TATA COMMUNICATIONS

OMDIA

OMDIA.COM

How the Manufacturing Industry is Engaging in Secure Network Transformation

From traditional supply chains to revolutionary Industry 4.0 practices, 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 in the manufacturing sector

The state of manufacturing

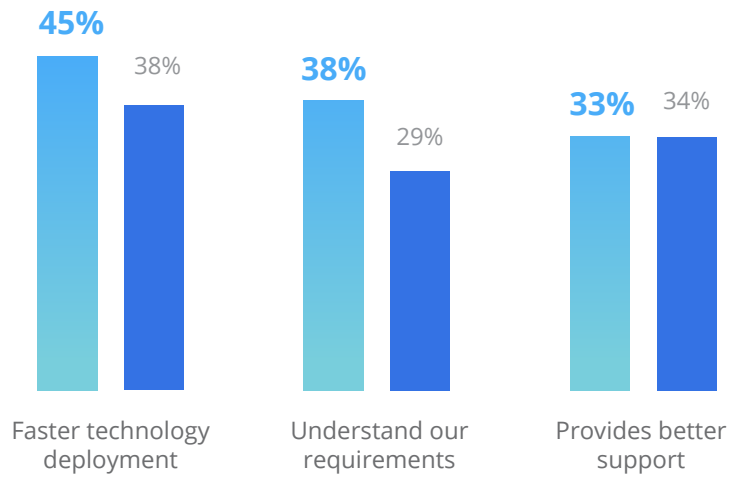
Manufacturers take in raw materials, process them, and create a standard product. Predictability and process efficiency are key for the sector: Factories need a dependable supply of raw materials that produce identical results. Processes must be quick and cost-effective, and often need to run uninterrupted. While 2020 has been a challenge to all industries, manufacturers recognize the crucial importance of sustaining IT. Omdia enterprise survey research conducted after the global spread of COVID-19 shows that the manufacturing sector's 2021 IT budgets are down less than 10% on average, faring slightly better than the average 10% reduction in ICT budgets reported across industries. Manufacturers are preserving IT and OT (operational technology) investments.

Manufacturers depend on IT for crucial functions. Enterprise resource planning/supply chain management (ERP/SCM) keep the factory operations flow running. Machines and processes in modern factories use real-time monitoring, with data analysis that issues alerts before a machine breaks down or a process is ruined. Innovation is moving rapidly: Digital twins, virtual/augmented reality applications, real-time cognitive analytics, massive data lakes for analytics around product lifecycle management are among the important developing fields.

Manufacturers need agile partners that can understand and meet their business requirements, and therefore provide adequate support (see Figure 1). Executive decision-makers in the manufacturing industry note that the key criteria for selecting partners is finding those that understand their digital business requirements.

Figure 1: Manufacturers want partners that keep pace with their needs

Manufacturing sector's top priorities from services partners

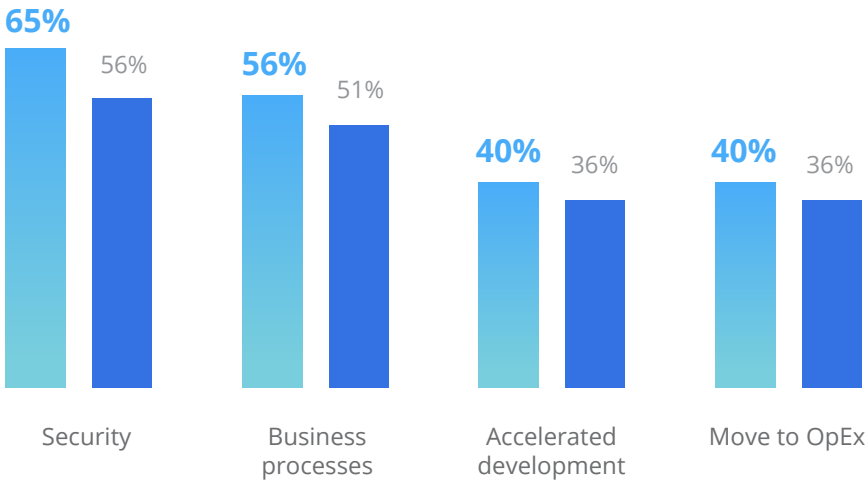


Source: Omdia COVID-19 enterprise ICT trends

Manufacturers still expect to increase investment in key areas: 41% of manufacturers plan to grow security budgets; while many manufacturers expect to shift existing budgets for network transformation, 24% plan to increase spending on managed network services including managed SD-WAN. Manufacturers are especially sensitive to the impact of security threats on their business. Improving business processes, speeding up development, and moving from CapEx to OpEx models are other factors important to the sector (see Figure 2).

