TATA COMMUNICATIONS

OMDIA

OMDIA.COM

How the Retail Industry is Engaging in Secure Network Transformation

From the digital transition to processing transactions, 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 retail industry

Retail businesses source and sell finished goods to consumers and businesses. The industry is a mix of physical stores, online e-commerce, and hybrid models for interaction and product delivery including click-and-collect and drop-off hubs. Retailers range in size from just one location to vast franchise networks. They may offer digital products, consumables, or durable goods; and offer customer experiences ranging from full self-serve and discount shopping to exclusive, high-touch luxury brands.

Regardless of their business model, retailers are under intense pressure to adopt digital tools. They need intelligence to identify and target the right prospects, and rely heavily on automation to increase efficiency and reduce costs. The end goal is to provide positive experiences to shoppers.

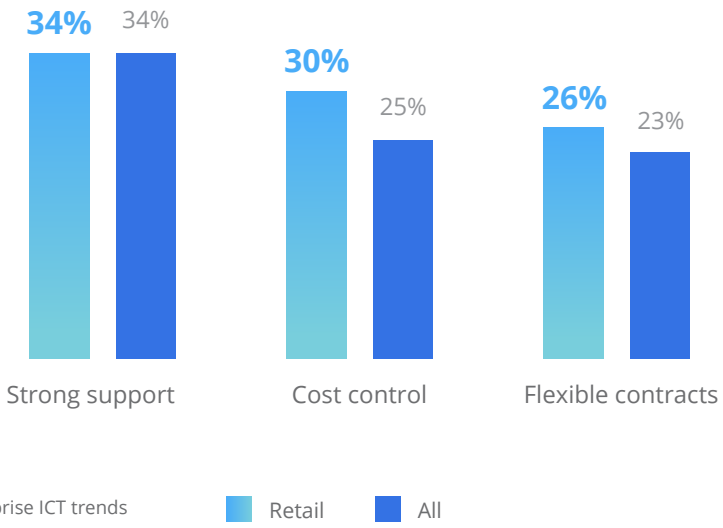
For retailers, 2020 has been a critically challenging year. Many businesses are fighting to survive, and are betting on the cyclical nature of the business to return to demand in 2021 and beyond. Omdia enterprise survey research conducted after the global spread of COVID-19 shows that the average retailer's 2020-2021 IT budget is down more than 15% year-over-year. These cuts are steeper than the average 10% reduction in ICT budgets reported across industries. More than in other industries, retailers need partners to help them control costs, and to provide more flexible contracting and billing relief.

While retailers cut budgets, they must invest in transforming the business to new digital practices. These new ways of doing business must handle financial transactions reliably and keep customer data secure. A data breach is ruinous to a retailer's business and can destroy its reputation. Since individual stores do not have dedicated IT, retailers traditionally used dependable but static hardware, secure and robust enough to operate reliably for years with minimal on-site maintenance.

With the speed of change, like other sectors, retailers need to be more nimble. They want service partners that deliver innovative new technologies and provide high levels of support. But the sector also needs partners that help keep down costs through flexible contracts, cost controls, and availability of financing (see Figure 1).

