VIEW POINT

ZERO TRUST SECURITY: A KEY IMPERATIVE FOR FINANCIAL SERVICES COMPANIES

Abstract

Financial institutions are in a race to embrace cloud technology to not just keep pace with FinTech firms but also cater to the growing demand for digital banking experiences. This fast-paced shift to cloud solutions can result in added complexity, operational burdens, and an urgent need for specialized talent and skills. This path is all the more challenging since it involves securing and managing both cloud and traditional infrastructure.

In this backdrop, banking and financial services firms are embracing the Zero Trust model for cybersecurity. This is a strategy based on the fundamental principle, "verify everything, trust nothing". This is critical in today's threat landscape where cloud computing, remote work, and interconnected devices are expanding and blurring network boundaries.

This paper discusses the need for Zero Trust security for the financial services industry, the core pillars of Zero Trust, and best practices for implementing a robust Zero Trust framework.

Infosys®
Navigate your next

Introduction

The financial services industry has reached a turning point with a significant number of users and applications located outside conventional boundaries. With a blended workforce becoming the norm, companies must be able to offer access from anywhere while maintaining exceptional user experience. The shift towards cloud-based application delivery, whether public or private, has allowed development teams to achieve faster results. However, this new way of delivering and consuming applications has also led to a rise in instances of implied trust, creating a wider attack surface, and making it easier for hackers to infiltrate systems. The increasing interconnectedness of infrastructure, both within and outside organizations, only exacerbates this problem.

With the rise of the Internet of Things (IoT), physical locations are becoming more reliant on connected devices, which often have more access than necessary and are therefore vulnerable to exploitation. Traditional IT security measures such as patching and maintenance are no longer enough to protect against these new threats.

Financial services companies continue to be a prime target for cyber criminals.

Since the emergence of the cyber era and the widespread use of the internet, this statement has consistently remained relevant in their yearly coverage. Given the large amount of money involved in transactions and the confidential nature of the information handled by financial organizations, it is no surprise that the world of finance is the prime target for cyber criminals. Considering this, it is crucial to implement innovative approaches focused on identity-based security and Zero Trust models that leave no risk unaddressed.

Cybersecurity Measures for Financial Services Companies

Financial institutions are aware of the significance of cybersecurity and have highly-skilled cybersecurity personnel closely monitoring their IT security operations. According to the Financial Services Sector Coordinating Council (FSSCC), chief information security officers (CISOs) from financial organizations reported that approximately 40% of their own as well as their team's time was taken up in reconciling various cybersecurity and regulatory frameworks. Despite having state-of-the-art banking cybersecurity systems and well-established procedures, these companies continue to be outsmarted by cybercriminals.

The security issues and solutions for financial services companies are similar to those needed by other online or Internet-based companies that handle personal information. Employees need the ability to work on their preferred devices in locations for maximum effectiveness and productivity, without concerns about security issues, diversity of device form factors, or access methods for different networks.

However, there is significantly high monetary value of the data that the financial industry processes on a daily basis. For this reason, financial services firms need to take a Zero Trust approach towards their internal infrastructure. Some of the basic security solutions include continuous and dynamic monitoring for threats from both internal and external sources. Traditional security measures include:

- Antivirus and anti-malware software
- Hardware and software firewalls
- Dynamic employee awareness training
- Vulnerability and threat scanning
- Penetration testing

Zero Trust Principles

A Zero Trust environment is established based on a few core pillars. These principles are:

Never trust, always verify

To ensure the protection of sensitive information, it is crucial that the system consistently and continuously validates the identities, devices, locations, and other relevant data of users and services before granting them access. Access should only be granted for a limited time using ephemeral tokens, sessions, and connections. Users and services must re-establish their identity on a regular basis to maintain access.

Continuous monitoring and observability

By maintaining constant surveillance and visibility, you can stay informed in real-time about who is attempting to access what resources, and how those access attempts are being evaluated. This allows for prompt identification of potential threats, unusual activity, and ongoing security incidents, enabling a rapid response and minimizing the impact of any potential security breaches.

Least privileges

Limiting access to just the essential resources is a vital aspect of the Zero Trust approach. It is important to understand precisely what resources are required by which users as well as the purpose of accessing these resources in order to prevent unauthorized access. This concept is central to the principle of microsegmentation.

Microsegmentation

To minimize the impact of a security breach, it is recommended to divide your data as a service (DAAS) into smaller, more specific segments within the network. These separate segments have their own distinct set of users, responsibilities, and access policies. These are regularly assessed to prevent malicious actors from operating within the network.

