White Paper

Building a Secure and Resilient Financial Enterprise

With Netskope, financial organizations can rapidly reach the full potential of their digital infrastructure investments with a modernized, agile, connected, and secure user experience.

INTRODUCTION

The financial industry is rapidly transforming due to several key drivers, including the need for competitive edge, enhanced risk management, and cost-saving opportunities. To succeed in this new landscape, financial institutions must embrace digital transformation as a core growth strategy. However, the adoption of digital infrastructure comes with significant cybersecurity challenges, as the financial sector requires balancing competing demands, managing legacy and modern apps, and complying with various regulations.

This paper provides an overview of the driving forces behind digital transformation in finance and highlights best practices for overcoming challenges. We introduce the Netskope solution and demonstrate how it can help financial organizations unlock new value by securing digital transformation. By embracing digitalization securely and with speed, financial institutions can deepen customer relationships, gain new revenue streams, and streamline operations while mitigating risks.

The path to successful digital transformation in the financial industry is not without challenges, but the potential rewards are significant. By embracing digital transformation, financial institutions can transform the industry for the better and unlock their full potential.

NAVIGATING THE DIGITAL TRANSFORMATION CHALLENGES

The financial industry's transition to digital presents a host of obstacles, but with proper planning and solutions, these challenges can be overcome. Ensuring seamless service and performance is paramount in the financial sector. Financial organizations must prioritize robust and highly available systems that can manage increasing user traffic while providing secure cloud services with low latency.

Protection of sensitive data is also critical. Financial institutions must implement secure storage and management solutions to ensure the protection of vast amounts of customer information. Most of this data is subject applicable laws, standards, and industry regulations—such as GDPR, and PCI-DSS. And those from the EBA, FCA, CBUAE, SARB, and other country specific regulators which is a significant challenge for financial organizations. These regulations create comprehensive requirements for data privacy, cybersecurity, and risk assessment, leading to mandated operational deliverables for IT and security teams.

Improving user experience is another challenge faced by financial institutions. Legacy MPLS and VPN networks are slow to deploy and can create network congestion. In addition, the financial industry's complex mix of digital technologies leads to disconnected security components that are costly and challenging to manage. Financial organizations must seek solutions that provide a streamlined, integrated, and user-friendly approach to security.

Cyber threats such as ransomware, malware, and APTs continue to escalate, with information security being named as the top issue by 70% of fintech companies[1] and a rise in network security threats reported by 39% of financial industry executives[2]. To counter these threats, financial organizations must secure remote access and protect against them through encrypted traffic using solutions based on zero trust frameworks.

[1] https://cybersecurity.att.com/blogs/security-essentials/the-biggest-concerns-within-the-us-financial-sector-in-2022

[2] https://cybersecurity.att.com/blogs/security-essentials/the-biggest-concerns-within-the-us-financial-sector-in-2022