Figure 1: Retail IT wants partners for strong support and cost controls

Enterprise IT priorities from services partners

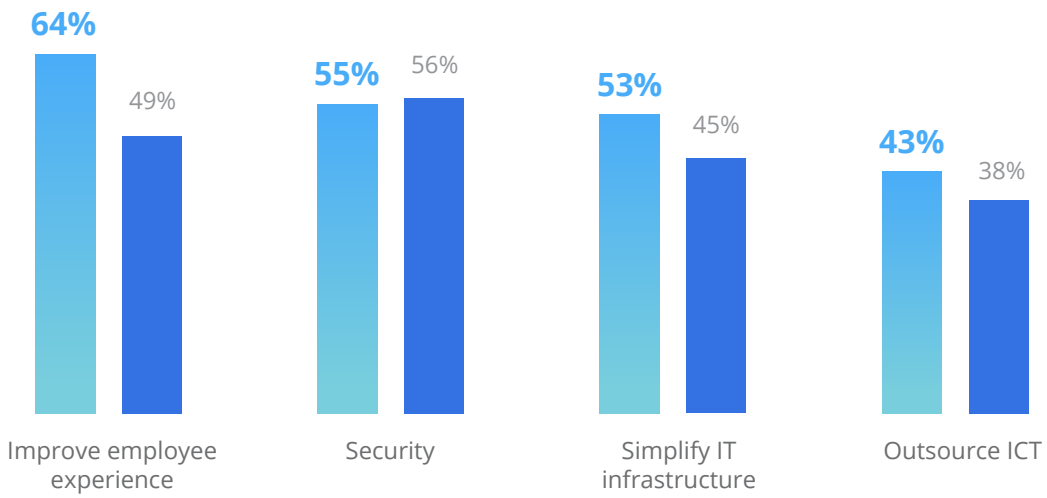


Source Omdia COVID-19 enterprise ICT trends

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: Retailers want to improve processes and reduce IT exposure

Retail sector investment priorities



Source Omdia COVID-19 enterprise ICT trends

Security plays a key role in the retail industry's network solutions

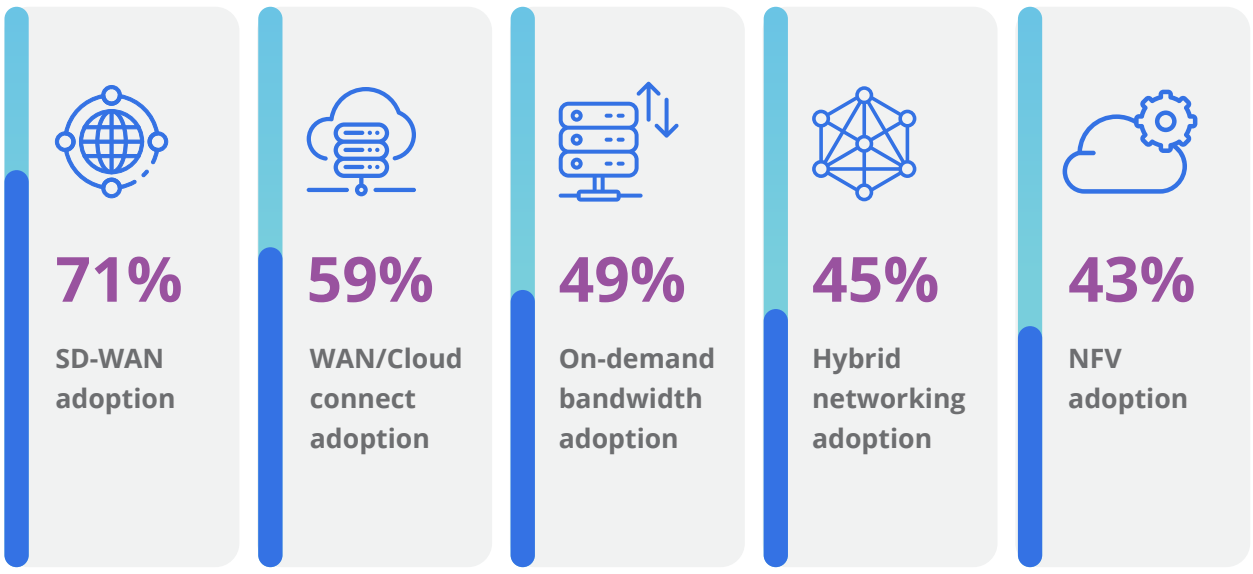
Retailers are keenly aware of the critical importance of keeping information secure. Cyber criminals target retail networks and e-commerce sites, to intercept financial transactions and gain access to customer data. Security compromises can be extremely damaging to a retail business. The company may lose inventory from fraudulent transactions; it is costly to conduct emergency forensics to isolate and patch security holes, and to audit and restore IT systems integrity. Cyber criminals may damage IT systems, making it difficult or impossible to recover. After the initial shock, the retailer faces knock-on consequences of possible liability for leaking customer data, and in the longer-term customers may lose trust in the brand affecting future sales.

Retailers conducting major brand credit transactions also must comply with well-established, rigorous security practices such as payment card industry (PCI) data security standard (DSS). Depending on the retailer's business, PCI compliance includes the following requirements:

- Ensure networks and systems are kept secure;
- Protect cardholder data;
- Ensure systems patches and security software are kept up to date;
- Enforce controls and tracking for access to cardholder data;
- Conduct regular tests of systems and procedures; and
- Document and maintain secure procedures.