Zero Trust Enterprise Framework

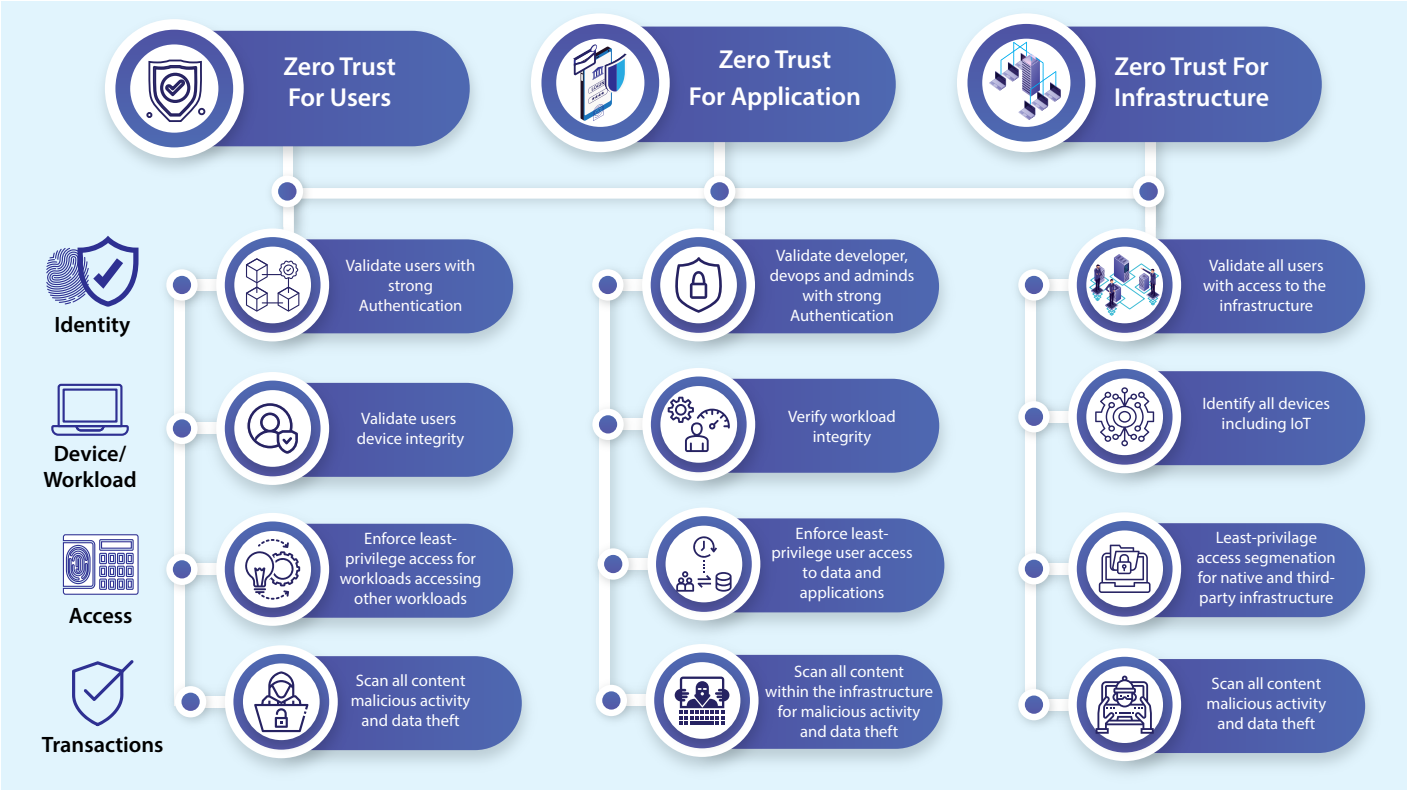

Figure 1 – Zero Trust Enterprise Framework

Zero Trust is a comprehensive approach that eliminates implicit trust within an organization, which includes users, applications, and infrastructure:

- For users, the first step in implementing Zero Trust is to have a strong authentication process to verify user identity, application of least-access policies, and device integrity verification.
- For applications, applying Zero Trust removes implicit trust between different application components and requires continuous monitoring of their behavior during runtime.
- For infrastructure, everything from routers, switches, cloud systems, IoT devices, and the entire supply chain, must be addressed with a Zero Trust approach to eliminate any implicit trust.

