SentinelOne

SAMSUNG SDS

Reinforced Proactive Endpoint Security with AI-based SentinelOne Endpoint Protection Platform

The Evolution of Cyber Attacks that Bypass Network Boundaries Calls for Greater Endpoint Security Measures

Samsung SDS has recognized the need to strengthen endpoint security as cyberattack techniques that bypass network boundary security are becoming more sophisticated. Therefore, the company is responding to the changing environment by analyzing IPs and URLs of the entire network to block routes, and by analyzing malicious files in sandbox through signature-based network security equipment operation. However, these measures proved to be less than ideal for responding to the latest fileless malware and ransomware attacks that bypass existing security devices, and hence a completely new solution was considered.

According to a Samsung SDS official, the company tested and verified various global Endpoint Detection and Response (EDR) solutions to strengthen endpoint security from these various network boundary bypass techniques, and decided to adopt SentinelOne EPP which showed the best performance among all solutions.

	Countermeasures	Security Solutions	Bypass Techniques
Route Blocking	✓ Origin/destination analysis ✓ IP, URL, URI, etc.	• Firewall • Proxy	One-time Address
Packet Analysis	✓ Communication packet analysis ✓ NW signature analysis	• IDS/IPS • WAF	Communication Encryption
File Analysis	✓ Packet combination → File creation ✓ Check for malicious files	• Sandbox	Anti-VM

He explained that the company is building an AI-based autonomous cyber security platform to defend against exploitation of zero-day vulnerabilities, malware, ransomware, and new attacks that could not be solved even with existing signature-based anti-virus software, and is developing a distributor business for the solution.

CHALLENGES

+ Telecommuting, cloud, smart work environment, etc. Greater need for security in an open environment
+ AI-based endpoint security system required to respond to automated variant malware
+ Endpoint security needs to be strengthened to respond to the evolution of cyberattacks that bypass network boundaries

> “
>
> SentinelOne provides an amazing set of features that autonomously and completely handles all malware and ransomware in verification tests for adoption review...
>
> SAMSUNG SDS OFFICIAL

SentinelOne

Blocking the Latest Endpoint Security Threats with AI-Based Security Analysis Technology

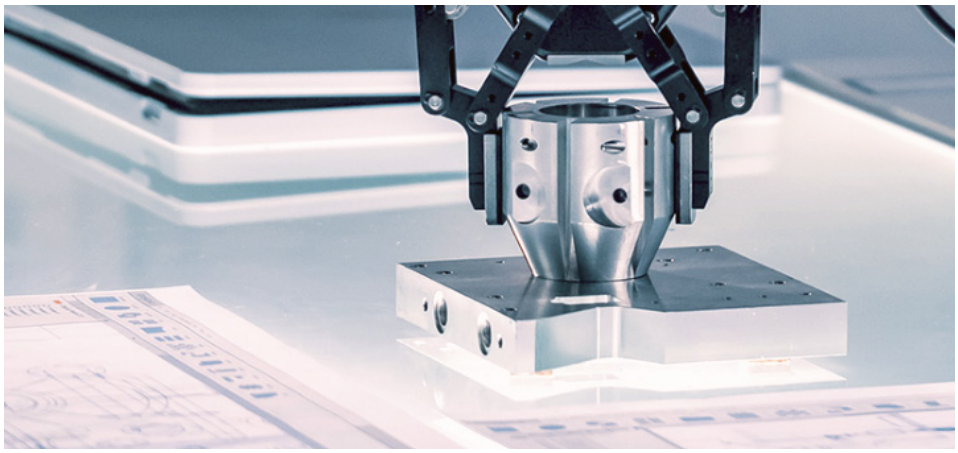
SentinelOne EPP not only prevents and blocks new and variant malware and hacking attacks based on a patented AI machine learning model but also provides a function to automatically restore after infection from the latest ransomware attacks. SentinelOne EPP features a static AI analysis function that analyzes header information without executing the file and a behavior analysis AI analysis function that analyzes malicious actions in real time, logging all activities within the endpoint and reporting anomalies through the 'deep visibility' intelligent detection technology. In addition, it has a patented restoration technology not featured by any of the competitors that can automatically disconnect endpoints if necessary, disconnect them from the network, and return to a pre-infection state.

"SentinelOne provides an amazing set of features that autonomously and completely handles all malware and ransomware in verification tests for adoption review," the Samsung SDS official said. "In particular, the SentinelOne solution greatly increases the productivity of administrators because it autonomously builds a perfect security environment from prevention to action by simply installing it like conventional antivirus software," he added.

Single-Agent Design Minimizes Resource Impact and Operating Costs

For complete security of endpoint devices, SentinelOne EPP detects threat patterns and blocks threats immediately, collects, investigates, analyzes, and automatically blocks and responds to security threats with only one agent. It automatically and safely blocks threats without the user having to worry about security management, and minimizes the impact of endpoint device resources despite having various analysis functions.

