# Securing Financial Institutions with Zero Trust Security

## How to Get Started with Your Zero Trust Journey

# INTRODUCTION

The Financial Services Industry is witnessing a major shift in the way they operate. With rapid digitization, disruptive technologies are dictating how Financial Institutions function. However, with the increasing dependency on digital tools to improve efficiency, financial institutions need to have a relook at their cybersecurity posture, which has become obsolete and flawed in the context of the present security challenges.

As the frequency of data breaches becomes more pronounced, it is apparent that financial institutions remain the preferred target for these attacks, witnessing an average of 65% more attacks than any other sector.

In this scenario, relying on a standardized security setup, which in turn depends on a trust-based model, goes on to increase the number of security risks that an organization could face. Coupled with the heavy scrutiny that financial enterprises face from regulators, and their mandatory adherence to a variety of compliance requirements like HIPPA and GDPR, most financial institutions are inadequately placed to face modern-day security challenges. In this scenario, a shift to more disruptive security models becomes the need of the hour.

# SECURITY RISKS AND CHALLENGES ASSOCIATED WITH INCREASING INTERCONNECTIVITY

***1. Increased Interconnectivity*** - As digitization becomes the buzzword associated with every financial sector, financial institutions become more and more interconnected with their partners, customers, banking systems, and other institutions. This inherently increases the security risks associated with the newfound interconnectivity, since there is greater scope for hackers and malicious actors to move laterally through systems and exploit critical goldmines of financial data.

***2. Regulatory Compliance*** - The regulatory implementation process and security setup system are not able to keep pace with the increasing number of novel and new threats that crop up every day. Although security systems have to adhere to various compliance requirements regarding data protection, it may take a long time for regulatory bodies to comprehend new threats and update their guidelines. In this scenario, financial institutions that have a security strategy which is dictated by compliance are prone to be successfully breached

***3. Managing Network Access and Remote Users*** - Financial Institutions migrating their data and critical applications to the cloud must be aware that each of their cloud assets may be potentially compromised. At the same time, analysts and remote users need to have secure access to this critical data without putting the security infrastructure at risk.

***4. Rigid Security Perimeter*** - Financial Institutions often choose to adhere to old conceptions of security, choosing to place a single perimeter around their network. This doesn't hold good when applications and data migrate to the cloud, and when this critical data is accessed by users all over the world. Critical data sets require a more specific set of security setups and policies built around them. With network complexity increasing by the day, traditional security setups won't hold good.

# WHAT IS ZERO TRUST?

A Zero trust Security Model cannot be divined to be just a single network architecture but is rather a set of guiding principles in terms of both network design and network operation, that dramatically revamps the security infrastructure of an organization, while at the same time, increasing visibility and the scope for analytics across the network. These include the following guiding principles:

- Distinctions between “inside” and “outside” the network perimeters no longer stand true. Network locality can’t be a lone factor in determining trust.
- Malicious threats exist on the network at all times, and may be internal or external in nature
- Every user, device, network, and data, is to be validated and authenticated before granting access
- Zero Trust Policies are to be dynamic in nature, taking into account multiple sources of data, and continuous monitoring of data is to be done for garnering new insights regarding any new vulnerabilities that may crop up
- A Zero Trust Security Architecture uses micro-segmentation, effectively creating isolated secure data zones/segments, allowing organizations to have a granular level access control, and define security policies for each critical segment

*BOX* - **Financial Institutions often have specific security needs**

- These institutions possess extremely sensitive data in secure facilities
- A majority of financial institutions are often continuously under attack from hackers and other malicious actors
- A number of critical applications need to have specific role-based access and security policies designed for them
- The security team requires an audit-ready security posture that adheres to multiple compliance requirements
- Complete visibility and monitoring of traffic flow across the network infrastructure, and especially the movement of critical data within the network is also an urgent requirement

