



Cybersecurity for Financial Services

Embrace Digital Transformation and Protect
Sensitive Data in the Age of AI with Zero Trust

FROST & SULLIVAN EXECUTIVE BRIEF

The contents of these pages are copyright © Frost & Sullivan. All rights reserved.

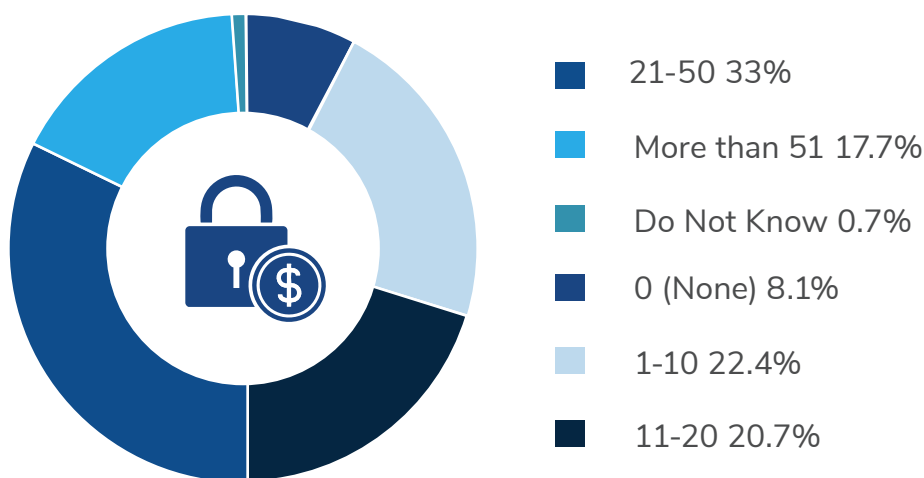
[frost.com](https://www.frost.com)



Improve Security Posture, Achieve Compliance, and Increase Resiliency

Financial services organizations are undergoing a profound digital transformation, leveraging mobile technologies, cloud platforms, and automation to improve operational efficiency, meet customer expectations, and unlock new revenue streams. As services like mortgage applications, payment processing, and fund transfers shift to online and mobile platforms, financial institutions gain unprecedented opportunities but also face heightened cyber risks.

Over the past 12 months, more than one-third of financial services organizations reported between 21 and 50 successful cyberattacks—demonstrating how evolving threats are testing the limits of traditional solutions and leaving sensitive data, operations, and customer trust vulnerable.



Frost & Sullivan. (2024, March 12). Voice of Customer Global Banking and Financial Services Security Trends





At the heart of this transformation is artificial intelligence (AI), which is revolutionizing BFSI operations and driving efficiency. However, adversaries are weaponizing AI to escalate risks through automated phishing, generative attack modeling, and advanced vulnerability identification. Simultaneously, financial institutions must grapple with safely leveraging AI while mitigating risks such as sensitive data leakage through generative AI tools or manipulation by adversarial actors.

These emerging threats, coupled with the complexity of regulatory landscapes, demand modern, adaptive, and intelligent security strategies that can safeguard sensitive information, ensure compliance, reduce costs, and preserve customer trust. Zero Trust principles, reinforced by AI-driven protections, offer a fundamental solution to address the operational, structural, and regulatory challenges faced by the financial services sector.

Modernize BFSI Security: Overcome Legacy Limitations for Digital

Transformation and Compliance

Many BFSI organizations continue to struggle with legacy systems and insufficient security approaches that fail to meet the demands of a modern, hybrid workforce. According to a recent Frost & Sullivan survey of chief information security officers (CISOs) in the BFSI industry, more than 30% of respondents admitted their systems are outdated, creating significant challenges:

01 On-Premises Infrastructure is Complex and Inflexible

Legacy solutions, such as VPNs and firewalls, were designed for static, on-premises work environments and are ill-suited for today's hybrid workforce. More than 40% of CISOs reported visibility gaps in their security setups, stemming from architectures that backhaul traffic through centralized data centers. This results in significant latency, reduced productivity, and inefficiencies.

Hybrid work environments, where employees, partners, and customers access resources from diverse locations and devices, further strain legacy systems, which cannot provide seamless connectivity. These tools are also inadequate against modern threats, such as AI-driven attacks, which exploit vulnerabilities at a faster pace than traditional defenses can respond.

Maintaining legacy systems increases costs and operational complexity. Aging technologies like virtual desktop infrastructure (VDI) can be up to five to ten times more expensive than modern solutions, limiting scalability and creating a persistent management burden.



02 Blind Spots Threaten Regulatory Compliance

Compliance with industry frameworks such as SOX, PCI DSS, and GLBA remains a priority for BFSI organizations, but frequent updates to regulatory mandates introduce complexities. Legacy systems often rely on disconnected tools, creating blind spots that weaken visibility and delay the identification of compliance risks.

