Akamai Customer Story

SBI Shinsei Bank Prepares for Risk After Ransomware Attack

The Japanese financial institution implemented microsegmentation to help protect against threats

Visibility into internal communications

Prevention of post-breach lateral movement

Establishment of a Zero Trust architecture

With the threat of ransomware spreading throughout Japan, SBI Shinsei Bank was faced with the issue of cyber risks after an attack, with a view to protecting its internal server environment in particular. This article details the route the bank took to strengthen security measures under the constraints inherent to financial institutions.

The server's "invisible communications" issue

SBI Shinsei Bank (formerly the Long-Term Credit Bank of Japan) is promoting a comprehensive financial model in collaboration with the SBI Group, focusing on retail, corporate, and financial services. The bank, overhauling and strengthening its network and security while building this next-generation financial platform, faced many challenges.

SBI Shinsei Bank's IT infrastructure consists of a hybrid environment combining on-premises and cloud. However, communication requirements had become increasingly complex due to configuration changes and additions having built up over the years. Akira Takahashi (Group Information Technology Division, Deputy General Manager of Group C-SIRT Management Department), who oversees the SBI Shinsei Bank Group's C-SIRT, reflects on the situation at that time:

"We had cases where the personnel in charge of building it at the time had since been transferred, and the communication requirements of some of our long-running servers had become a black box, making it difficult for us to understand the full picture. To overhaul the system, we had to start by figuring out what our existing servers were communicating with."

This wasn't just a matter of visibility. These servers would eventually need to be overhauled, but without an exact understanding of the communication requirements, there was no guarantee that they would work properly after moving to a new system. Different management approaches were required since on-premises and cloud environments use different technologies, further complicating the situation.

Security was also an issue. Among reports of damages caused by a series of ransomware attacks both in Japan and abroad, there was also a need to address post-attack lateral movement within internal networks.

SBI SHINSEI BANK

Location
Japan
sbishinseibank.co.jp

Industry
Financial Services

Solution
Akamai Guardicore Segmentation

Akamai

SBI Shinsei Bank established its Group C-SIRT Operations Team in 2021. This was due to there being an urgent need to establish an emergency response system owing to frequent incidents in the finance industry. The bank ran internal penetration testing at the same time as establishing this system. Hiroki Kobe (Information System Operation Division, General Manager of Next Generation Core-Banking Division), who is involved in the selection of security products at the bank, explained:

"The results of the penetration testing showed us that we had sufficient measures in place against an attack from the outside. However, our vulnerabilities were revealed when we tested an internal attack scenario. Following this being reported to management, a fundamental review of our internal countermeasures was started."

As a result of sharing the test results with management, a sense of crisis spread throughout the bank. Although patches were applied as a vulnerability countermeasure, the fundamental priority was protecting the internal network. Takahashi went on to explain the direction they took for the countermeasures:

"While endpoint protection using endpoint detection and response (EDR) is certainly important, that alone is not enough. Controlling communication in the network layer is what is effective in preventing internal movements after an attack. And so we came to the conclusion that using segmentation could prevent damage from spreading."

The importance of multilayered protection, which protects each layer of the endpoint and network, is also clearly stated in Japan's Financial Services Agency's "Guidelines on Cybersecurity for the Financial Sector." Segmentation technology can visualize communications and block them when necessary, meaning it is effective as a countermeasure against post-attack internal lateral movements.

Management's sense of impending crisis had been growing ever since. Each time a ransomware attack was reported in Japan or overseas, the Group C-SIRT Operations Team would brief management on the situation, enabling them to fully comprehend the risk of intrusion via affiliated companies through supply chain attacks. Strengthening security governance for not only the bank, but for the entire group, was positioned as a management issue.

The deciding factors in selecting a product capable of strengthening both network and security

Virtual infrastructure products were initially considered as candidate products for implementing segmentation. However, the company decided to look at a hosted firewall product that could enhance not only network visibility but also their overall security capabilities.

