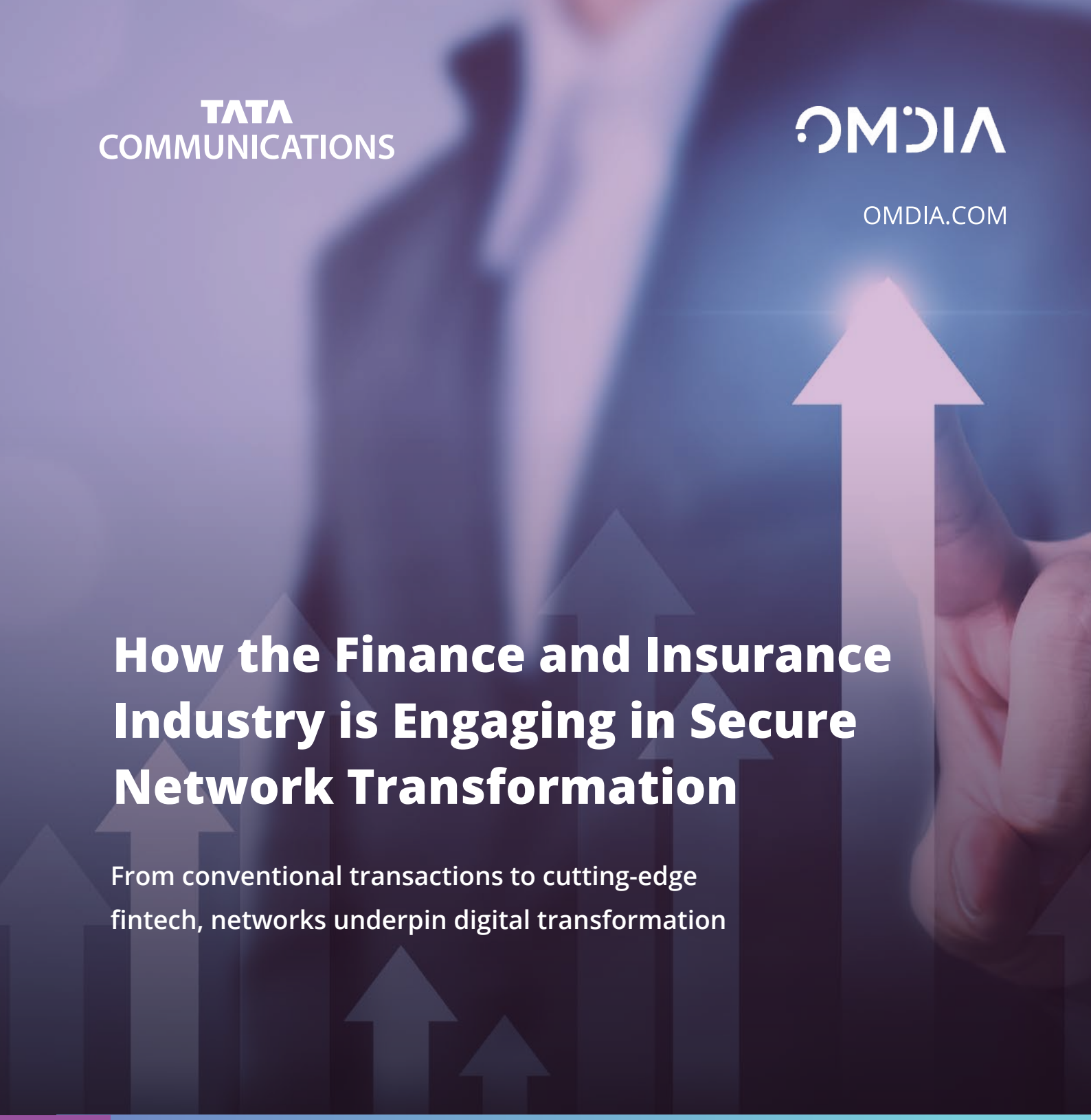


TATA COMMUNICATIONS

OMDIA

OMDIA.COM

# How the Finance and Insurance Industry is Engaging in Secure Network Transformation

From conventional transactions to cutting-edge fintech, 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 finance and insurance sector

## The state of financial services

The financial and insurance industry is responsible for tracking and managing assets and liabilities of clients. The industry includes retail consumer and commercial banks, investment and brokerage businesses, accounting management and advisory firms. The insurance side of financial services includes retail and commercial coverage for health/life, property and casualty, plus large-scale reinsurers. The financial services sector is both highly interconnected and highly regulated, and must comply with strict privacy and security terms to protect sensitive information and client assets. The sector is large enough to have a dedicated IT practice known as financial technology (fintech), which aims to help make companies more agile and competitive, while enforcing industry compliance.