This lack of real-time oversight exposes organizations to improper use of sensitive customer data, breaches, and compliance violations, all of which can erode stakeholder and customer trust. The adoption of AI further complicates adherence as institutions face additional risks, such as inadvertent data leakage through unsanctioned AI tools or errors stemming from unmonitored outputs. Legacy tools are ill-equipped to manage these regulatory expectations, particularly when it comes to securing and governing AI interactions.

03 Hybrid Cloud Architectures Require Purpose-Built Security

As BFSI organizations increasingly adopt hybrid cloud environments using AWS, Azure, or Google Cloud, traditional “lift and shift” strategies—migrating legacy systems to the cloud without redesigning security frameworks—introduce vulnerabilities. Tools like VPNs and firewalls expand the attack surface by exposing applications through public IP addresses, making them susceptible to AI-enabled recon operations and lateral attacker movement. Spinning up virtual VPNs and firewalls in the cloud doesn’t change those issues. Fundamentally that architecture is no longer fit for purpose.

Legacy systems struggle to adapt to the dynamic nature of hybrid cloud workflows, where greater user mobility and AI integration widen security gaps and demand constant monitoring. Institutions relying on outdated architectures find themselves constrained by misaligned security frameworks, leading to vulnerabilities and operational inefficiencies.





Embrace a Modern Cybersecurity Approach with Zero Trust: The Foundation for BFSI Resilience

A Zero Trust security model offers BFSI organizations a resilient approach to secure hybrid environments, address AI-generated risks, and improve compliance outcomes. By replacing the outdated “trust but verify” paradigm with “never trust, always verify,” Zero Trust continuously authenticates every request based on identity and context—whether from users, devices, networks, or AI services.

Enhanced Visibility

BFSI organizations highlight visibility gaps as a top challenge—more than 40% of CISOs surveyed by Frost & Sullivan noted these gaps impede effective security implementation. Zero Trust remedies this by providing continuous monitoring and real-time oversight of all activities across hybrid environments, including interactions with generative AI tools. Audit trails ensure accountability, while AI-driven insights expose malicious behaviors like encrypted traffic misuse and risky unsanctioned apps.

Simplified Compliance

Zero Trust simplifies adherence to regulatory frameworks such as GDPR, PCI DSS, and GLBA by automating reporting, enforcing centralized security policies, and monitoring AI-generated outputs. AI-driven classification of sensitive data and anomaly detection enhances compliance capabilities, reducing human error and ensuring secure workflows that align with industry mandates.

Cost Efficiency and Scalability

Migrating from legacy tools like VPNs, firewalls and VDIs to Zero Trust-based, identity-driven architectures streamlines costs and operational complexity. Organizations benefit from scalability, seamless user access, and secure integration, even for third-party contractors, while enhancing user experience—critical for hybrid and AI-driven environments.





Seven Elements of a Highly Successful zero trust Architecture

A robust zero trust architecture, built on the principle of least-privilege access, is essential for addressing the challenges of the BFSI sector. This approach incorporates seven key elements:



VERIFY

Who is connecting?
What is the context of the connection?
Where is the connection going?



CONTROL

Assess risk using context.
Prevent compromise.
Prevent data loss.



ENFORCE

Enforce policies continuously and everywhere.

Adhering to these principles ensures BFSI organizations benefit from better security, operational efficiency, and optimized compliance. AI integration provides additional contextual depth, enabling organizations to detect nuanced threats—like AI-generated social engineering or encrypted traffic misuse—across their ecosystems.





Zero Trust Architecture securely connects users, workloads, and devices only to the apps they are authorized to access—over any network from any location—without putting either the initiator or destination app on a routable network where it can be discovered and exploited. Zero Trust enables important capabilities:



Verify Identity: Authenticate the identity of the user, device, IOT/OT, or workload through third-party identity providers.



Validates Attributes: Check for specific attributes like role, location, and access context to establish the credibility of the request.



Certify Destination: Confirm the verified entity has the rights to access the requested application or resource, ensuring strict segmentation



Assess Risk: Calculate a real-time risk score for each connection based on device posture, behavior, and destination context.



Prevent Compromise: Decrypt and inspect traffic content to block any identified malware or threats within entity-to-resource communication.



Prevent Data Loss: Scan traffic to identify sensitive data and prevent unauthorized exfiltration, using decryption and deep inspection.



Enforce Policy: Enforce per session, dynamic policies to conditionally allow or block access based on verified identity, context, and risk analysis.





What to Look for in a BFSI Cybersecurity Partner

Choosing the right cybersecurity partner is critical for BFSI organizations to successfully implement a Zero Trust architecture that addresses security, compliance, and operational challenges. The ideal partner should demonstrate deep expertise in the BFSI sector, offer solutions purpose-built for hybrid environments, and enable scalable, efficient operations without requiring disruptive changes to existing infrastructure. Additionally, the partner must provide advanced threat intelligence capabilities, robust data protection, and seamless compliance support to meet evolving regulatory demands.

