AKAMAI CUSTOMER STORY

Large European Bank Selects Akamai to Reduce Security and Compliance Costs with Innovative Approach to Segmentation

Comprehensive network visibility

10x faster segmentation

Automated policy creation

The customer

A large European bank

A multinational investment and financial services company, providing services to customers across more than 50 countries in Europe, North America, and Asia, needed to improve its compliance posture. Facing cybersecurity regulations from multiple authorities in Singapore, the U.K., the U.S., and Europe, the organization's main goal was to achieve workload segmentation and separation of the environments in its data center.

The challenge

Meeting security and compliance requirements with segmentation

The increased focus from regulators on tightening data center security and ensuring financial services market stability resulted in new regulations that required the bank to meet technical requirements through segmentation.

Internal auditors had also alerted the organization to the security risks posed by flat networks, which will amplify the impact of a security breach. A major concern was an internal threat scenario in which human error or unauthorized activity would lead to an information leak or production error, potentially destabilizing the bank's entire environment.

To address these challenges, the bank began implementing internal data center network segmentation.

Selecting a solution

A struggle with legacy firewall complexity

The initial segmentation effort was done with traditional tools such as firewall rules and VLANs. This project was taking significant time, requiring multiple stakeholders and teams' attention, causing production downtimes and policy ambiguities. As a result, the bank was paying significant fines for noncompliance, in addition to high implementation costs.

Large
European Bank

Industry
Financial Services

Solution
Akamai Guardicore Segmentation

Key impacts
- Reduces compliance costs
- Segments IT environments
- Secures cloud and container environments
- Automates security processes

With the cost of traditional approaches being unviable, the bank's IT team started to look into alternative and more cost-effective segmentation solutions to meet the compliance requirements. In addition to the on-premises segmentation, the bank was also looking for a cloud and container-ready solution.

When the evaluation team came across Akamai Guardicore Segmentation, they were intrigued by the level of visibility and policy flexibility it demonstrated during the proof of concept (PoC). Additionally, the DevOps integration and automation impressed them. These capabilities simplified policy creation and enforcement in a unified manner across multiple infrastructures. But most important, the Akamai team showed full commitment to success throughout the PoC and after. This true partnership attitude distinguished Akamai's value even further.

After a thorough evaluation process that included multiple vendors, the decision-makers in the bank's infrastructure and IT security teams came to a consensus: Akamai's technology offered the simplest, most straightforward path to microsegmentation. Akamai also aligned with the bank's future strategy. It would give the organization both granular visibility into the east-west traffic and the ability to enforce segmentation policies in its new multicloud and container environments.

Akamai Guardicore Segmentation

Simplifying and accelerating microsegmentation

The bank deployed Akamai Guardicore Segmentation across multiple regions and IT infrastructure types, including container technology. Because there was no need for application changes, it caused no downtime in the production environment. It also allowed the bank to quickly achieve centralized visibility into data center workloads and isolate the production, test, and development environments. Using Akamai Guardicore Segmentation, the customer was also able to restrict access to servers from printers, other Internet of Things devices, and unauthorized users.

In less than three months, the project was complete. It went 10 times faster than initially estimated with traditional segmentation methods. By quickly mapping out the environment and creating policies based on the collected information, the bank improved its security posture and addressed the compliance requirements for more than 10,000 noncompliant assets. The speedy deployment resulted in risk reduction, and significant cost and resource savings.

Akamai's professional services team helped the bank to completely transform their segmentation processes. Today, the asset labeling and segmentation policies are fully automated, embedded in the application development and deployment processes. The label creation, change management, security incidents, and service requests are fully integrated into the ServiceNow workflows. The customer was extremely satisfied with the results from the platform and the value it delivered, along with Akamai's partnership attitude and the vendor's skilled and dedicated technical services teams.

Please visit akamai.com/guardicore for more information.

> [Akamai] helped us to implement tight network segmentation across on-premises and cloud environments. With [Akamai] we are effectively protecting our critical assets and applications.
>
> Vice President, Information Security, Large European Bank