# Fortinet and SentinelOne Integrated Security Solution

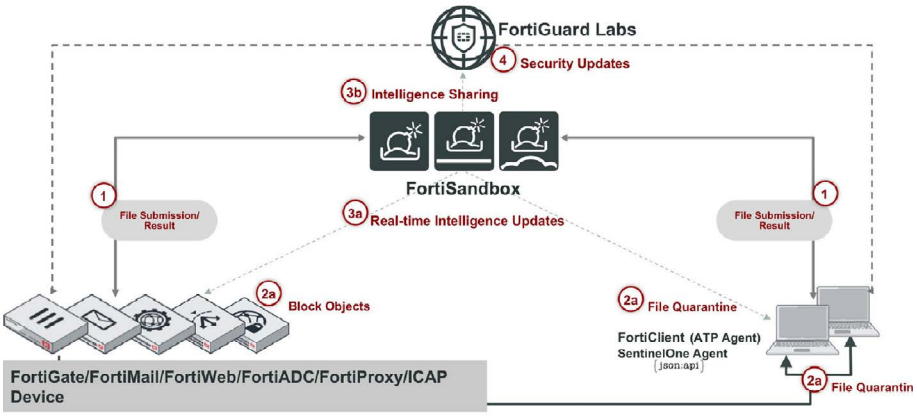
## Broad, Automated and Integrated Security with Total Endpoint and Network Protection

## Security Challenges

Security is at a tipping point - the complexity of IT has never been higher Cybercriminals continue finding new ways to exploit increasingly complex network environments. With more organizations adopting new network architecture in the cloud and running parallel IT, OT, and IoT dynamic networks, it has become imperative to ensure that endpoint, IoT, and other edge devices do not become a conduit for malware propagation.

Securing endpoints in today's highly dynamic network environments requires tightly integrated prevention, detection, and response capabilities that share intelligence, collaborate to detect and isolate threats, and synchronize remediation in real time at any point in the threat lifecycle.

The Fortinet and SentinelOne joint solution addresses the above challenges by delivering unparalleled security protection, detection, and response across networked, application, cloud and mobile environments by leveraging the Fortinet Security Fabric.




Threat Intelligence Sharing with Fortinet and SentinelOne

### Key Benefits

- Integrated Security Fabric protection across entire networks from endpoint to IoT to cloud, at all stages of the threat lifecycle
- Multi-layer, machine learning-driven endpoint prevention, detection, and response
- Policy-based automation enabled integrated control and proactive defence
- Zero-touch mitigation, robust containment, and fully automated remediation of threats
- Seamless defense adaptation with auto-immunization and cloud intelligence
- Cohesive security architecture for intelligence sharing between the network, cloud, and endpoints

FORTINET Fabric-Ready

# Joint Solutions Description

## FortiGate

The Fortinet FortiGate Firewall provides granular visibility across the entire digital attack surface, protecting enterprise networks from both known and unknown threats, zero-day exploits, and advanced malware. SentinelOne's advanced endpoint protection capabilities enable sharing of threat data with FortiGate's dynamic firewall policy for isolation of compromised endpoints via both IP and Mac addresses. It also makes it easier to manage network controls for clients with active threats, mitigating the risk of escalation. All endpoints, regardless of location inside or outside of the firewall - irrespective of a VPN - are protected with the joint capabilities of a unified endpoint and network layered security approach.

## FortiSandbox

FortiSandbox sits at the core of Fortinet's Advanced Threat Protection (ATP) capabilities, integrating with Fortinet's Security Fabric to provide actionable threat intelligence in real time. Integration with SentinelOne enables the solution to dynamically, and bidirectionally, synchronise blacklists with a protected endpoint, enhancing its ability to automatically detect and mitigate against zero-day and advanced malware threats.

## FortiClient

FortiClient Fabric Agent provides risk-based endpoint visibility by sharing endpoint telemetry and vulnerabilities. This allows enterprises to apply and enforce security compliance across an organization to preempt exposure to security threats. Enhanced intelligence and forensic insights from Fortinet and SentinelOne shared across the entire infrastructure in real-time provides protection at every stage of the threat lifecycle.

## FortiMail

FortiMail is a powerful email security solution that provides antispam, antiphishing, antimalware, data loss prevention (DLP), message archiving encryption, and sandboxing in a single platform to drastically reduce email-borne cyber threats. SentinelOne complements FortiMail's capabilities by detecting zero-day and sophisticated malware attacks hidden within email attachments or downloaded files. Once identified, all endpoints and the Fortinet Security Fabric assets are automatically immunized from the attempted attack.

## FortiAuthenticator

With Fortinet Single Sign-On (FSSO), FortiAuthenticator provides security identity and role-based access management for a Fortinet connected network. SentinelOne's advanced endpoint protection capabilities can dynamically send a message to the FSSO to block a user ID when an active threat is detected on an endpoint and the machine is compromised, stopping attackers from using the hijacked device. As soon as the threat is automatically remediated or further investigated, the device is reconnected.

## FortiSIEM

FortiSIEM addresses the growing complexity of manging network operations by providing a comprehensive, scalable way of monitoring all IT and security systems, from endpoints and IoT-enabled devices to cloud infrastructure. SentinelOne is able to share threat intelligence and comprehensive event logs with FortiSIEM to correlate security events across protected endpoints and all other Fortinet Security Fabric components.

## SentinelOne Connector

The SentinelOne Endpoint Protection Platform (EPP) unifies prevention, detection, and response in a single purpose-built agent powered by machine learning and automation. It provides 100% signatureless prevention and detection of attacks across all major vectors, rapid elimination of threats with fully automated, policydriven response capabilities, and complete visibility into the endpoint environment with full-context, real-time forensics. With the SentinelOne Fortinet Connector, joint customers have the ability to configure and enforce network access control on SentinelOne protected endpoints with FortiGate, FortiSandbox, FortiWifi, and FortiSwitch. Users can also quarantine and isolate threats with SentinelOne endpoints in conjunction with FortiAuthenticator, FortiGate, FortiSwitch, FortiMail, and share threat intelligence from the SentinelOne platform to FortiSandbox and FortiClient, instantly updating blacklists so additional Fortinet assets such as FortiGate can proactively lock next-gen threats inside and outside the network perimeter.



FORTINET

### FortiGate Enterprise Firewall

The Fortinet FortiGate network security platform provides high performance, layered security services and granular visibility for end to end protection across the entire enterprise network. Innovative security processor (SPU) technology delivers high-performance application layer security services (NGFW, SSL inspection, and threat protection), coupled with the industry's fastest SSL inspection engine to help protect against malware hiding in SSL/ TLS encrypted traffic. The platform also leverages global threat intelligence to protect individual customers, by using Fortinet's FortiGuard Security Subscription Services to enable visibility and control for next-generation protection against advanced threats, including zero-day attacks.

## About SentinelOne

SentinelOne's breakthrough platform unifies autonomous prevention, detection, and response driven by machine learning and intelligent automation. SentinelOne EPP is a certified antivirus replacement, recognized by Gartner and NSS Labs for its disruption, and trusted by more than 2,000 of the world's most forward-thinking companies to replace multiple legacy AV products with a unified EPP + EDR solution.

For more information, visit: www.sentinelone.com





123456-0-0-EN

Mac:Users:susiehwang:Desktop:Egnyte:Egnyte:Shared:Creative Services:Team:Susie-Hwang:Egnyte:Shared:CREATIVE SERVICES:Team:Susie-Hwang:2018:Collateral-Refresh-2018:Solution-Brief-Template:sb-template-gray Folder:sb-template-gray