Director, Service Provider Enterprise & Wholesale

askananalyst@omdia.com

Citation Policy

Request external citation and usage of Omdia research and data via citations@omdia.com.

Omdia Consulting

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 you. For more information about Omdia's consulting capabilities, please contact us directly at consulting@omdia.com.

Copyright notice and disclaimer