PORTFOLIO BRIEF

FortiGuard AI-Powered Security Services

One of the most effective ways to protect your organization from today's sophisticated threats is to disrupt the attack sequence. However, today's ever-expanding attack surface requires a security framework able to rapidly adjust your security posture to detect and respond to newly discovered attacks, regardless of where they occur.

The FortiGuard AI-Powered Security suite of services provides market-leading security capabilities designed to protect application content, web traffic, devices, and users wherever they are. It continuously assesses risks and automatically responds to and counters known and unknown threats anywhere across the distributed network. Its coordinated and consistent real-time services defend against the latest attacks

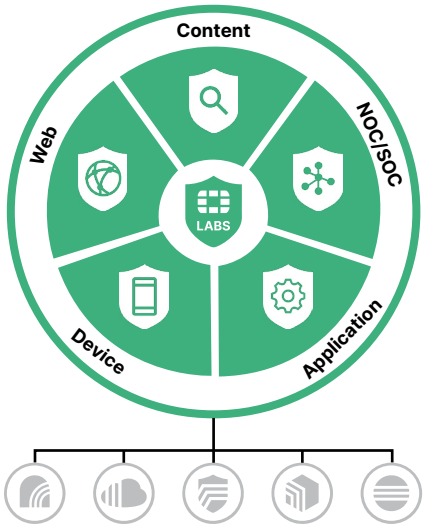
Counter Threats in Real Time with AI-Powered Coordinated Protection

FortiGuard AI-Powered Security Services is natively integrated into the Fortinet Security Fabric to deliver coordinated detection and enforcement across the entire attack surface. Its technology continuously assesses risks and automatically adjusts the Security Fabric to counter known and unknown threats, including evasive and malicious AI-powered threats in real time, regardless of where they occur, through context-aware, consistent security policy for users and applications, even across hybrid deployments that span the traditional network, endpoints, and clouds.

Our FortiGuard Labs cybersecurity experts are also constantly enhancing our industry-leading combination of static analysis augmented by rapid intelligence based on AI and ML (machine learning) models using large-scale, cloud-driven data sets and working with hundreds of intelligence-sharing partners.

Stay Ahead of the Game

Get your team focused by shifting to a security strategy that enables you to move faster and safer than ever before. FortiGuard Security Services delivers a powerful combination of actionable AI-driven intelligence integrated with inline protection to detect and counter evasive and never-seen-before threats. Coordinated market-leading security capabilities provide protection across the attack life cycle and surface.



100+B Global Events Analyzed per Day

1+B Actional Updates per Day

1,000 Zero Days Discovered

Figure 1: FortiGuard Security Domains

Consistent and Coordinated Security Detection and Response

The Fortinet Security Fabric is natively integrated with FortiGuard actionable threat intelligence, which continuously updates its rich content, web, device, and user security capabilities across the distributed Security Fabric.

The Security Fabric uses the FortiOS operating system, common standards, and open APIs, enabling you to connect and leverage your existing investments, creating a unified, proactive security posture.

		NGFW	SASE	SDWAN	WIFI	ADC	FCT	CNP	DECP	DDOS	EDR	FAZ	MAIL	NDR	PROXY	SBX	SIEM	WEB
Content Security	FortiGuard Antivirus Service	✓	✓	✓	✓	✓	✓	✓			✓		✓	✓	✓	✓		✓
	FortiGuard Credential Stuffing Defense Service					✓												✓
	FortiGuard AI-based Inline Malware Prevention	✓	✓	✓	✓	✓	✓	✓			✓		✓	✓	✓	✓		✓
	FortiGuard Data Loss Prevention Service (DLP)	✓	✓	✓	✓								✓					
Web Security	FortiGuard Anti-Botnet and C2 Service	✓	✓	✓	✓		✓							✓	✓			✓
	FortiGuard Domain Reputation Service [DDoS Only]									✓								
	FortiGuard DNS Filtering Service	✓	✓	✓	✓										✓			
	FortiGuard IP Reputation Service					✓				✓								✓
	FortiGuard URL Filtering Service	✓	✓	✓	✓	✓			✓						✓	✓		
	FortiGuard Video Filtering Service	✓	✓	✓	✓										✓			
Device Security	FortiGuard IPS Service	✓	✓	✓	✓	✓								✓	✓			
	FortiGuard OT Security Service	✓	✓	✓	✓													
	FortiGuard Attack Surface Security Service (IoT device coverage)	✓	✓	✓	✓													
Application Security	FortiGuard Application Control Service	✓	✓	✓	✓										✓			
	FortiGuard Antispam Service	✓	✓	✓	✓								✓					
	FortiGuard CASB Service		✓															
NOC/SOC Security	FortiGuard Indicators of Compromise and Outbreak Detection Service											✓					✓	
	FortiGuard Attack Surface Security Service (Security Rating Service)	✓	✓	✓	✓													

