

Extend Advanced Threat Protection Across Endpoint and Cloud Environments

SentinelOne & Netskope Joint Solution Brief



JOINT SOLUTION HIGHLIGHTS

- + Share real-time intelligence across SentinelOne & Netskope
- + Automate policy enforcement across endpoint and cloud environments

Protecting the Invisible Perimeter

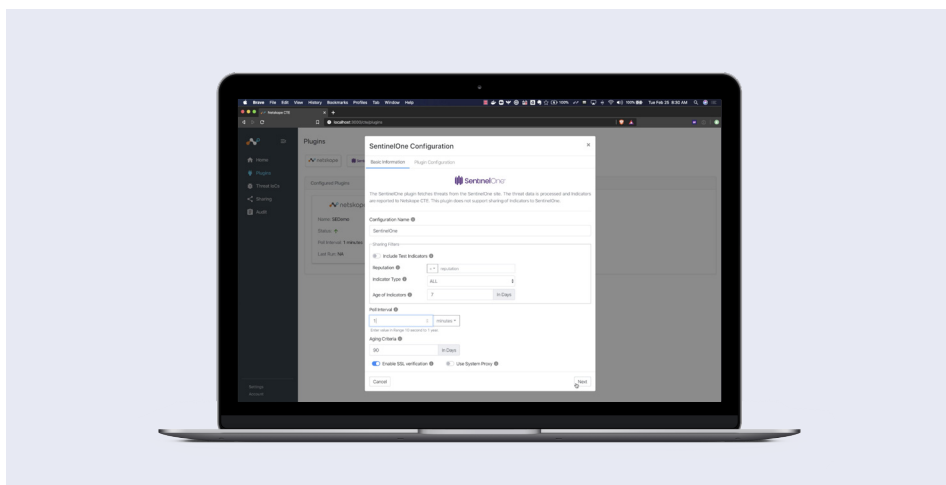
The ever-expanding perimeter has been a common trend in security for some time, but recent global events such as COVID-19 have accelerated remote working and dramatically increased cloud adoption. Security teams are challenged with the expanded attack surface while struggling to manage the complexity of multiple tools from multiple vendors. Visibility gaps between security tooling leave room for attackers to exploit and move undetected. With the rise of increasingly more evasive malware, the sharing of real-time threat intelligence across security investments has never been more crucial to making informed decisions for protection, detection and response.

Joint Solution




The integration with Netskope Cloud Threat Exchange provides SentinelOne with real-time intelligence feeds that contain malicious indicators of compromise (IOCs) observed across Netskope secure web-gateway (SWG), data loss prevention (DLP), and cloud access security broker (CASB) solutions. The bi-directional enrichment automatically adds malicious URLs and SHA256 hashes to the respective SentinelOne and Netskope blacklists. Automated blocking across solutions disrupt attempts at lateral movement creating a unified prevention, detection, and response surface from endpoint and cloud.

How It Works

Integration between SentinelOne and Netskope is easy to deploy and configure. All that is required to establish the connection is access to Netskope Cloud Threat Exchange (CTE) and

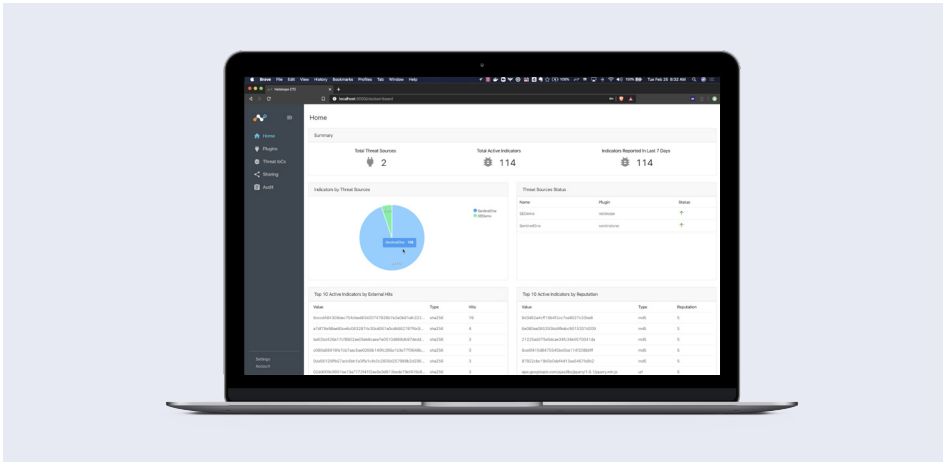


INTEGRATION BENEFITS

-  **Detect Multi-Vector Threat Activity**
-  **Autonomously Respond**
-  **Improve Time to Value**

the relevant information found in the SentinelOne management console (management URL, API token, site name). After selecting a polling interval, you can establish the connection and immediately begin sharing threat IOCs.

When SentinelOne detects malicious activity on an endpoint, it will prevent it and feed the malicious IOCs via API to Netskope Cloud Threat Exchange. Cloud Threat Exchange also ingests threat data from other complementary security tools, including SIEM, SOAR, firewalls, and CASBs for a unified view of IOCs across tools. As threat intelligence and IOCs are received by CTE, they are pushed via bi-directional API to connected solutions.



SentinelOne consumes the malicious hashes from CTE and automatically adds them to a blocklist, preventing previously seen threats in CTE from executing on an endpoint.

Additionally, IOCs from SentinelOne can be consumed by Netskope Threat Prevention List to enable real-time enforcement. As SentinelOne finds new malware, SHA256 hashes are shared with Netskope, preventing the malware from transiting through SaaS applications.

Conclusion

Together, SentinelOne and Netskope enable a more proactive stance against threats inside and outside the perimeter. The combined SentinelOne and NetSkope solution offers prebuilt automation and a network that is capable of immunizing itself – all the way from the endpoint to the cloud.

JOINT SOLUTION BENEFITS

The joint solution delivers a unified view of threats across endpoints and cloud and enables customers to:



Detect Multi-Vector Threat Activity

Use actionable indicators of compromise (IOCs) to identify multi-vector APT and malware activity



Autonomously Respond

Automate response with bi-directional policy enforcement in SentinelOne & Netskope helping reduce Mean time to respond (MTTR)



Improve Time to Value

Integrate intelligence across tools to unify security defenses

READY FOR A DEMO?

Visit the SentinelOne website for more details.

SentinelOne is a Customer First Company

Continual measurement and improvement drives us to exceed customer expectations.



97%

Of Gartner Peer Insights™ "Voice of the Customer" Reviewers recommend SentinelOne

97%

Customer Satisfaction (CSAT)



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?

sentinelone.com

sales@sentinelone.com
+ 1 855 868 3733