While retailers must comply with rigorous security practices, they are also driven to adopt innovation to improve the business while cutting costs. For this reason, the retail sector leads industries in SD-WAN adoption: 71% of large retailers are at some stage of SD-WAN deployment. Retailers also are major adopters of secure connectivity to cloud (see Figure 3). By contrast, retailers rank low in hybrid networking (45% adoption): This is partly because of retailers that have shifted to all-internet connectivity to try and bring down their network costs.

Figure 3: Retail firms lead with SD-WAN and embrace cloud



Source Omdia Enterprise Network Services Insights 2020

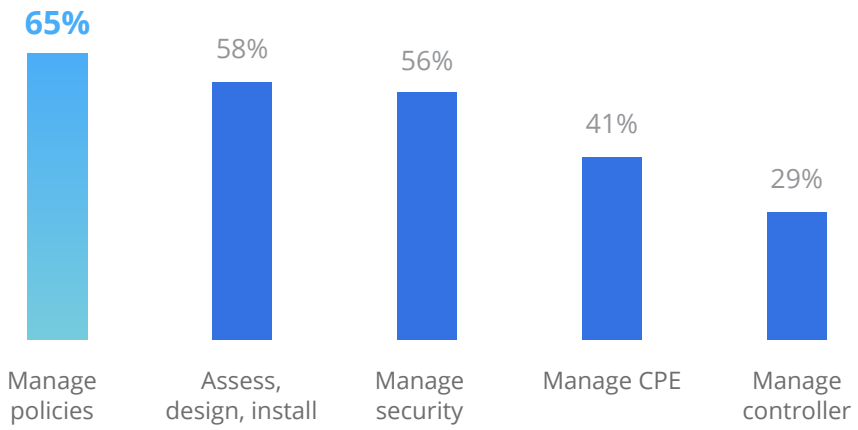
SD-WAN's role in secure network transformation

Omdia finds that larger enterprise retailers are a leading implementer of SD-WAN, but many of these deployments are a work in progress. About half of retail SD-WAN deployments are still pilots or connect only a few sites; a small but growing number of retailers (9%) have deployed SD-WAN throughout their organization. The rest of the retail industry still falls somewhere in between.

The retail sector leans especially heavily on managed services to help with deploying and operating SD-WAN (see Figure 4). In its survey that included nearly 100 retail IT executives, Omdia did not find any retailers that had implemented SD-WAN entirely independently. A majority of retailers turn to managed provider partners to assist them with key aspects such as design, installation and day-to-day management of policies and security for their SD-WAN deployment.

