SERVICE BRIEF

Reduce Risk and Maintain Compliance with the FortiGuard Attack Surface Security Service

Executive Summary

Today's attack surface is broader and more dynamic than ever, spanning IT, IoT, and OT environments. Constant configuration changes, new assets, and evolving threats make it difficult for organizations to maintain a strong security posture and demonstrate ongoing compliance using traditional, point-in-time assessments.

The FortiGuard Attack Surface Security Service integrates with FortiGate Next-Generation Firewalls (NGFWs) and provides continuous, real-time visibility into security posture across the Fortinet Security Fabric. By delivering continuous assessment instead of periodic audits, FortiGuard Attack Surface Security helps security and IT teams proactively reduce risk, maintain compliance, and communicate security posture clearly to executive leadership and auditors, without manual reports.

Overview

The FortiGuard Attack Surface Security Service, part of the FortiGuard AI-Powered Security Services portfolio, is a continuous assessment service designed to help organizations understand, measure, and improve their security posture across an expanding attack surface. Integrated into FortiGate NGFWs and the broader Fortinet Security Fabric, the service provides real-time visibility into configurations, vulnerabilities, and security controls across IT, IoT, and OT environments. By continuously monitoring the environment and evaluating settings against established best practices and industry frameworks, the service enables organizations to identify risk earlier and reduce exposure before issues can be exploited.

The service includes security rating capabilities that translate technical findings into clear, measurable security posture and compliance scores. These scores help organizations assess adherence to security frameworks, while tracking improvement over time. Unlike traditional point-in-time audits, FortiGuard Attack Surface Security delivers ongoing assessment, actionable remediation guidance, and executive-level reporting, enabling security teams to maintain a high security posture and demonstrate continuous compliance in dynamic environments.

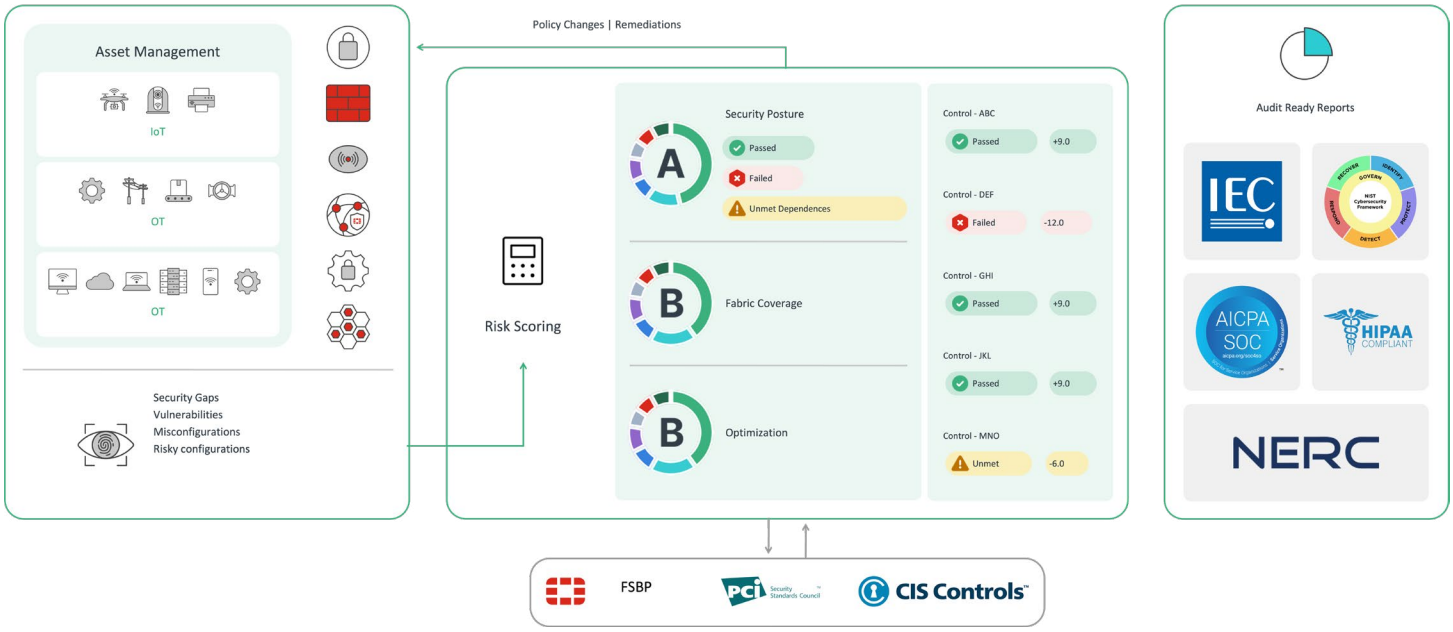


Figure 1: FortiGuard Attack Surface Security Service overview

With FortiAnalyzer integration, FortiGuard Attack Surface Security provides audit-ready compliance reports that map security posture and configuration data to widely adopted regulatory and industry standards. These reports support mandate requirements, enabling organizations to simplify audits and demonstrate compliance with consistent, evidence-based reporting.

