AKAMAI CUSTOMER STORY

Bank Deploys Solid Defense Against Cybercriminals

Daiwa Capital Markets Europe safeguards critical trading and payment systems with Akamai Guardicore Segmentation

Provides regulatory compliance

Protects against ransomware attacks

100%

Support of cloud migration roadmap

Securing the business against cybercriminals

To protect critical systems, including trading and payments, leading investment bank Daiwa Capital Markets Europe has deployed Akamai Guardicore Segmentation across its IT infrastructure. This enables the bank to isolate security breaches and prevent the lateral spread of malicious software across the organization. It also simplifies security audits so the bank can comply with the latest financial regulations.

Blocking cybercriminals, complying with regulations

Security is a priority for Daiwa Capital Markets Europe. To retain and attract clients, it must protect sensitive systems and data that relate to its main business areas of investment banking, including equity, fixed income, and global convertible bonds. In addition, Daiwa must provide evidence that the business is adequately secured in line with the latest legislation, or risk a substantial fine from the U.K. or European regulators.

To protect the bank's systems and stay one step ahead of cybercriminals, Daiwa regularly reviews the security of its technology infrastructure. Daiwa Chief Information Security Officer, Dave Wigley says, "During these exercises, we look closely at all our domains to ensure that the security posture supports the business's objectives and reporting requirements in today's highly regulated environment."

There are many factors that shape the bank's security strategy, but Wigley has focused on ransomware attacks, which doubled in 2021 according to the U.K. intelligence agency GCHQ. During these attacks, criminals use malicious software to access a network, encrypt files and databases, and unlock them in return for a substantial payment.

Daiwa Capital Markets

Daiwa Capital Markets Europe Limited
London, U.K.
www.uk.daiwacm.com

Industry
Financial Services

Solution
- Akamai Guardicore Segmentation

Akamai

"We were concerned that a compromised workstation would allow an attacker to move laterally throughout the organization and elevate their privileges until they had sufficient access rights to disrupt or encrypt our systems," says Wigley.

Taking a stand against ransomware

To repel the threats, Wigley looked at several approaches, including technology that creates secure zones across data center environments. These zones ringfence application workloads from one another so that if one is attacked, it can be isolated, preventing malicious software from spreading through the network.

When comparing solutions, the Daiwa team researched providers whose technology supported Daiwa's relatively complex IT infrastructure. The bank runs a mix of operating systems, including Microsoft Windows, Unix, and Solaris. Any solution must also support the bank's long-term IT roadmap, which includes migrating to the cloud.

"We had a number of options, but Akamai Guardicore Segmentation stood out for its scalability and coverage of different operating systems," says Wigley. "We were impressed by their proof of concept and found it much easier to use than the alternatives."

Akamai Guardicore Segmentation was much less complex than building multiple firewalls with different rules for separate applications. "With Akamai Guardicore Segmentation, we have significantly reduced our attack surface with none of the costs and delays associated with upgrading legacy firewalls," says Wigley.

Immediate visibility of suspicious behavior

The deployment of Akamai Guardicore Segmentation enables Daiwa to ringfence a number of its key systems, including business-critical trading and payment platforms. Wigley and his team can now set up policies that either prevent or contain an initial breach. This includes the ability to generate real-time alerts when policy violations are detected and to block attempts to use compromised assets as launch points for attacks into other parts of the network.

"Understanding your exposure and then being able to manage it is key," says Wigley. "The visibility of what is going on in your environment is a huge risk identifier. By monitoring red team activity, we were able to quickly build policies to block common attack vectors."

Enforcing compliance

Akamai helps Daiwa to strengthen its regulatory compliance posture. Segments of the infrastructure containing regulated data can be isolated, compliant usage can be tightly enforced, and audits are greatly simplified.

As for Daiwa's control assurance policies, Akamai Guardicore Segmentation helps provide evidence that the bank's security is operating successfully as changes are made to the system. "We have a source of data that offers a complete picture of our production environment so that we can see where those controls are," says Wigley. For instance, if Akamai Guardicore Segmentation sees a new workstation, Wigley can verify that the bank's endpoint detection response system is installed on the device.

> In all the time that I've worked in IT security, Akamai Guardicore Segmentation is one of the best systems I've ever used. It's highly effective, quick to deploy, and very intuitive.

Dave Wigley
Chief Information Security Officer, Daiwa Capital Markets Europe

An investment for the future

Wigley and his team have been continually impressed by the support from the Akamai team. From providing a comprehensive proof of concept during the tendering process and then deploying the software, the team was there every step of the way. “The Akamai team is extremely responsive when we have day-to-day inquiries. The team that helped us ringfence our systems was extremely knowledgeable about the product and got us up and running quickly.”

Looking to the future, Wigley has complete confidence in the protection of Daiwa’s systems, especially as the business prepares to migrate to the cloud. “In all the time that I’ve worked in IT security, Akamai Guardicore Segmentation is one of the best systems I’ve ever used. It’s highly effective, quick to deploy, and very intuitive. From the latest cybercriminal attacks to new regulation, Guardicore forms a key part of our defense.”

> With Akamai Guardicore Segmentation, we have significantly reduced our attack surface with none of the costs and delays associated with upgrading legacy firewalls.

Dave Wigley
Chief Information Security Officer,
Daiwa Capital Markets Europe

Daiwa Capital Markets

Daiwa Capital Markets Europe Limited is the wholly owned investment banking subsidiary of Daiwa Securities Group Inc., one of the largest brokerage and financial services groups in Japan. Its main business areas include investment banking, equity, fixed income, and global convertible bonds. uk.daiwacm.com