Figure 2: Security leads the manufacturing sector's investment priorities

Manufacturing sector investment priorities



Source: Omdia COVID-19 enterprise ICT trends

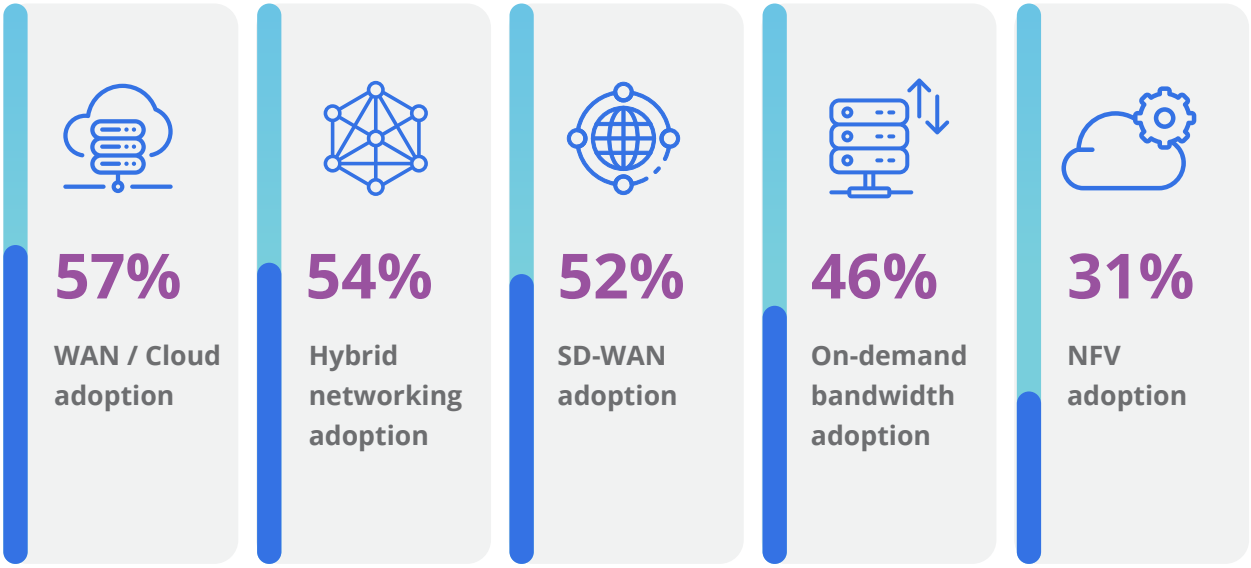
Security plays a key role in manufacturers' network solutions

Manufacturers are aware of how important it is to keep operations and information secure. Security threats are both targeted and opportunistic; their possible impacts include network disruption, unauthorized intrusion and stealing of information, compromised middleware and applications, and data held hostage or destroyed through malware/ransomware. A systems compromise may take proprietary information, halt operations on the factory floor, and disrupt the factory's supply chain. For these reasons, the manufacturing sector is especially guarded about protecting its network and IT assets.

The manufacturing vertical relies on new, flexible network tools to support transforming their business. For network transformation, WAN/cloud connect, hybrid networking and SD-WAN are popular solutions with manufacturers (see Figure 3). Each of these network transformation elements has the potential to add important security protections.