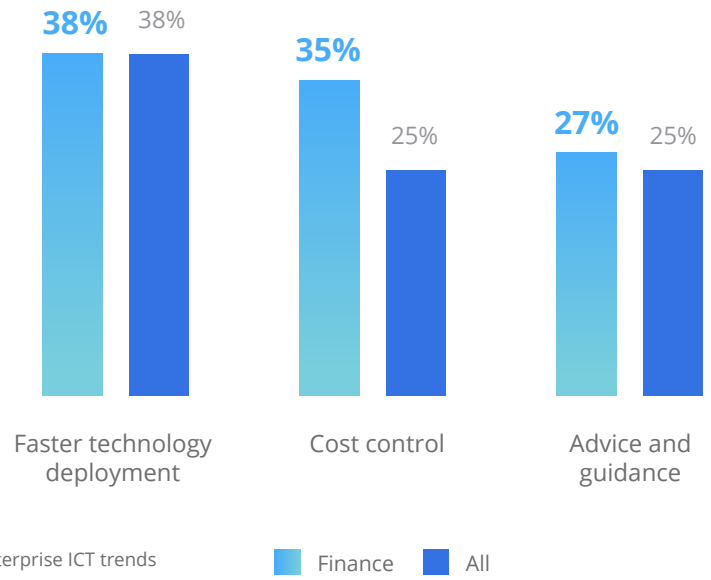
2020 has been a challenge to all industries. Many financial services firms were already pressed become more efficient and contain costs. Omdia enterprise survey research conducted after the global spread of COVID-19 shows that the average 2020-2021 IT budget in the financial services sector is down about 15% year-over-year. These cuts are steeper than the average 10% reduction in ICT budgets reported across industries. The finance and insurance sector is reducing spend in anticipation of unstable, unpredictable market changes and lower revenues.

The financial services sector relies heavily on IT automation for success. Large financial services firms undergo regular cycles of integration projects to migrate systems, normalize data, upgrade data center and network architectures, and replace applications. The industry depends on quality data and analytics for decision-making; on secure transaction processing, verifying and recording; and on communications that give clients a positive experience.

Financial services firms need flexible networks that can adapt quickly to changes. They also need to find ways to lower their costs, for example by bringing in partners as trusted advisors to help them in reaching their goals (see Figure 1). Executive decision-makers in the financial services industry note key criteria to select partners includes those who aligning IT with the business; and those who can provide them an edge in innovation.