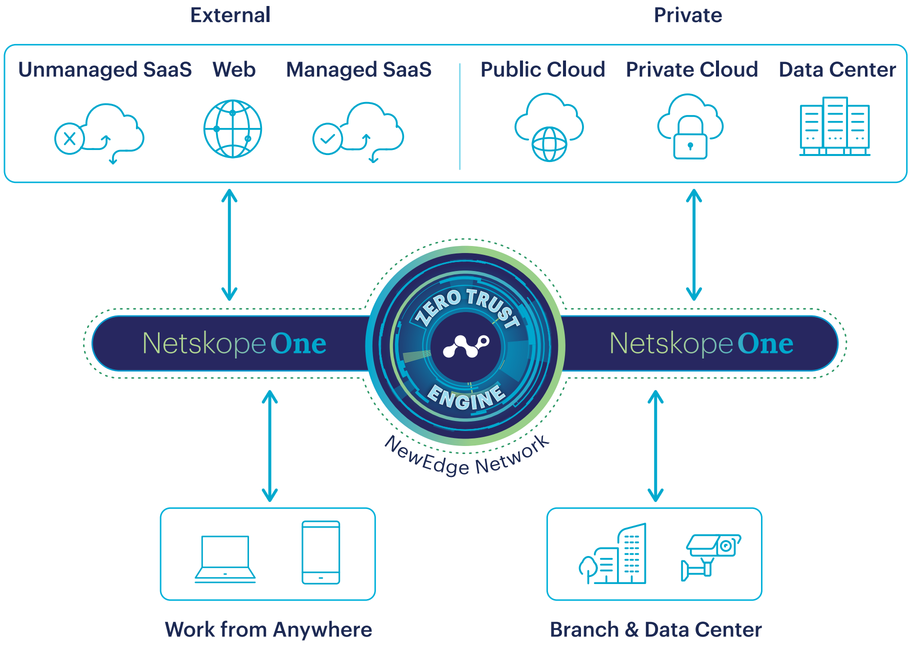
THE NETSKOPE SOLUTION FOR A MODERNIZED FINANCIAL ENTERPRISE

The Netskope One Platform

The Netskope One unified SASE platform provides optimized access and zero trust security for people, devices, and data anywhere they go, helping organizations reduce risk, accelerate performance, and get unrivaled visibility into any cloud, web, and private application activity. With a data-centric approach to security and performance, Netskope empowers financial institutions to tackle evolving threats, manage new risks, adapt to technology changes, accommodate organizational and network shifts, and comply with regulatory requirements.

With Netskope, you can:

- Simplify your security in the cloud with a cloud-native platform that offers converged security and networking services to enable your SASE and zero trust transformation;
- Understand context to better manage risk in order to protect people and data anywhere they go;
- Optimize network connectivity and performance with Netskope Borderless SD-WAN;
- Bring security closer to the edge with Netskope NewEdge network - the world's largest private SASE cloud; and
- Realize better returns on investment (ROI) from technology investments.



The Netskope One Platform

IMPORTANT USE CASES BRING VALUE

These example use cases highlight many of the challenges faced by financial institutions every day and the Netskope solutions that address them directly.

Use Case #1 - Analyst Research in a Risk Weighted Environment

Scenario:

An analyst in a financial institution needs to access various market data websites and SaaS applications. This information is required to enrich internal data which, in turn, will be used to support decision-making. Some of these websites and apps have been identified as risky. The analyst's access to the various websites and applications must be context-driven and adaptive, taking into account the various risk parameters instead of enforcing binary decisions such as full access or block.

The Netskope Solution:

- Enhance threat protection and secure browsing experience with Targeted Remote Browser Isolation (RBI) to safely isolate risky and uncategorized websites.
- Securely enabling the use of generative AI across organizations with the widest visibility and classification of GenAI apps through ML-assisted discovery and risk assessment. With enforcement measures to stop sensitive data uploads and coaching to educate users on security policies, reducing risky behavior.
- Identify and address malware and advanced threats hiding in cloud services and web traffic. Leverage multiple prevention defense layers, threat intelligence feeds, automated IOC sharing, and UEBA anomaly detection to mitigate threats.
- Netskope DLP goes beyond discovery and incident response to dynamically enable the proper protection by factoring in organizational context and security risks. Moreover, incident responses are tailored to true data security incidents, minimizing false positives, incident triage, and business disruption.
- Encourage better security decisions and behaviors, helping to meet compliance requirements and improve security without inhibiting employee productivity.

Benefits Delivered:

Benefits include improved risk management, a modernized and enhanced user experience, and improved productivity with secure and contextual access. The analyst is not blocked or prevented from accessing the information and services they need, nor have they been granted access without relevant controls creating excessive risk for the organization. The analyst can now perform their work, access the data they require, and their role is enabled to create value for the organization, supporting business growth, by the very nature of the business process and function they can safely perform.

Use Case #2 - Investment Banker Document Sharing in a Secure Environment

Scenario:

Two investment bankers from two different banks are working on a deal, and they need to securely share documents. One of the investment bankers needs to access documents in a shared folder hosted in the Microsoft 365 application of the other bank, along with accessing data in an internal application. This may introduce new attack vendors for threat actors to capitalize on. Many legacy security solutions fail to assess the risks associated with excessive sharing permissions or control data exposure and exfiltration through shared environments.