Figure 2: FortiGuard Security integrated across the Security Fabric

URL and Video Filtering

The FortiGuard cloud-delivered, AI-driven web filtering service provides comprehensive threat protection to address a wide variety of threats, including ransomware, credential theft, phishing, and other web-borne attacks. It leverages AI-driven behavioral analysis and threat correlation to immediately block unknown malicious URLs with near-zero false negatives. Also, it provides granular blocking and filtering for web and video categories to allow, log, and block for rapid and comprehensive protection and regulatory compliance.

DNS

Consistent protection against sophisticated DNS-based threats includes DNS tunneling, DNS protocol abuse, DNS infiltration, C2 server identification, and domain generation algorithms. DNS filtering provides complete visibility into DNS traffic while blocking high-risk domains, including malicious newly registered domains, parked domains, and more.

Antibot and C2

Block unauthorized attempts to communicate with compromised remote servers for both receiving malicious command and control information or sending out extracted information.

Web Security

FortiGuard web security is optimized to monitor and protect data and applications against web-based attack tactics while assisting you with meeting compliance requirements.

Critical use cases include URL filtering, DNS security, phishing, SWG, compliance, and SD-WAN.

MITRE ATT&CK–Based Reporting and Investigation Tools

Top-rated, behavior-based, and AI-powered static and dynamic malware analysis addresses today's rapidly evolving and targeted threats, including ransomware, crypto-malware, and others, across a broad digital attack surface.

It also delivers real-time actionable intelligence and prevention by automating advanced zero-day malware detection and response.

Antivirus

FortiGuard Antivirus delivers automated updates that protect against the latest polymorphing attack components, including ransomware, viruses, spyware, and other content-level threats. It uses industry-leading advanced detection engines to prevent new and evolving threats from gaining a foothold inside your network, endpoint, and clouds and accessing valuable resources.

AI-Based Inline Malware Prevention

Inline blocking of previously unknown threats with AI-based Inline Malware Prevention Service allows you to hold a potentially malicious file until a final verdict is received. Leveraging advanced AI and ML at cloud speed, FortiOS now offers real-time prevention with queueing optimization and hardware acceleration. Inline blocking for FortiGate is available with both FortiSandbox and FortiGuard AI-Based Inline Malware Prevention Service.

Data Loss Prevention

The FortiGuard Data Loss Prevention Service delivers a database with consistent DLP patterns to different solutions within the Fortinet security stack. It furnishes businesses with everything they need to keep their data and users secure and prevent costly data loss incidents.

Inline and API CASB

The FortiGuard CASB Security Service secures SaaS applications in use by your organization, providing broad visibility and granular control over SaaS access, usage, and data. This service for FortiGate Next-Generation Firewalls (NGFWs) and SASE integrates with the FortiClient Fabric Agent to enable inline ZTNA traffic inspection and ZTNA posture check.

Innovative Capabilities

FortiOS also includes a range of additional capabilities, like mobile malware, credential protection, content disarm and reconstruction, and virus outbreak prevention.

Antispam

Working in conjunction with our FortiMail solution to dramatically reduce spam volume at the perimeter, antispam gives you unmatched control of email attacks and infections to provide greater protection than standard blacklists.

Intrusion Prevention System

IPS blocks the latest stealthy network-level threats and network intrusions. It uses a comprehensive IPS library with thousands of signatures, backed up by FortiGuard research, which is credited with an industry-leading 1,000+ zero-day threat discoveries. Natively embedded in our context-aware policies, it enables full control of attack detection methods to address complex security applications and resist evasion techniques.