# WHAT DOES ZERO TRUST SECURITY ENCOMPASS?

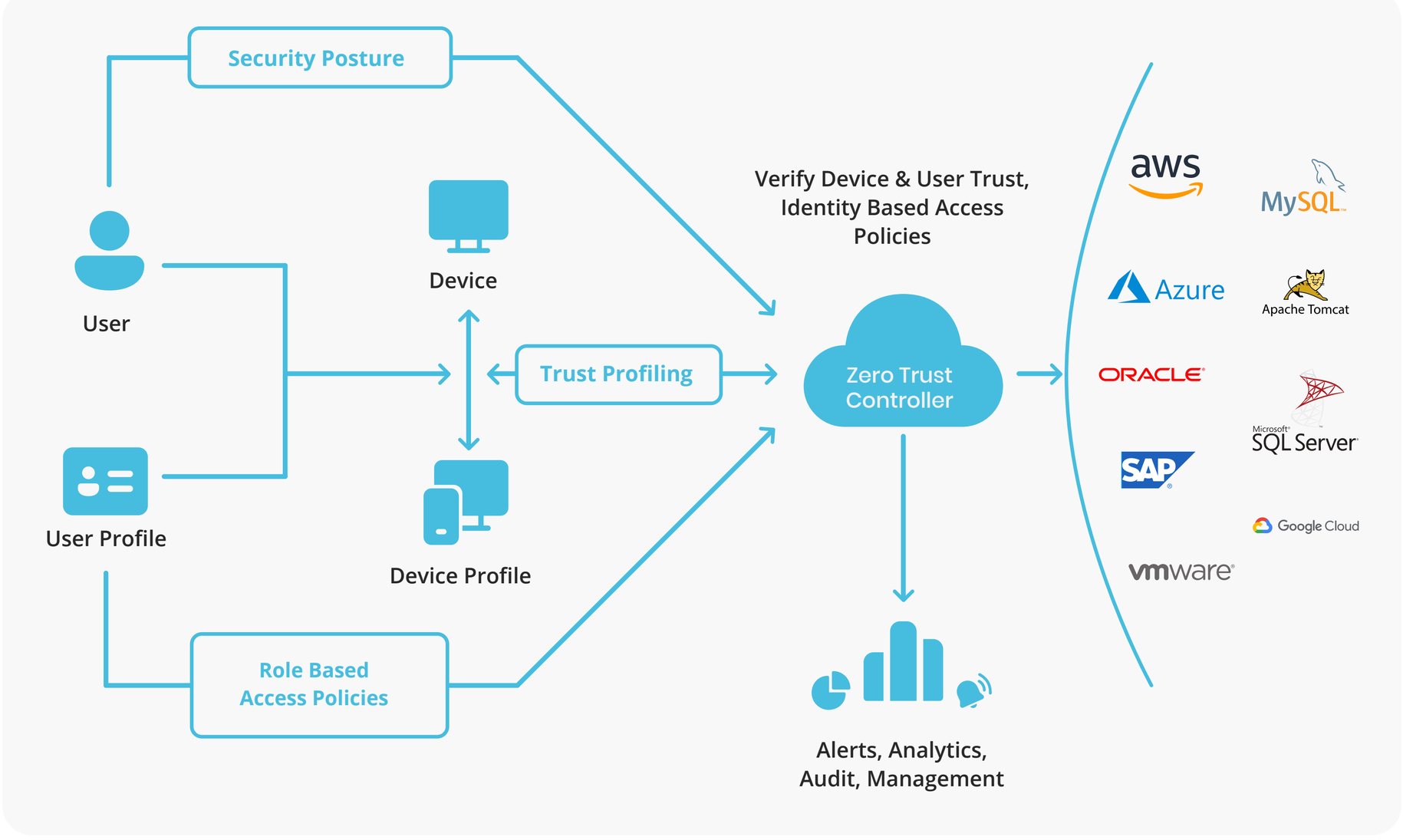
A Zero Trust Security Model depends on a number of components to ensure stringent security:

*1. Identity centric security:* The identity of a user grants him access to the applications that he is allowed to use. This means that the identity, and not the device or the job function of the user, unlocks the information. Authentication needs to be done by multifaceted security protocols, which include multifactor authentication and behavioral biometrics-based authentication

*2. Application-Centric Security:* Users, once authenticated, are not given unfettered access to the complete network, which usually happens in traditional security setups. Instead, users are only given access to those applications and data that they are allowed to see. This segmented access, based on the need to know model, is made possible through application-specific tunneling. Using this, the entire network is hidden from users, except specific applications that they have access to. This holds for customers, employees, and 3rd party contractors. Thus, a high ranking bank employee may have access to, say 10 critical applications of high sensitivity, while a contractor may have access to 5 applications of low sensitivity

*3. Microsegmentation:* The simplest defense in the event of an attempted breach is that once the breach is identified, it should be stopped right away, by restricting its movement within the network. Besides, security controls are to be developed in such a manner that the attack surface that may be open to exploitation is minimized. Using micro-segmentation, secure data zones are created which isolate data centers, cloud deployments, and applications with micro perimeters around them.

