VIEW POINT

SECURING DIGITAL TRANSFORMATION IN THE FINANCE SECTOR

Abstract

Cloud computing has become increasingly popular in the financial sector due to its ability to reduce cost and improve operational efficiency. However, the use of cloud services also presents significant security risks, particularly for financial institutions that handle sensitive financial information. Cyber-attacks can cause significant financial and reputational damage to banks, insurance companies, and other financial services providers. This POV discusses the importance of securing resources on cloud and, users who are accessing those resources with the help of solutions available to mitigate these risks. It further shares modern methods to protect cloud infrastructure. These modern methods include features such as Network Security, Data Protection, Data Encryption, Cloud Security, Analytics, Incident Management and Access Control, that financial institutions can implement to strengthen their cybersecurity posture for cloud environment.

Infosys®
Navigate your next

Overview of current trends in Financial sector

Today financial organizations are remodeling traditional business models by adapting new technologies. Following are some of the current trends prevailing:

Digital Banking: Digital banking has become a major trend in the financial sector. Banks and financial institutions are investing heavily in technologies such as mobile banking, online banking, digital wallets, and digital payment systems to improve customer experience and increase operational efficiency.

Artificial Intelligence and Machine Learning: Financial institutions are utilizing Artificial Intelligence (AI) and Machine Learning (ML), to analyze various type of data sources to get accurate analytics in areas such as risk management, pattern detection, fraud detection, and customer service such as chatbots.

Blockchain: Blockchain technology is being increasingly adopted by the financial sector to improve security of data transactions, end user experience and cryptocurrency.

Cloud computing and banking APIs: Cloud computing has gained popularity across all the verticals and financial services is not exception to it. Financial sector has adopted services delivered from cloud resulting in improved productivity, smoother operations, products and services delivered swiftly. Integrating with the cloud allows banks to use banking APIs. These APIs facilitate data sharing and improve the overall customer experience.

Open Banking: Open Banking is a system that allows third-party payment services providers and other financial service providers to access banking transactions and other financial data through financial institutions. Open banking utilizes APIs to interact with banking applications. This system is gaining popularity as it enables customers to have more control and flexibility over their financial data and provides access to a wider range of financial services.

Financial Technology (FinTech): Companies provide software based mobile applications and other technologies to improve traditional way of doing business in finance sector such as mobile payment apps, crowdfunding, and digital wallets. Fintech companies are often able to provide services more efficiently and at a lower cost than traditional financial institutions.

Above trends are driving significant changes in the financial sector, with traditional financial institutions increasingly adopting digital technologies and new business models to remain competitive.

Objectives of Digital Transformation

Revive customer experience: The financial sector aims at providing frictionless experience to their customers.

Leverage analytics: AI and ML provide accurate analytics which helps financial organizations to compare services and combinations to be offered based on market trends.

Develop new business models: Financial services strive to rapidly serve growing client demands and provide support to client's problems and enhance customer experience.

Challenges

Complex threat landscape: The financial sector is constantly facing threats from more organized and sophisticated cyber-attacks. Financial sector faces wide range of cyber threats, including phishing, ransomware, Advanced Persistent Threats (APTs), and payment frauds. It becomes crucial for financial organizations to detect and prevent such threats before they converge into successful infiltration.

Lack of talent and skills in cybersecurity: Cybersecurity professionals are high in demand across all verticals. Financial institutions often struggle to find and retain qualified cybersecurity professionals. This shortage of talent makes it difficult for organizations to build and maintain the necessary cybersecurity practices, processes which are defined to prevent and detect cyber-attacks.

Outdated systems and infrastructure: Many financial institutions still use legacy systems and infrastructure that were not designed with cybersecurity in mind. Upgrading these systems to modern, secure technology can be a significant challenge, particularly for smaller financial institutions with limited resources. In cloud transformation there is a possibility that these legacy systems can run on containerized environment as well, but, that does not solve security relevant risks.

Compliance and regulatory requirements: Financial institutions are subject to a complex web of compliance and regulatory requirements, such as the Payment Card Industry Data Security Standard (PCI DSS), the General Data Protection Regulation (GDPR), and the Federal Financial Institutions Examination Council (FFIEC) guidelines. Adhering to these requirements can be difficult and resource-intensive, particularly for smaller financial institutions.

Balancing security and customer experience: Financial institutions must balance the need to protect sensitive customer data with the need to provide better services. This can be a challenge, particularly in areas like mobile banking, where customers expect a seamless experience while also demanding robust security.

Staying ahead of attackers: The financial sector is under constant attack from highly skilled and well-funded cyber criminals. It is more important for financial sector to invest in right technologies and services to stay ahead of various attackers.

