

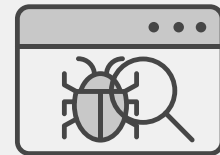
Navigating the Complex Cybersecurity Landscape with FortiGuard SOC-as-a-Service

Executive Summary

In today's digital world, organizations are inundated with data from an array of logs and alerts. Meanwhile, the rise of AI makes it easier than ever for even novice cybercriminals to execute attacks, and the proliferation of connected devices makes for an always-expanding attack surface. Even the most skilled, well-staffed security teams find it challenging to keep pace. As digital initiatives expand, attacks occur, and organizations need help keeping up with evolving threats and the demanding requirements of 24x7 security operations.

FortiGuard Security Operations Center-as-a-Service (SOCaaS), a cloud-based SOC, integrates advanced AI and ML to provide real-time threat detection and response.

This solution is crucial for organizations grappling with the cybersecurity skills gap, as FortiGuard SOCaaS offers continuous, expert monitoring and incident handling without requiring extensive in-house resources. Leveraging a SOCaaS offering is an effective response to escalating cyberthreats and resource scarcity, providing a comprehensive solution to organizations overwhelmed by the complexity of modern cybersecurity.



The top reason organizations believe security operations are more difficult than two years ago is that the threat landscape is evolving and changing rapidly.¹

Global Response Teams

- SOC
- Data Center
- Disaster Recover

99.99%
Availability

24x7x365
Service Hours

Unlimited
Log Capacity

FortiGate & Security Fabric Logs
Ingest Log Data

Fast & Simple
Onboarding



Critical Escalation Times

- P1, Priority 1:** 15 minutes
- P2, Priority 2:** 45 minutes
- P3, Priority 3:** 90 minutes
- P4, Priority 4:** 6 hours


Figure 1: FortiGuard SOCaaS global response teams, security operations, and data centers


Choose FortiGuard SOCaaS for 24x7 Security Monitoring and Threat Management


FortiGuard SOCaaS allows organizations to establish essential security monitoring and threat detection while avoiding the need for a significant initial investment in specialized personnel or technology infrastructure. FortiGuard SOCaaS leverages the expertise of Fortinet’s security professionals, who utilize advanced AI and ML for effective threat detection and alert triage. Following an incident investigation, the SOC team promptly notifies customers within 15 minutes, offering detailed insights into the incident’s nature and remediation steps. The SOC2-certified service features a user-friendly, cloud-based management console for operational integration, providing comprehensive visibility into security events, real-time communication with experts, and tools for continual improvement. It also includes customizable reporting options and quarterly expert reviews for strategic enhancement, addressing the challenges of threat volumes and cybersecurity skill shortages.

This expert-driven service allows businesses to refocus their efforts on more strategic priorities, entrusting daily monitoring to specialized professionals. In practical scenarios like phishing attacks, the proactive detection organizations get from FortiGuard SOCaaS ensures an early and effective response, significantly reducing the potential damage a threat may cause. Organizations can also augment their FortiGuard SOCaaS capabilities by integrating select Fortinet solutions and services with this offering.

Take Your Time Back

- 

24x7x365 Monitoring
Supplement FortiGate log and alert monitoring and triage with Fortinet security experts
- 

Get ahead
Reduce employee burnout and recapture critical work cycles
- 

Global Support
24x7 global coverage with live human experts

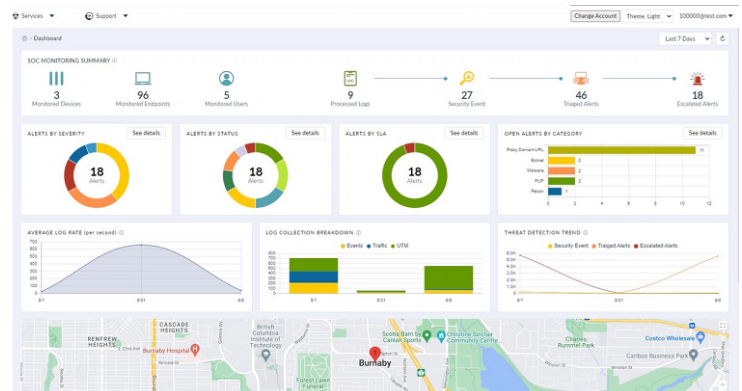


Figure 2: The FortiGuard SOCaaS cloud-based portal summary dashboard

FortiSASE Ensures Consistent Analysis for On-Premises and Remote Users

Integrating FortiGuard SOCaaS with Fortinet FortiSASE (secure access service edge) significantly enhances network security. FortiSASE functions by enforcing stringent security policies and managing network traffic in response to threats detected by the SOCaaS. Users can configure log forwarding from FortiSASE to SOCaaS through the management console, focusing specifically on FortiGate logs. This selective logging ensures that SOCaaS receives only pertinent data, enabling more effective monitoring and analysis. This approach effectively reduces data overload, streamlining the identification and response process to focus on legitimate threats. In daily operations, this integration means that when FortiSASE identifies a network anomaly, SOCaaS is immediately informed, facilitating a rapid, coordinated response. This seamless cooperation results in a more robust network defense and a resilient cybersecurity strategy.

