SentinelOne™

ALIGNING TO THE **NIST CYBERSECURITY FRAMEWORK**

The National Institute of Standards and Technology (NIST) established the Risk Management Framework (RMF) as a set of operational and procedural standards or guidelines that a US government agency must follow to ensure the compliance of its data systems. According to NIST, these standards, guidelines, and best practices are essential to managing cybersecurity-related risk. The Cybersecurity Framework's prioritized, flexible, and cost-effective approach helps to promote the protection and resilience of critical infrastructure and other sectors important to the economy and national security.

The Functions are the highest level of abstraction included in the Framework. They act as the backbone of the Framework Core that all other elements are organized around.

These five Functions represent the five primary pillars for a successful and holistic cybersecurity program. They aid organizations in easily expressing their management of cybersecurity risk at a high level and enabling risk management decisions.

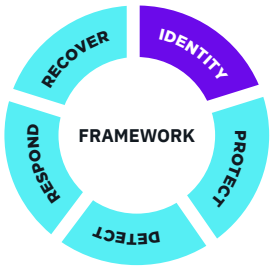
SentinelOne has been granted a FedRAMP Moderate certification Authority to Operate by its sponsor agency with full PMO sign-off expected Q3-2020.

The SentinelOne Endpoint Protection Platform unifies prevention, detection, and response in a single purpose-built agent powered by machine learning and automation. It provides prevention and detection of attacks across all major vectors, rapid elimination of threats with fully automated, policy-driven response capabilities, and complete visibility into the endpoint environment with full-context, real-time forensics.

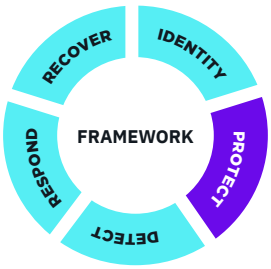
How Can SentinelOne Help?

SentinelOne helps to address these five function through our endpoint security platform, enabling organizations to match their endpoint security posture to these best practice risk guidelines. Below is a breakdown of how SentinelOne can address each of the five functions within the NIST Framework Core.

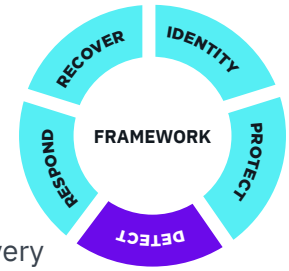
IDENTIFY

Function	How Can SentinelOne Help?
The Identify Function assists in developing an organizational understanding to managing cybersecurity risk to systems, people, assets, data, and capabilities. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. 	SentinelOne helps organizations to address this requirement with application vulnerability risk scoring. Without the need to scan, the SentinelOne agent automatically collects a full application inventory from all managed endpoints and maps the application versions to known vulnerabilities. This discovery provides automated risk identification for the enterprise and quickly enhances risk posture, enabling successful and prioritized patch management program. SentinelOne also automatically identifies computer assets and users associated with threats in the environment, so that an organization can quickly pinpoint who is affected.

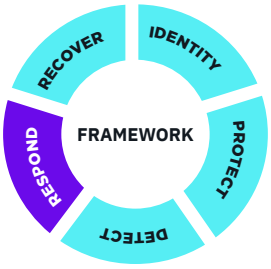
PROTECT

Function	How Can SentinelOne Help?
The Protect Function outlines appropriate safeguards to ensure delivery of critical infrastructure services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. 	SentinelOne specializes in protecting Windows, Mac and Linux endpoints from multiple vectors of attack, including file-based malware, script-based attacks, exploits, in-memory attacks, and zero-day campaigns. SentinelOne achieves this level of unmatched endpoint protection by using multiple AI models within a single agent. This allows the SentinelOne platform to convict and block files pre-execution, and identify and kill malicious process on-execution. These multiple layers of protection provide a defense-in-depth on every endpoint. SentinelOne also provides device control and endpoint firewall control. This allows organizations to protect endpoints from unwanted connected USB devices, and unsolicited endpoint network communication.

DETECT

Function	How Can SentinelOne Help?
The Detect function defines the appropriate activities to identify the occurrence of a cybersecurity event. The Detect function enables the timely discovery of cybersecurity events. 	SentinelOne automatically detects attacks across an organization's endpoint environment, regardless of how they are delivered to the machine. The agent leverages its multiple detection engines to scan files on write to disk, and model process execution with behavioral AI to detect advanced attacks executing on a system. SentinelOne's Active EDR capability allows the organization to hunt for threats, storing 14 to 365+ days of contextualized endpoint forensic data. This is an additional level of visibility that can be leveraged as a compliment to SentinelOne's automatic threat detection capability. SentinelOne Vigilance, our Managed Detection and Response service, adds another layer of detection through 24X7 threat monitoring by our trained security analysts.

RESPOND

Function	How Can SentinelOne Help?
The Respond Function includes appropriate activities to take action regarding a detected cybersecurity incident. The Respond function supports the ability to contain the impact of a potential cybersecurity incident. 	SentinelOne provides effective response measures through a patented endpoint remediation capability. The SentinelOne agent can automatically clean an infected machine by identifying changes made by malware, and undoing these changes with the click of a button. This greatly reduces the time to recover from any executed attack on a machine. SentinelOne also provides full remote shell capability to endpoints, for quick and effective access to systems to initiate additional response efforts. SentinelOne Vigilance, our Managed Detection and Response service, adds an additional layer of response through 24X7 threat monitoring by our trained security analysts. This ensures that all detected threats within an environment will be responded to, any hour of any day.

RECOVER

Function	How Can SentinelOne Help?
The Recover Function identifies appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident. 	SentinelOne provides a recovery option called Rollback. Rollback will restore a windows endpoint to a pre-attack state, by not only remediating a machine, but automatically restoring damaged file system info. Literally rewinding the effect of attacks such as ransomware, to quickly bring an infected machine back to an operable state.

Differentiated in Every Aspect

Unlike other products, SentinelOne is a unified, purpose-built agent that supports all modern Windows versions and back to XP, and more than 10 versions of Linux and Apple macOS.

Any OS	Any Deployment	Any Connection	Any Integration	Any Person	Any Response
Windows	Cloud	Online	300+ APIs	Big team	Automated
Linux	GovCloud	Offline		One person	
macOS	On-Prem			No team	
Virtualization	Hybrid				

SE Labs AAA Enterprise Endpoint Protection Oct-Dec 2019 | VB 100 Virus virusbtn.com | MITRE ATT&CK | AWS GovCloud (US) | HIPAA Compliant | PCI | ISO 27001 Certified by schellman | Gartner peerinsights customers' choice 2020

READY FOR A DEMO? Visit the SentinelOne website for more details.

SentinelOne

www.SentinelOne.com | Sales@SentinelOne.com
+1-855-868-3733 | 605 Fairchild Dr, Mountain View, CA 94043