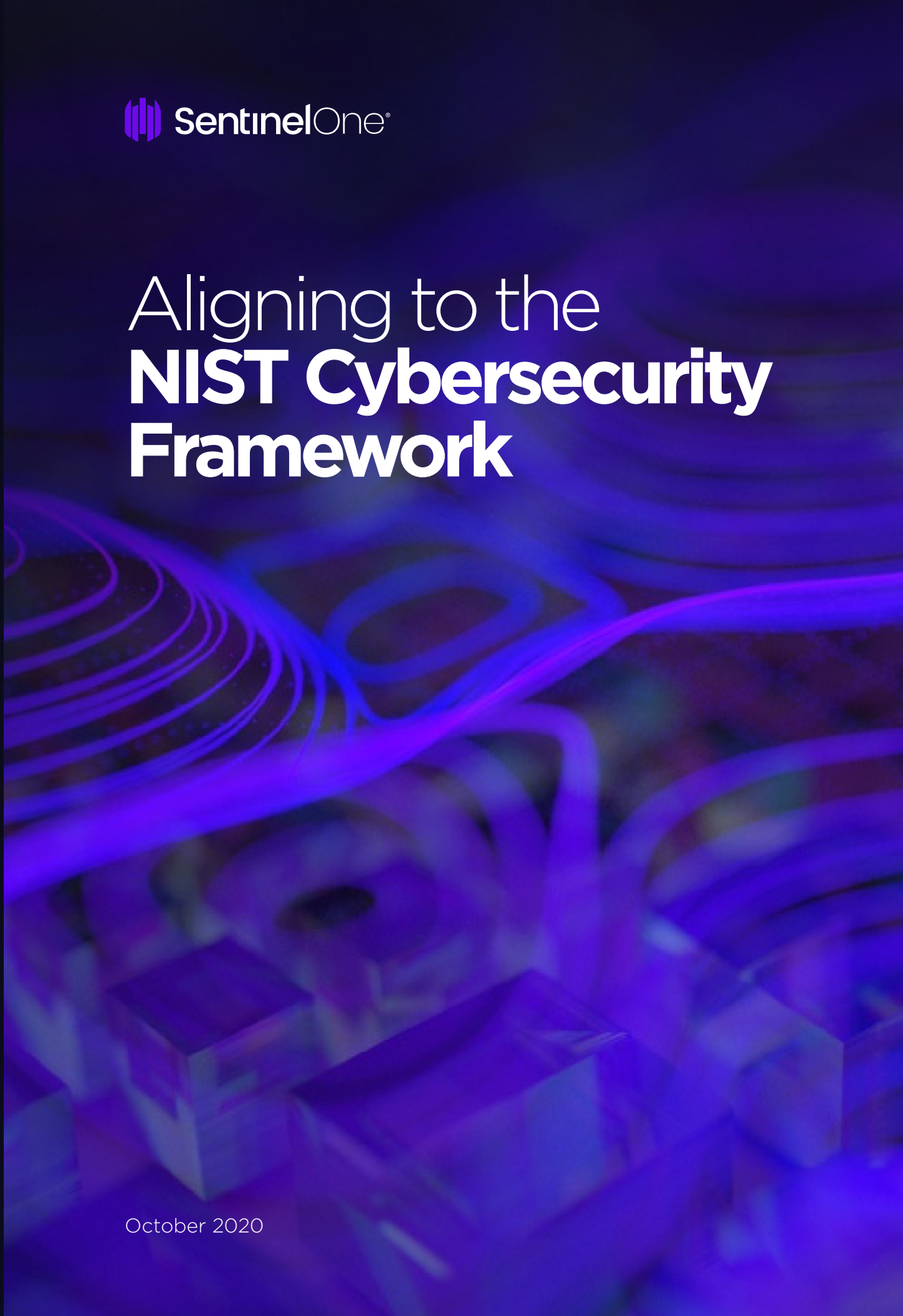
SentinelOne White Paper

SentinelOne®

Aligning to the **NIST Cybersecurity Framework**



October 2020

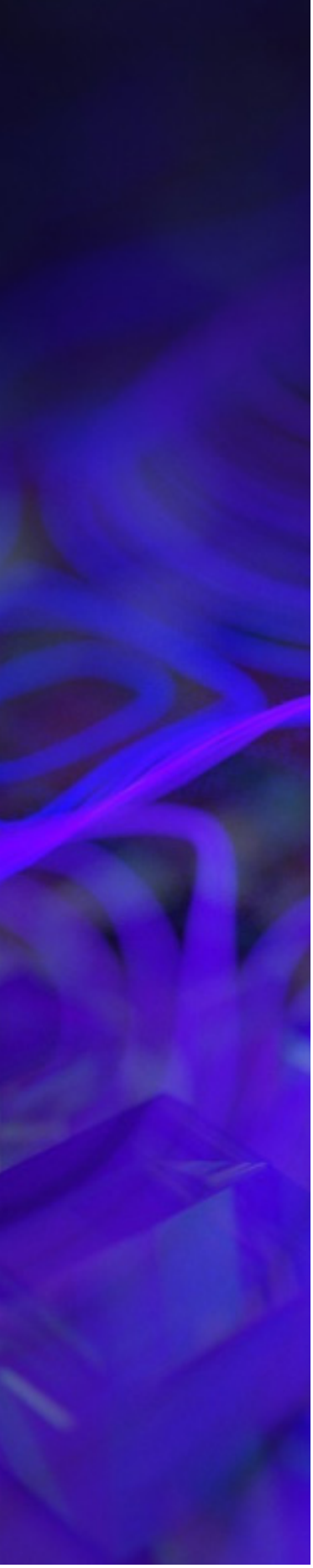


Table of Contents

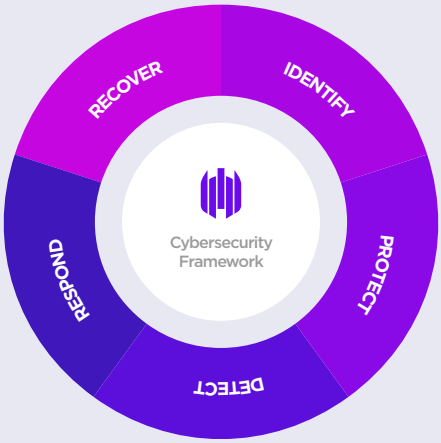
01

Introduction

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.



Functions 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.

02

How SentinelOne Lowers Risk

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

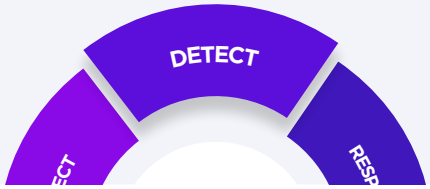
Function	How Can SentinelOne Help?
The Identify Function assists in developing an organizational understanding to managing cybersecurity risk to systems, people, assets, data, and capabilities. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.	SentinelOne is a full feature enterprise-grade EDR platform for use in identifying threats and responding to them. Our EDR is not ordinary. It features high levels of automation to make each analyst's job easier. SentinelOne also automatically identifies computer assets and users associated with threats in the environment, so that an organization can quickly pinpoint who is affected. SentinelOne identifies network devices that do not have agents installed. We also identify other IP-enabled devices on networks including IoT and other previously unknown yet connected devices. 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.

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 and Kuberetes containers from multiple vectors of attack, including file-based malware, script-based attacks, exploits, in-memory attacks, and zero-day campaigns. We achieve this level of endpoint protection with multiple AI models within each agent. SentinelOne convicts and blocks files pre-execution, and identifies and kill malicious process on-execution. These multiple protection layers provide a defense-in-depth on every endpoint. SentinelOne provides device control for all types of USB and Bluetooth devices and firewall control for inbound and outbound endpoint network communication control.

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 ActiveEDR 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 complement 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 1-Click greatly reducing the time to recover from any 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 taking the burden of our customers.

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 1-Click 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. This feature literally rewinds the effects of attacks such as ransomware, to quickly bring an infected machine back to an operable state.

