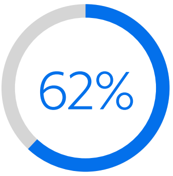
GUIDE

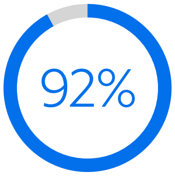
Achieve greater growth as a connected, secure organization

Prepare the network for these key financial industry trends

Spectrum BUSINESS®



of U.S. adults use two or more financial apps.[2]



of financial services leaders say they must adapt to cloud operations or fall behind competitors.[3]

Digital services and technology have become important growth drivers in financial services. Simply consider that 77% of retail banking customers prefer to do their banking via digital channels, compared to 8% who still opt for visiting a branch and just 5% who favor ATMs.[1] Local branches are responding by evolving their digital technology and integrating advancements, such as digital tellers and AI-powered interactive screens. At the same time, commercial banks and emerging FinTech firms are relying heavily on the cloud and ever-more-complex networks to support transaction growth. While they may differ in terms of products and customers, these financial services businesses share an escalating need for instant, reliable and secure connectivity and networking.

To remain relevant to their digital-minded users, companies must stay current with emerging trends and proactively adapt their network as they evolve. Skyrocketing data volumes need to move securely and seamlessly among private data centers, branch locations and the cloud. Security strategies must keep pace to reliably protect this data in transit and at rest. These requirements are key to realizing the desired return on investments in vital areas such as the customer and employee experience and advanced analytics.

This guide outlines priorities and strategies that support the evolving demands on networks and the technologies that make modernization possible for financial services organizations. Sought-after improvements include support for fast-growing bandwidth requirements, faster routing, simplified WANs and security strategies that extend beyond corporate firewalls.

Modernize financial services with scalable, flexible connectivity

The financial services marketplace has seen dramatic change in recent years. While ushering in exciting new operational opportunities, the transformation has also revealed the limitations of legacy networks. In some cases, the network infrastructure of these financial institutions has been neglected due to limited budgets, competing priorities or a lack of resources.

The limitations of legacy networks

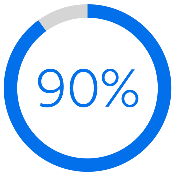
Legacy networks are increasingly being asked to handle a broader array of services and traffic types to support online banking, branch operations and the data growth that comes with emerging technologies, such as transaction processing, account management and recordkeeping. As new digital capabilities are introduced, the network requires more flexibility — to scale bandwidth, route traffic appropriately and customize different connection types. This can be expensive and time-consuming with older systems.

Security is just as critical. Relying on the potentially outdated security protocols of legacy networks can put a company's data and users at great risk. Nearly half of all breaches involve customer personally identifiable information (PII), which can include tax identification (ID) numbers, emails, phone numbers and home addresses.[4] One 2024 breach suffered by a mortgage lender exposed the private data of 16.9 million customers and caused disruptions at the company for nearly two weeks.[5] Adding to the complexity, network improvements to minimize these threats must be executed without negatively impacting the performance experienced by users, a tall order for lean IT teams.

The benefits of transitioning from MPLS to SD-WAN

Many companies continue to rely on networks originally built around multiprotocol label switching (MPLS) technology. Transitioning from private MPLS connections to using the internet and a software-defined wide area network (SD-WAN) as the controller overlay can help organizations modernize their legacy networks. The move can deliver numerous benefits to financial services organizations.

	SD-WAN	MPLS
Changes	Thanks to the virtualized infrastructure, changes can be executed in minutes.	Updates to complex point-to-point MPLS circuits can take months.
User experience	Critical traffic is prioritized, while local internet breakouts at branches can contribute to enhanced performance by sending traffic directly to the internet and cloud applications.	Backhauling to a central gateway can cause latency and impact application performance.
Security	Support for encrypted end-to-end tunnels and secure access service edge (SASE) capabilities can boost protection.	Although connections are private, they are not encrypted, and SASE capabilities are not supported.
Cost	Flexible hardware options and the agility of the public internet allow for fast, cost-effective deployment to new branches.	The approach requires specialized physical routers, expensive dedicated circuits and the same provider at all sites.



of financial services leaders who invest in cloud-based services say they have seen an increase in profit due to this investment.[6]

Streamline network management and growth with SD-WAN

When upgrading legacy networks, firms can achieve greater efficiencies by scheduling their SD-WAN rollout to align with established router replacement cycles. This move allows branch network resources to be centrally managed and efficiently consumed as needed. Organizations can implement fully or co-managed enterprise solutions customized to their IT resourcing strategy, freeing often overburdened or under-experienced IT teams to offload routine tasks and pursue more important growth-focused initiatives. With SD-WAN, IT can support cloud-based network administration from anywhere and utilize a self-service portal. This accessibility can empower IT teams with near real-time visibility into network performance, enabling staff to respond with greater confidence and agility to changing conditions across the business.

