Kaneka Improves Its Security Posture and Protects Direct-to-Internet Traffic with Akamai Enterprise Threat Protector

> *The concept of using DNS as a security measure is both groundbreaking and logical. This is a solution that only a company like Akamai can deliver."*
>
> *– Keiji Fujimoto, Manager of the Business Solutions Group, Kaneka Corporation IoT Solutions Center*

Improving Security Throughout the Entire Group

Kaneka is a comprehensive chemical manufacturer that makes and sells a wide range of materials and products, from chemicals to pharmaceuticals, food, medical equipment, and electronic materials.

With head offices in both Tokyo and Osaka, the company has 3,500 direct employees, and more than 10,000 employees across the group's consolidated workforce.

The company's IoT Solutions Center single-handedly oversees information systems and security for the entire company. Under the leadership of Tetsuro Yabuki, the head of the Business Solutions Group, the Center has been actively pursuing the use of SaaS/PaaS and the centralization of virtualized servers under its "cloud-first" policy, which began when Microsoft 365 was introduced company-wide in 2011. Currently, in addition to about 90% of Windows-based servers being deployed on Microsoft Azure or private cloud environments, a hybrid cloud configuration is also used for business-critical systems infrastructure.

The IoT Solutions Center has been working to solve specific issues while also pushing ahead with their cloud-first IT transformation, with the main issue being improving security across the whole Kaneka Group.

Ease and Speed of Global Deployment

Yabuki explains that, because of a lack of any serious cybersecurity incidents at Kaneka for a long time, they were not too concerned about cyberattacks and generally had little security awareness.

"However, a series of frightening security incidents that occurred in 2017 completely changed that," he continued.

"Although each individual security incident didn't amount to anything serious, the cyber risk became apparent, and the IoT Solutions Center had to single-handedly resolve the issues as quickly as possible. We developed a plan to comprehensively improve Kaneka's security posture, and set out a policy to enhance security governance across the entire Group, including our overseas locations," says Yabuki.

COMPANY

Kaneka Corporation
Tokyo, Japan
https://www.kaneka.co.jp/

INDUSTRY

Chemicals

SOLUTION

Enterprise Threat Protector (ETP)

KEY IMPACTS

- Improved outbound web traffic security globally in two months with a simple DNS change
- Quickly protected branch offices with direct-to-internet connectivity
- Proactively blocked and identified compromised endpoint devices

Kaneka Improves Its Security Posture and Protects Direct-to-Internet Traffic with Akamai Enterprise Threat Protector

Yabuki's comprehensive cybersecurity plan included enhancing its security posture against threats in its outbound and inbound network traffic and against threats that could impact endpoint devices. Having already selected Endpoint Protection Platform (EPP) and Endpoint Detection & Response (EDR) solutions, Kaneka was looking to complement these by adding an additional layer of protection for its outbound traffic. They decided to implement Akamai's Enterprise Threat Protector (ETP) cloud-based security solution as this additional layer of protection.

The Enterprise Threat Protector service blocks malicious traffic using Akamai's extensive real-time threat intelligence, proactively blocking malicious DNS queries simply by redirecting them to the Akamai platform. This preemptively prevents company devices from connecting to malicious websites and C2 servers, greatly reducing the risk of devices being compromised by phishing or malware, which could ultimately lead to the theft of company information. Automatic and continuous updates to the threat intelligence eliminates the need for any manual intervention by administrators.

Keiji Fujimoto, Manager of the Business Solutions Group, which is responsible for overall security measures, talks us through the reasons for adopting Enterprise Threat Protector.

"One of the factors that led us to choose Enterprise Threat Protector was the innovativeness and simplicity of using DNS as a solution to ensure security, which is truly unique. Our thinking was that this is a solution that only Akamai, the world's largest DNS provider, could deliver. We believe this is a groundbreaking cloud security service that expertly leverages Akamai's strengths."

In addition, Fujimoto believes that Enterprise Threat Protector perfectly suited Kaneka's outbound traffic protection requirements.

"The scope of this cybersecurity plan also included unifying security measures across the entire Kaneka Group and enhancing our security governance. The ease and simplicity of introducing Enterprise Threat Protector helped to speed up the deployment of these measures. We were also impressed by Enterprise Threat Protector's ability to block malicious communications, regardless of the structure of our company's network."

Rollout to Overseas Locations Completed in Two Months

Kaneka is already protecting all of its company network's egress points using Enterprise Threat Protector, and has almost completed rolling the solution out to group companies both in Japan and overseas.