Key Business Outcomes

Maintain a high security posture

Continuously understand and improve the overall health of your security environment as it evolves. The service:

- Assesses security configurations continuously across the Fortinet Security Fabric to identify gaps before they can be exploited
- Uses security rating scores to provide a clear, measurable view of overall security health and improvement over time

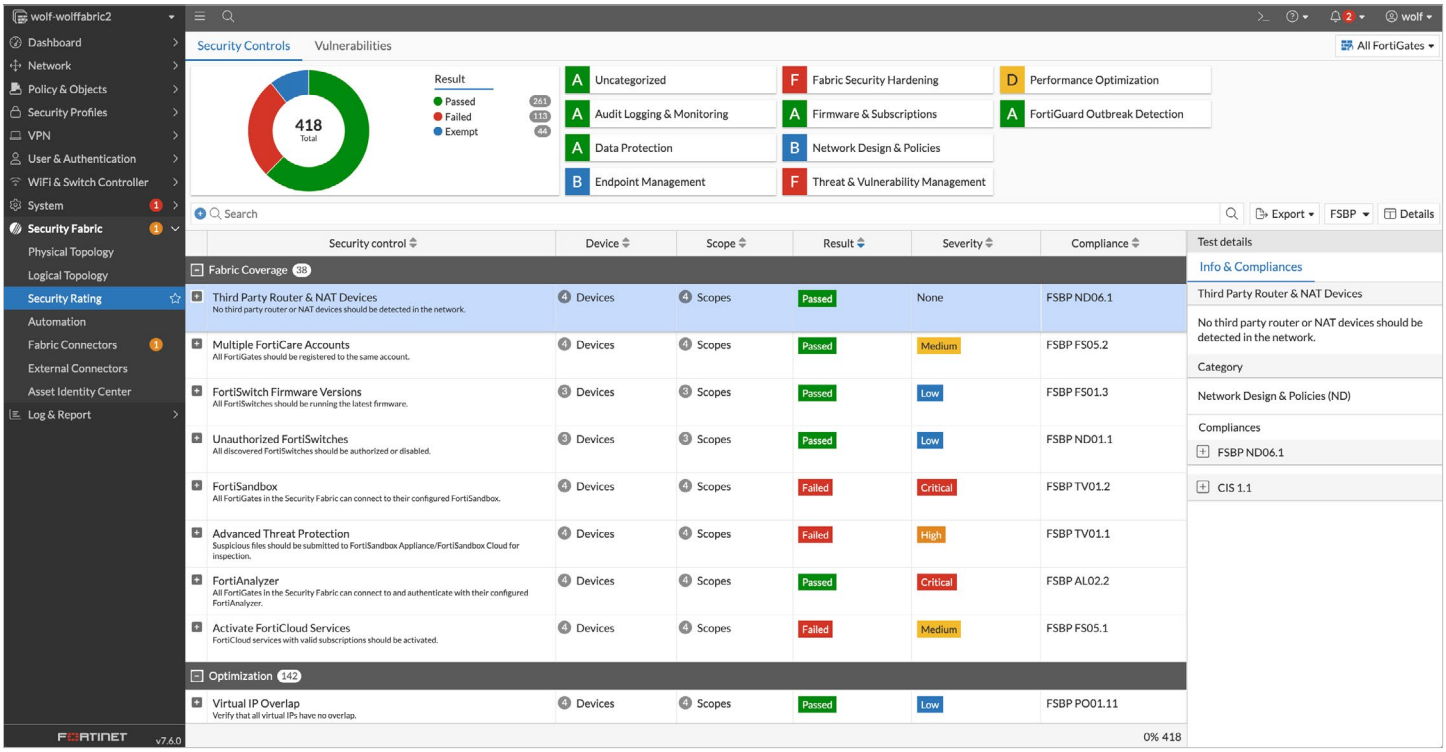


Figure 2: Security posture assessment

Reduce risk from misconfigurations and vulnerabilities

Proactively identify and address weaknesses that increase exposure across IT, IoT, and OT environments. The service:

