SentinelOne™

Deep Visibility

Regain Visibility Over Your Network and Assets

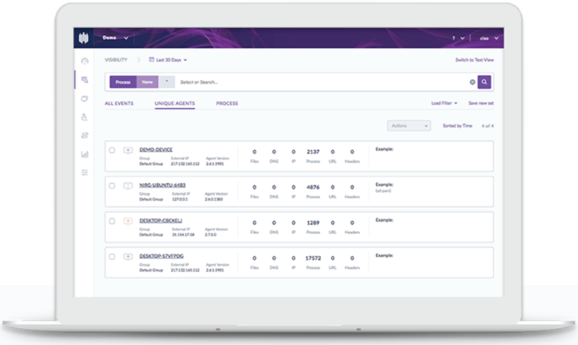
Datasheet

Executive Summary

You cannot stop what you cannot see. SentinelOne extends its Endpoint Protection Platform (EPP) to offer the ability to search for attack indicators, investigate existing incidents, perform file integrity monitoring and root out hidden threats. Deep Visibility supports the needs of Enterprise IT and provides visibility into encrypted traffic. This unique solution helps security teams gain comprehensive insight into all endpoints so that responses can be prioritized and efficient without highly trained personnel or outsourcing EDR needs. This is accomplished through a streamlined interface that allows you to automate and connect it to other products on your portfolio. Deep Visibility does not require additional installation and is already integrated into SentinelOne's single agent architecture.

Enterprise Need

Enterprise networks are more complicated than ever before. The explosion of cloud applications, coupled with the ability of users being able to access these cloud / SaaS applications from anywhere and any device, means the traditional network perimeter has disappeared. Keeping your business safe in today's world means protecting your corporate data, and this means protecting your endpoint devices. A data breach happens in milliseconds, but it may take months to recognise that a breach has even occurred. To make matters worse, most web traffic today is encrypted, providing a simple trick for attackers to hide their threats and communications channels. The endpoint is the most vulnerable and exposed attack surface in the network today. In order to keep your endpoint devices safe, you need to have deep visibility into their environment and activities.



Agent	Group	External IP	Agent Version	Files	DNS	IP	Process	URL	Headers	
DEMO-DEVICE	Default Group	217.132.165.112	2.6.1.5901	0	0	0	2137	0	0	Example:
NIRG-UBUNTU-6483	Default Group	127.0.0.1	2.6.0.1383	0	0	0	4876	0	0	Example: (sd-pam)
DESKTOP-CBCKELJ	Default Group	31.154.17.58	2.7.0.0	0	0	0	1289	0	0	Example:
DESKTOP-S7VFPDG	Default Group	217.132.165.112	2.6.1.5901	0	0	0	17572	0	0	Example:

SentinelOne's Automated EDR provides rich forensic data and can mitigate threats automatically, perform network isolation, and auto-immunize the endpoints against newly discovered threats. As a final safety measure, SentinelOne can even rollback an endpoint to its pre-infected state.

What is Deep Visibility

Deep Visibility offers full, real-time and historic retrospective search capabilities, even for offline endpoints, to improve proactive security. The telemetry data from endpoints and servers can help security teams correlate activity, such as lateral movement and callbacks, with other threat indicators to gain deeper insights. Deep Visibility extends to devices like laptops that may exist outside your network perimeter.

Compared to other offerings, SentinelOne's Deep Visibility is unique because it is simple. There is no need for a highly-trained security team tasked with full-time threat hunting. SentinelOne offers a comprehensive view of your endpoints using a search interface that allows you to see the entire context in a straightforward way.

Simplified Endpoint Protection and Response

Visibility and EDR Made Manageable

EDR is now widely recognized as an essential requirement for Enterprise networks, with an increasing number of security solutions offering visibility on corporate assets. However, many of these solutions are seen as difficult and complicated to manage by Enterprise customers. With only a few minutes per security incident, the growing number of alerts and the lack of highly-trained personnel, the modern enterprise needs a solution that can be managed and automated into existing security flows. An effective, streamlined security solution such as offered by SentinelOne lowers costs and improves efficiency, allowing the business to grow without interruption.

Solve the Blindspot of Encrypted Traffic

Regain Visibility Over Network Traffic

Most network traffic is now encrypted, improving privacy but eliminating the option for network products to see the traffic, a trend that has important consequences for Enterprise. According to Gartner, by 2019 more than 80% of all enterprise web traffic will be encrypted. Moreover, Gartner expects that during 2019, more than 50% of new malware campaigns will use some form of encryption and obfuscation to conceal delivery and ongoing communications, including data exfiltration.
Meanwhile, cyber attackers rely on social engineering and take advantage of increasing noise and decreasing attention to detail. Users are increasingly being manipulated to download and execute malicious code on Enterprise endpoints, while adversaries become more adept at avoiding detection.

SentinelOne and Deep Visibility provide an effective, easily manageable solution to these changing circumstances. Deep Visibility is unique in its ability to look inside encrypted traffic and to reveal the chain of events leading up to compromise attempts. With Deep Visibility, SentinelOne is able to protect against data breaches, monitor phishing attempts, identify data leakage and ensure cross asset visibility while automatically mitigating these attempts, incident by incident.

Integrated with other Security Solutions

Seamless Integration

Deep Visibility is part of the "API anywhere" approach of SentinelOne, so all capabilities are available via API, allowing you to integrate it with other security solutions on the network and reduce your IT burden.

Performance - No Additional Install

Same Agent, Cross Platform

Other endpoint security vendors typically require the client to install several agents in parallel on the same device, even sometimes managed by separate consoles. Endpoints may already have too many agents serving specific needs, taxing local resources and resulting in a poor end-user experience. When these kinds of solutions digest needed endpoint resources, they can degrade performance and impact productivity.

Unlike such solutions, SentinelOne offers a single lightweight agent that does it all with negligible impact on endpoint resources.

SentinelOne offers cross-platform protection. Linux and macOS devices may be less numerous than Windows devices across the typical Enterprise network, but they are no less important from a security perspective. A network is only as strong as its weakest link.

Summary

The Best EDR Capability, Delivered with EPP as a Single Agent

Deep Visibility monitors traffic at the end of the tunnel, which allows an unprecedented tap into all traffic without the need to decrypt or interfere with the data transport. This allows the engine to stay hidden from attacker evasions while also minimizing the impact on the user-experience.

Deep Visibility allows for full IOC search on all endpoint and network activities, and provides a rich environment for threat hunting that includes powerful filters as well as the ability to take containment actions.

Since Deep Visibility does not require an additional agent, and is a holistic part of the SentinelOne EPP platform, it is also fully integrated into the investigation, mitigation and response capabilities. Security teams can thus quickly dispose threats discovered via Deep Visibility such as gaining process forensics, file and machine quarantine, and full dynamic remediation and rollback capabilities.