AKAMAI CUSTOMER STORY

SBI Holdings Strengthened Ransomware Defense

Leading Japanese financial group elevated Zero Trust security across the organization with microsegmentation

Stopped lateral spread of attacks

Exposed hidden threats

Enabled Zero Trust strategy

Confronting rising cyberthreats across a vast financial group

SBI Holdings, one of Japan's leading financial groups, faced rising cyber risk across its sprawling ecosystem of more than 600 subsidiaries. With stealthy attacks increasing and regulators calling for stronger operational resilience, the organization needed a way to prevent lateral movement, strengthen Zero Trust, and operate efficiently at scale. Akamai Guardicore Segmentation helped SBI Holdings meet these goals by visualizing communication patterns, isolating systems through microsegmentation, and enabling fast, centralized control across multicloud and on-premises environments.

Japan's growing cybersecurity crisis demanded a new approach

SBI Holdings' diverse operations span banking, securities, insurance, asset management, venture capital, crypto assets, and more. That scale raised the stakes for Terumasa Ura, IT General Manager, who oversaw the group's cybersecurity strategy and directed its Computer Security Incident Response Team (CSIRT). He also contributed to national cybersecurity policy efforts, analyzing trends that shaped Japan's defensive posture.

At the same time, demands from regulatory authorities intensified the sense of urgency. In recent years, the Financial Services Agency pressed financial institutions to strengthen security across their supply chains and improve operational resilience, underscoring the need for a more robust and modernized approach.

SBI GROUP

Location

Japan
sbigroup.co

Industry

Financial Services

Solutions

Akamai Guardicore Segmentation

Akamai Hunt

Akamai

The CSIRT felt a mounting sense of crisis: “Cybersecurity has always been a top priority for financial institutions. However, we reached a point where the traditional approach was no longer viable,” explained Ura. High-profile incidents in Japan, including long-undetected breaches and sophisticated living-off-the-land attacks, confirmed that older prevention-only models were insufficient.

In particular, the rise of AI-driven, blended attack methods made it essential to bolster both prevention and rapid detection. “Based on the premise of Zero Trust, we needed to visualize whole environments, control processes, and hunt for threats so we could prevent, detect, and contain them,” he continued.

Cyber incident insights guided SBI Holdings’ microsegmentation strategy

Before new regulations took hold, Ura analyzed global cyber incidents to understand why breaches had escalated. Three lessons stood out: Breaches must not cascade across the group, mission-critical systems must be isolated from lower-tier systems, and overall security is only as strong as the weakest subsidiary. These insights guided SBI Holdings’ search for a solution that could enforce these principles at scale.

The group needed a microsegmentation solution capable of:

- Unifying security across AWS, Microsoft Azure, on-premises data centers, and legacy systems — covering thousands of endpoints and hundreds of servers
- Complying with Japan’s data governance rules
- Operating efficiently to minimize reliance on specialized staff

After evaluating multiple vendors, only Akamai Guardicore Segmentation met all requirements. Competing SaaS platforms hosted overseas could not satisfy regulatory demands.

Akamai Guardicore Segmentation is a Zero Trust security solution that enforces micro-level segmentation and deeply visualizes network communications. By controlling east-west traffic in real time, it prevents attackers from moving laterally across infrastructure, providing an essential defense against modern ransomware and stealth attacks.

The Akamai solution maps application dependencies and process-level activities to produce deep, dynamic visualizations of the entire infrastructure, whether workloads run on-premises or in cloud environments where IP addresses frequently change. These insights make it easy to spot problematic communications, set informed policies, and enforce precise host-to-host control. With label-based policy management, organizations can consistently apply security rules across diverse systems and maintain clear visibility even as environments evolve.

> “With Akamai Guardicore Segmentation, we finally gained a way to raise security standards across hundreds of companies without increasing operational strain.
>
> — **Terumasa Ura**
> IT General Manager,
> SBI Holdings, Inc.

Seeing the environment clearly: Proof of concept (PoC) reveals hidden issues

Because SBI Holdings chose to deploy the agent-based version of Guardicore Segmentation, the CSIRT initially worried about performance impacts on its financial systems. “We established a process to thoroughly check whether processing would become heavy or create excessive load,” Ura said.

Over four months of PoC testing across 40 clients and five servers, the team found no negative performance effects. It also resolved conflicts with existing security tools and proxy connections, confirming smooth integration.

Then came an unexpected discovery: The visibility offered by Akamai Guardicore Segmentation surfaced communication paths the team did not know existed. “We found unintended communication routes,” Ura recalled. “Identifying issues we hadn’t seen before was a major achievement.”

Boosting cyber resilience and operational efficiency with AI and global threat intelligence

Akamai Guardicore Segmentation also provided AI-driven threat hunting that learned normal behavior and flagged anomalies, including indicators of living-off-the-land attacks. This allowed SBI Holdings to detect reconnaissance behaviors and refine segmentation rules.

The threat hunting capabilities improved both security and operations. Through Akamai Hunt, Akamai’s managed threat hunting service, the CSIRT benefited from expert analysts and global threat intelligence. Ura noted that global threat intelligence from Akamai helps SBI Holdings stay ahead of attacks that often hit overseas before reaching Japan. “This capability is essential for continually updating our security strategy,” he said.