Figure 3: Manufacturers widely use hybrid networks, cloud connect, and SD-WAN

Network transformation adoption in manufacturing



Source: Omdia Enterprise Network Services Insights 2020

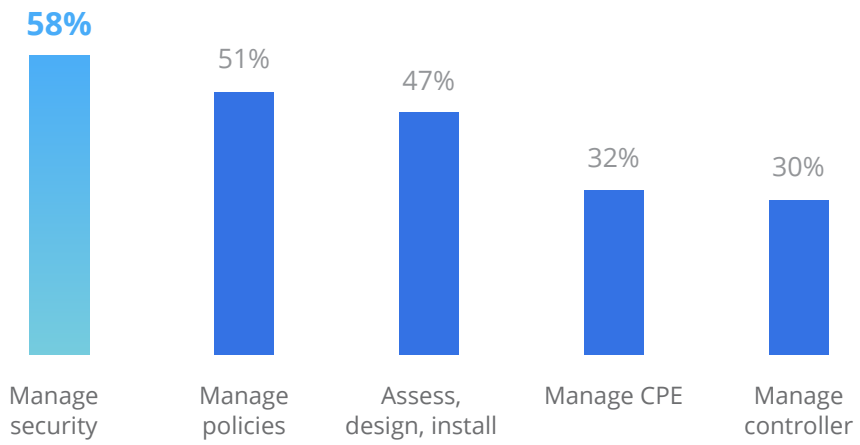
SD-WAN's role in network transformation

Omdia finds that about 52% of enterprises in manufacturing currently have SD-WAN. While adoption is healthy, SD-WAN is not yet as deeply deployed in the manufacturing sector as compared to some other key sectors. About 40% of manufacturer SD-WAN deployments are pilots or connect only a few sites; only a few manufacturers (6%) have deployed SD-WAN throughout their organization. Most manufacturers still fall somewhere in between.

As with all industries, the manufacturing sector relies heavily on managed services to help deploy and operate SD-WAN, just like other transformational network services (see Figure 4). Omdia finds that 58% of manufacturers turn to outside help for managed security with their SD-WAN; about half of manufacturers recruit a partner to help with SD-WAN design and installation, coupled with ongoing policy management. Just 4% of manufacturing firms deploy SD-WAN without getting any external help.

Figure 4: Security is a top reason manufacturers turn to providers for SD-WAN

Manufacturers turn to provider partners in SD-WAN



Source: Omdia Enterprise Network Services Insights 2020

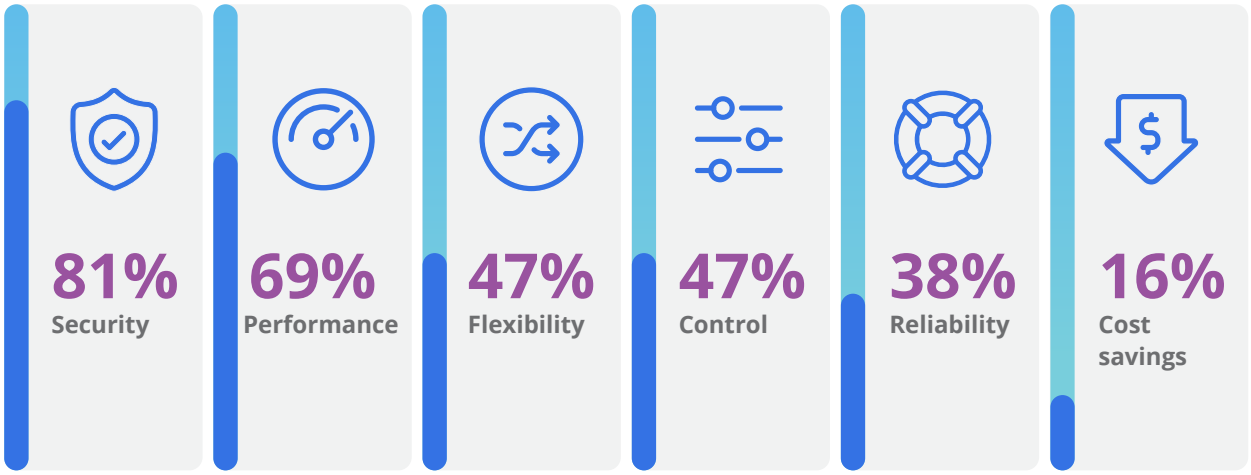
Manufacturers that adopt SD-WAN realize solid benefits. Nine out of 10 manufacturers with SD-WAN deployments report net positive returns, and executives at these companies estimate SD-WAN yielded a 40% increase in overall value on average. This value is realized in several ways: direct cost savings; indirect savings through factors such as improved efficiency and uptime; and gains from new features and improvements enabled by SD-WAN.

What aspects of SD-WAN are most important? For manufacturers, the top driver is improved security (see Figure 5). Manufacturers are leveraging SD-WAN's built-in security: firewalls; policy and path restrictions to better manage their applications; and network activity reporting and analytics collected by a central SD-WAN controller.

Besides security, manufacturers are interested in the performance improvements SD-WAN can bring. SD-WAN can help manufacturers prioritize applications to increase traffic throughput, decrease latency, and improve completed transactions. This helps manufacturers properly manage traffic across a diverse range of applications: from high-performance machine management and control; to large-scale, real-time operational analytics; to less demanding but vital transaction processing to track inventories, issue quotes, and handle orders.

