AKAMAI SOLUTION BRIEF

Akamai Guardicore Platform for Financial Services

Zero Trust offers the most effective defense against IT security challenges in financial services, including data protection and defense against ransomware. However, implementing this framework can be complex and costly, especially when safeguarding assets across on-premises and cloud environments, and managing a dispersed workforce. The Akamai Guardicore Platform simplifies this process by efficiently addressing all aspects of Zero Trust with a unified console and a single agent. It enables financial institutions to secure their expansive attack surfaces, mitigate ransomware risks, and seamlessly comply with regulatory mandates.

Cyberattacks against the financial services industry are growing in frequency, complexity, and sophistication. The stakes are incredibly high. Cyberattacks on the financial system have the potential to disrupt not only the operations of individual institutions but also the stability of the global financial ecosystem. The consequences of a large-scale cyberattack can ripple through economies, causing financial chaos and undermining the trust that is the bedrock of the financial industry. Financial institutions face immense pressure to secure their networks while maintaining operational efficiency. The Akamai Guardicore Platform offers a comprehensive Zero Trust solution to address these challenges by providing financial institutions with the tools and capabilities needed to implement a robust Zero Trust security model effectively.

The Akamai Guardicore Platform is built to enable Zero Trust projects by combining best-in-class microsegmentation, Zero Trust Network Access (ZTNA), DNS firewall, and threat hunting into one platform. Together, these components streamline Zero Trust efforts to significantly reduce the attack surface and strengthen security posture across the entire enterprise.

Microsegmentation

One of the key components of the Akamai Guardicore Platform is microsegmentation. Traditionally, network security has relied on perimeter-based defenses that focus on securing the outer boundaries of the network. It is no longer sufficient to rely solely on perimeter defenses. The cyberthreat landscape has evolved, and so must the defenses that protect against it. What's needed is a comprehensive platform with global visibility into threats and situational awareness that emphasizes security everywhere business touches the world. Since the financial services industry is a prime target for malicious actors who seek to exploit vulnerabilities for personal gain, Akamai helps financial institutions protect the customer experience, the workforce, critical systems, and sensitive data, allowing them to remain resilient, innovative, and secure in an environment where the possibilities are as limitless as the threats.

Microsegmentation takes a different approach by dividing the network into smaller, more manageable segments and applying security policies to each segment based on the principle of least privilege. This granular approach to security ensures that even if one segment is compromised, the rest of the network remains protected. With Akamai Guardicore Segmentation, every asset is protected, including on-prem data centers, cloud instances, legacy OSes, IoT devices, Kubernetes clusters, and more — without ever having to change consoles.

Key capabilities

Microsegmentation
Segment network to prevent lateral movement of threats and limit attack surfaces

Zero Trust Network Access (ZTNA)
Securely enable workforce access to resources, regardless of location

FIDO2 MFA
Phish-proof multi-factor authentication service for enhanced user identity protection

DNS Firewall
Advanced protection against DNS-based attacks leveraging unique Akamai feeds

Advanced Security Services
Comprehensive threat hunting and risk detection capabilities

Integrated AI
Leverage AI for expedited compliance efforts, incident response, and vulnerability assessments

Akamai

Zero Trust Network Access

In addition to microsegmentation, the Akamai Guardicore Platform also offers ZTNA capabilities. ZTNA removes implicit trust in your financial institution's applications, users, and devices. Instead, access to resources is granted based on strict verification of identity, device posture, and other contextual factors. It secures remote and hybrid workers, sensitive financial data, and networks and applications by constantly verifying user identity, device health, and access policies before granting access to network resources.

ZTNA eliminates vulnerable VPN clients, integrates device health, and allows granular access to resources defined by policies to give remote workers secure and seamless access to specific applications and data. Remote and external users and their devices are no longer implicitly trusted: They and their devices must earn trust constantly.

ZTNA policy can prevent a compromised device from connecting to applications and data, effectively preventing lateral movement and attacks like ransomware from getting a foothold on banking and financial services networks.

DNS firewall

Another critical component of the Akamai Guardicore Platform is the DNS firewall. DNS (Domain Name System) is a fundamental component of the internet that translates human-readable domain names into IP addresses. However, DNS attacks in financial services continue to be the costliest among all industries. DNS outages can have severe financial repercussions for banks and financial organizations. Even a brief disruption in DNS services can cause significant downtime, preventing customers from accessing online banking portals, making transactions, or accessing critical financial data. By deploying a DNS firewall, organizations can block malicious DNS queries and prevent malware from communicating with malicious domains, thereby reducing the risk of data breaches and other cyberthreats.

Threat hunting

Finally, the Akamai Guardicore Platform includes an adaptive segmentation service that enables financial institutions to proactively identify and mitigate security threats before they escalate into full-blown incidents. Threat hunting involves actively searching for signs of compromise within the network, such as anomalous behavior or indicators of compromise (IOCs). By leveraging threat hunting tools and techniques, financial institutions can stay one step ahead of cyber adversaries and protect their valuable assets from harm.

In addition to its core capabilities, the Akamai Guardicore Platform also offers several key benefits that set it apart from other security solutions on the market. For starters, the platform provides a lightweight and consolidated infrastructure that minimizes agent bloat and console fatigue, allowing financial institutions to deploy and manage their security stack more efficiently. Furthermore, the platform offers broad and rich visibility into network assets and communications, enabling security professionals to gain comprehensive insights into their network environment and respond to threats quickly and effectively.

> Enabling organizations to meet audit requirements around zero trust frameworks. Increasingly, regulatory bodies and cyberinsurance providers are applying pressure to implement microsegmentation as part of the zero trust framework.
>
> **— Gartner® Webinar: Buyer Trends and Market Insights From Security and Risk Leaders — Microsegmentation, Adam Hils, Garrett Astler, 27 March 2024**

Benefits

- Meet compliance and regulatory audit requirements around Zero Trust frameworks.
- Automate security for new workloads.
- Prevent ransomware from spreading throughout the extended data center without having to use performance-intensive threat detection.

To learn more, visit akamai.com or contact your Akamai sales team.