Forcepoint

Microsoft Sentinel Integration

with Forcepoint ONE

Key Benefits:

- **Enhanced Threat Detection and Response** Leverage the combined capabilities to improve threat detection and response.
- **Centralized Security Analytics** Enable the aggregation of security logs, events, and telemetry from the Forcepoint ONE platform into a centralized system like Microsoft Sentinel.
- **Automated Incident Response** Empower your organization to automate incident response processes.
- **Integrate** without incurring additional compute costs in Azure.

Forcepoint ONE and Microsoft Sentinel work together to offer Security Operations teams an integrated solution for precise web, cloud and private applications security reporting.

Forcepoint ONE combines Zero Trust and SASE security technologies, including three secure access gateways (SWG, CASB and ZTNA) with shared threat protection and data security services, all built on a cloud-native platform. Using Forcepoint ONE REST APIs, detailed logs are sent to Microsoft Sentinel for further analysis and reporting. By using the fully managed (SaaS) Codeless Connector Platform (CCP) of Microsoft Sentinel in building data connectors, customers are eliminating the cost of building additional compute resources to retrieve or process logs.

Forcepoint ONE makes security simple for distributed businesses and government agencies that need to adapt quickly to changing remote and hybrid workforces. It aggregates traffic from the Secure Web Gateway (SWG), Cloud Access Security Broker (CASB) and Zero Trust Network Access (ZTNA) solutions, reducing the hassle of pulling data from separate sources. Microsoft Sentinel can then correlate with other relevant sources to create a comprehensive view of an organization's security posture.

Enhanced Threat Detection and Response

By integrating the Forcepoint ONE platform with Microsoft Sentinel, organizations can leverage the combined capabilities to improve threat detection and response. The Forcepoint ONE platform provides real-time visibility into network traffic, user behavior and application usage, while Microsoft Sentinel aggregates and analyzes security event data from multiple sources. The integration allows for more accurate threat detection, correlation of events and faster incident response.

Centralized Security Analytics

Integrating Forcepoint ONE with Microsoft Sentinel enables the aggregation of security logs, events and telemetry from the Forcepoint ONE platform into a centralized system. This consolidation of data provides a holistic view of the organization's security posture, allowing for comprehensive security analytics, trend analysis and proactive threat hunting.

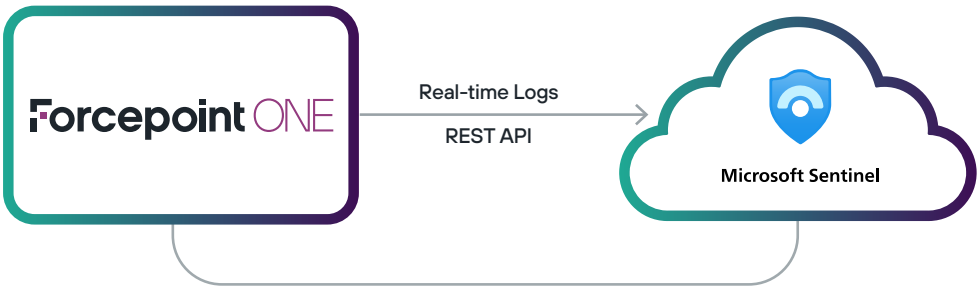
Forcepoint

Automated Incident Response

The integration of the Forcepoint ONE platform with Microsoft Sentinel empowers organizations to automate incident response processes. When a data security incident, security event or anomaly is detected by the Forcepoint ONE platform, the integration with Microsoft Sentinel can trigger automated response actions, such as blocking malicious traffic, quarantining compromised devices or initiating investigation workflows. This reduces response time, enhances efficiency and minimizes the impact of security incidents.

Policy Enforcement and Compliance

The integration of the Forcepoint ONE platform with Microsoft Sentinel empowers organizations to automate incident response processes. When a data security incident, security event or anomaly is detected by the Forcepoint ONE platform, the integration with Microsoft Sentinel can trigger automated response actions, such as blocking malicious traffic, quarantining compromised devices or initiating investigation workflows. This reduces response time, enhances efficiency and minimizes the impact of security incidents.



Forcepoint ONE Platform Features

→ Contextual access control

→ Data Loss Prevention (DLP)

→ Field Programmable SASE Logic (FPSL)

→ Malware scanning

→ Unified management console for configuration, monitoring and reporting for SWG, CASB and ZTNA

→ GRE and IPSEC support

→ Unified on-device agent

→ 99.99 percent service uptime

About Forcepoint

Forcepoint simplifies security for global businesses and governments. Forcepoint's all-in-one, truly cloud-native platform makes it easy to adopt Zero Trust and prevent the theft or loss of sensitive data and intellectual property no matter where people are working. Based in Austin, Texas, Forcepoint creates safe, trusted environments for customers and their employees in more than 150 countries. Engage with Forcepoint on www.forcepoint.com, Twitter and LinkedIn.

Forcepoint

[FP-Forcepoint ONE-Microsoft-Sentinel-Integration-Flyer-US-EN] 21Sep2023