SentinelOne

SOLUTION BRIEF

Extend Detection and Response to Email and Cloud Collaboration Apps

SentinelOne & Perception Point Joint Solution Brief

Market Challenges

Today, attackers are using all content channels to attack organizations, including email, file sharing, and cloud collaboration apps. In the 2021 Gartner Market Guide for Email Security, Gartner notes that with the shift to remote and hybrid working models, these communication tools and collaboration apps, with users outside of the organization, have the potential to be used by attackers for phishing and malware distribution. Ransomware can sit in an organization's environment just waiting to be executed on an endpoint. The task of cleanup and hunting for these artifacts, even after a successful detection on the endpoint is complicated, burdening SOC teams and taking time away from other important duties. SentinelOne and Perception Point have joined forces to enable the autonomous detection and response capabilities of SentinelOne to extend beyond the endpoint into all content channels of the organization.

Joint Solution

SentinelOne and Perception Point together offer a powerful solution for the modern enterprise. The integration between SentinelOne and Perception Point combines SentinelOne's industry-leading XDR protection with Perception Point's broad scope of threats from email, web, and cloud collaboration apps to provide extensive coverage of attack surfaces. With the two solutions working together, threat prevention is simplified and consolidated to stop attacks, with remediation and no additional time spent by security teams to quarantine files.

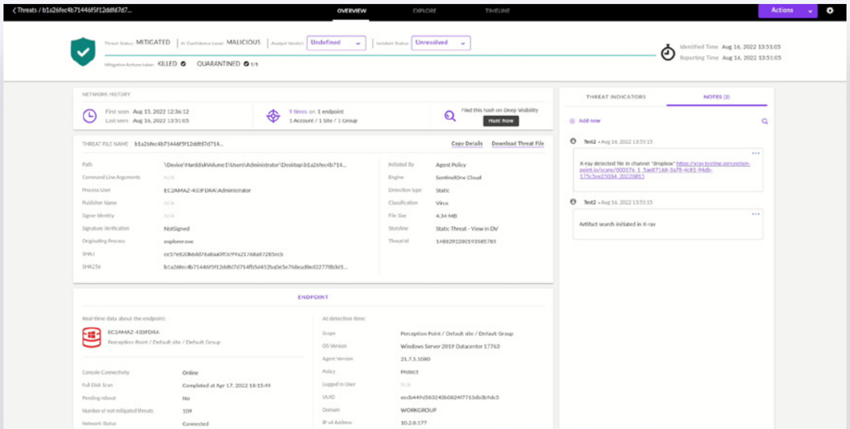
How it Works

- Perception Point integrates with SentinelOne via the SentinelOne API. When SentinelOne Singularity XDR detects an emerging threat, it will quickly mitigate the threat and send the file hash to Perception Point.
- Perception Point will trigger a file hash search for this artifact within the customer's different channels protected by Perception Point, including email, cloud collaboration apps, cloud storage and web browsers. The file is then quarantined by the Perception Point Incident Response team, containing and remediating it from the additional channels where it was found (e.g. removing emails from inboxes, OneDrive, SharePoint and more that contain the file).
- All threat files marked by Perception Point are retained for customers in Perception Point's management and operation dashboard - the X-Ray.
- Each action taken by Perception Point is annotated in the SentinelOne platform.

PERCEPTION POINT™

JOINT SOLUTION HIGHLIGHTS

- + Extend SentinelOne's autonomous malware detection and response capabilities to email and cloud collaboration apps
- + Accelerate containment and remediation capabilities to identify and quarantine attacks
- + Optimize security workflow across organization's technology stack, including endpoints, email, and cloud collaboration applications



Threat Status: MITIGATED | AI Confidence Level: MALICIOUS | Analyst Verdict: Undefined | Incident Status: Unresolved

Mitigation Actions taken: KILLED QUARANTINED 1/1

Identified Time Aug 16, 2022 13:51:05
Reporting Time Aug 16, 2022 13:51:05

NETWORK HISTORY

First seen Aug 15, 2022 12:36:12
Last seen Aug 16, 2022 13:51:05

9 times on 1 endpoint
1 Account / 1 Site / 1 Group

Find this hash on Deep Visibility

THREAT FILE NAME b1a26fec4b71446f5f12ddfd7d714...

Path	\Device\HarddiskVolume1\Users\Administrator\Desktop\b1a26fec4b714...	Initiated By	Agent Policy
Command Line Arguments	N/A	Engine	SentinelOne Cloud
Process User	EC2AMAZ-433FDRA\Administrator	Detection type	Static
Publisher Name	N/A	Classification	Virus
Signer Identity	N/A	File Size	4.34 MB
Signature Verification	NotSigned	Storyline	Static Threat - View in DV
Originating Process	explorer.exe	Threat Id	1488292280193585785
SHA1	ce57e820b6dd76a8aa0ff3c99a21768a87285ecb		
SHA256	b1a26fec4b71446f5f12ddfd7d714fb5d452ba065e768ead0ed22778b3d1...		

