FUJIFILM Holdings deploys Verizon's Advanced Security Operations Centre.

Case Study

Fuji Photo Film Co., Ltd. (now FUJIFILM Holdings Corporation) was founded in 1934, during the emergence of the domestic photo film production industry in Japan. The company initially produced photographic sensitised materials including photo film and photographic paper. Later, it cultivated proprietary technology that would eventually become the foundation of its four new business domains: Healthcare, Materials, Business Innovation, and Imaging.

In 2021, the Fujifilm Group laid out its digital transformation (DX) vision to reinforce its commitment to digital transformation. The vision states that by further driving DX, Fujifilm will dramatically increase the value it provides to customers through products and service innovation, and by addressing social issues.

The Fujifilm Group's challenge and its impact.

The Fujifilm Group does business across the globe, with 280 consolidated subsidiaries worldwide. As each business unit builds and operates its own security system according to its needs, there were no uniform, groupwide protective measures. As a result, Fujifilm has been unable to promptly respond to security incidents. It needed to efficiently detect complex attacks and identify malicious breaches disguised as regular communications.

The FUJIFILM Holdings ICT Strategy Division formulates, implements and governs the company-wide ICT strategy, devising fundamental countermeasures to improve the level of security across the group. Kentaro Watanabe, the ICT Division's general manager and head of the infrastructure security group, said, "Fujifilm's aim is to remain a company that contributes to societal solutions. As a global provider of products and services that benefit society, responding to cyberattacks is a critical business issue we must address in every region."

To adapt to diverse remote working arrangements in a changing IT landscape, the company must monitor various systems in external cloud environments, beyond on-premises devices. This requires Fujifilm to shift from its conventional infrastructure-centric monitoring to monitoring of systems within each business unit.

Hackers have been adapting their cyberattack methods at an alarming rate in recent years. This shift requires the Fujifilm Group's cybersecurity strategy to adjust from a conventional approach of entry and exit point counterattacks, to understanding the traits of more sophisticated, targeted attacks and developing increasingly advanced preventive measures.

However, just as Fujifilm recognised its level of security monitoring was not sufficient and began to strengthen security, unauthorised external access to the company's servers occurred, forcing it to temporarily shut down its potentially affected servers, PCs, and networks.

Mr. Watanabe said, "With cyberattacks becoming more sophisticated and cunning, it was clear to us we needed to step up our preparations."

"Fujifilm's aim is to remain a company that contributes to societal solutions. As a global provider of products and services that benefit society, responding to cyberattacks is a critical business issue we must address in every region."

Kentaro Watanabe, General Manager,
FUJIFILM Holdings ICT Strategy Division

verizon business

Members of FUJIFILM project, from left: Kaori Tajima; Masaru Takahashi; Kentaro Watanabe; Kazuyoshi Mochizuki; Ryosuke Kurio.

Verizon's role in solutions for the Fujifilm Group.

FUJIFILM Holdings explored Verizon's Advanced Security Operations Center (SOC) Services. Verizon has nine SOCs and six forensics labs around the globe that handle over 27 trillion security events a year through one of the world's largest IP networks.

FUJIFILM Holdings asked Verizon to produce a scenario to determine whether the SOC could detect a security event of the same magnitude as the one Fujifilm had experienced.

Mr. Watanabe said, "Our first priority was to be able to respond to emergencies 24/7 worldwide, and our second was to be able to statistically identify and analyse suspicious behavior with security information and event management (SIEM), to promptly detect and respond to sophisticated cyberattacks. We needed a partner company that could provide us with the right technical advice and guide us toward stronger action on cybersecurity."

Using a wealth of threat information to identify attacker traits, and providing security analysis by a highly skilled team, Verizon has worked with the Fujifilm Group to monitor events, warn of emerging threats, and provide customisable services and improvements.

Business outcomes and benefits of working with Verizon's SOC.

Verizon's support has vastly strengthened the Fujifilm Group's cybersecurity monitoring and intelligence, enabling more precise monitoring worldwide.

ICT Strategy Division Manager and the infrastructure security group's security team leader, Kazuyoshi Mochizuki, explained, "We've tended to focus our surveillance on Japan, so executing the same surveillance for overseas offices was an issue – particularly as we partner with businesses and networks worldwide."

He added, "Fujifilm has four regional headquarters in addition to Tokyo – in America, the EU, the Asia-Pacific,

"We've tended to focus our surveillance on Japan, so executing the same surveillance for overseas offices was an issue."

Kazuyoshi Mochizuki, Division Manager and security team leader, FUJIFILM Holdings ICT Strategy Division

and China – each of which manage many other connected companies and offices. Our partnership with Verizon will allow each region to collect the logs saved on subsidiary companies' systems so we can do a better job responding and collaborating between regions."

The partnership with Verizon also allows FUJIFILM Holdings to detect incidents that its previously used surveillance method, which relied on pattern-matching security software, could not.

"We would previously only notice a problem after an incident had occurred, but as we can now monitor security logs with the SOC and a SIEM platform, we can identify suspicious behavior in advance."

Ryosuke Kurio, Division Manager and infrastructure security team member, FUJIFILM Holdings ICT Strategy Division

Using Verizon's SOC has allowed Fujifilm to promptly put an end to incidents that could become threats if left alone.

Kaori Tajima, manager of the information security and technology division at FUJIFILM Systems, is involved in monitoring incidents at the Fujifilm Group and the collaboration with the Verizon SOC. She said, "By working with Verizon's SOC to perform efficient, 24/7 surveillance worldwide, we have expanded the number of overseas locations we can monitor, and we can execute effective, centralised surveillance."

Masaru Takahashi, who also works on surveillance at the FUJIFILM Systems information security and technology division, added, "We have a variety of servers and security devices around the world and a large quantity of logs that are not in a uniform format, but Verizon's expert advice on gathering threat information and their knowledge on security monitoring has enabled us to perform better-suited, more advanced surveillance."

Working with Verizon's SOC to promptly detect potential security incidents has accelerated the Fujifilm Group's plan to create a FUJIFILM SOC, which the company is working to establish for the era of zero trust security.

verizon business