deep instinct™

CASE STUDY
RETAIL

Yamada Holdings selects Deep Instinct to prevent malware

>99%
ZERO DAY ACCURACY

50%
REDUCTION IN OPERATIONAL LOAD

OPERATE IN-HOUSE WITH SMALL IT TEAM

The Company

Yamada Holdings, Japan's largest electronics retailer, operates more than 1,000 stores in 47 prefectures around the country.

Industry: Retail

Company size: Enterprise

Existing Security Solution: Antivirus

The Need: Shift from damage control to a prevention-first technology approach

When people shop at Yamada's stores, they expect to see the latest mobile phones, gaming consoles, home appliances, and other consumer electronics. Knowledgeable store associates are ready to answer customers' questions and provide recommendations. At headquarters, employees work diligently to deliver on the company's "total-living" business strategy.

Neither shoppers nor employees give a second thought to ransomware or other malware aimed at point-of-sale systems, mobile phones, tablets or other devices.

That's because Yamada Holding takes a prevention-first approach to cybersecurity, which allows employees to work safely and conveniently, while putting the customer first. Proactive cybersecurity measures work in the background to protect the retailer's stores and offices and maintain data privacy at the highest levels.

Yamada has long relied on antivirus software to protect point-of-sale systems and other endpoints, but as cyber threats rose, the work of keeping antivirus signatures up-to-date became increasingly time-consuming and cumbersome. The antivirus software also slowed down users' systems, impacting their experience.

"The goal is to stop all malware and ransomware to protect our business while allowing employees to concentrate on their tasks," says Kenji Totsuka, Manager, System Development Department, IT Business Division, Yamada Holdings.

Yamada wanted a next-generation endpoint security solution that would prevent advanced threats and was operationally efficient. It was essential that Yamada's IT Business Division could operate the solution in-house. The IT staff considered a variety of endpoint detection and response (EDR) products, but in many cases, the EDR solutions were so complex that outside assistance was required.

"EDR products are based on the concept of investigating and responding to intrusions after they've been detected, so we have to take some kind of action after detection, which requires specialized knowledge," says Mr. Totsuka. "We wondered if we, as a small group, would be able to use a product that required such support."

The Solution: Stop responding and start preventing malware

Deep Instinct, with the world's first and only purpose-built, deep learning cybersecurity framework, allowed Yamada to prevent threats before they could ever enter the environment. Rather than use a solution that would potentially allow a threat to enter and then respond and remediate, Yamada chose a solution that stops threats from the outset.

Yamada is deploying Deep Instinct to protect 15,000 clients at its headquarters and stores. Once the initial rollout is complete, Yamada plans to deploy Deep Instinct at its subsidiary businesses.

"Deep Instinct was intuitive and could be used immediately without anyone having to teach it to us," says Mr. Totsuka. "We also appreciated the direction of Deep Instinct, which is not damage control like EDR, but prevention-first."

Deep Instinct's deep neural network brain prevents cyberthreats by learning to stop them instinctively without human involvement. With cyberthreats automatically detected and prevented, no action from employees or IT staff is required.

Deep Instinct gets smarter on its own, stopping known, unknown, and zero-day threats with better accuracy and speed than other endpoint protection or legacy AV solutions. Deep Instinct delivers greater than 99% unknown threat accuracy with less than 0.1% false positives. Every file, script, and macro is scanned pre-execution to stop threats in less than 20 milliseconds.

The Results

Prevent malware before it detonates

Deep Instinct doesn't wait until an attack is in motion. It harnesses the power of deep learning to stop known, unknown and zero-day attacks before they execute.

A prevention-first approach to malware enables Yamada to lower risk as well as maintain compliance with Japan's Personal Information Protection Law and the country's Information Security Management System (ISMS) framework.

Deep Instinct ensures the integrity of custom applications and shields against malicious file downloads.

As an innovator, Yamada develops many of its applications. "We wanted to avoid EDR products that had over-detections in our unique environment, which has a lot of EXE and DLL files for our in-house developed applications," says Mr. Totsuka.

Always-on prevention

Yamada's previous antivirus solution left a security gap especially critical in today's era of remote work. When employees traveled and their laptops were not connected to the corporate network, the antivirus definition files would not be updated, putting the company at risk of zero-day attacks.

Yamada closed that gap with Deep Instinct. Frequent cloud checks and agent updates are unnecessary. Yamada's endpoints are always protected with the latest security without requiring the device to be connected to the cloud. Even a Deep Instinct brain that is six months old – or older – will stop known, unknown and zero-day threats with better accuracy and speed than other endpoint protection products.

Increase security operations efficiency

Yamada's previous antivirus required constant maintenance, with definition files updated every day, disrupting the end-user experience and increasing the security operations center (SOC) workload.

Because Deep Instinct prevents malware and significantly lowers false positives, there are fewer security events for the SOC to investigate. When high-fidelity events do occur, the SOC has more resources available to respond with immediacy.

As a result, Yamada has seen a significant reduction in IT operational work. "The operational load has been reduced to less than half," says Yuichiro Harada, Vice President, System Operation Department, IT Business Division, Yamada Holdings.

"Deep Instinct has made a great contribution to Yamada that operating costs have remained almost the same while the security level has improved," says Mr. Harada.

> *"Deep Instinct allows us to take a prevention-first approach to cybersecurity, protecting our endpoints while allowing us to operate easily and at an efficient operating cost."*
>
> ***– Yuichiro Harada, Vice President, System Operation Department, IT Business Division, Yamada Holdings***

Request an online demonstration of the Deep Instinct Platform

See how Deep Instinct can help protect your organization in this live demonstration of our solution capabilities against unknown threats.

REQUEST A DEMO

deep instinct

www.deepinstinct.com | info@deepinstinct.com

Deep Instinct takes a prevention-first approach to stopping ransomware and other malware using the world's first and only purpose built, deep learning cybersecurity framework. We predict and prevent known, unknown, and zero-day threats in <20 milliseconds, 750X faster than the fastest ransomware can encrypt. Deep Instinct has >99% zero-day accuracy and promises a <0.1% false positive rate. The Deep Instinct Prevention Platform is an essential addition to every security stack—providing complete, multi-layered protection against threats across hybrid environments.