Zero Trust Architecture

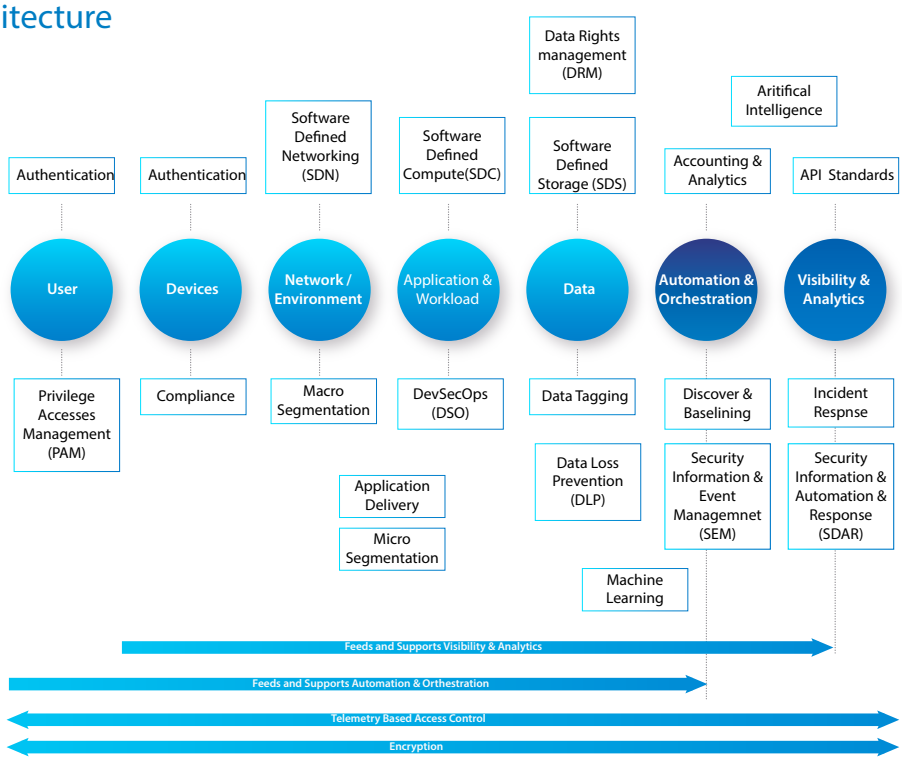

Figure 2 – Zero Trust Architecture

Zero Trust architecture can help governments and other agencies adopt a more data and user-centric approach, rather than focusing solely on perimeter security. By integrating data loss prevention (DLP) with behavioral analytics, agencies can establish adaptive data policies, gain behavioral insights, and improve data discovery and classification.

A behavior-based cybersecurity strategy can also adapt to changing levels of risk, providing enterprise-wide visibility into network, endpoint, and cloud activities. Risk scores can change depending on user behavior, allowing targeted policies to be tightened or actions to be blocked if necessary. By analyzing behavior in context, security teams can better distinguish between innocent and suspicious actions, reducing false positives and leveraging intelligent data security to revisit decisions as new information is gathered and analyzed.

To effectively implement Zero Trust architecture, organizations must incorporate user identification, behavioral analysis, attack surface mitigation, and data management to continuously and adaptively improve their security posture. These components are crucial to achieving the Biden administration's goal of "identifying, deterring, protecting, and responding" to cyber threats.

Best Practices for Zero Trust Security Implementation

Before implementing Zero Trust security, it is vital to take a step back, evaluate best practices, and define a clear strategy for a flawless Zero Trust rollout.

- Limit the impact of potential security incidents by implementing network segmentation and microsegmentation. Begin by establishing a baseline understanding of your environment through telemetry and analytics to increase visibility. Take a phased approach, starting with coarse-grained network segmentation such as separating production and non-production environments, and gradually moving to more specific application ring-fencing.
- Implement a "least privilege" approach to access control, ensuring that each identity such as employees, service accounts, customers, and third parties have access only to the resources they need to perform their specific tasks. Centralize decision-making for access control and continuously monitor user and device behavior to detect any anomalies. This will help reduce static access and promote the use of dynamic just-in-time access, which allows for greater control in the event of a breach.
- Ensure that robust security measures are in place prior to moving any workloads to the cloud. Ensure a smooth transition by aligning the technology stack across both cloud and traditional environments, automating processes wherever possible, and securing privileged accounts. Additionally, take steps to protect data, both when it is stored and in transit, and address any cloud configuration concerns forthwith.
- The integration or divestiture of entities through mergers and acquisitions (M&As) can make the environment more challenging in terms of complexity. To address this, modern solutions such as software defined perimeter (SDP) or secure access service edge (SASE) can be utilized to provide secure network access to enterprise resources in accordance with Zero Trust principles, while ensuring the implementation of broad and consistent cybersecurity controls.
- Improve your understanding of where your data is located, its importance, how to secure it, and who should have access to it by enhancing your data inventory, classification, and governance abilities. This can assist you in meeting data privacy and sovereignty regulations while improving your overall data security posture.