Security regulatory compliance is a central requirement for financial services companies. A firm's SD-WAN devices can form an encrypted overlay across any underlying transport service, including MPLS. If employing SD-WAN within a SASE framework, devices primarily route traffic to the cloud, where security inspection can be performed quickly regardless of volume or features. Local SD-WAN devices can strengthen an organization's overall security strategy and help ensure regulations are met. In addition, updated disaster recovery strategies can easily include redundant connections and more affordable bandwidth for routine backups.

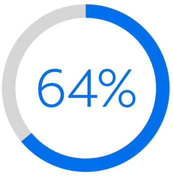
SASE explained

Learn more about this powerful security framework in our glossary for evolving network security.

Explore glossary

Maximize the benefits of the cloud

Financial services organizations must contend with and respond to a variety of forces accelerating change across the industry. Cloud adoption ranks high on the list of drivers, having become a top priority for a growing number of financial services leaders. Major contributors to this trend are sizable remote and hybrid workforces — 83% of U.S. financial services companies offer work location flexibility.[7] Some online-only banks already rely predominantly on cloud-based architectures.



of financial services leaders worry about complying with regulations in cloud operations.[8]

Optimize cloud traffic with SD-WAN

The transition to the cloud, while offering a host of benefits, does come with considerations, including:

- Meeting the same regulatory safeguards as data stored locally.
- Adapting the industry's highly complex, intertwined and customized legacy networks.
- Managing the proliferation of cloud services with an eye on possible impacts to performance and the user experience.
- Adding WAN edge connectivity to public cloud platforms and data centers to meet evolving needs.

Adopting SD-WAN can help organizations address issues and make the most of their transition to the cloud, with benefits including:

- Improved management of the company's cloud traffic.
- Streamlined connections to business-critical cloud services via traffic prioritization.
- Direct, secure and flexible access to services with Layer 2 Ethernet connections to preferred cloud service providers.
- Greater visibility, if equipped with a central control dashboard, into areas experiencing high latency or jitter.
- Optimal traffic flow in real time and the ability to make fixes that do not affect end users.
- Efficiencies across hybrid networks to help firms accelerate the introduction of new digital services.

Simplify and enhance branch connectivity

Brick-and-mortar branches still have an important role in meeting the needs of customers in a cluttered, competitive marketplace. Some customers desire the peace of mind that can come with meeting a representative in person. As a result, many firms are adopting a "phygital" model that blends in-person and virtual resources. Bridging this digital divide within branches and across locations, some of which are situated well outside urban centers, requires thoughtful planning and execution with ongoing optimization and management.

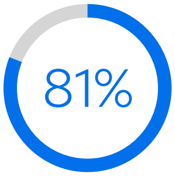
As connectivity expands and a greater volume of sensitive data is shared among branches, offices, mobile users and the public cloud, firms can find complying with stringent industry regulations more challenging than ever. For example, one Payment Card Industry Data Security Standard (PCI DSS) requirement specifies encrypting the transmission of cardholder data over public networks, while another specifies installing and maintaining a firewall configuration to protect cardholder data. Keeping track and keeping up is crucial.

Meet the needs of branches with networking modernization

Delivering for today's users requires a network solution that offers flexibility and high availability. In addition to connectivity for immediate transactions, organizations must support their branches with reliable access to processing centers and off-site data storage as well as low-latency mobile apps and uninterrupted web performance.

Simplified IT management becomes critical as banks modernize their branches and virtual offices. This includes streamlining WAN management across locations and equipping IT teams with the ability to visualize and manage this complex network as a single entity. Additionally, the tools and technologies employed in branches need to be uniform across locations to allow easy synching and a consistent experience.

The right networking technologies can reduce IT workloads and increase performance by providing solutions that bring a variety of services into a single platform. As part of the modernization effort, new customer premises equipment that integrates branches into a centrally managed SD-WAN can provide financial services organizations a path for replacing their dedicated, hardware-based branch routers. A growing number of IT and infrastructure leaders have made the switch or intend to do so to take advantage of the integrated routing and security enhancements.



of financial services executives say a lack of appropriate technology impedes their business goals.[9]

Experience the benefits of all-in-one branch networking

Given the complexity that can come with network modernization, firms need enterprise financial technology solutions able to minimize growing task lists, streamline workloads and support regulatory compliance. All-in-one networking platforms offer a host of benefits:

- Decrease the demands on busy IT teams thanks to automated maintenance and security updates.
- Remotely address configuration and troubleshooting via a single portal.
- Integrate smart cameras and sensors to oversee physical security demands via the portal.
- Directly integrate WiFi to better support connectivity for customer devices at branches and other locations.
- Support scalable fiber connections to introduce and manage virtual tellers and unified communications (UC) solutions, all with minimal latency.
- Drive return business and greater customer brand loyalty through enhanced convenience and service.