SBI Shinsei Bank selected Akamai Guardicore Segmentation (AGS) after comparing and reviewing solutions based on the above requirements. There are three reasons that led them to choose AGS.

First was its ability to centrally visualize the entire network across platforms. It simplifies management and visualization by presenting complex infrastructure viewpoint information such as subnets and IP addresses in a label-based format that is easy for humans to understand.

Second, it comes equipped as standard with granular communication control functions and protection policies against ransomware. Kazuyuki Nakazawa (Manager of Information System Operation Division), who is involved in the introduction of AGS at the bank, highly values this point.

“I highly valued its ability to make decisions using Akamai’s threat intelligence database, rather than simply controlling communications sources and destinations with port numbers. It also comes with policies for high-risk ports.”

Third was the ability to share use cases and implementation examples with Akamai even before the rollout, based on a wealth of case studies from Japan and overseas. Being provided with detailed information, such as the time frame required for implementation and the expected number of personnel required for operation, enabled the bank to create a concrete image of what the system would look like.

AGS Implementation Process (Courtesy of SBI Shinsei Bank)

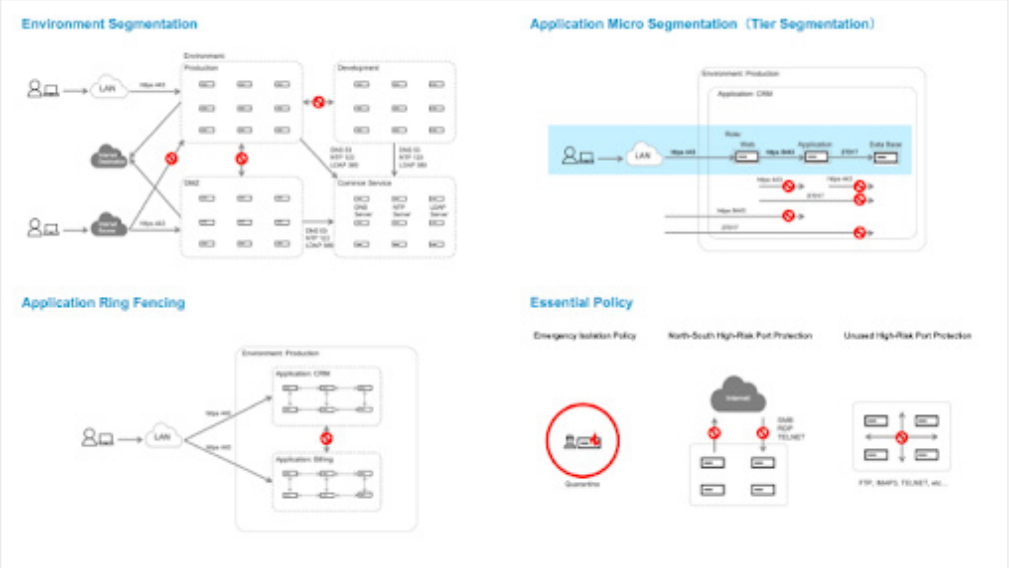
Kobe expressed his trust in Akamai, saying, “I felt that they were great at security solutions as a whole, including front-end protection. During the planning phase, members of their overseas professional services team came to Japan and set up multiple opportunities to personally discuss matters such as operating AGS. This generous support from the planning stage onward fostered trust,” he explained.

Side-by-side support from PoC to training

SBI Shinsei Bank began looking at AGS around May 2024, before deciding on adopting it approximately a year later in June 2025. During this time, the bank held a series of requirement consultations, demonstrations, and discussions regarding its operation. During the PoC (proof of concept) stage, Akamai also held workshops in which the need for microsegmentation was explained using case studies based in Japan as examples.