Furthermore, SentinelOne EPP provides a cohesive view of the entire network in any environment with endpoint protection and endpoint detection and response. SentinelOne EPP supports more than ten endpoint device types including Linux and Apple Mac OS in addition to all Windows versions, meeting essentially all enterprise needs. The solution establishes an integrated operating system, checks all threat events and response results on a single, integrated screen, and can immediately identify the cause of an incident and respond with countermeasures against breaches and threats.



> "
>
> The SentinelOne solution greatly increases the productivity of administrators because it autonomously builds a perfect security environment from prevention to action by simply installing it like conventional antivirus software.
>
> SAMSUNG SDS OFFICIAL

> "
>
> SentinelOne tracks, analyzes, and monitors in real time from the beginning to the end of an attack to not only block current attacks, but also respond to new and variant attacks that may occur in the future.
>
> SAMSUNG SDS OFFICIAL

> "
>
> It is an optimal security solution that records all attack behaviors that have occurred, and can respond appropriately when other attacks occur compared to previously detected attack types.
>
> SAMSUNG SDS OFFICIAL

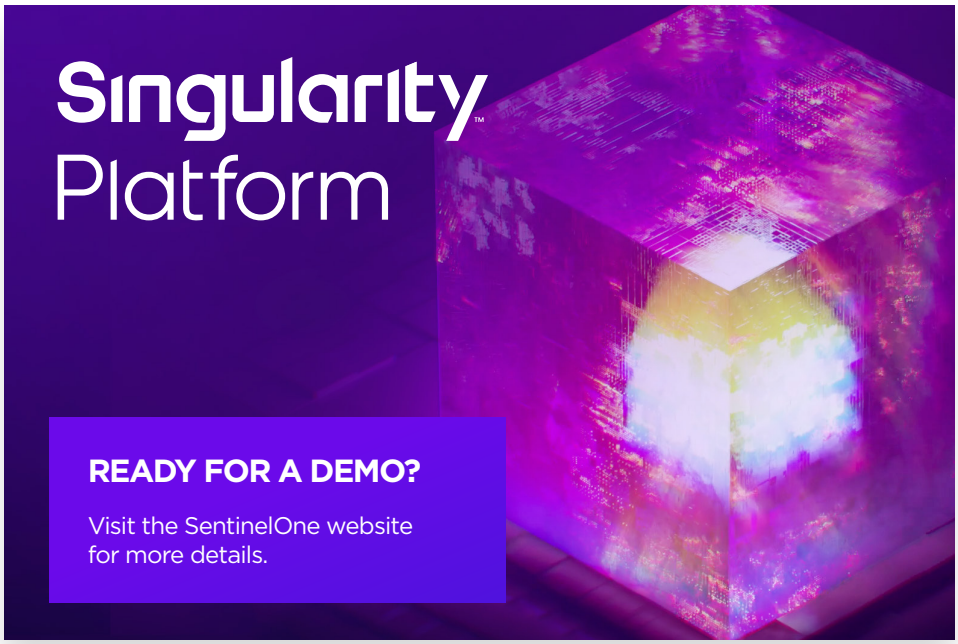
SentinelOne

Complete Defense Against All Attacks at Every Stage from the Latest Security Threats

"We need to visualize the cyberattack on all assets of the company and prepare counter-measures for the overall attack, including before, during, and after the attack," the Samsung SDS official said. "SentinelOne tracks, analyzes, and monitors in real time from the beginning to the end of an attack to not only block current attacks, but also respond to new and variant attacks that may occur in the future. It is an optimal security solution that records all attack behaviors that have occurred, and can respond appropriately when other attacks occur compared to previously detected attack types," he emphasized.

About Samsung SDS

Samsung SDS was established in 1985 as a company to meet Samsung's all ICT needs. Over the last three decades, it has been leading the digital transformation of its customers in various industries and have now grown into an IT solution provider providing services to over 30 countries around the world. Samsung SDS makes the most innovative leap forward for customers in various business areas such as manufacturing, finance, logistics, and retail based on enterprise solutions that innovate productivity and IT technologies such as AI, cloud, block chain, and security that lead the 4th industrial revolution.



SOLUTION

+ SentinelOne Endpoint Protection Platform

BENEFITS

+ Comprehensive protection and response to all malicious security threats, including malware, ransomware, and zero-day attacks
+ Building a fully automated policy-based response system with AI-based detection technology that covers from the attack phase to the countermeasure phase
+ Simplifying security management with minimal impact to end users

"

SentinelOne EPP solution is the best security solution that can fully analyze every stage of an attack and defend against the latest threats with unique AI-based intelligent security technology in real time.

Nam Seung-hyun

IT SECURITY EXPERT,
SAMSUNG SDS

About SentinelOne

More Capability. Less Complexity. SentinelOne is pioneering the future of cybersecurity with autonomous, distributed endpoint intelligence aimed at simplifying the security stack without forgoing enterprise capabilities. Our technology is designed to scale people with automation and frictionless threat resolution. Are you ready?

sentinelone.com

sales@sentinelone.com

© SentinelOne 2021