Cyber threats

The finance sector is one of the most heavily targeted industries for cyber-attacks due to the high value of financial assets and sensitive data that it holds. Financial organizations typically store a wide variety of sensitive data, including:

- Customer account information, including name, address, and account details
- Transactional data, including information on deposits, withdrawals, and transfers
- Credit and debit card information, including card numbers, expiration dates, and CVV codes
- Personal identification information, including social security numbers, dates of birth, and other identifying information
- Financial performance data, including balance sheets, income statements, and cash flow statements

That's why financial institutions are a top target for cybercriminals due to the sensitivity of the financial information they possess, and the potential for financial gain. Cybercriminals may attempt to steal data, money, or other valuable assets from financial institutions. Some of the most common cybersecurity threats faced by the finance sector include:

Distributed Denial of Service (DDoS) attacks: Attackers flood a website or network with traffic, causing it to crash and preventing customers from accessing their accounts and services

Ransomware attacks: Malware can encrypt sensitive data and demand payment in exchange for the decryption key. In some cases, attackers may threaten to release the data publicly if the ransom is not paid.

Insider threats: Employees or contractors with access to sensitive data may intentionally or unintentionally cause harm to the financial institution, by stealing or leaking data, or inadvertently infecting the network with malware.

Advanced Persistent Threats (APTs): Sophisticated attackers use targeted attacks and multiple techniques to gain unauthorized access to a network, steal data, and maintain persistence in the system.

Third-party risks: Financial institutions often work with third-party vendors, which can introduce vulnerabilities into their systems if they have weak security controls.

Phishing and social engineering attacks: Attackers send emails or messages that appear to be from a reputable source, such as a bank or financial institution, and trick users into clicking on links or downloading malware, which can compromise their computers and financial accounts.

These threats derive upon the solution requirement to mitigate these threats. The following section covers such requirements.

Approach to modernizing cybersecurity

Financial organizations should consider investing in modern solution approaches to mitigate cybersecurity threats as traditional cybersecurity solutions for several reasons rely on complex systems and technologies such as big data, cloud computing. These technologies are complex due to system design, architecture and hence traditional security solutions won't be able to keep-up with evolving threat landscape.

Implementation of advanced threat detection and response measures: Financial institutions should deploy advanced cybersecurity technologies, which should have combination of next-generation firewalls, intrusion detection and prevention systems, Next-gen Security Information and Event Management (SIEM) which leverages deep learning and AI to analyze user behavior to detect and prevent sophisticated cyber-attacks.

Threat detection and response: Cloud security solutions for the finance sector must use advanced threat detection and prevention technologies to protect against cyber-attacks. This includes the use of AI & ML to detect and prevent sophisticated threats, protect against emerging threats and provide a comprehensive security posture.

Implementation of real-time threat detection and mitigation: Financial organizations must implement real-time threat detection and mitigation capabilities, which can help to identify and respond to threats quickly. This includes monitoring network traffic, analyzing application behavior, and detecting anomalies that may indicate a security breach.

Remote workforce security: The COVID-19 pandemic has accelerated the trend of remote work, which presents new security challenges for financial organizations. Modern solutions must provide solutions for users to be able to get secure remote access to corporate resources, secure access to internet, and with advanced threat detection and response capabilities.

Continuously monitor and improve: It is important for financial organizations to continuously monitor and improve cybersecurity posture. Keep cloud infrastructure updated with latest security patches, improve threat intelligence, conduct regular security assessments, and implement best practices for cybersecurity.

Maintain compliance: Financial organizations are subject to stringent regulatory requirements, such as PCI-DSS, GLBA, SWIFT and SOX etc. Organizations in financial sector must consider modern solutions which will provide visibility, interoperability, and control to ensure compliance with regulatory requirements.

Incident response planning: Financial sector must have incident response solution for cloud security to quickly respond to cybersecurity incidents. This should include regular testing and updates to ensure that the plan is effective.

To secure network and applications on cloud, solutions based on modern approach can bring significant benefits to the finance sector.

Infosys has identified these approaches in following five transformation themes

- Secure Access-as-a Service
- NextGen Network Security
- Secure Workplace-as-a-Service
- Secure Workload-as-a-Service
- Secure Cloud
- NextGen Protection Detection and Response

As per current cybersecurity trends above themes can be translated into approaches like Secure Access Service Edge (SASE), Extended Detection and Response (XDR), and Cloud Native Application Protection Platform (CNAPP) are to secure network and applications on cloud. SASE, CNAPP, and XDR are critical technologies for financial organizations to enhance their cybersecurity posture, support their cloud adoption journey, and protect against emerging threats. By investing in these technologies, organizations can strengthen their security defenses, reduce the risk of cyber-attacks, and maintain customer trust.

Benefits of modern approach

Comprehensive security: SASE, XDR, and CNAPP solutions provide comprehensive security capabilities, including identity and access management, network security, application security, and endpoint security. This can help financial institutions better protect their sensitive data against cyber threats.

Performance improvement: SASE provides secure and reliable connectivity for remote workers and branch offices based on the compliance requirements and CNAPP solutions can provide complete visibility of cloud infrastructure.

Simplified management: SASE, XDR, and CNAPP solutions provide a unified platform for managing network security, endpoint security, and application security, making it easier for IT administrators to manage security policies and configurations across the organization.

