SentinelOne

SOLUTION BRIEF

# Combine Behavioral Analytics, SOAR, and EDR for Enhanced Detection and Automated Endpoint Response

SentinelOne & Exabeam Joint Solution Brief

exabeam

## Market Challenges

With threats constantly targeting end-users, and devices, endpoint detection and response (EDR) solutions are valuable tools for proactive threat prevention, detection, investigation, and response. To understand the scope of an attack, security teams also must collect and contextually analyze information from a broad array of inputs, including servers, firewalls, and cloud-based services, to detect, investigate and respond to suspicious activity.

## Joint Solution

With Exabeam and SentinelOne, security teams can detect and investigate advanced attacks and insider threats by applying user and entity behavior analytics (UEBA) to SentinelOne events and alerts. SentinelOne's patented Behavioral AI prevents and detects threats at machine speed, delivering high-quality detections without human intervention. Exabeam establishes a behavioral baseline and ties all activity back to a user. Then when anomalous activity is detected, it adds risk to a user in their risk score so analysts can focus on the highest risk users versus chasing alerts. Analyst investigation is kicked off with a timeline that automatically stitches together all user activity, normal and abnormal, for any given session. When corrective action needs to take place, automated playbooks trigger automated response actions in SentinelOne.

## How It Works

01. SentinelOne monitors endpoint activity across all major operating systems and cloud workloads

02. SentinelOne's patented Behavioral AI detects malicious endpoint activity

03. Exabeam ingests alerts from SentinelOne

04. Exabeam baselines normal user and endpoint activity using UEBA and then automatically detects deviations from those behavioral baselines

05. Risk is added to the relevant user or entity for each anomalous activity detected

06. Threats are automatically prioritized by risk score to focus analyst efforts on high-risk anomalies

07. Response playbooks can be used to take automated corrective actions in SentinelOne to prevent data loss such as disconnecting an endpoint from the network

## JOINT SOLUTION HIGHLIGHTS

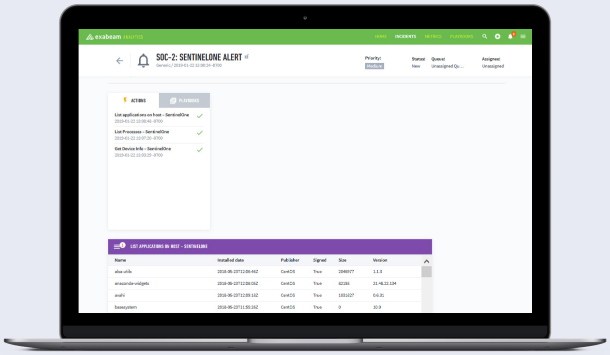
- Modernize SOC operations with AI-driven EDR and security analytics
- Improve your security posture
- Enhance analyst productivity

## INTEGRATION BENEFITS

**Lateral Movement Protection**
Monitor endpoints with Behavioral AI and report to Exabeam for consolidated alerting and correlation

**Intelligently Investigate**
Dramatically reduce analyst time spent investigating incidents with context-rich alerts from SentinelOne and Smart Timelines from Exabeam

**Rapidly Respond**
Boost response productivity with pre-built playbooks that automate and standardize actions including containment, mitigation, and endpoint response



SOC-2: SENTINELONE ALERT
Generic / 2019-01-22 13:00:24 -0700

Priority: Medium
Status: New
Queue: Unassigned Qu...
Assignee: Unassigned

List applications on host – SentinelOne ✓
2019-01-22 13:08:48 -0700

List Processes – SentinelOne ✓
2019-01-22 13:07:20 -0700

Get Device Info – SentinelOne ✓
2019-01-22 13:03:29 -0700

LIST APPLICATIONS ON HOST – SENTINELONE

| Name | Installed date | Publisher | Signed | Size | Version |
|---|---|---|---|---|---|
| alsa-utils | 2018-05-23T12:06:46Z | CentOS | True | 2046977 | 1.1.3 |
| anaconda-widgets | 2018-05-23T12:08:05Z | CentOS | True | 82195 | 21.48.22.134 |
| avahi | 2018-05-23T12:09:18Z | CentOS | True | 1031827 | 0.6.31 |
| basesystem | 2018-05-23T11:55:26Z | CentOS | True | 0 | 10.0 |

Exabeam automatically obtains key details from Sentinel One as part of analyst investigations, such as understanding the list of applications run on a host

## READY FOR A DEMO?

Visit the SentinelOne website for more details.

# Solution Use Case

## Threat Detection, Investigation and Response

- Data exfiltration
- Lateral movement
- Compromised credentials
- Evasion
- Malware
- Phishing
- Privilege abuse
- Privilege escalation
- Ransomware

## SOC Operations

- Incident investigation
- Ticket tracking and resolution
- Automated Incident Response

# Conclusion/Summary

The combination of SentinelOne and Exabeam uses behavior analytics to bridge the gap between endpoint activity and other security tools as part of a modern security management strategy.

## SentinelOne is a Customer First Company

Continual measurement and improvement drives us to exceed customer expectations.

Gartner peerinsights customers' choice™

97% Of Gartner Peer Insights™ 'Voice of the Customer' Reviewers recommend SentinelOne

97% Customer Satisfaction (CSAT)

FR FedRAMP

ISO 27001 CERTIFIED by schellman

EU GDPR COMPLIANT

SE Labs AAA AUGUST 2020 BREACH RESPONSE (PROTECT)

TEVORA PCI DSS Attestation HIPAA Attestation

Gartner peerinsights™ 4.9 ★★★★★

### 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 Exabeam

Exabeam helps security teams outsmart the odds by adding intelligence to their existing security tools – including SIEMs, XDRs, cloud data lakes, and hundreds of other business and security products. Out-of-the-box use case coverage repeatedly delivers successful outcomes. Behavioral analytics allows security teams to detect compromised and malicious users that were previously difficult, or impossible, to find. Automation helps overcome staff shortages by minimizing false positives and dramatically reducing the time it takes to detect, triage, investigate and respond. For more information, visit www.exabeam.com.

**sentinelone.com**

sales@sentinelone.com
+ 1 855 868 3733