PORTFOLIO BRIEF

FortiGuard AI-Powered Security

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 provides market-leading security capabilities designed to protect application content, web traffic, devices, and users wherever they have been deployed. 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 and can be deployed close to protected assets to ensure rapid, real-time detection and response.

Counter Threats in Real Time With AI-Powered Coordinated Protection

FortiGuard AI-Powered Security services are 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 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.

New in FortiOS 7.2

Stop playing hide and seek with malware

Get your team focused by shifting to a security strategy that enables you to move faster and safer than ever before. Packed with new features, FortiOS 7.2 delivers a powerful combination of actionable AI-driven intelligence integrated with inline (IL) prevention to detect and counter evasive and never-seen-before threats. FortiOS 7.2 has introduced IL Sandbox, IL CASB, advanced device protection unified for OT and IoT, and additional enhancements to our SOC security portfolio. Coordinated market-leading security capabilities provide protection across the attack lifecycle and surface.

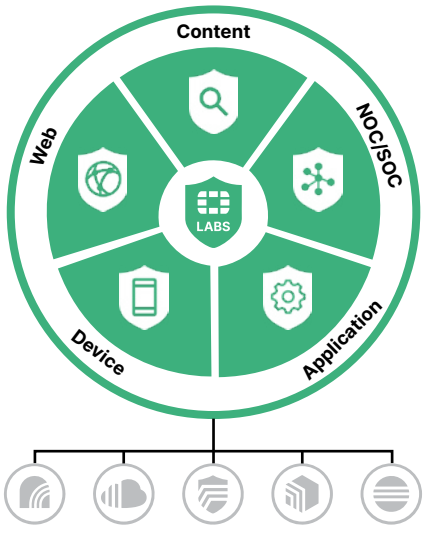


Figure 1: FortiOS 7.2 diagram.

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 FortiOS, common standards, and open APIs, enabling you to connect and leverage your existing investments, creating a unified, proactive security posture.

		FGT	Proxy	FortiTrust	XDR	FortiWeb	FortiMail	FortiADC	SOC Platforms	FNDR
Content Security	Antivirus	✓	✓	✓	✓	✓	✓	✓		✓
	IL SBX	✓		✓	✓	✓	✓	✓		
	Credential Stuffing	✓	✓			✓		✓		
Web Security	URL	✓	✓	✓	✓	✓	✓			✓
	DNS	✓	✓	✓	✓					
	IP-REP	✓				✓	✓			
Device Security	DVC PROT	✓								
	IPS	✓	✓	✓			✓			✓
	BOT/C2	✓	✓	✓	✓					
Application Security	WAF SIG					✓				
	ANN						✓			
	Antispam							✓		
SOC Services	MITRE ATT&CK								✓	
	Threat Hunting				✓				✓	
	Auto IR				✓				✓	
	Outbreak							✓	✓	✓
	IoC				✓				✓	✓

Figure 2: FortiGuard Security integrated across the fabric/mesh.

Web Security

FortiGuard's web security solution 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, SD-WAN, Cloud Access Security Broker (CASB)

Web and Video Filtering

FortiGuard's 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. It provides granular blocking and filtering for web and video categories to allow, log, or 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 (DGAs). DNS filtering provides complete visibility into DNS traffic while blocking high-risk domains, including malicious newly registered domains (NRDs), parked domains, etc.

Antibot and CS

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

Geo IP

Geo IP adds additional protection to this category by providing location information on IP traffic to help manage region-based threats.

Inline CASB

NEW in FortiOS 7.2: SaaS Security (IL CASB) service is focused on securing SaaS business data. When combined with SASE, you benefit from inline traffic inspection and ZTNA posture check.

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: ransomware prevention, insider threats, lateral movement of malware and attackers, data center segmentation, and real-time detection and prevention of known and unknown viruses and malware

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.

Infinite Sandbox

NEW in FortiOS 7.2: Inline blocking of previously unknown threats with IL Sandbox allows you to hold a potentially malicious file until a final verdict is received. Leveraging advanced AI and ML at cloud speed, FortiOS 7.2 now offers real-time prevention with queueing optimization and hardware acceleration.

Antivirus

FortiGuard Antivirus delivers automated updates that protect against the latest polymorphing attack components, including 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.

Innovative Capabilities

FortiOS also includes a range of additional capabilities, like mobile malware, credential protection, content disarm and reconstruction (CDR), virus outbreak prevention, data loss prevention (DLP), and dynamic adult image analysis.

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.