Figure 4: Retailers turn to SD-WAN managed services partners

Retailers turn to provider partners in SD-WAN



Source: Omdia Enterprise Network Services Insights 2020

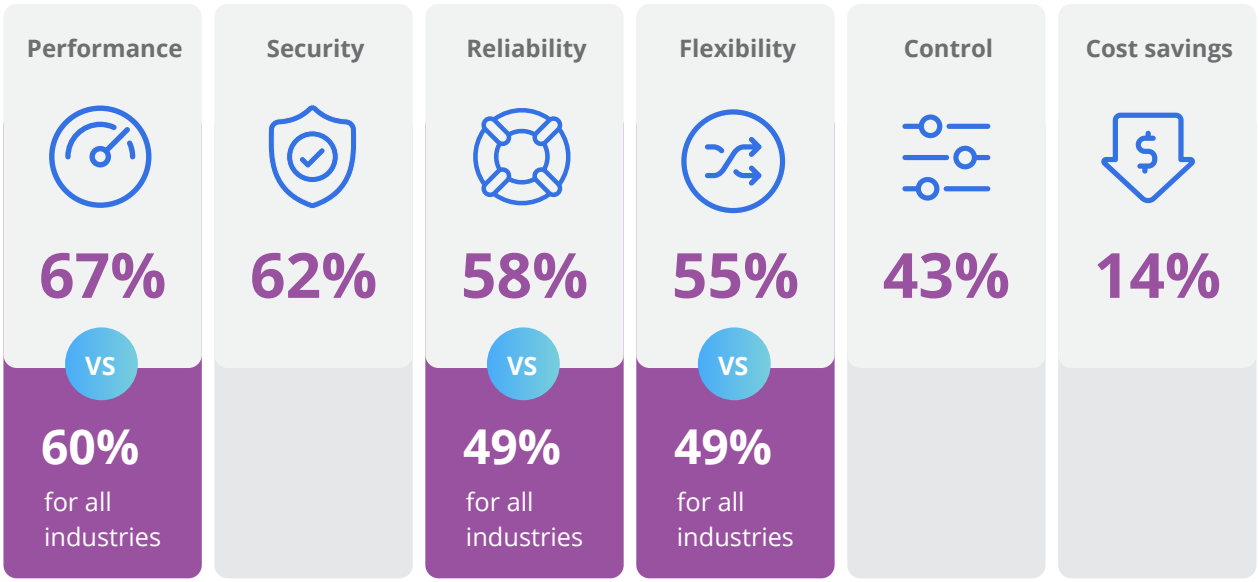
Even though many of their SD-WAN deployments are still works in progress, most retailers (86%) report net positive returns. These companies estimate a 41% increase in returned value from their deployments on average. Enterprises realize SD-WAN value in ways including direct cost savings; indirect cost 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 retailers? The top drivers are better performance, higher reliability, and greater flexibility: These are all related to improving service while controlling cost (see Figure 5). Like other industry sectors, retailers also highly value SD-WAN security features such as firewalls, applications policies and path route restrictions, and management analytics that verify applications are secure.

Retailers use SD-WAN's ability to identify and prioritize applications to support traffic types with very different performance profiles. On one hand, retailers need to support highly reliable, secured financial transactions and transfer of private customer data. On the other hand, retailers have communications and collaboration tools; a range of enterprise applications including inventory and HR systems; on-site digital signage; and public and/or private WiFi traffic for worker and guest internet access.

Figure 5: Retailers value SD-WAN performance and reliability

How the retail sector prioritizes SD-WAN benefits



Source: Omdia Enterprise Network Services Insights 2020

Hybrid networks unify WAN and internet safely

In its efforts to contain costs, parts of the retail industry turn to internet-only connectivity for their branch sites. Retailers also reduce their costs through hybrid networks that combine private WAN with secure internet VPNs, for at least some of their sites. Among enterprise retailers that use hybrid networking, about 40% of deployments connect only one or a few sites, and some (11%) use hybrid networking across the organization. Most retailers that still use hybrid networks fall somewhere in between.

When retailers adopt hybrid networks, they turn to service provider partners for help. Most (64%) retailers bring in partners to help with securing their hybrid networks. Many (45%) retailers bring in partner-managed firewalls and hosted secure gateways. When it comes to the decision whether to protect the network through site-based managed firewalls or centralized managed gateways, most (59%) retailers prefer security at the CPE firewall level for local internet breakout (see Figure 6).

Figure 6: Retailers prefer distributed internet security

How the retail sector connects WAN/internet securely

Source: Omdia global enterprise WAN services survey 2019

The top benefits retailers want out of hybrid networking projects are cost savings (66%), followed by improved control (61%) through centralized management. Retailers also adopt hybrid networks for improved network performance (57%) from using public internet connections alongside private WAN. Security is also important, but retailers need hybrid networks to be consistent with existing security practices; they do not buy hybrid networks to improve their security posture.

> **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

> **We have made our workforce mobile. We have released people from their physical locations; they can work from anywhere. All that mobility requires more internet connectivity. As we move to a disaggregated [cloud model], we will probably need faster links like 40 Gbps or 100 Gbps Ethernet.**
>
> **IT executive**
> retailer headquartered in Europe

