SentinelOne™

DATASHEET

Replace Your Legacy AV with Next-Generation Endpoint Security

Unlike traditional AV, NGAV identifies malicious activity using a system-centered, technical approach that examines every process on an endpoint. This allows NGAV to proactively detect and block the tools and tactics hackers use to gain entry. While traditional AV is focused on detecting malware at the endpoint alone, NGAV addresses a larger range of modern threat scenarios including non-malware and ransomware attacks.

▶ Why SentinelOne

The Powerful Combination of Static + Behavioral AI

The key is to prevent anything that can be prevented pre-execution and to deal with what cannot by looking at the behavior of processes executing on the endpoint. This is effective because, despite the large and increasing number of malware variants, they operate in very similar ways. Even if an attack is fileless, script based, or is delivered in an esoteric way, the powerful behavioral AI engine of SentinelOne catches these abnormal behaviors. The number of malware behaviors is considerably smaller than the number of ways a malicious file might look, making this approach suitable for prevention and detection. SentinelOne delivers autonomous endpoint protection through a single agent that successfully prevents, detects and responds to attacks across all major vectors. Designed for extreme ease of use, the SentinelOne platform saves customers time by applying AI to automatically eliminate threats in real time for both on-premise and cloud environments and is the only solution to provide full visibility across networks directly from the endpoint.

EDR that Helps You See and Do More in Less Time

By looking at the whole context of behavior rather than just isolated incidents, EDR offers a more effective means of recognizing and deterring unknown malware and sophisticated attacks. This rich contextual information allows SentinelOne to understand the cause of the attack and thus prevent future ones. Rapid deployment and cloud access/management are also key features of SentinelOne. It offers increased endpoint detection, better response capabilities, and a greater number of preventative measures. We replace traditional endpoint protection products.

Click here for a demo and more information on SentinelOne Endpoint Protection

Replace Your Legacy AV with the SentinelOne Endpoint Protection

REDUCE AGENT BLOAT: Detection, prevention, response, and visibility capabilities in a single agent

BOOST PROTECTION: Stop advanced attacks with next-generation technology

VISIBILITY & RESPONSE: Gain SSL traffic visibility directly from the endpoint with highly nuanced and automated EDR capabilities such as rollback

SAVE TIME: Improve IT and Security productivity by reducing the manual labor to correlate and understand the root cause - get network-wide visibility on your assets with an automated response

IMPROVE ROI: Block malware, respond to threats, and maintain compliance with just one solution

OPERATIONAL COSTS: The NSS AEP report identified SentinelOne with the best overall TCO over a three-year period

IMPROVE YOUR OVERALL SECURITY POSTURE by full Rest API that can integrate SentinelOne into your existing solutions

MAINTAIN COMPLIANCE: Meet and exceed PCI and HIPAA security compliance requirements

SentinelOne™