Device Security

Optimized to monitor and protect against device and vulnerability-based attack tactics while assisting you with meeting compliance. Critical use cases include: IPS, exploit protection, vulnerability detection, virtual patching, IoT/OT/IT identification and protection.

IPS

IPS blocks the latest stealthy network-level threats and network intrusions working. It uses a comprehensive IPS Library that includes thousands of signatures, backed up by FortiGuard research credited with an industry-leading 850+ 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.

NEW in FortiOS 7.2: 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 NGFW while preserving operations and compliance practices.

OT and IoT

Identify and police common ICS/SCADA protocols and equipment for granular visibility and control with our OT service. Reduce your attack surface with automated discovery, real-time query, segmentation, and enforcement for IoT devices.

Additional capabilities like device and OS detection and IoT hardware MAC address vendor mapping updates provide additional protection.

NEW in FortiOS 7.2: Device detection and protection services for IoT and OT devices have been expanded to include vulnerability correlation and virtual patching.

Application Security

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

Critical use cases include: secure web email, WAF, DDoS, IL CASB, Application Delivery Control (ADC)

IL CASB

NEW in FortiOS 7.2: The new FortiGuard Inline 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 NGFW integrates with the FortiClient Fabric Agent to enable inline ZTNA traffic inspection and ZTNA posture check.

Web Application Firewall (WAF)

FortiWAF has access to our fabric-level, coordinated FortiGuard AI-Powered Security services optimized for WAF functionality. These include sandbox, anti-malware, IP reputation, web security, and credential stuffing defense.

Secure Email Gateway (SWG)

Includes access to our fabric-level, coordinated FortiGuard AI-Powered Security services optimized for SWG functionality. Services include DLP, sandbox, anti-malware, antispam, outbreak prevention, and anti-phishing.

Application Delivery Control (ADC)

Includes access to our fabric-level, coordinated FortiGuard AI-Powered Security services optimized for ADC functionality. These include IPS, sandbox, anti-malware, web filtering, IP reputation, WAF signature, and credential stuffing defense.

FortiGuard Security for SOC and NOC Teams

Our suite of advanced security services and managed SOC offerings have 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—allowing you to focus on innovation. Critical use cases include:

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

SOC-as-a-Service, MDR, and Incident Response (IR)

Free your teams to focus on major executions by offloading all tier-one analysis to the FortiGuard Labs team of experts. We will notify you of any significant events that need your attention, recommend an action plan, and take proactive actions.

Whether you are under attack or simply wish to assess your security readiness against ransomware, phishing, and other common attacks, our teams are here to help you every step of the way, from planning and design to monitoring to incident response.

Our proven professionals provide guided experience for designing, implementing, and continually advancing your security posture.

Fabric Rating

Our unique Fabric Rating Service provides audit checks, identifies critical vulnerabilities and configuration weaknesses, and recommends best practice implementations.

Indicators of Compromise (IoC)

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.

Outbreak Detection and Threat Hunting

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.

Vulnerability Scans

Regular on-demand or scheduled vulnerability scans can assess network assets for security weaknesses. Comprehensive reports on the security posture of your critical assets and automated scanning of remote locations are then generated to help guide optimization, updating, and the selection of new solutions.

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

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. These include:

Real-Time Threat Intelligence

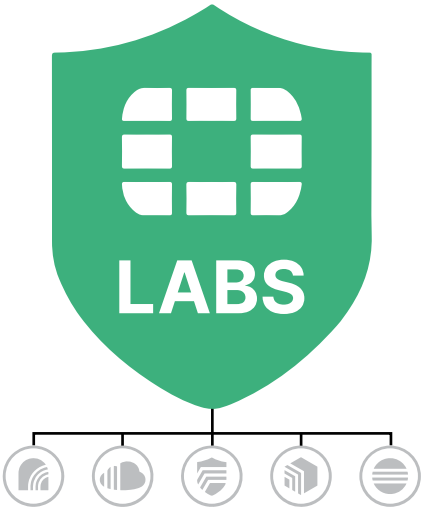
Continuous security updates across the Security Fabric are based on in-house research, zero-day discoveries, and industry alliances.

Trusted ML and AI

Our AI and ML models use large-scale, cloud-driven data lakes (Sandbox, EDR, NDR, Botnet/C2, Web, DNS, SaaS Learning, etc.), combined with local learning and static analysis, to uniquely identify anomalies.

Threat Hunting and Outbreak Alerts

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.



April 1, 2022 9:00 AM
1551325-0-0-EN