AKAMAI CUSTOMER STORY

Hello new data center, goodbye firewalls

Leading life insurance company strengthened security with Akamai Guardicore Segmentation — a nimbler way to protect the business

<1 HOUR
To change rules for production apps

Seconds
To change rules for apps in development

Zero
Performance impact on databases

Simplified retirement, simplified security

When a leading life insurance company was acquired, the company had a rare opportunity to design a new data center from scratch. To simplify and strengthen security, the security team decided to steer clear of firewalls and their complex rules. Instead, they installed Akamai Guardicore Segmentation software on virtual and physical servers to see the resources they depended on, and then built rules to block all other communications. Microsegmentation limits the spread of malware, helping the company keep its service commitments to clients, distribution partners, and the workforce.

Just because the business is complex, security doesn't have to be

The opportunity to design a greenfield data center doesn't come around often. However, that chance came when a leading insurance company was acquired by another larger, well-known insurer. "The annuities business is complex, requiring massive nightly calculations and self-service apps for our clients and their advisors," says the company's chief information security officer (CISO). "We had an opportunity to start with a fresh slate, simplifying IT so that we can focus on a great customer experience."

Since the company's business is protecting clients' retirements, security is a top priority. The CISO's first act was to call a previous teammate to bring him back as a security architect. "We got the band back together!" he says. The pair set to work planning the new data center. "We saw the move as an opportunity to leapfrog the old ways of delivering IT services and become more nimble as a business," says the CISO.

Limiting the spread of malware

Malware can manage to sneak past the best defenses, so the pair needed a way to limit its spread if that happened. They're not fans of firewalls. "In our previous data center, keeping firewalls' rules up to date took an entire team," the CISO recalls. "What's more, firewalls can become bottlenecks in busy networks like this one."

U.S. Life Insurance Company

Leading U.S. life insurance company
United States

Industry
Financial services

Solution
- Akamai Guardicore Segmentation

Each night, the company calculates the value of about half a million policies and annuities based on the day's market performance and other variables, delivering it to partners like financial advisors by 4 AM. These calculations, plus nightly backups, generate a massive amount of traffic. "In the old data center, the firewall was maxed out all night and had the potential to slow things down," the security architect says. "We wanted a simpler way to segment the network — with less management overhead and without the expense of redundant, high-throughput firewalls."

Simpler security, better visibility

The duo found their solution in Akamai Guardicore Segmentation. "With Akamai Guardicore Segmentation, server-to-server communications don't have to go through a firewall, eliminating a potential bottleneck," the security architect explains. "When we installed the agent on our SQL Server database, we saw zero performance impact. I was expecting a small hit at least — I was shocked."

The visibility for a smart migration plan

To prevent any hiccups in the user experience during the transition to the new data center, the pair wanted to move each application and its dependencies at the same time. That would avoid the latency that arises when an application in one location talks to a database in another. Identifying dependencies can be tricky, a problem solved by installing the software agent on about 750 servers and 750 workstations to see which systems communicated with one another. "By showing us each application's dependencies, Akamai Guardicore Segmentation helped us plan which assets to move to the new data center at the same time — and build nice clean rules for server-to-server communications," the security architect says. "Having detail down to the process level is awesome."

A stronger security posture

Every system and process is now in its own segment, giving the company tight control over which assets can communicate with one another. "Akamai Guardicore Segmentation limits the spread of attacks that could disrupt our business," says the CISO. "It supports our commitment to protect our customers' retirement — and their peace of mind." When the Log4j attack hit, Akamai Guardicore Segmentation made it easy to see potentially vulnerable applications, enabling the quick remediation of the vulnerability before it could be exploited.

Faster adaptation to business change

A simpler alternative to firewall rules also helps the business quickly introduce new digital experiences. Modifying firewall rules briefly interrupts communications, so previous changes were limited to a one-hour window from 9 to 10 PM. If a new rule caused a problem that showed up the next morning, the team couldn't attempt a fix until after work hours.

"Troubleshooting firewall rules could sometimes take up to a week — and in the meantime, the new application or feature wouldn't be available to our users," the security architect says. "With Akamai Guardicore Segmentation, we can introduce new client and advisor services faster, changing rules in the production environment in less than an hour, and in the test environment in seconds."

Simpler management, freeing time for new projects

Akamai Guardicore Segmentation rules are also simpler to keep up to date than firewall rules. For example, when the company adds capacity for an application, the application's existing rules automatically apply to the new virtual machines.

> We weren't sure how easy it would be to manage Akamai Guardicore Segmentation. Turns out it was the easiest part of the data center transition. It helps us meet our brand promise to keep things simple — for the clients whose retirements we protect, our distribution partners, and our internal users.
>
> **CISO**
> leading life insurance company

To save more time, the security architect gave the company's application developers read-only access to Akamai Guardicore Segmentation. "Now they can see if an application problem is due to communications rules," he says. "If there is a problem with rules, I can correct it with a few clicks while we're on the phone."

The duo is already planning new ways to use Akamai Guardicore Segmentation. One way is to better understand communications by integrating their Arista switches and F5 load balancers with the solution.

"We weren't sure how easy it would be to manage Akamai Guardicore Segmentation," says the CISO. "Turns out it was the easiest part of the data center transition. It helps us meet our brand promise to keep things simple — for the clients whose retirements we protect, our distribution partners, and our internal users." There's nothing complicated about that.

> Akamai Guardicore Segmentation limits the spread of attacks that could disrupt our business. It supports our commitment to protect our customers' retirement — and their peace of mind.
>
> **CISO**
> leading life insurance company