SentinelOne

SOLUTION BRIEF

Respond to Breaches Faster with 1-Click Forensics

SentinelOne & Cado Security Joint Solution Brief

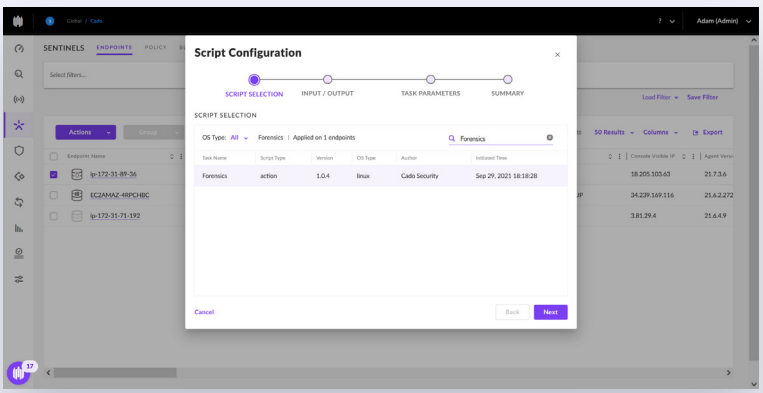
When malicious activity is detected, the speed at which you can dive deep - determine root cause and scope - is essential to fully remediating an incident before it's at risk of escalating. Delays in the investigation process or hurdles that prevent a proper analysis from occurring all together have significant impact and leave your organization vulnerable to future breaches. SentinelOne & Cado Security have joined forces to help organizations accelerate investigations and respond to incidents faster.

Joint Solution

SentinelOne Singularity provides comprehensive visibility across your environment - giving you the breadth you need to detect malicious activity as soon as it occurs. Cado Response streamlines forensic analysis to deliver essential context and depth to your investigation allowing you to quickly identify root cause. Combined, organizations can detect, investigate, and remediate breaches with unmatched speed.

How it Works

Using the SentinelOne Remote Script Orchestration (RSO) capability, with a single click, analysts can remotely capture forensic evidence across endpoints of interest to simplify forensic data collection and accelerate triage. Captured data is consumed by Cado's cloud-based processing engine which automatically scales up and down to provide rapid processing when needed, and save costs when not. Forensic investigations often require massive amounts of data to be processed. To ensure security teams are able to start their investigation without delay, Cado Response enables countless systems to be processed simultaneously.



CADO

JOINT SOLUTION HIGHLIGHTS

+ 1-click forensic data capture
+ Expanded threat hunting
+ Broad coverage across on-premises and cloud systems
+ Real-time and historical context

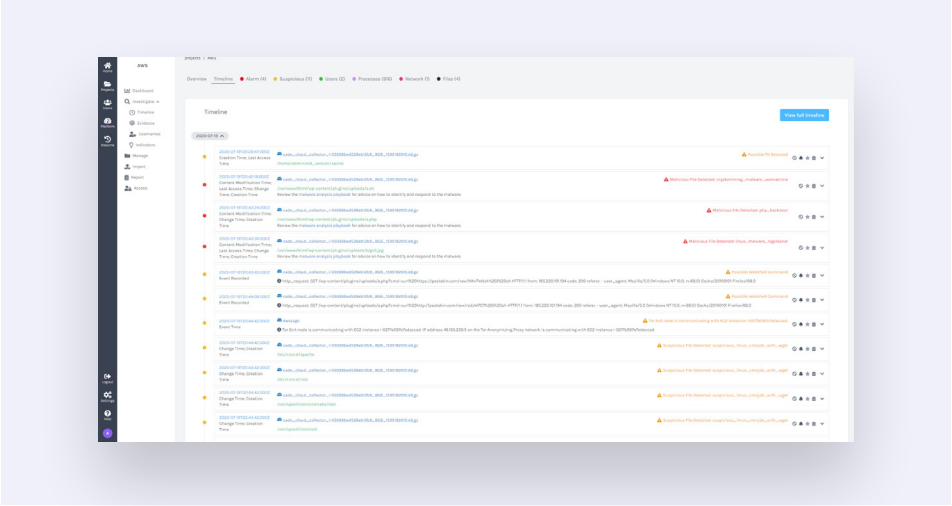
"

The integration between SentinelOne Singularity and Cado Response ensures security teams have the breadth and depth they need to detect, investigate, and remediate breaches with unmatched speed.

Chris Doman

CADO SECURITY CO-FOUNDER

The Cado Response platform analyzes forensic evidence using machine learning and threat intelligence making investigations easier by adding context and awareness to the data. With a complete timeline of events, analysts can conduct an investigation in aggregate and seamlessly dive into critical evidence. Cado's flexible search and filter capabilities allow analysts to easily pivot across evidence items including impacted systems, users, processes, files, and more, so they can rapidly visualize incident scope.



Conclusion

SentineOne and Cado Security's combined solution empowers security teams to rapidly perform in-depth investigations and minimize time to respond. When it comes to attack containment, time is of the essence. Augment your real-time threat detection platform with rich historical context to identify root cause, understand the impact of breaches, and respond faster.

INTEGRATION BENEFITS

Respond to breaches faster

Rapidly perform in-depth incident investigations to minimize time to respond.

Add depth to your investigation

Dig deeper with rich historical context enabling you to quickly identify root cause and understand the full impact of breaches.

Gain complete visibility

Combine broad threat detection with deep investigation capabilities across your entire environment - on premises, hybrid, and cloud.

Innovative. Trusted. Recognized.

Gartner

A Leader in the 2021 Magic Quadrant for Endpoint Protection Platforms

Highest Ranked in all Critical Capabilities Report Use Cases

MITRE ENGENUITY

Record Breaking ATT&CK Evaluation

- No missed detections. 100% visibility
- Most Analytic Detections 2 years running
- Zero Delays. Zero Config Changes

Gartner peerinsights 4.9 ★★★★★

98% of Gartner Peer Insights™

Voice of the Customer Reviewers recommend SentinelOne

FedRAMP · ISO 27001 CERTIFIED by schellman · VB 100 VIRUS virusbtn.com · TEVORA PCI DSS Attestation HIPAA Attestation

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?

About Cado Security

Cado Security provides the first and only cloud-native digital forensics platform for enterprises. Its Cado Response platform automates data capture and processing to expedite investigations, enabling security teams to quickly understand the impact of compromises and respond to cyber incidents at cloud speed.

sentinelone.com

sales@sentinelone.com
+ 1 855 868 3733

cadosecurity.com

contact@cadosecurity.com