SentinelOne

CUSTOMER CASE STUDY

Major Financial Technology Company Gains Protection, Value, and Confidence with SentinelOne

Challenges

- Deploy endpoint security in Amazon Linux environment
- Detect advanced malware and targeted attacks across all endpoints
- Preserve endpoint processing performance

Solution

SentinelOne Endpoint Protection Platform

Key Benefits

- Improved threat detection significantly
- Extended protection across all endpoints, including workstations, databases, and application servers
- Eliminated endpoint downtime and processing latency

Autonomous protection and API-enabled automation eliminate need for manual intervention

The Challenge—Finding Endpoint Protection for the Long Haul

This rapidly growing high-profile financial technology company has thousands of workstations, database servers, and application servers to protect and finite security resources. When its antivirus began to consume more and more of the security team's time, they began searching for a replacement and had a long list of criteria.

"We're a cloud-first company and we prefer the vendor to host the console," said the Cyber Security Architect. "As we began to evaluate vendors and products, we knew that the new product had to be cloud-based. We organized our criteria and researched vendors in the endpoint security space before narrowing our POC to 5 potential solutions."

The team's criteria included data leak protection, firewalling, application control, device control, sandboxing, web reputation filtering, IDS/IPS, updates and maintenance, management console, reporting, CPU consumption, SIEM integration, technical support, and scalability. They created a scorecard and rated vendors on a weighted scale, letting the results speak for themselves.

Cyber Security Engineer

"Having an autonomous solution is a huge benefit. SentinelOne tells us how many agents we have, how many threats it found, and how many it has removed—all without our intervention. It's indispensable."

"We created 1,200 pieces of our own malware and threw them at all of the systems," said the Cyber Security Engineer. "That way, we knew we would be submitting samples that were not known by the usual threat databases. We initially tested all products offline to identify each one's effectiveness."

The team compared their existing vendor, Trend Micro, with BitDefender, Cylance, F-Secure, and SentinelOne. The results were completely unexpected.

"Based off marketing, we expected Cylance to win our tests," said the Cyber Security Architect. "But it performed poorly in the offline tests and had 12 to 15 percent lower detection rates than SentinelOne. SentinelOne ranked head and shoulders above all other competitors."

Starting with Workstations, Expanding to Amazon Linux

The company deployed SentinelOne on its workstations quickly and easily. Next, the security team wanted to deploy endpoint protection to servers in its Amazon Linux environment. As the team worked to deploy Trend Micro agents to its database and application servers, they began experiencing downtime and significant processing latency. Database access and processing is crucial to the company's operation, and downtime became so frequent that business users' work was affected.

"We lost two security professionals due to their frustration with Trend Micro and deployment failures," said the Cyber Security Architect. "Not being able to protect our databases is a big problem, so we decided to look for another solution."

Although the company's Linux servers had not been part of the original endpoint security POC, the team decided to try SentinelOne in its Amazon Linux environment. They were able to install it, and with a little help from SentinelOne, were able to extend SentinelOne protection to their entire environment.

Autonomous Protection

SentinelOne now protects over 8,000 endpoints with no intervention needed by the security team. They can easily generate reports and metrics to demonstrate the solution's value to the business.

Augmenting Staff Through Automation

"I really appreciate SentinelOne's APIs," said the Cyber Security Architect. "Like most security teams, we're stretched, so anything we can automate helps make our team more successful. The API is well developed and enables us to build automated processes. We can orchestrate response to threats, which is a powerful capability."

The company's team also is pleased that feature requests are implemented and delivered rapidly by SentinelOne.

"During our POC, when we asked other vendors about their future API plans, their answers were not satisfactory," said the Cyber Security Architect. "SentinelOne on the other hand, had robust APIs for all its functions. SentinelOne gives us more bang for our buck capabilities —not to mention confidence in their future."