**Figure 1:** Financial services IT wants partners to help contain costs

**Finance and insurance sector priorities from services partners**



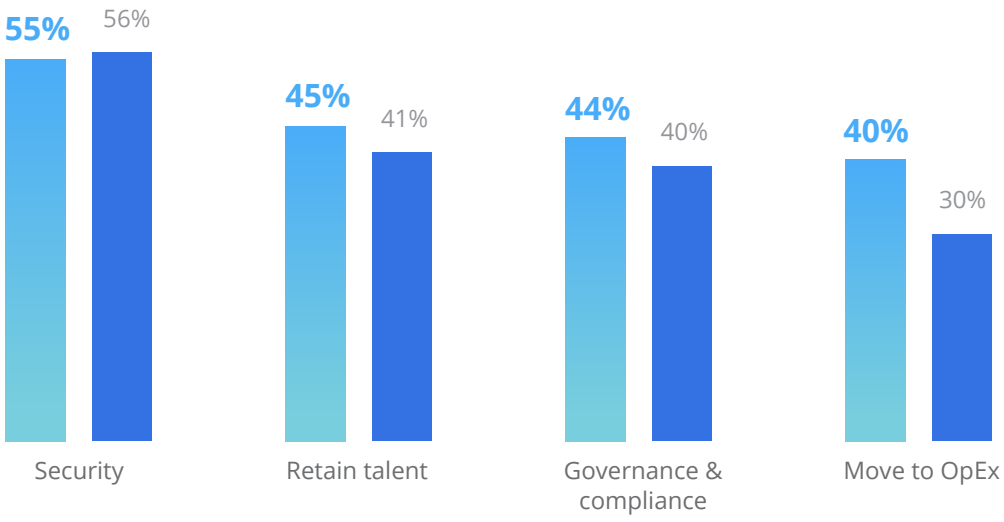

**Source** Omdia COVID-19 enterprise ICT trends

The financial services industry is still investing in key areas: 45% of the sector plans to make new team collaboration investments; 42% expects to grow its unified communications spend. Further, 35% of financial sector companies plan to add to their already considerable investments in security services and platforms, and 24% plan to increase spending on managed network services including managed SD-WAN.

Security, along with proper governance and compliance, remain top priorities for the financial services industry.  Financial services companies are also much more likely explore moving from CapEx to OpEx models as another way to help control costs (see Figure 2).

**Figure 2:** Financial services firms seek security and compliance

**Finance and insurance sector investment priorities**




**Source** Omdia COVID-19 enterprise ICT trends

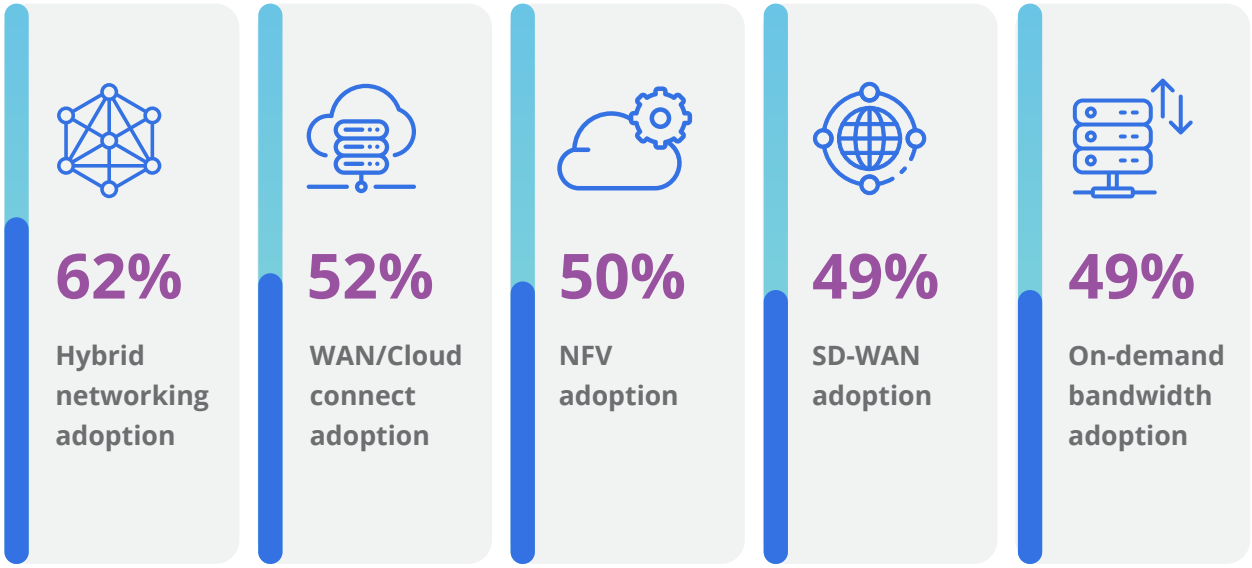
## Security plays a key role in the financial sector's network solutions

The financial services industry is keenly aware of the critical importance of keeping information secure. Cyber criminals actively target financial services companies to infiltrate and steal data, or to disrupt systems and operations. A security breach can mean immediate, disastrous financial losses, but it has even more far-reaching, damaging consequences. A compromise can trigger a series of costly follow-up actions for compliance: Investigation, remediation, reporting, client notification. The company may be found liable and be subject to penalties if security practices are found not to be compliant. Most damaging in the long term is the shaken customer confidence in the institution.

The financial services industry already spends heavily in cybersecurity – by some measures as much as 10% of its total IT budget. The financial services sector also leads other industries in secure hybrid networking and network function virtualization (NFV) adoption. Financial services companies also adopt SD-WAN, dynamic bandwidth and secure WAN connectivity to cloud (see Figure 3). Each of these network transformation elements can add important security protections.

