SentinelOne

SentinelOne Endpoint Protection: Deep Visibility

You cannot stop what you cannot see. Extend the power of your SentinelOne Endpoint Protection Platform (EPP) with rich visibility to search for attack indicators, investigate active incidents and root out latent threats.

It is a well-known fact that threat actors today are highly evasive and employ every trick to infiltrate organizations and extract information. Protecting against such threat actors requires a multi-layered approach that accelerates detection of known and unknown threats, hunts for signs of hidden threats, automates response to minimize impact and extracts rich forensic insights to ensure holistic protection.

SentinelOne Deep Visibility

SentinelOne Deep Visibility extends the SentinelOne Endpoint Protection Platform (EPP) to provide full visibility into endpoint data. Its patented kernel-based monitoring allows a near real-time search across endpoints for all indicators of compromise (IOC) to empower security teams to augment real-time threat detection capabilities with a powerful tool that enables threat hunting.

Advanced attackers are always looking for ways to stay hidden. The growing use of traffic encryption — over 50% of Web traffic today is encrypted — provides a simple trick for attackers to hide their threats and communications channels. Exploit kits, malware, adware, callbacks, as well as command & control channels leverage encrypted communications to infiltrate organizations and exfiltrate information. Deep Visibility unlocks visibility into encrypted traffic, without the need for a proxy or additional agents, to ensure full coverage of threats hiding within covert channels.

Deep Visibility extends the EPP capabilities to provide an integrated workflow from visibility & detection to response & remediation. The single agent, single console architecture provides deployment simplicity and operational agility to improve productivity and minimize business impact of threats.

How does Deep Visibility work?

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 layer. This allows the engine to stay hidden from attacker evasions while also minimizing user-experience impact.

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.

Deep Visibility offers full real-time and historic retrospective search, even for offline endpoints. This 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. It also provides valuable insights when endpoints exist beyond traditional perimeters.

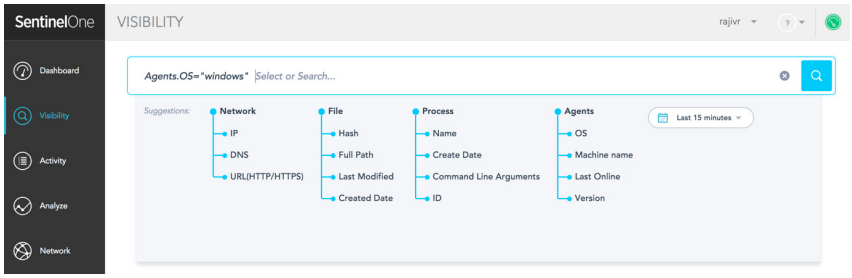

Figure 1: SentinelOne Deep Visibility

Deep Visibility does not require an additional agent and is a holistic part of the SentinelOne EPP platform. As a result, it seamlessly integrates into the base investigation, mitigation and response capabilities. Security teams can thus quickly diagnose and respond to threats discovered via Deep Visibility, including process forensics, file and machine quarantine, and full dynamic remediation and rollback.

Deep Visibility also supports external threat feed ingestion via the Deep Visibility API.

Figure 2: Security Workflow

Benefits

- **Full visibility into encrypted traffic:** Uncover organizational blind spots with full visibility into key assets on the network
- **Enrich forensic profiles:** Gain cross-enterprise forensic insights, including from offline endpoints, to ensure complete protection
- **Single agent architecture:** Reduce operational overheads with a single agent
- **Improve the hunt-to-response workflow:** Empower the hunting process with rich insights with seamless integration into mitigation, remediation, and recovery
- **Full workflow automation:** Leverage endpoint and server telemetry coupled with API support to power security workflows.

SentinelOne is a certified AV replacement for Windows and MacOS.

SentinelOne

For more information about the SentinelOne Next-Generation Endpoint Protection Platform and the future of endpoint protection, **please visit: sentinelone.com**