Reduced costs: SASE, XDR, and CNAPP solutions can help reduce costs associated with network and application security by consolidating multiple security functions into a single cloud-based platform, eliminating the need for multiple security solutions.

Flexibility: SASE, XDR, and CNAPP solutions provide flexibility in terms of deployment models, enabling financial institutions to choose the best approach that suits their specific requirements.

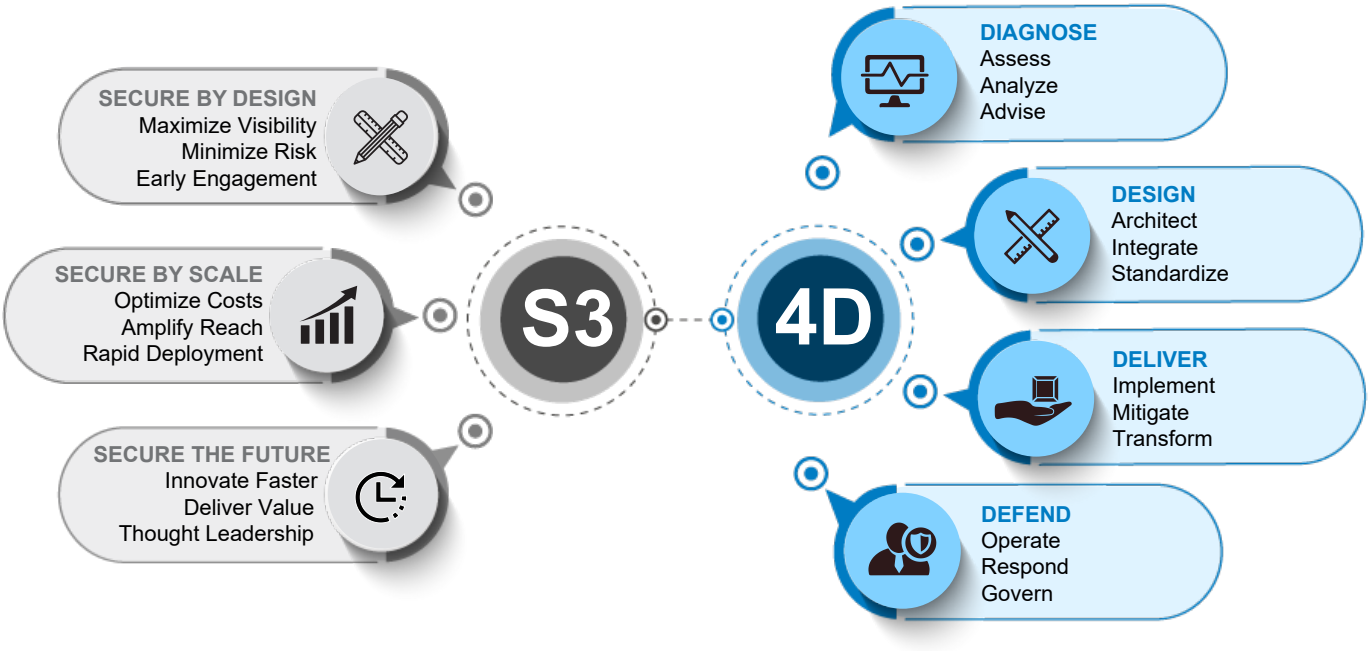
Why Infosys

Infosys CyberSecurity enables your business to scale with assurance. By driving an enterprise mindset towards secure by design at every stage of the business lifecycle, we minimize security risks while maximizing visibility of the security threat, impact & resolution. We also optimize cost and amplify reach while making you secure by scale, ensuring that our focus on innovating next-gen threat protection solutions in newer technologies will secure your business's future.

S3-4D approach and methodology

S3 : The S3 model is a set of guidelines or principles related to cybersecurity and IT services. The model emphasizes early engagement, maximizing visibility, minimizing risk, optimizing costs and amplifying reach to provide secure and efficient services to clients. The goal is to deliver value while also ensuring thought leadership.

4D: The 4D model is a set of principles intended to bring standardization to project delivery. The model emphasizes diagnosing the current security posture and coming up with a set of recommendations to be implemented as part of project completion. The solution will be designed and delivered based on reusable artefacts and templates leveraging the best practices from past projects. The security monitoring and response activities are clubbed together under defend, which is primarily executed from our CDCs. The goal is to provide comprehensive solutions that help in improving the security posture and help defend against potential threats.



Author

Shashank Salaskar

Principal Consultant

Shashank is a cybersecurity expert bringing over 22 years of experience in multiple roles such as consulting, pre-sales, and post-sales. With an intense understanding of the ever-evolving cyber threat landscape, Shashank has established himself as a trusted advisor in the field of cybersecurity. Having worked in diverse consulting roles, Shashank has collaborated with numerous clients across various industries, enabling them by find effective solutions for the complex challenges within cybersecurity.

For more information, contact askus@infosys.com

Navigate your next