**Figure 3:** Financial firms adopt hybrid networks and cloud connect

**Network transformation adoption in financial services**




**Source** Omdia Enterprise Network Services Insights 2020

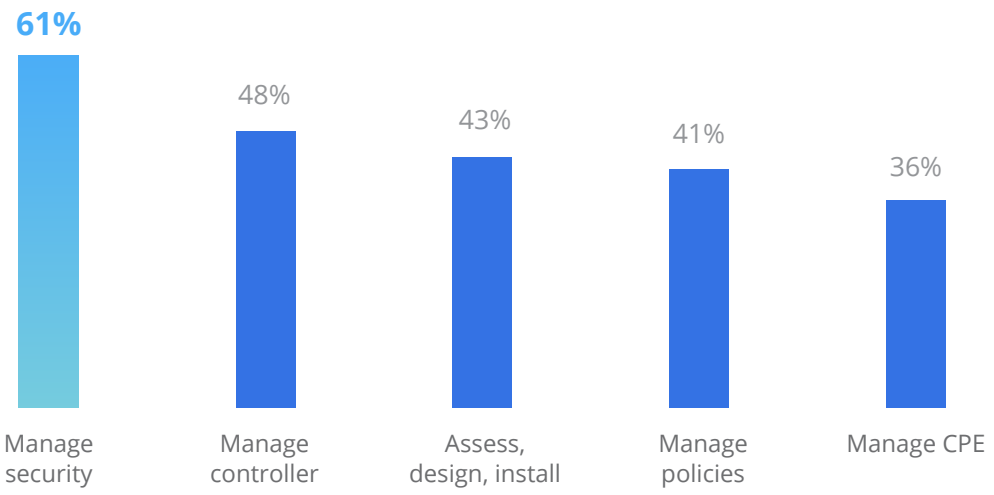
## SD-WAN's role in network transformation

Omdia finds that about 49% of enterprises in financial services currently use SD-WAN. There are fewer SD-WAN deployments in financial services compared to other key sectors. But financial services firms that do use SD-WAN build bigger deployments. About 20% of financial services SD-WAN is deeply deployed throughout the organization. At the other end, one-third of financial services adopters are still piloting SD-WAN or reach just a few sites. The rest fall somewhere in between.

As with all industries, the financial services sector relies heavily on managed services to help deploy and operate SD-WAN (see Figure 4). Omdia finds that 61% of financial services companies deploying SD-WAN turn to outside help for managing related security. Nearly half of financial services companies recruit a partner for the SD-WAN controller. Just 7% of financial services firms deployed SD-WAN without seeking help from managed services partners.