FortiClient Forensics Service Offers Detailed Security Investigations


FortiClient Forensics Service enhances FortiGuard SOCaaS capabilities by providing in-depth investigation of complex threats. For instance, when FortiGuard SOCaaS flags a sophisticated malware attack, teams can use FortiClient Forensics Service, accessible directly through the SOCaaS portal, to conduct a comprehensive examination. This integration is crucial for businesses dealing with complex security scenarios, as it combines the real-time detection and monitoring capabilities of FortiGuard SOCaaS with the detailed forensic analysis of FortiClient, significantly strengthening the incident response process.



Managed FortiGate Service Unifies Network and Security Operations

Integrating the Managed FortiGate Service with FortiGuard SOCaaS is vital for enhancing network security, offering a unified approach to network and security operations. This integration provides robust perimeter defense with managed next-generation firewall capabilities, making it ideal for businesses aiming to boost network security without the significant management overhead. Especially beneficial for organizations with limited cybersecurity resources, it effectively reduces the internal burden of security management.

Once FortiGuard SOCaaS identifies a potential threat, the Managed FortiGate Service can automatically strengthen network defenses. This could involve automated adjustments to firewall settings or deploying additional security measures in response to SOCaaS alerts, ensuring the organization maintains a comprehensive and agile defense against evolving threats. In cases of breach detection, the Managed FortiGate Service will swiftly implement security measures, such as isolating network segments, underscoring its essential role in a well-rounded and dynamic defense strategy.



Customers say that, on average, Fortinet endpoint detection and response technologies helped them to reduce their mean time to detect by 99% or more.²

Service Integrations

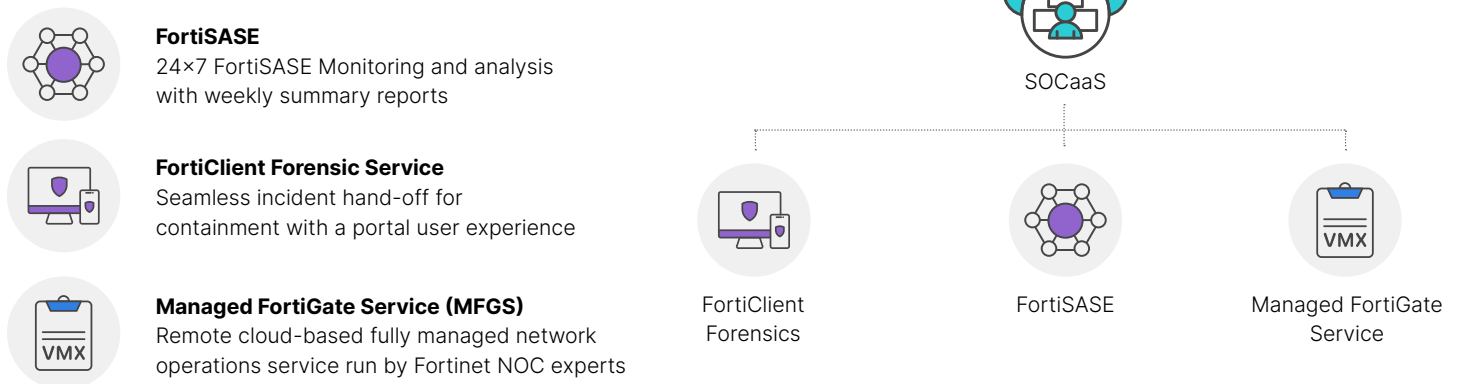


Figure 3: FortiGuard SOCaaS integrations overview

Conclusion

Integrating the FortiGuard SOCaaS with FortiSASE, FortiClient Forensics Service, and Managed FortiGate Service helps security teams create an effective cybersecurity solution. Each service complements FortiGuard SOCaaS and enhances capabilities across the cyber kill chain, leading to more operational efficiencies, quicker threat response times, more in-depth investigations, and robust network defense.

FortiGuard SOCaaS, combined with strategic integrations, equips businesses to confront modern cybersecurity challenges effectively. This holistic approach addresses the evolving digital threat landscape and offers substantial operational and strategic benefits, providing organizations with enhanced cyber resilience and stronger defenses. Our unified Fortinet Security Fabric platform that combines secure networking, unified SASE, and AI-driven security operations redefines cybersecurity, helping you to respond to an ever-evolving threat landscape to meet constantly changing business needs.

¹ Jon Oltsik, [Active Defense and Deception Technology: The Time is Now](#), Enterprise Strategy Group, June 2023.

² Aviv Kaufmann, [The Quantified Benefits of Fortinet Security Operations Solutions](#), Enterprise Strategy Group, July 2023.