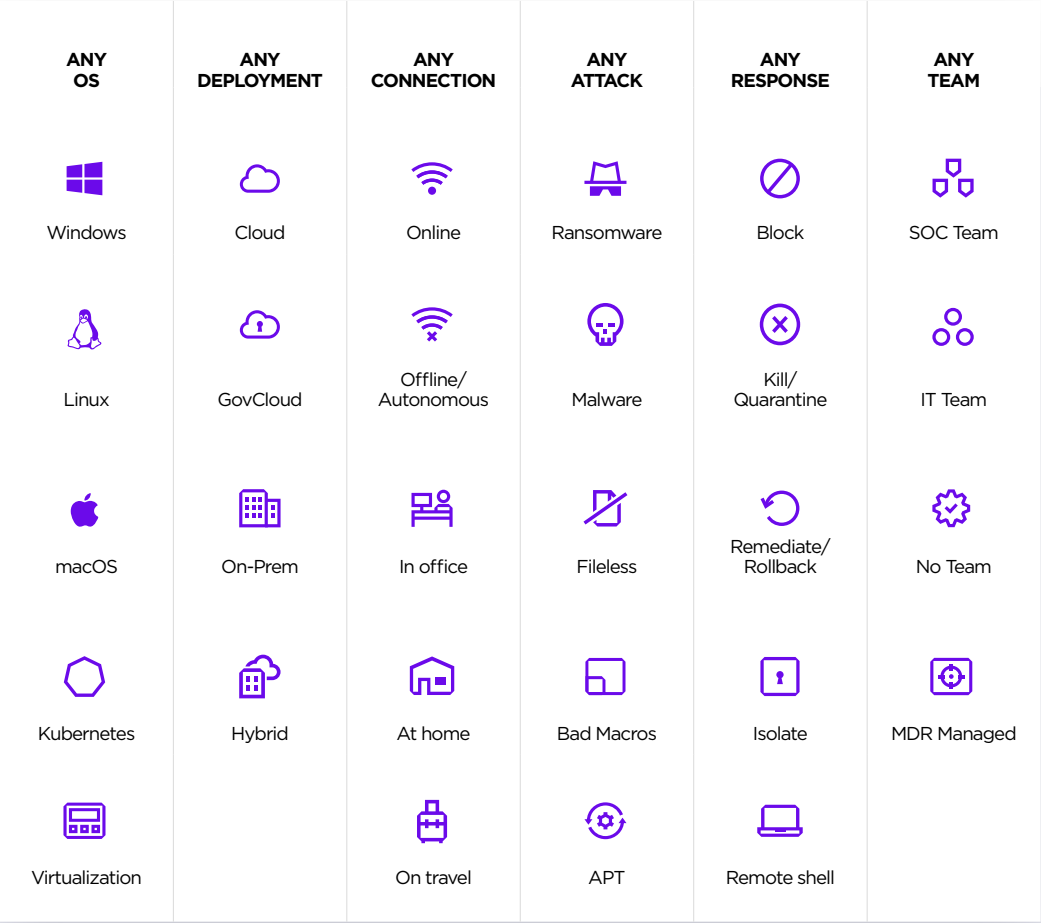
03

Comprehensive without Complexity

SentinelOne Singularity delivers differentiated endpoint protection, endpoint detection and response, IoT security, cloud security, and IT operations capabilities - consolidating multiple existing technologies into one solution.

We offer resource efficient, autonomous “Sentinel” agents for Windows, Mac, Linux, and Kubernetes and support a variety of form factors including physical, virtual, VDI, customer data centers, hybrid data centers, and cloud service providers.

Sentinels are managed via our globally available multi-tenant SaaS designed for ease-of-use and flexible management that meets your requirements. Our Vigilance Managed Detection & Response (MDR) services subscription is available to back your security organization 24x7.



ATT&CK®

2020 MITRE ATT&CK

- Fewest Misses
- Most Correlations
- Best Data Enrichment Coverage

FORRESTER®

2020 FORRESTER WAVE™ EDR

"Strong Performer"

kuppingercole ANALYSTS

2020 KUPPINGERCOLE MARKET COMPASS

Featured EPDR Innovator

SentinelOne is a Customer First Company

Continual measurement and improvement drives us to exceed customer expectations.

Gartner peerinsights customers' choice™

97%

Of Gartner Peer Insights™ 'Voice of the Customer' Reviewers recommend SentinelOne

97%

Customer Satisfaction (CSAT)

FedRAMP

ISO 27001 CERTIFIED by schellman

EU GDPR COMPLIANT

SE Labs AAA AUGUST 2020 BREACH RESPONSE PROTECT

TEVORA

PCI DSS Attestation
HIPAA Attestation

Gartner peerinsights™ 4.9 ★★★★★

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

Contact us

sales@sentinelone.com
+1-855-868-3733

sentinelone.com

S1_Aligning_to_the_NIST_Framework_19102020