- Identifies configuration weaknesses, unpatched vulnerabilities, and suboptimal settings across IT, IoT, and OT assets
- Provides actionable remediation guidance so teams can quickly address the most critical risks

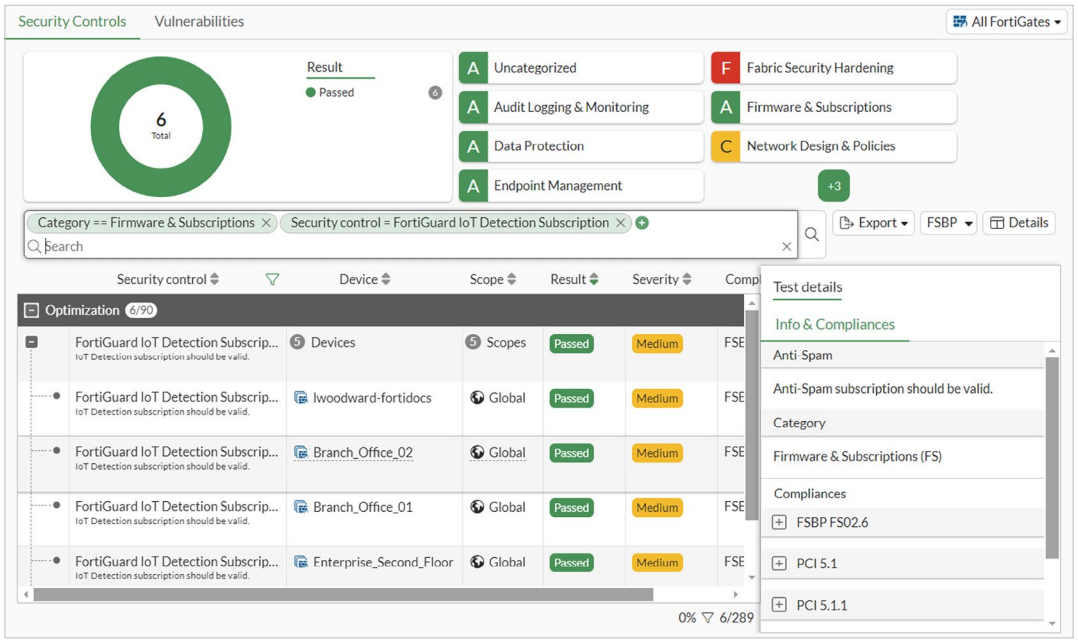


Figure 3: IoT visibility and protection

Demonstrate continuous compliance

Move beyond point-in-time audits to ongoing compliance assessment and validation. The service:

- Measures adherence to established frameworks such as CIS Controls, PCI DSS, and Fortinet Security Best Practices
- Replaces point-in-time compliance checks with ongoing assessment and reporting that reflects true operational conditions

Improve visibility across the expanding attack surface

Gain a consolidated, real-time view of assets, configurations, and risk across distributed environments. The service:

- Delivers consolidated visibility into assets, configurations, and risk across distributed and hybrid environments
- Extends attack surface awareness to connected IoT devices to help uncover hidden exposure
- Provides protection against outbreaks