**Figure 4:** Financial services turn to SD-WAN services partners for Security

**Financial services sector turns to provider partners in SD-WAN**




**Source:** Omdia Enterprise Network Services Insights 2020

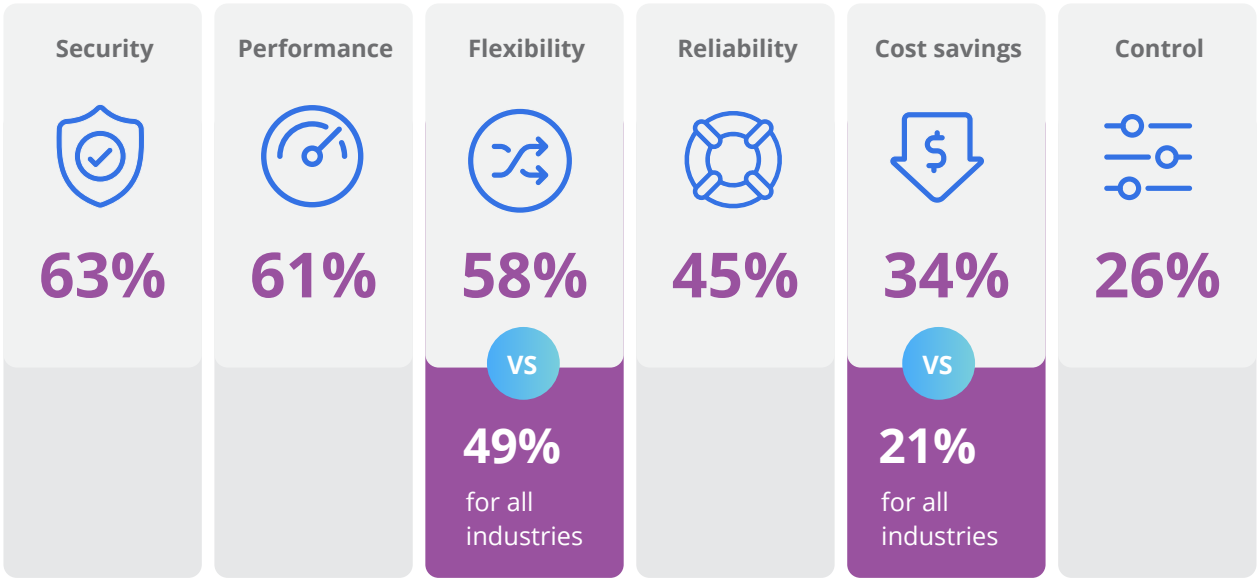
Virtually all financial services companies that adopted SD-WAN report net positive returns. These companies estimate a 49% increase in returned value from their deployments on average. Enterprises realize this SD-WAN value in terms of direct cost savings; from indirect cost savings such as improved efficiency and uptime; and from 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 the financial services industry? The top driver is security, closely followed by improving network performance (see Figure 5). Like other industry sectors, the financial services industry leverages SD-WAN's built-in security features such as firewalls, applications policies and path route restrictions, and management analytics to secure their applications.

For performance, SD-WAN also assigns priorities based on application, which is especially helpful to large brick-and-mortar retail banks that support up to hundreds of active applications and resources. Retail financial and insurance businesses, for example, deal with applications that have very different performance profiles: There are high-priority, low-latency transactions; high-priority, latency-tolerant transactions; high-performance, best-effort streaming applications; and best-effort traffic such as guest/worker internet access.

**Figure 5:** Financial sector values SD-WAN for security and performance

**How the financial services sector prioritizes SD-WAN benefits**




**Source:** Omdia Enterprise Network Services Insights 2020

## Hybrid networks unify WAN and internet safely

Many companies in the financial services sector have turned to hybrid networks to help control costs while maintaining network security. Hybrid networking mixes private WAN and secure internet VPNs to connect sites. Many financial services companies limit their exposure to hybrid networking. Nearly half of hybrid network adopters in financial services are still testing the technology or have connected only a few key locations. A few finance and insurance businesses (15%) have been comfortable rolling out hybrid networks across the business. One-third of the industry still lies someplace in between for hybrid networking adoption. Financial services companies are keen to use hybrid networking selectively, but security and compliance requirements favor conservative change.

When financial services firms adopt hybrid networks, they turn to service provider partners for help. Most frequently, the sector uses partners to aggregate hybrid networking access. But about half (51%) of hybrid networking adopters in financial services tap services partners for a security role, and some (38%) companies use partner-hosted secure gateways. The sector prefers centralized gateways, with 60% preferring regionally or fully centralized gateways over managed site CPE firewalls that support distributed local internet breakout (see Figure 6).

**Figure 6:** Financial services sector prefers centralized security

**How the financial services sector connects WAN/internet securely**


**Source:** Omdia global enterprise WAN services survey 2019

The financial services sector's lead reason for using hybrid networks is improved control (75%): These companies want centralized network management and better applications traffic management. Other important reasons these companies adopt hybrid networks include cost savings (60%) and improved network performance (46%) from merging private WAN with public internet connections. Increased security is not a driver for financial services to buy hybrid networks. But they do require hybrid networking to show an equivalent level of protection to private networks.