In addition, by taking advantage of Akamai’s global threat intelligence, SBI Holdings can use Akamai Guardicore Segmentation’s dynamic deception technology to automatically lure attackers into honeypot traps for monitoring and analysis.

Enhancing security efficiency through automation and partnership

Managing thousands of endpoints manually requires a large workforce. As the financial industry grapples with a shortage of skilled security personnel, Ura saw additional value in Akamai Guardicore Segmentation’s usability.

The solution’s label-based management and prebuilt templates for use cases like ransomware prevention allowed SBI Holdings to operate it with minimal resources. “Akamai Guardicore Segmentation enabled us to raise security across the entire group while minimizing operational burden,” he said.

As Ura underscored, “Solutions like this need to be intuitive enough for nonexperts while powerful enough for specialists. With strong operability and clear visualizations, the Akamai solution freed our skilled staff to focus on more strategic tasks.”

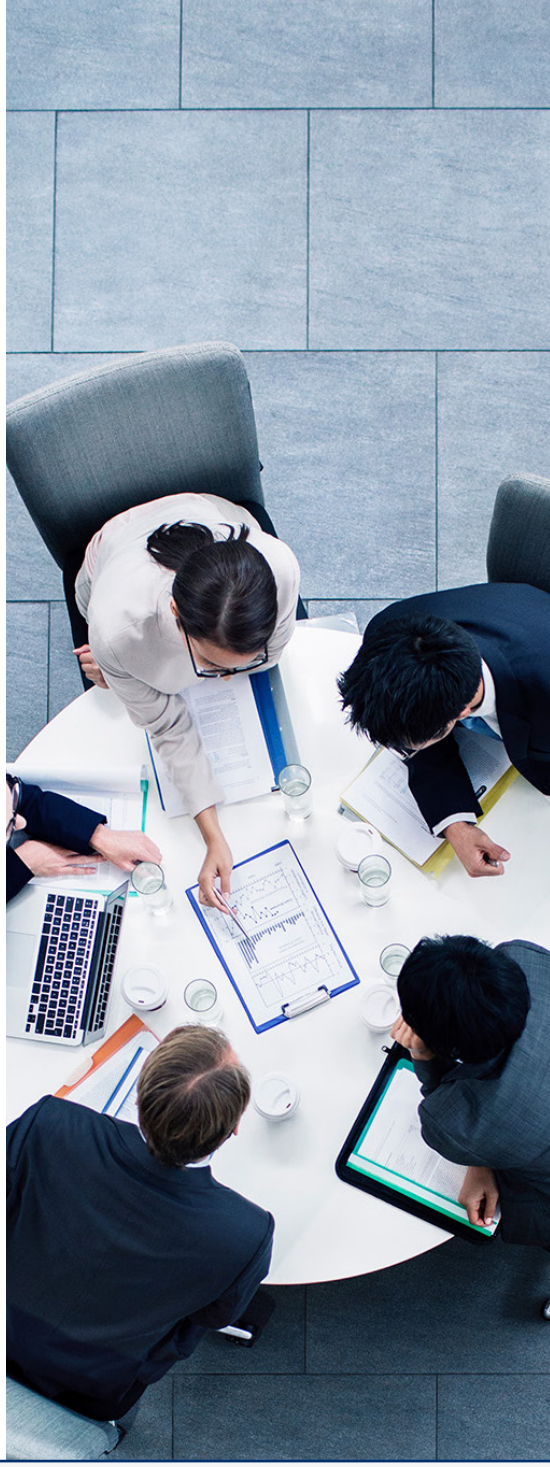
SBI Holdings had already trusted Akamai for more than a decade for DDoS protection, and the support behind the Akamai Guardicore Segmentation deployment further strengthened that relationship. “From the PoC to the design phase, we received high-quality support for the technical challenges we faced,” he continued.

A foundation for sustainable Zero Trust across SBI Holdings

SBI Holdings’ experience demonstrates the power of microsegmentation to enforce logical network segments (or secure zones), isolate critical systems, and improve security across large, diverse organizations. With Akamai Guardicore Segmentation at its core, the group is advancing a next-generation Zero Trust architecture built for both security and operational efficiency.

Ura emphasized that Akamai Guardicore Segmentation aligns perfectly with the group’s long-term Zero Trust vision: “Akamai Guardicore Segmentation’s visualization and verification features are extremely well suited to the idea of Zero Trust, or ‘trust nothing.’ We believe it will be a key part of our Zero Trust security strategy and architecture.”

Looking ahead, Ura expressed confidence in the partnership: “We look forward to Akamai’s continued support in improving the defense capabilities of our entire group.”



SBI GROUP

SBI Group was founded in 1999 as a pioneer of internet-based financial services in Japan. The company operates a broad portfolio of businesses that includes financial services, which provides various financial products and related services with a focus on securities, banking, and insurance; private equity investment, which encompasses the management of venture capital and other types of funds; and asset management, offering services related to wealth and investment management. In addition, the group is engaged in the crypto assets business, operating domestic cryptocurrency exchanges and a market-making business, as well as next-generation businesses such as bio-healthcare & medical informatics and Web3-related initiatives.

 | Published 12/25

Akamai