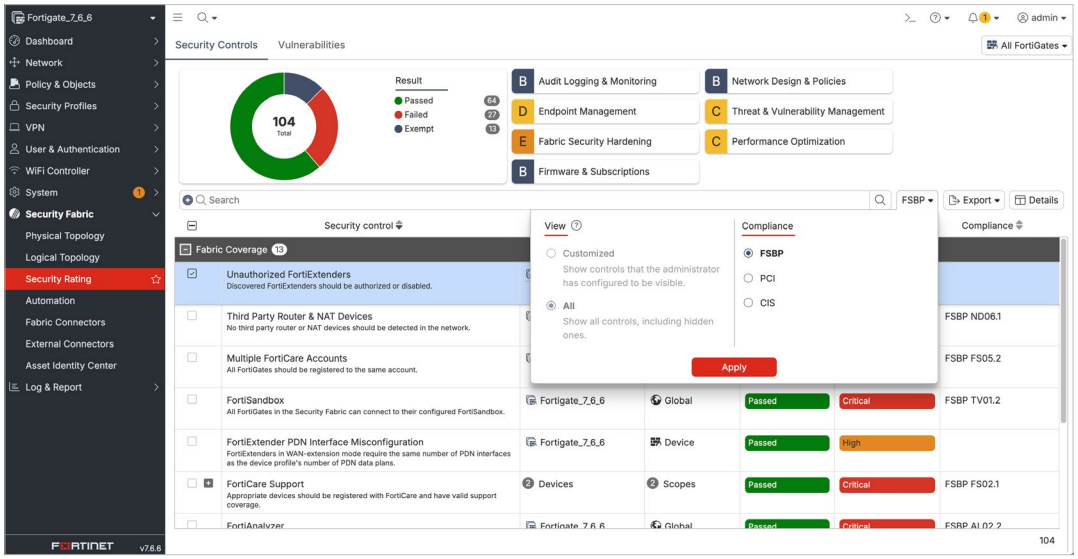


Figure 4: Protection against outbreaks

Enable audit-ready reporting and executive communication

Translate technical posture data into clear, defensible reporting for audits and leadership. The service:

- Provides consumable dashboards and reports that help security leaders communicate posture, compliance status, and progress to executives, boards, and auditors
- Integrates with FortiAnalyzer to produce audit-ready compliance reports aligned to key standards such as NERC CIP, NIST CSF, IEC 62443, HIPAA, and SOC 2

FortiGuard Attack Surface Security Service Benefits

The FortiGuard Attack Surface Security Service:

- Guides admins in the design, implementation, and maintenance of target security postures
- Identifies critical vulnerabilities and configuration weaknesses
- Provides continuous, consolidated, and granular visibility into scoring of your organization's security posture against best practices and major frameworks
- Generates clear remediation guidance for addressing areas of risk
- Expands attack surface visibility to cover IoT devices
- Protects against outbreaks

Key Fabric Integrations

The FortiGuard Attack Surface Security Service is tightly integrated with FortiGate NGFWs and NGFW-based solutions. Key integrations include:

- FortiGate NGFW
- FortiAnalyzer
- Fortinet Secure SD-WAN
- Fortinet Unified SASE

How the FortiGuard Attack Surface Security Service Works

The FortiGuard Attack Surface Security Service continually assesses security infrastructure, validates that configurations are working effectively, and provides awareness of risks and vulnerabilities that could impact business operations.

The rating aspects of the service apply to all devices in the organization's Security Fabric. Real-time monitoring analyzes the Security Fabric deployment, identifies potential vulnerabilities, highlights best practices to improve the network's security and performance, and calculates Security Fabric scores.

By enabling the service in the FortiGate user interface, organizations can easily identify key deficiencies, take action based on automated recommendations, secure the entire Security Fabric, and perform passive monitoring based on Fortinet Security Fabric scores.

The security rating gives grades in the following areas:

- Fabric security hardening
- Audit logging and monitoring
- Threat and vulnerability management
- Network design and policies
- Endpoint management
- Firmware and subscriptions
- Performance optimization

Scoring is calculated when a security rating check is run based on the severity level of the passed or failed checks. A higher score represents a more secure network environment. Points are added for passed checks and subtracted for failed checks.

Why FortiGuard Attack Surface Security?

As digital environments continue to change at machine speed, security posture and compliance can no longer be managed through periodic assessments or disconnected tools. Organizations need continuous awareness of how configuration changes, new assets, and evolving threats impact their real-world risk and regulatory standing. FortiGuard Attack Surface Security addresses this challenge by embedding ongoing posture assessment, measurable security ratings, and compliance validation directly into the Fortinet Security Fabric, turning security oversight into an operational capability rather than an after-the-fact exercise.

By combining real-time visibility, actionable insights, and audit-ready reporting, FortiGuard Attack Surface Security helps organizations stay ahead of risk while simplifying how they demonstrate accountability to regulators, auditors, and executive stakeholders. This enables security leaders to focus less on proving security after the fact, and more on confidently maintaining a resilient, compliant security posture as the business evolves.



FortiGuard Labs, Fortinet's elite threat research organization, uses AI, ML, and deep learning to provide real-time, contextual, and actionable threat intelligence that enables FortiGuard AI-Powered Security Services to proactively protect against all types of threats in real time.

FortiGuard AI-Powered Security Services deliver real-time, proactive, and layered defense across your entire infrastructure. Composed of 20+ services integrated throughout the Fortinet Security Fabric, they provide comprehensive protection from the full spectrum of threats including zero-days and AI-powered threats. Networks, files, content, web traffic, SaaS deployments, data, users, and critical infrastructure are safeguarded, ensuring compliance, data integrity, and real-time protection.

Copyright © 2026 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's SVP Legal and above, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

April 16, 2026 3:22 PM / MKTG-3157-0-0-EN