The Netskope Solution:

- Enable context-driven zero trust access to specific private applications for remote users through Netskope ZTNA Next, while shielding the rest of the applications from discovery and attacks.
- Leverage multi-data sources and UEBA to determine the user risk posture and enforce dynamic access controls for the shared documents in the Microsoft 365 environment. Restrict the access in case the user risk profile changes or the user device gets compromised, to minimize the risk of data exfiltration.
- Monitor oversharing of sensitive data in the cloud, prevent insider threats exposing sensitive data accidentally or negligently, block data exfiltration to personal accounts to protect highly confidential documents at all costs.
- Alert and coach users on data loss risks, including the context of app risk and user risk, when performing activities with the option to proceed or cancel for managed and unmanaged apps, and web sites so business processes can continue.

Benefits Delivered:

Benefits include risk reduction, improved decision-making, increased agility, and the creation of additional value. The applications' access isn't blocked nor the external user is granted an exception that opens up access to the entire internal network, which might result in lateral movement of threats. Value is created for both financial organizations by securely enabling the normal course of business. Risk is managed within the bounds set by the financial organizations to deliver on their strategic agendas.

Use Case #3 - Improving Branch Office Connectivity and Experience

Scenario:

A leading financial institution has moved many of its business-critical applications to the cloud to enable seamless access to internal data to its branch offices. The deployment of legacy and expensive MPLS has limited the bandwidth for branch sites, making it difficult to access cloud operations in a seamless manner for executing business operations. Further, the remote workers' traffic was getting backhauled to centralized servers via VPNs, leading to latency and performance issues.

The Netskope Solution:

- Netskope Borderless SD-WAN provides every remote user, device, and site with simple, secure, high-performance access to multi-cloud and hybrid-cloud environments.
- Secure and direct access to private applications hosted anywhere through Netskope ZTNA Next eliminates the need for heavy VPN clients.
- Provide assured application experience for critical voice, video with app aware prioritization, dynamic path selection and sub second failover, granular context-aware adaptive quality of experience, and link remediation.

Benefits Delivered:

Benefits include seamless access to corporate resources from every branch site, while reducing the costs at the corporate network in the form of MPLS and VPN infrastructure. Simplified traffic steering through Borderless SD-WAN to the Netskope One Platform and NewEdge Network, delivering security without performance trade-offs and accelerating the adoption of SASE.

> “Netskope has created an opportunity to reduce the footprint on the outside. With NPA we are able to not only allow internal access but also reduce the usage of VPN. Additionally, it helped create opportunities for our international expansion.”
>
> Sr. CISO & CIO,
> Medium Enterprise Diversified Financial Services Company

CUSTOMER SUCCESS STORY

With a mission to guide families and individuals towards homeownership, this Financial Services company has established itself as one of the largest privately-owned lenders in North America. Over the course of 17 years, the company has undergone significant growth, expanding its workforce to over 5,000 employees, opening hundreds of locations across the region, and building a servicing portfolio that encompasses hundreds of thousands of loans, totaling over $50 billion. This Financial Services company's unwavering commitment to their clients and their journey towards homeownership is evident in their continued success and growth.

The Challenge

“COVID changed everything. Suddenly we had to switch from a centralized model to one where our employees could be anywhere in the world and the network perimeter was impossible to control.” These are the words of the Cybersecurity Services Manager at the Financial Services company. The pandemic made remote working at scale fundamental to this company’s survival, but it also introduced new security threats.

The Cybersecurity Services Manager explains: “When we moved to the remote workforce model, we had no controls on our endpoints beyond basic endpoint detection and response. Putting a solution in place became our number one security priority. We needed a much better understanding of what was happening on our employees’ machines, so we could identify potential threats and resolve them.”

The company’s biggest concern was that employees’ corporate devices were connecting to the network via home broadband connections shared by untold other devices such as smart TVs, printers, and smart speakers, any one of which represents a potential way in for hackers, or which could interfere with the digital experience.

