SentinelOne

SOLUTION BRIEF

Respond to Breaches Faster with Cloud Automation

SentinelOne & Cado Security Joint Solution Brief

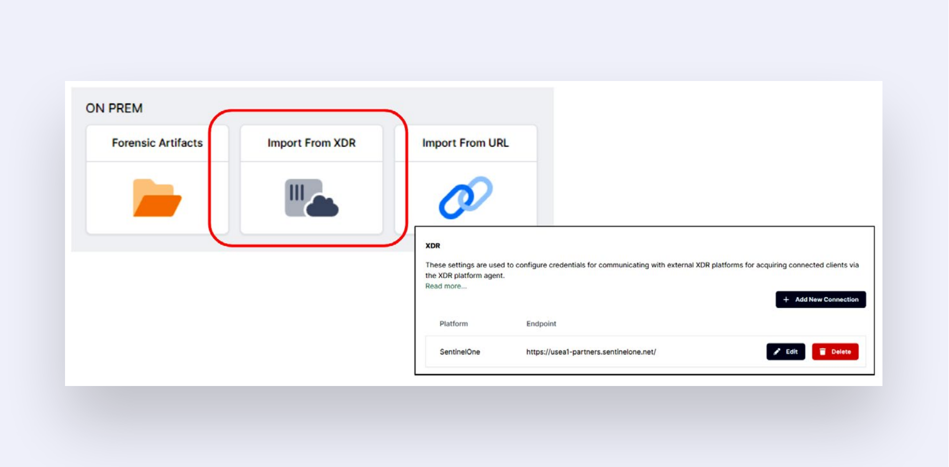
When malicious activity is detected, the speed at which you can dive deep – determine root cause and scope – is essential to fully remediating an incident before it's at risk of escalating. Delays in the investigation process or hurdles that prevent a proper analysis from occurring all together have 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. The Cado platform automates deep-dive investigations to deliver essential context and depth, allowing you to quickly identify root cause and craft an effective response plan. Combined, organizations can detect, investigate, and remediate breaches with unmatched speed.

How it Works

Through the power of automation, analysts can kick off an in-depth investigation without delay. As soon as malicious activity is detected by the SentinelOne Singularity platform, Cado will automatically capture forensic-level detail across the impacted systems. From on premises to cloud, container and serverless environments, Cado collects hundreds of data sources across full disk, memory, cloud-provider logs and more. Captured evidence is consumed by Cado's cloud-based processing engine to provide rapid, parallel data processing.



These settings are used to configure credentials for communicating with external XDR platforms for acquiring connected clients via the XDR platform agent.

Platform	Endpoint
SentinelOne	https://usea1-partners.sentinelone.net/

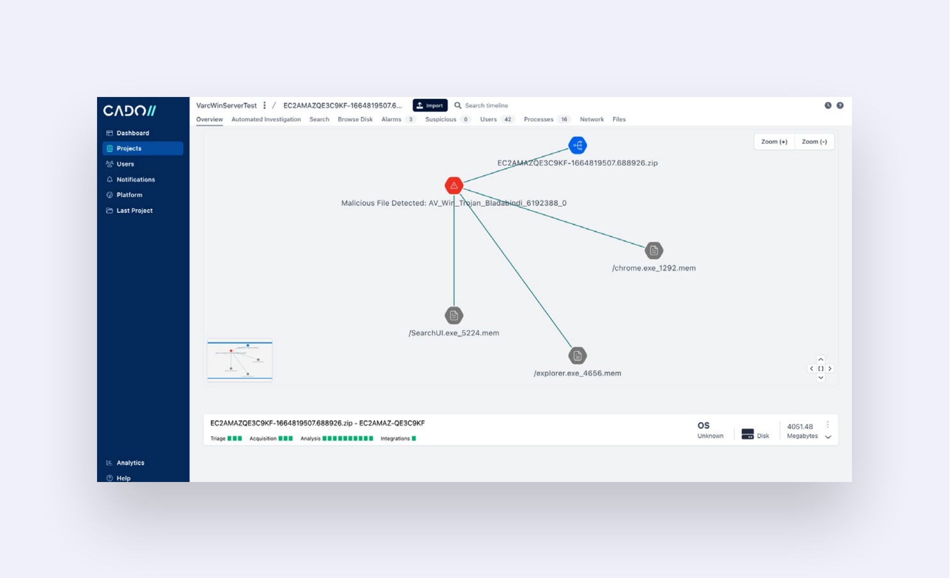
CADO//

JOINT SOLUTION HIGHLIGHTS

+ Automated 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 the Cado platform 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 platform, powered by machine learning and threat intelligence, automatically flags key malicious activity and compromised roles and assets so that analysts can rapidly understand incident scope. Further, Cado delivers a complete timeline of events and advanced search capabilities, allowing security teams to easily pivot their investigation and dive as deep into the data as required.



Conclusion

SentinelOne 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 forensic-level detail and context to identify root cause, understand the impact of breaches, and respond faster.

JOINT SOLUTION BENEFITS

✓

Respond to Breaches Faster

Automate in-depth incident investigations to drastically reduce time to respond.

✓

Add Depth to Your Investigation

Dig deeper with rich historical and forensic-level 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

MITRE ENGENUITY

Record Breaking ATT&CK Evaluation

- 100% Protection. 100% Detection.
- Top Analytic Coverage 3 Years Running
- 100% Real-time with Zero Delays

Gartner peerinsights 4.9 ★★★★★

99% of Gartner Peer Insights™

EDR Reviewers Recommend SentinelOne Singularity

FedRAMP

AICPA SOC

TEVORA
PCI DSS Attestation
HIPAA Attestation

vb 100 VIRUS virusbtn.com

SE Labs AAA Enterprise Endpoint Protection

SE Labs BEST Innovator WINNER 2021

About SentinelOne

SentinelOne (NYSE:S) is pioneering autonomous cybersecurity to prevent, detect, and respond to cyber attacks faster and with higher accuracy than ever before. Our Singularity XDR platform protects and empowers leading global enterprises with real-time visibility into attack surfaces, cross-platform correlation, and AI-powered response. Achieve more capability with less complexity.

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