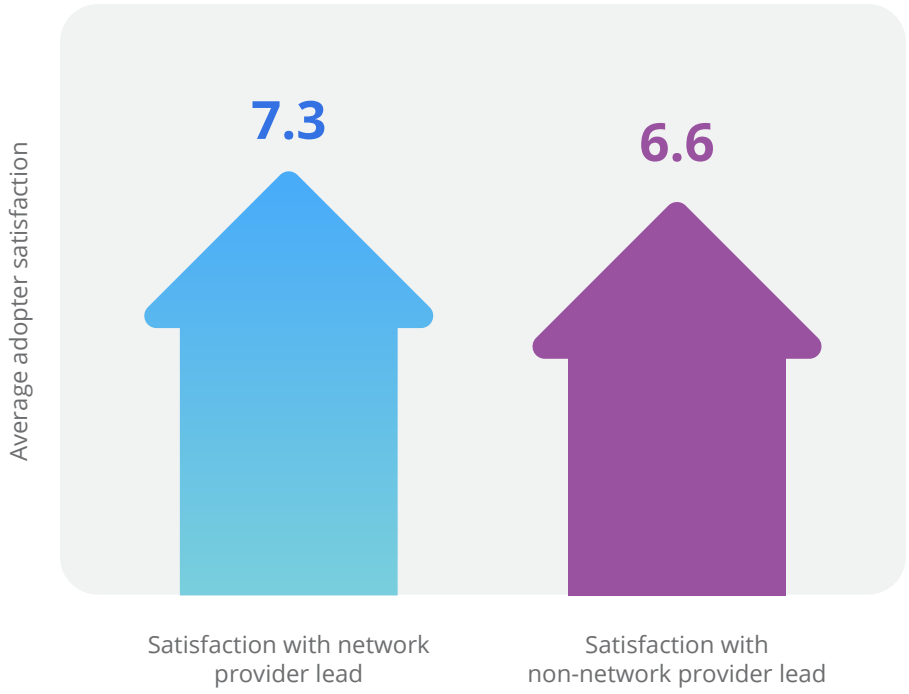
Network providers as partners to the retail sector

When it comes to leading network transformation services, the retail industry looks to network providers as lead partners 50% of the time for SD-WAN; retailers look to network providers as lead partner 43% of the time for hybrid networking. Enterprises may also choose integrators, vendors, cloud providers and managed services specialists as lead partner. Even if network providers do not lead, they still are active participants helping enterprises with their network transformation projects.

Retailers that deploy SD-WAN with a network provider in the lead realized higher customer satisfaction on average in their SD-WAN experience. When it comes to design, installation, securing, managing, and supporting these new platforms, enterprises rate network providers more highly (see Figure 7).

Figure 7: Retailers prefer telco lead partners for SD-WAN

Retailers rate network providers highly as lead hybrid networking partners



Source: Omdia Enterprise Network Services Insights 2020

Recommendations for retailers

SD-WAN is highly complementary to retailers' goals: Retailers adopt SD-WAN for better service reliability and to improve performance, whether they pair SD-WAN with MPLS/internet hybrid networking or choose internet-only connections. 86% of retailers that deployed SD-WAN say they realize net gains through benefits including network performance (a priority to 67% of enterprise retail respondents) and security (a priority to 62% of enterprise retail respondents).

When retailers choose hybrid networking, they realize cost savings: While some retailers go all-internet others prefer to hedge with hybrid networks. Retailers should look to hybrid networks as a way to achieve cost savings (a priority for 66% of respondents), while improving network control and reliability. 93% of retailers that adopted hybrid networking adopters say they already realize benefits.

Connect network strategy to cloud strategy: Retailers are also big consumers of cloud services: 59% of the sector has adopted network-to-cloud connect services, and 49% of the sector also uses dynamic bandwidth services. Both are ways for retailers to reduce their costs through pay-on-demand, helping manage retail's down- and up-swings.

> **We are only starting to move our applications to cloud. We have many very old applications that cannot move to cloud, so we have to code away from those. That will be a long-term process.**
>
> **IT executive**
> retailer headquartered in Europe

Work with partners for secure, managed network transformation: Retailers understand that network transformation is a consultative process. Retail businesses should explore how new services provide security information that eases PCI DSS compliance. New management controls and analytics, as part of a holistic security strategy, can help retailers better detect, analyze, and respond to potential threats.

> **We are using a number of advanced innovations in-house. I am working with our cloud partner's Center of Excellence to explain how the partner can help us by improving its cloud strategy. To have that discussion, you need to have knowledge of our business, IT infrastructure, enterprise architecture and network infrastructure.**
>
> **CIO**
> retailer headquartered in Middle East

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