Working with a single experienced service provider can advance the firm's modernization goals, from the integration of fiber connectivity and UC to TV services and cloud security technologies. The rewards can be significant, with financial services firms able to simplify their branch IT management while improving their visibility and reporting capabilities.

Secure the entire organization

Financial services organizations spend an average of more than $6 million to remediate a data breach, including not just notification, detection and escalation costs but also disruptions to business and damage to reputation, customer loyalty and regulatory compliance.[10] To mitigate the considerable threats, these companies require networking solutions that incorporate always-up-to-date security technologies. Ingredients should include enhanced firewalls, SSL inspection, web filtering and web application control. The security strategy should also account for the risk of distributed denial of service (DDoS) attacks and include means for mitigating these threats through the firm's connectivity provider.

Protecting branches, employees and cloud data has never been more important — or more challenging — for financial services organizations. With an all-in-one network platform, companies can safeguard branch locations through automatic updates. Integrated capabilities can incorporate a firewall, advanced malware protection and intrusion prevention.

IT needs to secure employee access to services outside the network as well. Systems with weak or no credentials are the top initial access vector for attacks in the cloud, accounting for over 45% of breaches during the latter half of 2024.[12] A cloud security platform that includes cloud-based firewalls, secure web gateways and zero trust network access can consolidate and strengthen security measures across cloud services. The platform must also offer multi-factor authentication (MFA). Centrally managed MFA adds another layer of protection when employees access internal networks and the cloud.

Effective and efficient user access control is another fundamental requirement. Comprehensive identity management (IdM) supports remote and hybrid work models, simplifying the control, oversight and governance of user identities and access. This helps ensure that only authorized individuals can access a firm's applications, critical data and systems. Modern access control solutions help simplify the setup of virtual private networks (VPNs), as well, by configuring the necessary infrastructure and protocols that enable users to more easily and securely access network resources. Managed network services provide firms with VPN management solutions that oversee updates spanning user access, authentication and encryption keys.

The state of data security according to financial services leaders[11]

90%

say data security is their top IT priority.

48%

are highly confident they have the right security measures in place.

Accelerate modernization with Spectrum Business®

Financial services leaders understand the benefits of SD-WAN, scalable fiber connectivity and streamlined networking solutions to connect branches, offices and the cloud. To make the most of these technologies, companies are turning to experienced managed services providers to help them exceed user expectations, streamline operations and improve their competitive edge.

At Spectrum Business, our reliable, secure, enterprise-grade services can be fully or co-managed to meet your requirements. Our portfolio combines managed network services, enterprise cloud services and connectivity services to help firms move data faster, reduce total cost of ownership, strengthen security and enhance the user experience. Partner with Spectrum Business for installation and management, backed by a service-level agreement (SLA) that guarantees 100% uptime all the way to the handoff point at your location* and 100% U.S.-based support, available 24/7/365.

Learn more

*100% uptime SLA guarantee applies only to Dedicated Fiber Internet, Secure Dedicated Fiber Internet, Ethernet Services, Cloud Connect and Enterprise Trunking.

1. "National Survey: Record Number of Bank Customers Use Mobile Apps More Than Any Other Channel to Manage Their Accounts," American Bankers Association, November 22, 2024.
2. Keith Nissen, "One-Third of Americans Use Three or More Financial Apps," S&P Global, August 8, 2024.
3. "Harnessing Technology: The 2024 Financial Services Market Report," Egnyte, 2024.
4. "Cost of a Data Breach Report 2024," Ponemon Institute and IBM Security, July 2024.
5. Carter Pape, "The Biggest Data Breaches of 2024 in Financial Services," American Banker, December 16, 2024.
6. "Technology Adoption in Financial Services: A Sector View of KPMG's 2024 Global Technology Study," KPMG, 2024.
7. "The Flex Report: Q4 2024," Flex Index, 2024.
8. "Harnessing Technology."
9. "Propel Top-Line Growth With Your Cloud Journey: Fast-Track Efficiency, Innovation, and Superior CX," Capgemini Research Institute, November 2024.
10. "Cost of a Data Breach Report 2024."
11. "Harnessing Technology."
12. "H2 2024 Threat Horizons Report," Google Cloud Security, 2024.