
De-Risking The Cloud
Top 3 SSE Use Cases for Financial Services
netskope

Introduction

Cloud adoption among banking, insurance, and other financial services companies is rapidly accelerating as a means to increase productivity and reduce costs. Pandemic market dynamics have caused many companies to fast-track their cloud migration plans and other digital transformation projects. Competition from start-ups, internet giants, and industries outside of banking, along with increased regulations, are also driving banks to accelerate digitalization.[1]

But the rewards of cloud migration also bring new risks: organizations are still responsible for maintaining regulatory compliance and protecting customer data (not to mention their own proprietary information) when outsourcing functions like data storage to cloud services. According to the European Banking Authority (EBA), financial institutions should engage in effective ICT and security risk management for the safe use of cloud computing services.[2]

In light of these circumstances, a security service edge (SSE) is becoming an essential approach to securing the growing number of access points across web, cloud, and private applications. An SSE solution combines several essential services—such cloud-native secure web gateway (SWG), multimode cloud access security broker (CASB), and zero trust network access (ZTNA)—to make up the security component of a broader SASE (Secure Access Service Edge) architecture.

Anyone that wants to maximize the cloud's potential for productivity and cost savings should consider the following critical use cases for securing cloud migrations with SSE:

- Managing the risks that come with more cloud and web usage
- Identifying and protecting sensitive data
- Ensuring compliance and reporting requirements

[1] "The State of Digital Transformation in Banking," International Banker, Marh 18, 2022.
[2] "EBA Guidelines on ICT and security risk management," European Banking Authority, 29 November, 2019.

01

Managing the Risks That Come with More Cloud and Web Usage

Increasing use of cloud services and web applications simultaneously expands an organization's attack surface. While digital transformation makes financial organizations a bigger target, threat volumes have also grown—as cybercriminals try to take advantage of any and all new opportunities for attack. The vast majority (72%) of financial services companies have seen an increase in cyber threats over the last two years.[3]

Unfortunately, risk management at most financial institutions has not effectively kept up with the accelerated pace of digitalization. A recent survey shows that nearly half (48%) of respondents in the financial sector feel that their security measures are falling behind their digital transformation deployments (worse than the all-industries average of 39%).[4] The longer it takes to spot a problem, the greater the potential for damage to be done—and it currently takes an average of 233 days to find and contain a breach in the financial sector.[5]

Financial services organizations need to be able to identify, understand, and manage all the risks that come with their expanding cloud and web usage. The integrated capabilities of an effective SSE solution can simplify management of your company's security policies to help eliminate risks—while providing continuous, adaptive controls for access, data movement, and threat protection.

Functional Requirements:

- Gain granular visibility into your cloud and web usage, so you can strike the right balance between risks and expected business benefits
- Discover which cloud services and websites are being used
- Assess enterprise-readiness of cloud services
- See usage details about users, activities, and data

[3] "Financial Cyber Survey," Deloitte, June 2021.
[4] "Report finds 'glaring gaps' in financial sector's cybersecurity measures," Insurance Business Magazine, December 1, 2021.
[5] "How can a zero trust policy improve your industry?," Security Intelligence, January 14, 2022.

02

Identifying and Protecting Sensitive Data

Successful system intrusions in the financial sector have more than doubled in recent years—going from 14% in 2016 to 30% in 2022.[6] Ransomware is one of the main reasons for this upswing—with the banking industry weathering a staggering 1318% increase in ransomware attacks last year.[7] Ransomware attacks can do irreparable damage to a financial organization's brand—not to mention losses due to disruption of operations, exfiltration of proprietary data and/or private customer information, remediation costs, and other potential downstream damages (e.g., fines, penalties, litigation costs).

Even when organizations aren't specifically targeted, the synchronization and sharing functionality of popular cloud services can offer a perfect medium for broad-spectrum distribution of malware. Breaches involving cloud services highlight the importance of sound security controls and management's understanding of the shared responsibilities between cloud service providers and the institution's clients.[8]

Financial organizations need modern cloud security that uses granular context and deep visibility to control cloud usage of sensitive data. SSE can help you identify and protect all of your sensitive data, wherever it resides—such as design plans stored in the cloud or control data being uploaded, downloaded, and shared. An effective solution will offer data protection driven by artificial intelligence and machine learning analytics for scale and efficacy.

Functional Requirements:

- Accurately detect all your sensitive content
- Support your data classification system
- Protect sensitive data with strong encryption
- Prevent data exfiltration to non-authorised cloud services

[6] "2022 Data Breach Investigations Report," Verizon, May 24, 2022.
[7] "Banking industry sees 1318% increase in ransomware attacks in 2021," Security Magazine, September 20, 2021.
[8] "Joint Statement: Security in a Cloud Computing Environment," Federal Financial Institutions Examination Council, April 30, 2020.

03

Ensuring compliance and reporting requirements

Arguably more than any other industry, financial services must maintain compliance with strict government and industry regulations—or face steep fines and other potential penalties. Regulatory expectations for financial services institutions have been increasing —and accordingly, operating costs spent on compliance have risen by over 60% for retail and corporate banks.[9]

When it comes to the resilience and security of their rapidly expanding cloud infrastructure, regulatory concerns are a complicating factor that financial organizations must anticipate and address.[10] To ensure compliance, SSE can help you understand activity-level usage of your cloud services and websites, in the context of applicable laws, standards, and industry regulations—such as GDPR, PCI-DSS, ISO27001, NIS2, and DORA. As well as those from the EBA, FCA, CBUAE, SARB, and other country specific regulators.

A fully featured SSE solution should also simplify auditing and reporting processes. It should provide you with a granular, contextual audit trail of all cloud activities to facilitate reporting in accordance with regulatory requirements.

Functional Requirements:

- Govern access, activities, and data across cloud and web
- Build a detailed audit trail of cloud and web activities
- Create regular reports for policy compliance
- Govern usage across all cloud and web services
- Restrict non-compliant activities
- Create regular reports for auditors
- Provide details about users, activities, and data
- Drill down for further investigation

[9] "Regulatory productivity: Is there an answer to the rising cost of compliance?," Deloitte, May 23, 2022.
[10] "Regulator concerns about resilience and security could slow cloud adoption in financial services," Computer Weekly, September 23, 2021.

Summary

Choosing an SSE solution that's ready for anything

To remain competitive, financial services companies need to embrace digital tools that offer greater agility, productivity, and cost savings. But modern infrastructure requires modern security to keep the broader business safe from attack and exploitation.

Verifying an SSE vendor's ability to support the use cases of cloud risk management, data governance, and regulatory compliance is a great place to start. SSE will soon be recognized as the linchpin of SASE.

The SSE market is poised to gain a significant market share in the coming years. Identifying suitable vendors to meet the business needs of financial institutions will be highly influenced by the maturity of core services available within the SSE portfolio and level of integration across those services that allows vendors to offer comprehensive security capabilities from a single, cloud-native platform. By 2025, 80% of organizations seeking to procure SSE-related security services will purchase a consolidated SSE solution, rather than stand-alone cloud access security broker, secure web gateway and zero trust network access offerings, up from 15% in 2021.[11] For financial institutions that want to secure transactions at the edge while simplifying their security infrastructure, Netskope One offers a unified, cloud-native platform that helps you reduce risk, increase agility, and streamline operations. Securing applications, data, and users far beyond the network perimeter doesn't have to be costly or complicated—which is why Netskope One is both reliable and easy to use, helping you drive down costs and eliminate roadblocks to deliver protection wherever your people and data go.

[11] "Critical Capabilities for Security Service Edge," Gartner, February 16, 2022.

For More Information

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.