Content Security

Our content security solution is optimized to monitor and protect against file-based attack tactics while assisting with meeting compliance.

Critical use cases include prevention of known and unknown ransomware, viruses, and malware. They also have data loss prevention, insider threats, lateral movement of malware and attackers, data center segmentation, and SaaS security.

Device Security

Optimized to monitor and protect against device and vulnerability-based attack tactics while assisting you with meeting compliance.

Critical use cases include intrusion prevention system (IPS), exploit protection, vulnerability detection, virtual patching, IT/OT/IoT identification, and protection.

Dedicated IPS includes end-to-end updates for IPS administration, including support for finance and other regulated deployments. It enables migration from separate hardware to NGFWs while preserving operations and compliance practices.

OT Security

Identify and police over 70 ICS/SCADA protocols and industrial equipment for granular visibility and control with our OT Security Service featuring over 3,000 OT-specific vulnerability and application signatures.

Additional capabilities like device and OS detection and IoT hardware MAC address vendor mapping updates provide additional protection. Device detection and protection services OT devices have been expanded to include vulnerability correlation and virtual patching.

Attack Surface Security Service

Assessment and rating of security infrastructure in terms of security and compliance, plus IoT Detection and Vulnerability Correlation. Reduce your attack surface with automated discovery, real-time query, segmentation, and enforcement for IoT devices.

Indicators of Compromise and Outbreak Detection

Our automated breach defense system continuously monitors your network for attacks, vulnerabilities, and persistent threats. It also protects against legitimate threats, guards your data, and defends against fraudulent access, malware, and breaches.

Our cybersecurity experts develop detailed outbreak alerts and provide outbreak detection updates to our SOC platform. These save you research time by identifying attacks and ensuring ongoing readiness for threat hunting, including valuable tips and tricks.

Purchasing Options

We provide organizations with the freedom to mix and match solutions using a variety of options, including:

- A la carte
- Optimized bundles for products and use cases
- Enterprise Agreement

Application Security

This suite of advanced security technologies protects, monitors, and optimizes application performance. FortiGuard Security Services blends context and application-aware technologies with global and organizational protection across networks, endpoints, and cloud environments.

FortiGuard Security for SOC and NOC Teams

Our suite of advanced security services and managed SOC offerings has been optimized for SOC and NOC teams. We provide faster identification, containment, and response to attacks across the expanding enterprise network using AI-powered automation, real-time outbreak detection, threat-hunting tips, and training so you can focus on innovation.

FortiGuard AI-Powered Services Include FortiGuard Labs Real-Time Threat Intelligence

FortiGuard Labs maintains AI-powered analysis environments that span solution databases, ensuring that all products operate from the same up-to-the-minute data. Each solution has access to all the security intelligence appropriate to its function and location across the attack surface. This ensures that security is deployed consistently and enforced cohesively. In addition, AI-based analysis and local ML capabilities operate within products to provide full-spectrum detection and mitigation of known and unknown threats.

FortiGuard Security for SOC and NOC Teams (cont.)

Critical use cases include:

- Advanced forensics and threat hunting
- Outbreak detection and remediation
- Managed SOC-as-a-Service
- Managed detection and response
- SOC team augmentation
- Proactive assessments
- Simplified migration
- Cloud management

Real-Time Threat Intelligence	Trusted AI and ML	Threat Hunting and Outbreak Alerts
Continuous security updates across the Security Fabric are based on in-house research, zero-day discoveries, and industry alliances.	Our AI and ML models use large-scale, cloud-driven data lakes (sandbox, EDR, NDR, botnet/C2, web, DNS, SaaS learning, and more), combined with local learning and static analysis, to uniquely identify anomalies.	Services combine FortiGuard Labs research, MITRE ATT&CK sightings, and global partnerships to provide alerts, analysis and detection, prevention, and remediation tools for fast detection and mitigation of outbreaks.

FORTINET

www.fortinet.com

November 6, 2023 10:24 PM

2364701-0-0-EN