SentinelOne

SOLUTION BRIEF

Begin Your XDR Journey with Frictionless 1-click Integrations

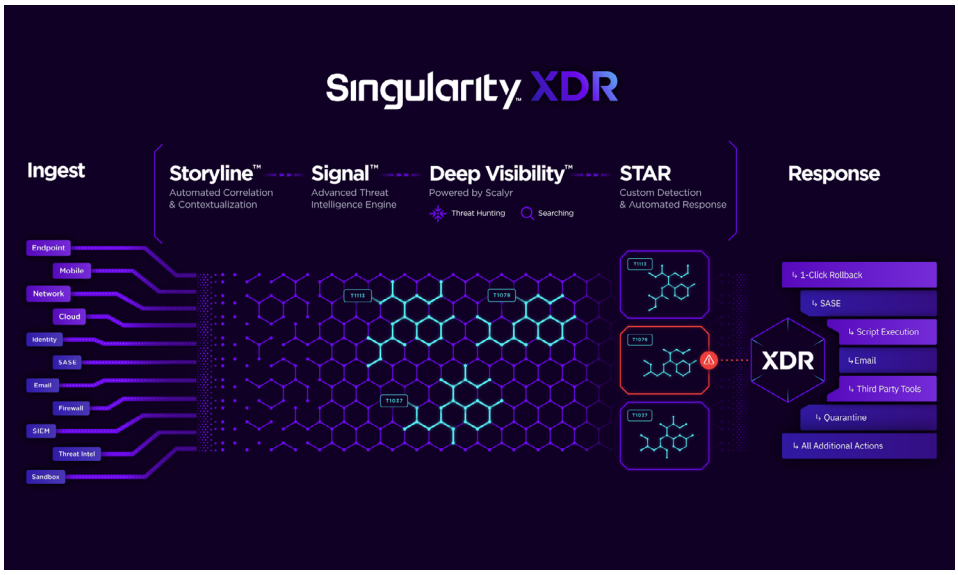
SentinelOne Singularity XDR Apps Solution Brief

SECURE ISS

SentinelOne Singularity XDR unifies and extends detection, investigation and response capability across the entire enterprise, providing security teams with centralized end-to-end enterprise visibility, powerful analytics, and automatable response across the technology stack. The solution empowers security teams to see data collected by disparate security solutions from all platforms, including endpoints, cloud workloads, network devices, email, identity, and more, within a single dashboard. The solution delivers increased flexibility, automation and simplicity with unparalleled scale to every environment based on an industry leading foundation of EPP & EDR.

Through Singularity Marketplace, customers can extend the SentinelOne Singularity XDR platform with bite-sized, one-click applications to help enterprises unify prevention, detection, and response across attack surfaces to implement and embrace XDR. With SentinelOne's Singularity Marketplace, organizations can integrate any security applications and tools regardless of vendor into a single platform without coding or scripting required.

Singularity Marketplace extends the power of the SentinelOne platform across the entire security and IT stack to build an effective threat defense posture with layered security, collaborative processes, and integrated products. Singularity Marketplace enables security teams to converge on a single pane-of-glass for extended detection and response workflows to minimize context switching and distractions during triage and incident response. It helps them gain insights from shared security events without requiring a massive time investment in custom business logic, code, and complex configuration.



KEY HIGHLIGHTS

Automate Triage and Investigation

Auto-enrich threats with integrated and 3rd party threat intelligence

Unify Cross-System Response

Defeat high-velocity threats by driving a unified, orchestrated response among security tools in different domains

Frictionless Integration with Leading Ecosystem Vendors

No massive time investment, custom business logic, code, or complex configuration necessary

Key XDR App Use Cases

Accelerate investigations and triage by correlating threats to your entire stack

Threats within SentinelOne are enriched with context and intelligence from connected security tools into unified alerts that provide campaign-level insight and allows enterprises to correlate events across different vectors to facilitate triage of alerts as a single incident. This enables analysts to automate elements of triage and rapidly uncover the breadth of a breach. Example use cases include:

- Get immediate visibility into suspicious privileged access in the hours and days leading up to an endpoint infection
- Halt threats faster with insight into the privilege escalation paths attackers will uncover via exposed credentials on infected endpoints and close those exploit paths
- By asking other vendors for their conclusions, not just their data, an SentinelOne threat can uncover suspicious network activity with a single number like Netskope's user risk score

Automate response across the security ecosystem

XDR response actions are the single click that can stop attack expansion. If an analyst finds a threat where an internal user's credentials have been used to log into email and send phishing links, XDR can suspend the user's email access or just block the hash from being passed around. Until the credentials can be trusted again, that analyst can also move the user to a more restrictive SASE policy to ensure access to data like financial results and IP stored in cloud apps are protected. Example use cases include:

- Automatically limiting how quickly an attack can spread by restricting a user's access by presuming that when their endpoint is infected their credentials are compromised too
- Automatically limiting how quickly an attack can spread by restricting a user's ability to send email when their endpoint is infected
- Automatically limiting an attacker's ability to uncover IP and perform data exfiltration by limiting their access to cloud apps

Gartner peerinsights™

"Ease to deploy, great API integration with SOAR tools.

★★★★★

DIRECTOR, GLOBAL INFOSEC
SERVICES, 10B - 30B USD

Gartner peerinsights™

"Powerful tool with great vision... Integration is easy.

★★★★★

SECURITY EXPERT
RETAIL, 30B+ USD

Gartner peerinsights™

"It has great integrations, and it's feature rich with a strong roadmap.

★★★★★

DIRECTOR, INFORMATION SECURITY
RETAIL, 3B - 10B USD

Attivo Networks · CyberArk · Microsoft Azure
mimecast · netskope · okta
proofpoint · Recorded Future · Remediant
servicenow · VECTRA · zscaler

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.com

sales@sentinelone.com
+ 1 855 868 3733