



SentinelOne: Fortinet Integration

SentinelOne Connector for Fortinet

Bringing together network and endpoint technologies to enable end-to-end autonomous security

SentinelOne Complements Fortinet with AI Based Advanced Threat Detection, Protection and Response Capabilities on the Endpoint

- Closing the gap on today's advanced security attacks requires tight integration between security solutions to detect new and existing threats, and to automatically respond within minutes. The old guard of legacy, traditional antivirus solutions simply can't keep pace with this fast-evolving threat landscape.
- SentinelOne provides autonomous endpoint protection through a single agent that prevents, detects and responds to attacks across all major vectors.
- Fortinet's partners can now deliver two best-of-breed products that work together seamlessly to provide enhanced levels of security for customers against sophisticated unknown threats, zero-day attacks and file-less attacks.

EMPOWERING THE FORTINET SECURITY FABRIC

- Fortinet and SentinelOne protect organisations from all types of threats with rich visibility in the network and at every endpoint, across every stage in the threat lifecycle.

THIS PROVIDES

- Complete visibility into all network and endpoint activity without performance drag
- Advanced static prevention and dynamic behaviour detection to protect against threats across all major vectors
- Integration and automation of threat management, prevention, detection, mitigation, response and remediation

Key Benefits

New Market Opportunities for Fortinet Partners

- Opportunities to provide additional services to customers combining Fortinet and SentinelOne's best-of-breed network and endpoint protection solutions.

Additional Services for Fortinet Partners

- Unlock new revenue streams and provide customers with even greater confidence in their existing Fortinet investments with enhanced capabilities: the integration delivers advanced security protection across networked, application, cloud and mobile environments.

Offer Best of Breed Solutions to Customers

- Seamless protection and ease of deployment; integration provides full interoperability with Fortinet's Security Fabric; FortiGate, FortiSandbox, FortiMail, FortiAuthenticator, FortiAnalyser and FortiSIEM.

USE CASES



Fortigate

Enhanced Network Access Control:

- Share threat data with Fortigate to isolate the endpoint (IP address) with dynamic firewall policy
- Manage network access control for clients with active threats.



FortiSandbox

- Dynamically synchronise blacklist and white lists between endpoint and FortiSandbox
- Validate suspicious threats on endpoint against FortiSandbox



FortiAuthenticator

- Dynamically send a disable message to FSSO to block user ID when active threat detected on endpoint and machine is compromised



FortiMail

- Enhance with zero day and sophisticated malware attacks in email attachments



FortiAnalyser

- Send Endpoint data to FortiAnalyzer for central logging and correlation



FortiSIEM

- Sharing threat intelligence with FortiSIEM to correlate events with all other security Fabric components