*4. Threat Monitoring and Behavioural Analytics:* Continuous monitoring and visibility into the entire network for immediate detection and response to abnormal activities and other threat vectors is a defining feature of Zero Trust Models. A Zero Trust Security Model allows for cross-environment visibility, enabling complete visibility into the network, and easy detection of potential threats




# SECURE CRITICAL FINANCIAL DATA WITH INSTASAFE ZERO TRUST ACCESS

**1. Security Benefits:**

- Continuous and Instant Monitoring and Visibility of the entire network
- Reduced Attack Surface by separation of data and access control planes
- Microsegmentation of data and workloads to prevent lateral movement attacks
- Segmenting and isolating Critical infrastructure (e.g. - SWIFT applications) from the rest of the infrastructure. Designing role-based access policies centered around access to these apps
- Allows control of all connections based on pre-vetting of who can connect; from which devices; and to what services, infrastructure, and other parameters
- Continuous data identification and classification
- Behavioral biometric-based authentication and Adaptive Multifactor Authentication for better security based on the identity of the user
- Application logging and identity logging visibility, along with network layer visibity
- Easy classification of users to implement role-based access policies
- Access based on ‘need to know’ model

**2. Business Benefits:**

- Better Business Agility and Innovation
- Easy transition from on-premise to remote workforce based business model
- Easy outsourcing of non-core business functions to 3rd party contractors
- Audit ready compliance adherence through complete network visibility
- Cloud-based solution; Easy deployment and scalability across multiple locations
- Increased IT operational agility
- Compliance data collection, reporting, and auditing processes can be improved by using Zero Trust Security Models
- Empowering digital transformation by enabling companies to securely adopt cloud architectures

# GETTING STARTED WITH ZERO TRUST SECURITY

***1. Audit Security Posture:*** Analyse whether your organization has a relevant and pragmatic Identity, Credentials, and Access Management strategy, which is in synchronization with the business needs of the organization. Review whether or not all of our resources are being accessed securely.

***2. Inventory connected devices:*** Update your asset inventory, to log all managed as well as unmanaged devices that have had access to your critical assets. Design a policy designed to urge all device users to update their devices in line with current security requirements

***3. Classify, Identify, Catalogue:*** To garner a granular view of what occurs in the network, it is of paramount importance that enterprises classify, identify, and catalog all traffic without distinction based on encryption or hopping. This step serves to stress on the “verify before you trust” tenet that Zero Trust Network Access adheres to

***4. Create Zero Trust Architecture and Policy:*** While it is conventional for network design to have the creation of its architecture as the first step of its design, it must be understood that zero trusts are not a universal design, but highly customized, depending on the organization adopting it. Further, given that it is improbable for an organization to undergo migration to a ZTNA network in a single technology refresh cycle, it is necessary to perform the aforementioned surveying steps to ensure a successful deployment. The entire Zero Trust Policy may be designed using Ohno’s ‘Why?’ method

***5. Continuous Monitoring, Continuous Improvement (Kaizen-ize):*** Perform a deep dive analysis of all incoming and outgoing traffic, to garner new insights for improvement.

# WHERE ARE YOU ON YOUR ZERO TRUST JOURNEY?

According to Gartner by 2022, 80% of new digital business applications opened up to ecosystem partners will be accessed through zero trust network access (ZTNA), and by 2023 60% of enterprises will phase out their remote access virtual private networks (VPN) in favor of ZTNA.

When it is up to you to choose a security solution that protects your cloud environment effectively, you should know more about how a Zero Trust Solution provider like InstaSafe can help you secure your enterprise assets with ease.

With InstaSafe’ Zero Trust Application Access solution, you get a cloud-delivered Security-as-a-Service, which not only provides cost-efficient access control and secure remote connectivity capabilities, but also integrate seamlessly with all major cloud providers to give an enhanced, and secure user experience.

With a scalable on-demand cloud configuration and zero hardware requirements, InstaSafe Zero Trust Application Access helps in securing your cloud environments, extending secure access of enterprise applications to remote workforces situated anywhere across the world

# ABOUT INSTASAFE

InstaSafe's mission is to secure enterprises from the abuse of excessive trust and privilege access. We empower organizations across to globe in preparing their security infrastructure for digital transformation in a cloud-dominated world. Recognised by Gartner as one of the top representative vendors providing Zero Trust Security, InstaSafe Secure Access and InstaSafe Zero Trust Application Access follow the vision that trust can never be an entitlement, to offer securely enhanced and rapid access of enterprise applications to users situated anywhere across the globe. We secure 500,000 endpoints for more than 150 customers, spread across 5 continents, with our 100% cloud-delivered solutions, ensuring that our offerings are in line with our mission of being Cloud, Secure, and Instant.

# CONTACT US


**InstaSafe Inc,**
340 S Lemon Ave #1364
Walnut,
CA 91789,
United States
+1(408)400-3673

**InstaSafe,**
Global Incubation Services,
CA Site No.1, Behind Hotel Leela Palace
Kempinski,
HAL 3rd Stage, Kodihalli, Bengaluru – 560008

/InstaSafe
/instasafe_diaries
/InstaSafe
/company/instasafe