Iconic Cosmetics Manufacturer Replaces McAfee Antivirus with SentinelOne EPP

Endpoint Protection Platform Enhances Global Security Posture with Behavioral Threat Detection and Full-Context Forensics

We recently caught up with the head of the security engineering team at one of our most iconic customers to talk about his SentinelOne experience. Since this interview reveals details of the security environment of a well-known global manufacturer with over $3B in annual revenues, he requested that we not mention his company's name. This established corporation replaced its entire McAfee antivirus installation (roughly 3,000 endpoints) with the SentinelOne Endpoint Protection Platform (EPP). The static AV-based solution that the company had been relying upon for more than a decade was not able to block all of the spear-phishing and other more sophisticated cyber attacks targeting the company's user endpoints. Even when an attack was successfully detected, the security team had no means of seeing where the attack first landed, or if it had spread laterally to other endpoint devices or parts of the IT infrastructure.

SentinelOne has made real-time unified endpoint protection a reality for this organization. EPP's behavior-based threat detection has proven highly effective in preventing sophisticated attacks across all major vectors, most notably the ransomware variant 'cryptolocker'. This dramatically better prevention has slashed the number of hours previously spent re-imaging 8-10 infected laptops each week. SentinelOne EPP's integrated mitigation and remediation capabilities have enabled the company to easily roll back affected files to trusted states, thus preserving user up-time. And finally, the company's security team has armed itself with SentinelOne EPP's full-context forensics, providing complete visibility into the activity on all protected endpoint devices.

GLOBAL COSMETICS COMPANY

- 3,000+ endpoints
- 7 data centers, worldwide (5,000 Windows- and Linux-based servers)
- Previous endpoint protection solution: McAfee Antivirus
- Faces regular ransomware attacks that McAfee Antivirus doesn't prevent
- Almost 100 hours per week spent re-imaging infected laptops
- Replaced McAfee AV with SentinelOne EPP

WITH SENTINELONE EPP:

- The organization is protected from exploits and live attacks, in addition to malware
- PCI and corporate compliance is satisfied
- The number of weekly laptop infections has been dramatically reduced
- Full attack context is available in real-time via SentinelOne EPP forensics
- Detected threats are fully mitigated at machine speed

Q. Can you tell me a little about your company and your IT organization?

A. I manage a team of security engineers focused on desktop, server, application, and network security. We are responsible for every aspect of security, including the evaluation of new technologies to see how they will impact our network, servers, endpoints, and users from a holistic security perspective. We work closely with our compliance and risk teams to make sure everything is PCI and corporate compliant. We have roughly 3000-3500 endpoint desktops and laptops, 99% of those are Windows-based, 150 Macs, and 5000 servers, predominantly running Windows Server 2008. We also have a growing UNIX base. From the endpoint protection standpoint, we were running McAfee antivirus.

Q. What ultimately prompted you to start looking around for a new endpoint protection solution?

A. Our endpoint machines were being compromised on a regular basis. We were getting 8 to 10 alerts a week, and each compromised machine required more than 8 hours to reimage. Obviously, our existing AV solution wasn't catching many of the malware attacks headed our way. We were seeing a lot of cryptowall and ransomware variants. Our biggest attack vector is phishing emails, where emails come in and users click on a link that would either compromise their machine or reach out to the Internet and try to pull down malicious software.

We didn't have the forensic capabilities to see where and how the endpoints were getting compromised. When one machine was attacked, we couldn't tell if it had spread to another machine or our shared files until we saw indicators of compromise from those systems. So we started looking around to try and find the next-generation of endpoint protection. We needed better protection--not just from malware, but from other sophisticated types of attacks that don't always involve an executable file. We knew we needed the forensic capabilities that McAfee wasn't providing.

Q. What solutions did you look at?

A. We looked at several next-generation endpoint protection solutions. One had a really bad setup process. The vendor sent us a machine, but the management console didn't work so they sent us a new one. Once we finally got it working, 7 out of 10 laptops we loaded it on immediately blue-screened so we stopped the POC. Since we couldn't get it running on the desktops, we knew there was no way we would put it on our servers. That's when we turned to SentinelOne.

> "The things that stood out for us were the forensic capabilities and the ability to stop multiple different types of attacks from happening."
>
> —Joe Miller, *Security Engineering Team Lead*

Q. Can you tell us about your SentinelOne Proof of Concept?

A. SentinelOne came gave us a demo of their Endpoint Protection Platform, and we fell in love from that point on. The things that stood out for us were the forensic capabilities and the ability to stop multiple different types of attacks from happening. With EPP, we can configure remediation to automatically kill, quarantine, or just alert us when a device gets infected. We can also remove the device from the network, shut the NIC down, or just power down the device in case a desktop is locked and we can't get network support on the phone in time to shut the network down. We can do it ourselves and keep it from spreading throughout the network to other desktops or production servers. After the demo, we deployed the EPP agent on to our IT team's laptops and desktops to make sure we didn't see a performance hit. It ran beautifully.

Since we were constantly getting phishing attacks, we decided to keep the malware that was coming in and load it onto different machines to see how it would react, testing out its alerting capabilities. We got exactly what we wanted with SentinelOne EPP--the forensic and mitigation capabilities, and the ability to easily rollback our systems. The side-by-side comparison against McAfee enabled us to sell the idea of adopting SentinelOne to our executives.

Q. How is the global rollout of SentinelOne EPP progressing?

A. We have already deployed EPP across the majority of our user endpoints. We went from several infected machines a day, to just a few per week, and we are confident that when we get it fully rolled out that number will be cut back even more. After we finish the US rollout, we will start on our Latin America endpoints. We are also planning to start a POC for our servers with the intention of rolling out SentinelOne's data center protection solution across our server environment in 2017.

Q. Given your experience doing a complete rip and replace of your legacy antivirus solution, what is your advice to other similarly-sized organizations looking to do the same?

A. Initially, we had planned on augmenting our McAfee AV solution with SentinelOne EPP's advanced protection capabilities. But when SentinelOne got certified as an AV replacement by AV-Test, we decided to do a total replacement. In today's threat environment, you're fooling yourself if you think antivirus is going to block every attack headed your way. Seeing that malware and other attacks can easily get by AV, you need endpoint protection that uses behavior-based detection instead of signatures. The results don't lie--you can show your IT management on the spot how SentinelOne EPP blocks threats that AV has no chance of detecting. You also need to think about the benefits of having complete forensics available in real-time, and the ability to automatically respond when threats are detected. You will save a lot of valuable time with capabilities like these, and you get all of this functionality and more with SentinelOne EPP.

"In today's threat environment, you're fooling yourself if you think antivirus is going to block every attack headed your way. Seeing that malware and other attacks can easily get by AV, you need endpoint protection that uses behavior-based detection instead of signatures."

—Joe Miller, *Security Engineering Team Lead*

SentinelOne

2513 E. Charleston Rd., Suite 100
Palo Alto, CA, 94043
Phone: (855) 868 3733
www.sentinelone.com/contact