Implementing Zero Trust Security for Cloud-based Applications and Data

Zero Trust security is not a one-time activity. Businesses must continuously monitor their network and maintain observability, enabling them to detect potential threats in real time and respond quickly to any security incidents. Implement least privilege access control to ensure that each identity has access to only those resources that they need to perform their specific tasks. Centralized decision-making for access control improves visibility and reduces the risk of errors. In addition, several other measures need to be in place to implement Zero Trust for cloud-based applications.

- Identify the types of applications and data your company uses, as well as the level of sensitivity for each. Determine which assets are most critical to your business and create a "protect surface" to safeguard these resources.
- Map out how transactions flow within your applications, including which users and systems have access to specific data and services.
- Use this information to architect a new cloud infrastructure that clearly defines boundaries between users and applications, limiting access to sensitive data as much as possible.
- Develop and enforce Zero Trust policies that are based on the principles of least privilege, ensuring that only those who need access to a given resource are allowed to use it. Educate all users on your security policies and standards.
- Continuously monitor your environment for any unusual activity using logging and analysis tools to identify and respond to potential threats.
- Regularly review your Zero Trust policies and make adjustments as needed to stay ahead of evolving threats.

Benefits of Zero Trust Security

Financial institutions can reap multiple benefits when they strategize and successfully execute a robust Zero Trust security policy.
These include:

- Improved threat detection and mitigation through continuous monitoring and verification of user and device identity
- Limitation of attack surfaces by enforcing least privilege access and dynamically controlling user access
- Enhanced security for remote workforces and third-party access to resources
- Protection of sensitive data by reducing the attack surface and limiting data exposure
- Simplification of security operations through harmonized security controls across hybrid and multi-cloud environments
- Better alignment with regulatory requirements for data sovereignty and privacy protection

Overall, when financial institutions adopt a Zero Trust approach to security, they can improve their security posture and reduce their risk of cyber-attacks. By focusing on data and user-centric security, they can better protect their customers' sensitive information and enhance their reputation as a trustworthy financial institution.

Conclusion

In addition to being a critical imperative, implementing a Zero Trust security model can bring numerous benefits to financial organizations, including better security outcomes, a simplified infrastructure, and reduced operational costs. By continuously validating every stage of a digital interaction and relying on a single control deployed across the entire organization, Zero Trust can help reduce risk, complexity, and costs while enhancing overall security and resilience. With the ever-evolving threat landscape and the increasing need for digital transformation, it is crucial for financial services firms to adopt a Zero Trust approach to ensure the protection of their assets, data, and users. By laying down a clear strategy and following certain best practices, it is possible to define and implement a Zero Trust security model that is robust, cost-efficient, and resilient against cyberattacks.

About the Authors

Ravindra Vijaykumar Sali

Technology Architect, FSSTAR, Infosys

Ravindra Sali has worked across domains such as financial services, including mortgages and open banking platforms, life sciences and healthcare, and telecommunications. He is well-versed with technologies such as microservices, SpringBoot, WSO2 APIM, Keycloak, Spring-Cloud, OpenAPI/Swagger, MySQL, OAuth-OIDC, Apache Kafka, Apache Camel, Camunda, and Neo4j Browser.

https://www.linkedin.com/in/ravindra-sali/

Ravikiran Perumalla

Principle Technology Architect, Banking and Financial Services, Infosys

RaviKiran Perumalla has worked in the retail banking and open banking implementation domains. He is an open source enthusiast involved in technical architecture design. He works with global clients in the areas of open banking and FinTech integrations in the digital banking ecosystem.

https://www.linkedin.com/in/rperumalla/

References

- Zero Trust with Zero Exception
- Cyber Security for Fintech Enterprises
- Zero Trust in Banking and Financial Services
- Zero Trust Pillars and Capabilities
- Zero Trust Strategy

Glossary

- IoT – The Internet of Things
- CISO- Chief Information Security Officer
- DAAS – Data as a service

For more information, contact askus@infosys.com

Infosys®
Navigate your next