Nakazawa shared this knowledge with relevant departments within the bank to promote understanding around introducing this product. Since AGS installs agents on servers in order to visualize and control communications, it was vital that each team managing the targeted systems understood this when it came to its implementation.

“The materials shared at the workshops were incredibly easy to understand, including the analogy about dividing a ship’s cabin into smaller sections to minimize flooding damage, so I was able to use this as-is for explanations within the bank,” said Nakazawa.



Segmentation Illustration (Courtesy of SBI Shinsei Bank)

Latency was measured to alleviate concerns around deploying agents. A consensus was reached among the relevant departments after demonstrating numerically that load on their systems was within an acceptable range when actual measurements were taken in the PoC environment.

Akamai's side-by-side support also extended to training. Shinako Fukuchi (Group Information Technology Division. Group C-SIRT Management Department), who is involved in the AGS implementation project at the bank, completed Akamai's GCSA (Guardicore Certified Segmentation Administrator) training. Through this one-week intensive course, she was able to systematically learn everything from the product's terminology framework to construction procedures and operational steps.

"The handbook provided was comprehensive, and I was able to gain an understanding of its design philosophy through repeated reading. The major benefit was being able to gain a clear understanding of what operations would look like after implementation."

A cautious approach to deployment for core systems

At the end of 2025, the bank was working on designing its deployment with Akamai's Professional Services team. This deployment included 420 servers, 400 of which have implemented Akamai Guardicore Insight to enable the detailed querying and investigation of server contents. This included core systems and core banking systems, which required a cautious approach.

Deploying agents to all servers first before establishing communications control policies proved difficult. This required carefully determining the right time that core systems could be shut down, which meant the entire deployment took some time.

"Akamai proposed a plan to sequentially implement communications controls, starting with systems for which agent deployment was already complete. We found their flexible approach tailored to the bank's environment reassuring," said Fukuchi.

Although the deployment period became longer, during that time the bank was still able to detect and block dangerous communications using essential policies (recommended policies offered to all customers).

Transitioning to a group-wide Zero Trust platform

SBI Shinsei Bank aims to embed the knowledge and expertise it gained through the implementation of AGS as a group-wide Zero Trust platform technology. The bank will first introduce the system before rolling it out to its group companies. A roadmap will be developed jointly with major subsidiaries and this expertise will be shared. Takahashi describes security strategy going forward as follows:

“On this occasion, we introduced segmentation first. Since its approach to protection is different from that of EDR, neither one of them alone is enough. We want to achieve multilayered protection that combines both.”

Kobe expressed his expectations for Akamai going forward as follows: “The main thing for us is the ability to quickly contain incidents when they occur, whether on-premises or in the cloud. As attacks using generative AI are increasingly becoming more sophisticated, we hope that security products will also continue to evolve. Given the stringent deployment requirements for the bank’s core systems, we are looking forward to having more options, such as more lightweight agents.”

SBI Shinsei Bank aims to establish an incident response process utilizing segmentation technology via a phased implementation. Building a Zero Trust platform that integrates on-premises and cloud environments will not only strengthen the bank’s security, but also improve protection for the group overall.

This article is a restructured version of content produced by the ITmedia editorial department, originally published in February 2026.

SBI SHINSEI BANK

Since becoming a member of the SBI Group in December 2021, we at the SBI Shinsei Bank Group have been putting the SBI Group’s fundamental business philosophy of “customer centricity” into practice with innovation and speed. As the core bank of the SBI Group, we are evolving and deepening our collaboration with regional financial institutions to realize the “Fourth Megabank Concept,” strengthening our contribution to regional revitalization. Furthermore, in the rapidly evolving digital finance field, we aim to provide “next-generation finance” to more customers by making the most of the leading SBI Group’s knowledge and network. The SBI Shinsei Bank Group will enhance corporate value through innovative initiatives that go beyond the boundaries of traditional finance, and contribute to the realization of a sustainable society.

© 2026 Akamai Technologies | Support |
| Published 03/26