> “We see Netskope as a platform. We could quickly get the tools needed to meet our initial challenge, but now we can also add new functionality and solutions as Netskope brings them online.”
>
> Cybersecurity Services Manager,
> Financial Services Company

The Solution

“When looking for a solution to this challenge, we were clear that integration would be a key consideration,” they add. “We have a robust stack comprising brand-new best-of-breed solutions, but that comes with significant admin overheads. Any new solution must therefore help us consolidate our security functions to bring our expenditure down.”

Security Service Edge (SSE): cloud access security broker (CASB), to quickly identify and manage the use of cloud applications and enable data loss prevention (DLP); and secure web gateway (SWG) to protect cloud services, applications, websites, and data across endpoints. In addition, the company uses Advanced Analytics from Netskope to achieve a complete view of its cloud risk posture. “We see Netskope as a platform,” says the Services Manager. “We could quickly get the tools needed to meet our initial challenge, but now we can also add new functionality and solutions as Netskope brings them online. What’s more, working with Netskope we’re in a great position to help shape its product roadmap.” With Netskope at the heart of its cloud security, the Cybersecurity Services Manager and their team are now able to leverage rich sources of data to help with decision making. It’s an approach that’s driving significant benefits for the company.

The Business Benefits

Thanks to the Netskope CASB and Advanced Analytics, this FInancial Services Company now has complete visibility of the applications its employees use. “We went from seeing nothing, to seeing everything,” says the Cybersecurity Services Manager, “and the results were unreal. We discovered thousands of apps in use that we had no idea about—the shadow IT sprawl was astonishing.” This unprecedented visibility enables the Cybersecurity Services Manager and their team to make better informed technology decisions. They provided an example: “We have over 4,000 people using Office 365 as our official collaboration platform. But through the Netskope CASB, we discovered that nearly all of them also regularly use Google Workspace. We now know that when we look to trim some fat off our cloud estate, we must ensure Workspace remains in place or risk harming productivity.” With Netskope, this Financial Services Company can make risk-based decisions on its cloud investments. The Cybersecurity Services Manager comments: “Netskope provides us with data on how our users behave, which we can then use in contracts to specify the expected security policies of potential vendors. We know where our security weaknesses are, and that means we can select companies best placed to mitigate these weaknesses.”

> “We went from seeing nothing, to seeing everything, and the results were unreal. We discovered thousands of apps in use that we had no idea about—the shadow IT sprawl was astonishing.”
>
> Cybersecurity Services Manager,
> Financial Services Company

Financial services is

300

times more likely - to be the victim of a cyberattack than other organizations.[3]

48%

of all malware downloads originate from the cloud as cloud malware[4]

401

different apps were the source of malware downloads[5]

39%

of financial industry executives think that the overall security threat to the financial sector has increased[6]

55%

of financial services firms were victims of at least one ransomware attack in 2021[7]

$18.3 million

is the annual cost of cyberattacks per company in the banking industry[8]

[3] https://securityboulevard.com/2022/11/why-security-it-teams-in-the-financial-industry-are-under-enormous-strain/

[4] https://www.netskope.com/netskope-threat-labs/cloud-threat-report

[5] https://www.netskope.com/netskope-threat-labs/cloud-threat-report

[6] https://www.csbs.org/newsroom/community-banker-concerns-shift-funding

[7] https://assets.sophos.com/X24WTUEQ/at/29t7bmfvtz659x8xj86wfggb/sophos-state-of-ransomware-financial-2022-wp.pdf

[8] https://www.archonsecure.com/blog/banking-industry-cyber-threats

SUMMARY

Netskope helps financial organizations effectively embrace digital transformation to safeguard customer data, support compliance, reduce cyber risk, and ensure operational resiliency and effectiveness. The result is that financial organizations can securely adopt any mix of digital devices and cloud services to enhance collaboration, drive growth, and improve productivity.

Netskope, a global SASE leader, helps organizations apply zero trust principles and AI/ML innovations to protect data and defend against cyber threats. Thousands of customers trust Netskope and its powerful NewEdge network to address evolving threats, new risks, technology shifts, organizational and network changes, and new regulatory requirements. Learn how Netskope helps customers be ready for anything on their SASE journey, visit netskope.com.