The information systems of Kaneka's overseas locations and headquarters are distributed across four regions: North and South Americas, Europe/Africa, Malaysia, and Japan/Asia. With Japan taking the lead on the system for enhancing governance in terms of security, the information security teams representing the other three regions followed Japan to globally deploy Enterprise Threat Protector.

"Cooperating on implementing Enterprise Threat Protector across regions was easy. I say implementing, but all we needed to do was change the recursive DNS query destination. So overseas rollout went smoothly and we were able to complete it in two months," recalls Fujimoto.

Kaneka Improves Its Security Posture and Protects Direct-to-Internet Traffic with Akamai Enterprise Threat Protector

Protection for Direct-to-Internet Connections

For its group companies in Japan, Yabuki and his team visited and gained the cooperation of those companies who were not using the Kaneka data center – which meant that they were running their systems in their separate environments and had separate direct-to-internet egress points.

In addition to rolling out Enterprise Threat Protector to Kaneka itself, they now also use Enterprise Threat Protector to provide protection for outbound traffic from locations that had direct-to-internet connection.

"At Kaneka, although we are currently only allowing direct-to-internet connections at some locations, we needed a way to protect outbound traffic from these locations. I really appreciate the fact that Enterprise Threat Protector has made it so easy for us to do this," says Fujimoto.

Quick Identification of Compromised Devices

With Enterprise Threat Protector now adopted throughout the entire Kaneka Group, and with Kaneka and all of its Group companies now proactively blocking communications to malicious websites and C2 servers from all devices, the IoT Solutions Center is now able to quickly detect and confirm any devices that are making malicious communications. Yabuki says that as a result, the company is able to take immediate action to deal with risky devices in all Kaneka Group companies.

"All it takes is one 'risky device' in the Group to potentially develop into a major problem later on. Being able to identify these kinds of devices across the entire Group with Enterprise Threat Protector has been extremely effective," says Yabuki.

Fujimoto adds that occasionally someone in the organization would start up a device that hadn't been used for a long time, and that device would then be identified as risky.

"These are cases where you can end up using an old device that was infected with malware and outside the control of the Information Systems department without realizing it. When security risks like this become reality, another benefit of using Enterprise Threat Protector is the ability to quickly detect the device, block communications from it and put a stop to it," Yabuki adds.

"Security measures are an essential element of business," Yabuki continues. "That is exactly why we believe we must invest in security in a way that is consistent with the scale of our sales and our reputation. The reason for the sudden occurrence of cybersecurity incidents at Kaneka is likely linked to a significant increase in recognition due to recent promotional activities. The more a company's value increases, it naturally follows that cyber risks also increase. That is why it's important to focus on leveraging innovative technologies like Enterprise Threat Protector while continuing to improve our measures to protect our company value."

Kaneka Improves Its Security Posture and Protects Direct-to-Internet Traffic with Akamai Enterprise Threat Protector

About Kaneka Corporation

The company was established in September 1949 by separating from the Kanegafuchi Spinning Company, Ltd. At its founding, the company was known as Kanegafuchi Kagaku Kogyo Co., Ltd. (changed to the current name in 2004). The company started as a chemical manufacturer with the development of the polyvinyl chloride Kanevinyl. Today, the company offers a wide range of chemicals, functional resins, foamed resins, food products, pharmaceuticals, medical equipment, electronic materials, solar cells, and synthetic fibers. In recent years, the concept of the company making the world healthy has also been used to contribute to the preservation of the global environment, such as by developing the biodegradable polymer PHBH, which is 100% biodegradable in seawater, as well as providing supplement materials such as the reduced form of coenzyme Q10 and manufacturing and selling dairy products such as the product Milk for Bread.

Akamai secures and delivers digital experiences for the world's largest companies. Akamai's intelligent edge platform surrounds everything, from the enterprise to the cloud, so customers and their businesses can be fast, smart, and secure. Top brands globally rely on Akamai to help them realize competitive advantage through agile solutions that extend the power of their multi-cloud architectures. Akamai keeps decisions, apps, and experiences closer to users than anyone – and attacks and threats far away. Akamai's portfolio of edge security, web and mobile performance, enterprise access, and video delivery solutions is supported by unmatched customer service, analytics, and 24/7/365 monitoring. To learn why the world's top brands trust Akamai, visit www.akamai.com, blogs.akamai.com, or @Akamai on Twitter. You can find our global contact information at www.akamai.com/locations. Published 12/20.