SentinelOne

SOLUTION BRIEF

SentinelOne Singularity XDR Use Cases

The cybersecurity threat landscape is rapidly evolving and expanding. As attack vectors multiply, from endpoints to networks to the cloud, many enterprises address each vector with a best-in-class solution to protect those specific vulnerabilities. However, these point tools don't connect the dots across the entire technology stack. As a result, security data is collected and analyzed in isolation, without any context or correlation, creating gaps in what security teams can see and detect. Besides, the manual investigation process can often be slow and cumbersome, causing security teams to fall behind in containing and remediating threats.

Singularity XDR

SentinelOne Singularity XDR unifies and extends detection and response capability across multiple security layers, providing security teams with centralized end-to-end enterprise visibility, powerful analytics, automated response across the complete technology stack. With Singularity XDR, customers can get unified and proactive security measures to defend the entire technology stack, making it easier for security analysts to identify and stop attacks in progress before they impact the business.

Key Use Cases

01 | Eliminate blind spots with cross-stack visibility

Singularity XDR enables enterprises to seamlessly ingest structured, unstructured, and semi-structured data in real-time from any technology product or platform, breaking down data silos and eliminating critical blind spots. The solution empowers security teams to see data collected by disparate security solutions from all platforms, including endpoints, cloud workloads, IoT devices, networks, and more, within a single dashboard. Singularity XDR lets analysts take advantage of insights derived from aggregating event information from multiple different solutions into a single contextualized "incident". It also provides customers with a central enforcement and analytics layer point hub for complete enterprise visibility and autonomous prevention, detection, and response, helping organizations address cybersecurity challenges from a unified standpoint.

02 | Uncover stealthy attacks with cross-stack correlation

SentinelOne patented Storyline™ technology provides real-time, automated machine-built context and correlation across the enterprise security stack to transform disconnected data

SOLUTION BENEFITS

Increased SOC Efficiency and Productivity

No context switches or multiple dashboards in response minimizes delays. One platform and one workflow reduces the number of alerts, eliminates blind spots and data gaps, and reduces the number of interfaces that security must access during a response.

Rapid Time to Value

Out-of-the-box integrations across multiple different products. Enables you to maximize value from your existing cybersecurity investment rapidly.

Streamlined Operations & Workflows

Achieve single-pane visibility & analysis for siloed data streams.

Reduced Total Cost of Ownership (TCO)

Reduce the costs associated with configuring and integrating multiple point solutions with a fully integrated cybersecurity platform.