PARTNER BRIEF

Reduce the Enterprise Attack Surface with Unparalleled Asset Intelligence

A Joint Solution by SentinelOne and Armis

Overview

In today's rapidly evolving digital landscape, cloud sprawl, SaaS adoption, remote work, interconnectivity, automated exploit chains, and shadow IT have introduced new entry points and operational complexities. As a result, organizations are now facing the expanded challenge in reducing their exposure by implementing a comprehensive Cyber Exposure Management (CEM) program. To mitigate risk, security teams require unified visibility, contextual intelligence, and rapid response capabilities.

SentinelOne and Armis have partnered to provide a joint solution that combines industry-leading Extended Detection and Response (XDR) with comprehensive CEM. Together, the joint solution empowers security teams to gain real-time insights into managed and unmanaged devices, enrich threat context, automate workflows, and proactively reduce the enterprise attack surface.

State of the Market

As enterprises embrace digital transformation, networks and workflows are becoming increasingly complex. Analysts must monitor a myriad of different devices and assets across hybrid environments. Yet, nearly 84% of organizations still have high-risk vulnerabilities exposed throughout their digital estate. Traditional asset management processes are manual, fragmented, and often incomplete, leaving gaps that adversaries can exploit.

XDR solutions are now a strategic priority, providing consolidated visibility, real-time situational awareness, detection, response and mitigation across the enterprise. However, XDR's effectiveness depends on contextual intelligence and prioritization based on real risk to the business from a comprehensive CEM platform to ensure that all assets and their pathways are assessed and secured.

The Challenge

Modern enterprise environments are increasingly complex, with a growing mix of managed and unmanaged devices, including IT endpoints, IoT, and operational technology. Security teams struggle to maintain comprehensive visibility, security and manageability across diverse landscapes. Traditional asset management is almost solely predicated on a process that often relies on manually gathering and correlating data from multiple systems, which is time-consuming, frequently incomplete and often error prone. Without real-time context, deduplication, contextualization and prioritizing efforts based on business risk, analysts face difficulties in responding to threats quickly and effectively. This sub-optimal approach leaves organizations exposed, allowing adversaries to exploit gaps and increasing the risk of lateral movement, operational disruption, and data compromise.

The Solution

The joint Armis and SentinelOne solution addresses these challenges by combining comprehensive CEM with industry-leading XDR capabilities. Armis delivers unmatched visibility, contextualization and prioritization into every asset and potential attack pathway. SentinelOne takes this intelligence and provides continuous monitoring, protection, and response across all endpoints. Together, the joint solution enriches threat alerts with contextual device information, automates labor-intensive tasks, and enables prioritized proactive risk reduction. This unified approach empowers security teams to quickly identify vulnerable assets, pathways and behaviors, accelerate investigation and response, and implement precise segmentation and other compensating controls to effectively reduce the enterprise attack surface and improve operational resilience.

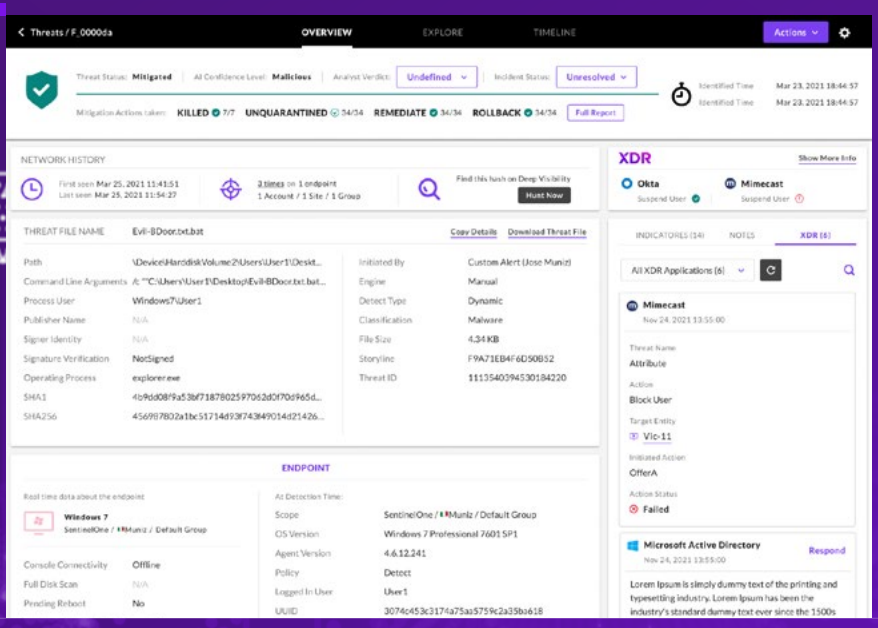
How It Works

Unified Asset Visibility - SentinelOne endpoints are enriched with Armis metadata, application inventory, device characteristics and threat data. All endpoint findings, from IT to OT, IoT, and medical devices are deduplicated, consolidated, and tagged in a single view.

Threat Enrichment - Potential threats are automatically correlated with Armis alerts and device contextualization and prioritization, providing analysts with critical insights within a seamless single User Interface (UI).

Network Visibility and Control - SentinelOne Singularity Ranger can isolate or quarantine high-risk devices based on Armis tags, preventing lateral movement.

Automation and Orchestration - Tasks, such as device inventory, contextualization, threat triage, mitigation and compensating controls leverage AI and are automated to ensure unparalleled efficacy and efficiency on the CEM program.



Use Cases

1. **Unified Asset and Risk Visibility -** Real-time device inventory and application context from the joint solution identify, contextualize, prioritize vulnerabilities and other risk elements.
2. **XDR Threat Enrichment -** Armis intelligence enriches SentinelOne threat alerts, enabling faster investigation and containment.
3. **Network Visibility, Security, and Control -** Ranger and Armis work together to identify, tag, and isolate unmanaged or risky assets and their attack pathways.

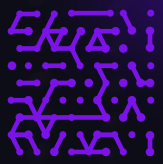
Key Business Outcomes and Benefits

- **Full Asset Visibility and Situational Awareness -** Assess and monitor risk across IT, IoT, OT, and IoMT devices and likely attack pathways.
- **Accelerated Triage -** Automatically enrich SentinelOne alerts with Armis context to streamline and prioritize investigation workflows.
- **Reduced Attack Surface -** Improve Ranger asset fingerprinting with Armis intelligence to isolate unmanaged and high-risk devices using compensating controls.
- **Rapid Time To Value -** One-click installation via Singularity Marketplace with API credentials, operational in minutes.

Conclusion

By integrating SentinelOne Singularity XDR with Armis Asset Intelligence, organizations achieve a unified security workflow that reduces attack surfaces, accelerates incident response, and enhances operational efficiency. Shared intelligence and automated context enable security teams to proactively identify and mitigate risks across the entire enterprise, including IT, OT, and IoT environments.

For a demo of how SentinelOne and Armis can secure your organization's assets and reduce risk, contact our sales team today.



ARMIS®

Understand the Armis difference:

- Comprehensive visibility
- Intelligent insights
- Proven outcomes

Try Armis Centrix™ Today

Armis, the cyber exposure management & security company, protects the entire attack surface and manages an organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, protect and manage all critical assets - from the ground to the cloud. Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society stay safe and secure 24/7.

Armis is a privately held company headquartered in California.

+1 888 452 4011

armis.com