Key characteristics to look for in a cybersecurity partner include:

Proven BFSI Expertise

- ▶ Advanced understanding of the BFSI sector, including unique regulatory and operational needs
- ▶ Strong track record of success with large-scale BFSI customers
- ▶ Leadership in Secure Service Edge (SSE) deployment for financial organizations

Cloud-Native Platform

- ▶ Integrated, purpose-built architecture designed for scalability and flexibility
- ▶ Avoids “lift and shift” solutions and integrates seamlessly with hybrid environments (AWS, Azure, Google Cloud)
- ▶ Comprehensive authentication of identity across environments
- ▶ Industry-leading zero trust approach aligned with NIST 800-207 requirements
- ▶ Globally distributed infrastructure to ensure consistent performance and availability
- ▶ AI enhances authentication, enforces real-time adaptive policies, and mitigates misconfigurations, ensuring secure, seamless hybrid cloud operations



Comprehensive Visibility and Control

- ▶ Real-time monitoring and elimination of blind spots across all environments
- ▶ Zero Trust enforcement across all data locations
- ▶ Protection for data in motion, at rest, SaaS applications, endpoints, and public clouds
- ▶ Full support for BYOD and contract employee security requirements
- ▶ AI-driven analytics detect threats at scale by identifying anomalous behaviors across diverse environments

Architecture Focused on BFSI Innovation

- ▶ Robust integrations with BFSI-specific business, IT, and security tools to support modern digital transformation
- ▶ Cloud- and Zero Trust-centric network design
- ▶ Scalable solutions across geographies, with compatibility for both cloud and on-premises infrastructure, minimizing complexity
- ▶ Comprehensive security controls aligned with the MITRE ATT&CK framework
- ▶ Rapid response to changing regulatory landscapes, including support for data and content sovereignty laws

Advanced Threat Intelligence

- ▶ Multi-tenancy model enabling effective threat information sharing across organizations
- ▶ Advanced protection against zero-day attacks
- ▶ Deep visibility with automated policy creation for proactive risk reduction
- ▶ Find once, block for all” threat intelligence capabilities
- ▶ AI-powered threat detection to address emerging risks, including generative AI misuse

By choosing a partner with these capabilities, BFSI institutions can confidently secure their environments, streamline operations, and adapt to the constantly evolving threat and regulatory landscape.



Case study: How Verisk Leveraged zero trust to Enhance Security, Streamline Compliance, and Drive Operational Efficiency¹

Verisk, a global predictive analytics and decision-support firm, embarked on a cloud transformation journey that included adopting a zero-trust security approach. To support this initiative and gain better insights into application performance, Verisk implemented Zscaler solutions, creating a comprehensive zero trust environment for its workforce of approximately 9,000 employees, both in-office and remote. The deployment of Zscaler solutions provided Verisk with unified, centralized visibility into user experience, enabling faster issue resolution. This holistic zero trust model, coupled with Zscaler’s AI-driven analysis capabilities, not only enhanced Verisk’s security posture but also directly addressed regulatory requirements. The implementation of streamlined access to cloud resources, simplified user experience monitoring, and improved overall operational efficiency, supports Verisk’s goal of delivering premier experiences that enable end users to work productively and securely from anywhere.

Zscaler has been able to assist numerous, large, and complex BFSI organizations in achieving digital transformation with strong zero trust protection.

Read about them at:

Capitec Bank	Guaranteed Rate	CapTrust
OneMain Financial	Canada Life	Fannie Mae
Tower	Mercury Financial	Liberty Mutual

¹For more information on this case, visit: <https://www.zscaler.com/customers/verisk>



Transform Security and Efficiency with Zero Trust

By adopting Zero Trust principles, BFSI organizations gain resilient security, streamlined compliance, and operational efficiency. Core Zero Trust capabilities, such as identity-based verification, least-privileged access, and segmentation, reduce lateral threats and safeguard critical systems like payment platforms.

When combined with AI, Zero Trust provides end-to-end visibility into user activity and application interactions, enabling the detection of advanced threats like encrypted traffic misuse and prompt injections. AI further simplifies compliance by automating data classification, anomaly detection, and audit trails, ensuring alignment with standards like GDPR, PCI DSS, and GLBA, while robust access controls protect both public and private AI usage.

Zscaler has a proven track record of empowering BFSI institutions to scale Zero Trust with AI-enhanced protections, delivering granular access controls, real-time monitoring, and advanced threat detection. Leverage Zero Trust to secure sensitive operations, meet regulatory demands, and drive innovation in the age of AI.



YOUR TRANSFORMATIONAL GROWTH JOURNEY STARTS HERE

Frost & Sullivan's Growth Pipeline Engine, transformational strategies and best-practice models drive the generation, evaluation, and implementation of powerful growth opportunities.

Is your company prepared to survive and thrive through the coming transformation?

Join the journey. 

FROST  SULLIVAN