ENDPOINT

Real-time data about the endpoint:

EC2AMAZ-433FDRA
Perception Point / Default site / Default Group

Console Connectivity	Online
Full Disk Scan	Completed at Apr 17, 2022 18:15:49
Pending reboot	No
Number of not mitigated threats	109
Network Status	Connected

At detection time:

Scope	Perception Point / Default site / Default Group
OS Version	Windows Server 2019 Datacenter 17763
Agent Version	21.7.5.1080
Policy	Protect
Logged in User	N/A
UUID	eecb449d5832436b0824f7713db3b9dc5
Domain	WORKGROUP
IP v4 Address	10.2.0.177

Test2 • Aug 16, 2022 13:53:15

X-ray detected file in channel "dropbox" https://xray.testing.perception-point.io/scans/000176_1_5ae87168-3a78-4c81-94db-175c5ee25034_20220815

Test2 • Aug 16, 2022 13:53:15

Artifact search initiated in X-ray

SentinelOne has detected a threat file on the user's endpoint and Perception Point has now detected the same file within the Dropbox channel.

During the remediation phase, security analysts can retrieve SentinelOne threat notes and add them to the corresponding case in QRadar SOAR. Artifacts specific to the threat in SentinelOne can be added to the QRadar SOAR case during the investigation. As an incident is resolved in QRadar SOAR, the same incident is automatically closed within the SentinelOne console.

This powerful integration enables customers to easily coordinate endpoint triage and response efforts from within QRadar. The rich capabilities of this integration enables a complete response from the initial detection and alert down to one-click response actions, streamlining your security operation center (SOC) and alleviating the manual and repetitive tasks inundating security analysts.

Solution Use Cases

- **Advanced Email Security**

  Currently, 40% of ransomware attacks start through email, making it a crucial source that needs secure protection.1 These attacks open the threat environment for adversaries to deploy ransomware or malware to cloud collaboration applications, as well as other internal email accounts. When SentinelOne's patented behavioral AI detects a malicious file, security teams need to know if that file lives anywhere else within their content applications. This integration will enable the remediation of any additional files within email or cloud apps.

- **Cloud Apps and File-Sharing Security**

  Third parties may have access to shared folders in cloud storage sharing applications. This introduces an attacker to a new channel to deploy malware from a trusted third party. When this file is executed on a SentinelOne protected endpoint, quick autonomous response is provided with the integration to quarantine the file that is hosted outside of the endpoint to reduce the opportunity of spreading it.

INTEGRATION BENEFITS

✓ Rapid remediation with additional triage from Perception Point managed Incident Response service

✓ Reduce workloads on the SOC team by up to 75%, simplifying and shortening containment time

✓ Provide full visibility to attacks across the endpoint, email & cloud collaboration apps

> ❝ The threat landscape is only becoming more complex with attacks threatening organizations across multiple vectors," said Orit Shilvock, VP Sales at Perception Point. "We're excited to partner with SentinelOne to protect users from all threat types across their most used communication channels - endpoints, email, cloud collaboration apps, and cloud storage. The joint solution consolidates and simplifies threat prevention and remediation, boosting our customers' security posture while reducing the SOC team's workloads.
>
> PERCEPTION POINT

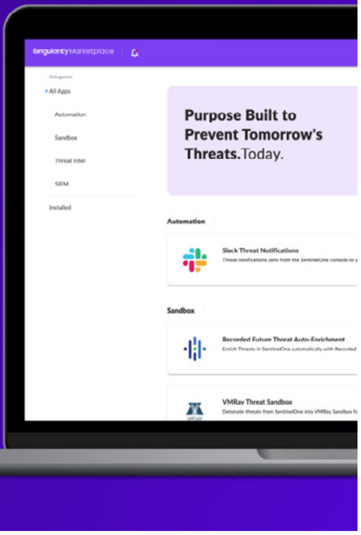
Conclusion

With the SentinelOne and Perception Point integration, joint customers can leverage SentinelOne's XDR protection and Perception Point's comprehensive coverage of email, web, and cloud collaboration applications for consolidated and simplified best-in-class security for an organization's attack surface. Together, security teams can better protect their organizations with XDR and autonomous containment and remediation.

Proactively resolve threats in real-time at the site of the cybersecurity battle: the computing and cloud edge.

Learn more in the Singularity Marketplace

Singularity Marketplace



Singularity Marketplace

Categories

- All Apps
- Automation
- Sandbox
- Threat Intel
- SIEM
- Installed

Purpose Built to Prevent Tomorrow's Threats. Today.

Automation

Slack Threat Notifications
Threat notifications sent from the SentinelOne console to y

Sandbox

Recorded Future Threat Auto-Enrichment
Enrich Threats in SentinelOne automatically with Recorded

VMRay Threat Sandbox
Detonate threats from SentinelOne into VMRay Sandbox fo

Ready for a Demo?

Visit the SentinelOne website for more details.

Singularity Platform

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 JAN–MAR 2021 ENTERPRISE ENDPOINT PROTECTION

SE Labs INTELLIGENCE-LED TESTING 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 Perception Point

Perception Point is a Prevention-as-a-Service company for the fastest and most accurate next-generation detection and response to all attacks across email, cloud collaboration channels, and web browsers. The solution's natively integrated incident response service acts as a force multiplier to the SOC team, reducing management overhead, improving user experience, and delivering continuous insights; providing proven best protection for all organizations.

sentinelone.com

sales@sentinelone.com
+ 1 855 868 3733

proofpoint.com