Figure 5: Manufacturers value SD-WAN security and performance improvements

How the manufacturing industry prioritizes SD-WAN benefits



Source: Omdia Enterprise Network Services Insights 2020

Hybrid networks unify WAN and internet safely

The manufacturing sector is also a fan of hybrid networking, which mixes private WAN and public internet services to connect locations. The breadth of hybrid network deployment varies widely. About one-quarter of manufacturers have use hybrid networks in just a few sites; at the other extreme, to date 9% of manufacturers have stretched hybrid networking across most or all sites. Most hybrid networking adopters are selective, choosing some sites but not others. Sites without hybrid networking may use all-private WAN or all-internet connections. They may attach sites using both private WAN and public internet, but keep the two network types separate.

Almost all manufacturers that build hybrid networks turn to service provider partners for help, which can include network design, consolidating access providers, managing CPE, and managing security and hosted gateways. 64% of manufacturers tap services partners for a security role, and 42% of manufacturers specifically use partner-hosted secure gateways. Enterprises that turn to network-hosted secure gateways use these about equally on a fully centralized (19%) and regionally centralized (19%) basis. The balance (62%) prefer distributed models that offer secure local internet breakout, offering security services that manage internet access across site firewalls and router CPE (see Figure 6).

Figure 6: Manufacturers employ both distributed and centralized security

Source: Omdia global enterprise WAN services survey 2019

The manufacturing sector's lead priority for hybrid networks is clearly cost savings (73%), followed by improved performance from merging private WAN with public internet connections (52%). While security is a consideration, it is less frequently a driver to implement: 45% of manufacturing businesses expect to improve their security posture as they shift to hybrid WAN.

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

We do not use local internet breakout. For security reasons, we do not allow any of our remote offices to go directly onto internet – all our internet traffic goes through two data centers. Instead of local breakout, we are investing in bandwidth and WAN optimization to provide a better user experience. This approach helps us keep our enterprise secure.

IT executive
Electronics manufacturing group headquartered in Asia

Network providers as partners to manufacturers

When it comes to leading network transformation, manufacturers have a network provider as lead partner for SD-WAN in 28% of projects, and lead partner for hybrid networking in one-third of projects. Enterprises may also choose integrators, vendors, cloud providers or 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.

Manufacturers that deploy hybrid networking with a network provider in the lead have higher customer satisfaction with their overall hybrid networking experience. When it comes to aggregating, securing, managing and supporting a mix of private and public networks including secure gateways, the manufacturing sector finds that network operators provide better experiences (see Figure 7).

Figure 7: Manufacturers that adopt hybrid networking led by a telco partner are more satisfied

Manufacturers rate network providers highly as lead hybrid networking partners

Source: Omdia Enterprise Network Services Insights 2020

Recommendations for manufacturers

Explore SD-WAN as a safe bet with proven gains: Manufacturers are experiencing that SD-WAN, deployed properly, improves performance and enhances security. More than half of the manufacturing sector has adopted SD-WAN, more than half operate hybrid networks, and many use both together. Nine out of 10 manufacturers that deployed SD-WAN report net gains, realizing improvements in security (and important value to 81% of manufacturers) and in network performance (an important value to 69% of manufacturers).

Take advantage of the internet's pervasive reach with a hybrid networking plan: Hybrid networking has also been adopted by more than half the manufacturers. Nine out of 10 manufacturers that deployed hybrid networks see benefits: The main driver is cost savings (an important value for 73% of manufacturers), followed by improved network performance and greater network flexibility (important values to 52% and 48% of manufacturers, respectively). Once manufacturers mix private and public networks, they turn to outside assistance to secure and manage them. This includes using managed security services partners to manage on-premise devices and host secure gateways between networks..

> **Improving the network is not magic. SD-WAN and proactive monitoring is contributing to better KPIs. We are measuring responsiveness, network downtime, reported incidents, operational cost savings, and redeployment of our resources to create better capabilities, and of course for bottom-line cost savings.**
>
> **Head of IT**
> Healthcare manufacturing firm headquartered in US

> **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

Connect network strategy to the cloud strategy: Manufacturers turn to secure cloud connectivity and dynamic bandwidth to make their networks more flexible and secure. 57% of manufacturers adopt WAN/cloud connect services, compared to 50% of industries on average. When it comes to re-designing the network around cloud, manufacturers are also ahead: 39% have completed such a network re-design, compared to 31% of enterprises across all industries.

Work with partners for secure network transformation: Successful network transformation is a consultative process that relies on service partners for success. That is especially the case for security. Manufacturers realize a serious compromise can threaten to shut down their business, and thus invest accordingly. This is why manufacturers frequently turn to managed security assistance for managed firewalls and hosted secure gateways, to cloud access security broker (CASB), DDoS protection, security information and event management (SIEM) and threat management.

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