> **Many of our applications cannot use the cloud. We are compliant with [financial industry] requirements like PSD2. With these security and government regulatory compliances in place, our customer data cannot go into the cloud.**

**Vice president**
financial services firm headquartered in US

> **We use a lot of MPLS because of regulations. We have direct circuits to some of our partners to protect their data. We do a lot of processing with different banks, and for regulatory reasons we like point-to-point circuits... we keep internet access separate for security reasons.**

**IT manager**
financial services company headquartered in Europe

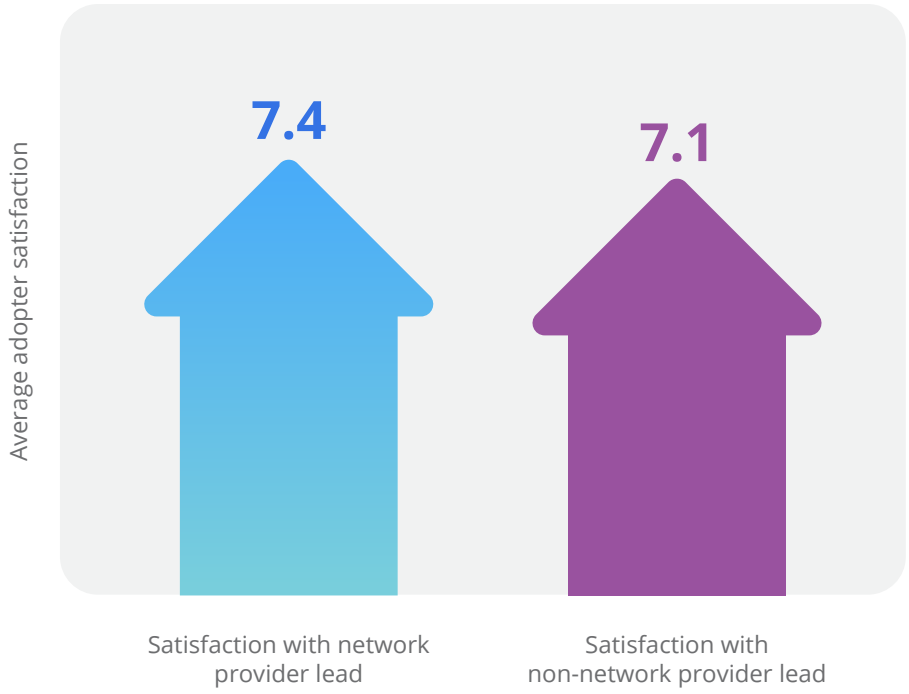
## Network providers as partners to the financial services sector

When it comes to leading network transformation, financial services look to network providers as lead partners 46% of the time for SD-WAN; they look to network providers as lead partner 40% of the time for hybrid networking. These organizations might instead 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.

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

**Figure 7:** Financial firms prefer telco lead partners for hybrid network

**Financial services sector rates network providers highly as lead hybrid networking partners**




**Source:** Omdia Enterprise Network Services Insights 2020

## Recommendations for financial services companies

**Explore SD-WAN as a proven safe bet that brings a range of benefits:** The financial services sector uses SD-WAN to improve performance and enhance security controls. While fewer financial services companies (49%) to date work with SD-WAN, adopters to date have bigger deployments and say they realize greater benefits. More than 95% of financial services companies that deployed SD-WAN say they have realized net gains, prioritizing benefits including security (a priority to 63% of respondents) and network performance (a priority to 61% of respondents).

**Tap the internet's pervasive reach through managed hybrid networking to control costs:** The financial services sector has widely turned to hybrid networking to help with network performance and cost control, with a high 62% adoption rate. About 85% of these hybrid networking adopters say they have already realized benefits. The main adoption drivers are better network control (a priority to 75% of respondents), and cost savings (a priority for 60% of respondents).

**Connect network strategy to cloud strategy:** Depending on the type of business and market, the financial services sector faces compliance restrictions on cloud services. But there are plenty of less-restricted operations needs where firms can take advantage of cloud economics. 52% of the sector has adopted network-to-cloud connect services; 49% of the sector also uses at least some dynamic bandwidth services.

> We are building a spine-leaf architecture around our data centers. That means traffic will no longer travel all the way through a hub router to connect users and systems. Traffic will be routed faster. Our data centers are using 100 Gbps and 40 Gbps modules and discontinuing 10 Gbps models.

**Vice president**
financial services firm headquartered in US

**Work with partners for secure, managed network transformation:** Successful network transformation is a consultative process. The financial sector must extend security and compliance measures across its network services, and services partners help validate and maintain compliance. The financial services industry relies on partners for network security as diverse as managed firewalls and hosted secure gateways, cloud access security broker (CASB), DDoS protection, security information and event management (SIEM), and threat management.

> **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 manager**
> e-commerce arm of financial services firm headquartered in Europe

# 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