

Samsung Life Insurance Advanced Zero Trust with Akamai

Leading insurer gained process visibility and tighter access controls across hundreds of apps and thousands of servers



Gained
process-level visibility



Strengthened
identity-based access



Accelerated access
policy changes

Building a stronger foundation for Zero Trust

Samsung Life Insurance is one of South Korea's leading life insurers, serving customers across a broad range of financial and insurance products. As the company pushes deeper into digital and AI transformation, its IT environment keeps growing more complex. Samsung Life Insurance needed a practical way to strengthen **Zero Trust** across both legacy and modern systems while giving its security team real visibility and control. Akamai Guardicore Segmentation became the foundation that made that possible.

The problem: Extending trust without visibility

Samsung Life Insurance's IT environment combines legacy systems with newer, more dynamic applications. Its security model relied heavily on perimeter defenses like firewalls and Active Directory. However, once traffic crossed those boundaries, the internal network ran almost entirely on trust.

The company recognized that Zero Trust had to extend inside the traditional network perimeter. A firewall could provide a strong first line of defense, but Samsung Life Insurance also needed controls that could limit lateral movement if an attacker made it into the internal environment.

Its existing approach left a critical gap: Samsung Life Insurance couldn't control access at the application level. **Endpoints** could reach internal servers far more broadly than Samsung Life Insurance wanted, and its increasingly dynamic applications made IP-based controls harder to manage by the day.

Managing policy was its own drain on the security team. A user who needed access had to submit a request for the security team to review. The team then had to create or modify firewall rules to allow that access. In some cases, opening a firewall policy could take up to a week, making it difficult to apply access controls as quickly as business needs changed.

SAMSUNG
LIFE INSURANCE

SAMSUNG

Location

Seoul, South Korea
samsunglife.com

Industry

Financial Services

Solution

Security

Product

Akamai Guardicore
Segmentation



But the biggest gap was visibility. Samsung Life Insurance couldn't easily identify unauthorized **lateral movement**. "We needed to see what was actually happening inside our environment," said a Samsung Life Insurance IT Security Representative. "That visibility was crucial to understanding which communications were legitimate and which ones posed a security risk."

Traditional network visibility only showed connections between IP addresses and servers. Samsung Life Insurance wanted a more granular view of those connections, including the users, applications, and processes behind them. That need grew more urgent as the company's attack surface expanded.

Perimeter security still mattered as a first line of defense, but Samsung Life Insurance wanted a way to contain a threat that made it past the perimeter. **Microsegmentation** was the answer.

Why Samsung Life Insurance chose Akamai Guardicore Segmentation

Samsung Life Insurance evaluated the leading microsegmentation platforms on the market. Scope was the deciding factor.

"We needed a solution that fit our environment, built around Windows desktops and laptops, along with Windows and Linux servers," said the IT Security Representative.

Some competitive solutions didn't support user identity-based segmentation. Others lacked process-level blocking on Linux servers. Or they couldn't support dynamic fully qualified domain name (FQDN) policies based on the domains accessed by server processes. Samsung Life Insurance needed all three capabilities in one solution.

Broad network segmentation wasn't enough on its own: Samsung Life Insurance wanted to control access based on who was connecting, what they were trying to reach, and how applications talked to each other.

The company appreciated that Akamai Guardicore Segmentation used Active Directory identities, application labels, and FQDNs to enforce those policies. It also liked that the solution's **Layer 7** capabilities delivered the granularity a real Zero Trust approach demands.

"We wanted one solution that could cover everything from endpoints to workloads," the IT Security Representative said. "Akamai Guardicore Segmentation gave us that coverage."

Samsung Life Insurance started with visibility and policy control

Samsung Life Insurance rolled out the Akamai solution in phases. Phase one focused on building visibility, integrating identity data, and establishing the policies needed to control access.

The security team started by connecting Akamai Guardicore Segmentation to Active Directory, pulling user and group information directly into access policies. That step enabled a simpler way to manage access.

Instead of creating a new segmentation rule each time a user needed access, the team could add the user to the appropriate Active Directory group. The existing security policy stayed in place, while the user's group membership determined whether access was allowed. "Since our security teams no longer needed to create or modify a firewall policy for every access request, authorized users could quickly gain required access," said the IT Security Representative.



Akamai Guardicore Segmentation gave us the visibility we needed to move from network-level control to process-level security.

Samsung Life Insurance IT Security Representative

From there, the security team used a built-in feature that builds policy recommendations by watching how applications and users actually communicated. “This feature gave our administrators a real starting point for deciding what to allow and what to block,” the representative continued.

The team wrote allow and block rules based on those recommendations. It then used automated policy migration to bring existing security policies into the new model. Rather than starting from assumptions about what access should look like, Samsung Life Insurance built its controls on what its traffic actually showed. “This approach helped us build controls around the way our applications and users actually communicate,” the IT Security Representative continued.

Process-level visibility exposed what was really happening

The biggest shift was visibility itself. Before deployment, Samsung Life Insurance’s team could see network connections at the IP level: a server talking to a server. Akamai Guardicore Segmentation provided process-level visibility, showing which programs initiated connections, which systems they contacted, and how those communications moved through the environment.

That gave the security team a much sharper picture of what was actually happening inside their environment.

With that visibility, Samsung Life Insurance rolled out label-based policies to lock down unauthorized communication between business units, applications, and workloads. “Seeing the actual communication between processes enables us to identify potential lateral movement and decide where to apply controls,” the IT Security Representative said.

Policy management got simpler too. Instead of constantly rewriting firewall rules and opening and closing ports across multiple security boundaries, the team could set policy once, based on labels, applications, and identities.

The approach also gave Samsung Life Insurance a way to apply Zero Trust principles beyond the perimeter. By controlling communication at the endpoint, application, and workload levels, the company could limit lateral movement even after traffic had entered the traditional network boundary.

In addition, the deployment strengthened Samsung Life Insurance’s confidence in the stability of its own controls. “By using a commercial kernel module supported by Akamai rather than an open source kernel module, we achieved more stable operations,” the IT Security Representative said.

Achieving a Zero Trust model that evolves with the business

Samsung Life Insurance now runs Akamai Guardicore Segmentation across hundreds of applications and endpoints, and thousands of workload servers. A year into reliable operation, the company continues to expand its footprint.

Akamai's solution now sits at the center of Samsung Life Insurance's broader Zero Trust architecture, paired with [ZTNA \(Zero Trust Network Access\)](#) for internal networks and [SASE \(secure access service edge\)](#) for external environments. Together, these technologies let Samsung Life Insurance move toward dynamic access control, weighing user identity, device, location, and other context instead of relying on network location alone.

That shift is helping Samsung Life Insurance build stronger controls around the systems powering its digital and AI initiatives. With greater visibility and more responsive access controls, the company has a stronger security foundation for expanding those initiatives while protecting critical IT assets.

"Security can help us conduct more proactive business in this changing financial industry environment, compared to other financial institutions," the IT Security Representative concluded.

SAMSUNG
LIFE INSURANCE



Samsung Life Insurance has been devoted to protecting the lives and assets of the people with its insurance services since its founding in 1957. The company has focused on making a contribution to society by promoting the culture that treasures family values. Their efforts have been recognized by Korea's most prestigious National Customer Satisfaction Index, as we have been ranked as the top institution for 10 consecutive years. For more information, visit samsunglife.com.