Leading Auto Parts Distributor Takes Cybersecurity to the Next Level with FFRI yarai

Profile

Customer	DENSO Products and Services North America
Industry	Automotive Service
Country	United States

When security professionals at a large auto parts distributor saw ransomware and other malware on partner networks, they asked cybersecurity vendor FFRI about ways to better protect their business.

FFRI's yarai endpoint protection product, using machine learning and advanced algorithm, promised to flag malware for the company before those attacks were made public. In six months of testing, FFRI yarai delivered as advertised for DENSO Products and Services North America, a subsidiary of a Japanese auto parts vendor.

"DENSO North America was already using a well-known antivirus vendor, but it didn't protect against new malware," said Emerson Stamps, manager of network systems, DENSO.

DENSO's antivirus product was "not detecting the zero-day malware, especially the ransomware payloads that were out there, the leaks that come in unsolicited email," he said. "We saw that needed another level of defense from the standard enterprise package of antimalware we were using."

DENSO began exploring another level of defense after the company observed malware attacks on customer and vendor networks. Several incidents "happened close to home," Stamps said.

The company saw malware on partner networks that "some of our people in the field connect to," he added. "We said, 'We can't risk having something like that detonate on our network.'"

"DENSO ran a series of tests on a walled-off LAN, and a version of FFRI yarai tweaked for the company's needs killed every piece of malware testers could throw at it," Stamps added. "We were able to thwart randomly downloaded malware from the internet, and FFRI yarai stopped all of the ransomware. No payloads ever detonated."

FFRI yarai uses a heuristics component to conduct specialized behavioral analysis for each customer. The product "stopped everything from taking over the hard drive and encrypting the data," Stamps said. "It didn't happen. That was the signal to us: 'This is at a place where we seriously need to look at procuring this product.'"

Stamps continued, "As of September 2017, DENSO North America had been using FFRI yarai for about a year, and the product continues to keep the company safe from ransomware and other malware."

FFRI yarai's precognitive defense often blocks malware many months before it is publicly disclosed. For example, the endpoint protection product detected the Adylkuzz cryptocurrency mining malware in October 2016, well before the May 2017 public disclosure. FFRI yarai detected the PETYA ransomware in July 2015, eight months before it was made public.

FFRI yarai has prevented more than 100 zero-day attacks before they were publicly disclosed, according to FFRI. The product uses five specialized malware detection engines to identify and quarantine advanced cyberthreats.

FFRI yarai is designed to stop "heavily targeted attacks," such as code trigger point injections and phishing attacks, said Pablo Garcia, CEO of FFRI North America. "We're focused on stuff that maybe hasn't been seen or discovered yet in the wild."

As DENSO was putting FFRI yarai through the paces, the company tested other cybersecurity products as well. "We had some recommendations to look at some other products, and they were just woefully inadequate," Stamps said. "FFRI yarai was a superior product; it was like, 'Ok, this is exactly what we need.'"

The ability of yarai to stop ransomware and other malware in its tracks was a major selling point for DENSO, but it was not the only one. The ease of installation was also an important feature.

"FFRI yarai sits at network endpoints – PCs, laptops, and smartphones – making it simple to install without interrupting the underlying network. DENSO wasn't looking for an expensive total enterprise product, and the company didn't want to spend months on deployment. FFRI yarai, as an endpoint product, offered a quick installation process at an attractive price," Stamps stated. "Defense at the enterprise level can get expensive. There's an exponential learning curve."

But the FFRI product was "something we did not need to tweak our infrastructure for," he added. "We did not have to interrupt our business or have down time in order to implement the product."

"We had some recommendations to look at some other products, and they were just woefully inadequate, FFRI yarai was a superior product; it was like, 'Ok, this is exactly what we need.'"

Emerson Stamps, manager of network systems, DENSO

Yarai

And FFRI yarai played nice with DENSO's existing cybersecurity protections. "It worked well with our current setup, it worked well with our current antivirus product," Stamps said. "It didn't step on any toes."

"FFRI yarai is designed to easily co-exist with legacy, signature-based antivirus products," said Garcia. "Those signature-based antivirus tools obviously still have value as part of a multilayered security plan."

FFRI made a full version of FFRI yarai available while DENSO was testing the product, and DENSO network admins found the product's management console "very intuitive," Stamps said. "It was an easy flow."

FFRI yarai has allowed DENSO to refocus its network security team. Before installing FFRI yarai, two DENSO employees were spending 20 to 25 hours a week identifying malware, blocking rogue websites, and updating the company's antivirus policies. Since adopting FFRI yarai, one employee is now spending about four hours a week checking the product's management console.

"FFRI yarai has helped DENSO put its network security employees to a higher purpose because the product is proactive," Stamps said. "Now the time is spent investigating instead of defending."

"DENSO has new assurances that it is protected from malware," he added. "We can dedicate our time to the things we need to do as far as network infrastructure, versus fighting an uphill battle gradually trying to defeat malware."

"The extra level of malware detection provides DENSO's network security team peace of mind," Stamps continued. "FFRI yarai gives us a countermeasure if someone clicks on something they shouldn't. We get a report on it, and then we can remediate it."

"FFRI yarai is a major step for us in securing the network at the endpoint level," he added. "That's really a great comfort level for us."

"Now the time is spent investigating instead of defending."

View all FFRI yarai case studies at www.ffri-inc.com

FFRI North America, Inc.
65 Enterprise, Aliso Viejo, CA,92656
Sales@ffri-inc.com