PORTFOLIO BRIEF

FortiGuard AI-Powered Security Services

The attack surface of today's digital landscape is constantly evolving—spanning on-premises, cloud, and hybrid environments that extend across IT and OT. And with the rapid adoption of AI, this surface has now become more dynamic, unpredictable, and expansive, introducing both new opportunities and vulnerabilities. To stay ahead, organizations require solutions that are capable of proactively adapting to these ongoing changes to identify, detect, respond to, and defend against an increasingly diverse range of attacks, wherever they occur.

FortiGuard AI-Powered Security Services delivers a multilayered, proactive defense to safeguard networks, applications, files, web traffic, data, devices, SaaS, and users from the growing threat of AI-driven attacks. These include ransomware, malware, phishing, known and unknown threats, and zero-day exploits, as well as emerging AI-powered risks such as promptware, data poisoning, data exfiltration, and polymorphic malware. These services continuously assess and mitigate risks in real time, providing comprehensive protection across your distributed, ever-changing attack surface.

Counter Threats with Proactive, Always-On Protection

FortiGuard AI-Powered Security Services is seamlessly integrated into the Fortinet Security Fabric, providing proactive detection and protection across the entire attack surface. By harnessing the power of AI and machine learning (ML), these services continuously assess risks and deliver automatic, real-time protection against both traditional and AI-powered threats. Whether deployed on-premises, in the cloud, or across hybrid environments, FortiGuard AI-Powered Security Services ensures context-aware, proactive, and layered security with always-on protection.

With FortiGuard Security Services in place, your security teams can operate faster and more securely than ever before. These services combine actionable AI-driven threat intelligence coupled with inline protection, empowering your teams to detect and mitigate evasive and never-before-seen threats, effectively countering emerging risks.

FortiGuard Labs: Real-Time AI-Powered Threat Intelligence

FortiGuard Labs, Fortinet's dedicated threat research and intelligence organization, powers FortiGuard AI-Powered Security Services with real-time threat intelligence and actionable insights. Leveraging telemetry data from millions of Fortinet sensors deployed globally, FortiGuard Labs uses AI and ML to process trillions of events. This data is further enriched with research from a team of cybersecurity experts and hundreds of threat intelligence partners.

The result is actionable threat intelligence that is seamlessly integrated into the Fortinet Security Fabric, enabling real-time protection across your entire attack surface. And because this intelligence is continuously updated, FortiGuard services ensure proactive defense and swift response to emerging threats, ensuring you stay protected at all times.

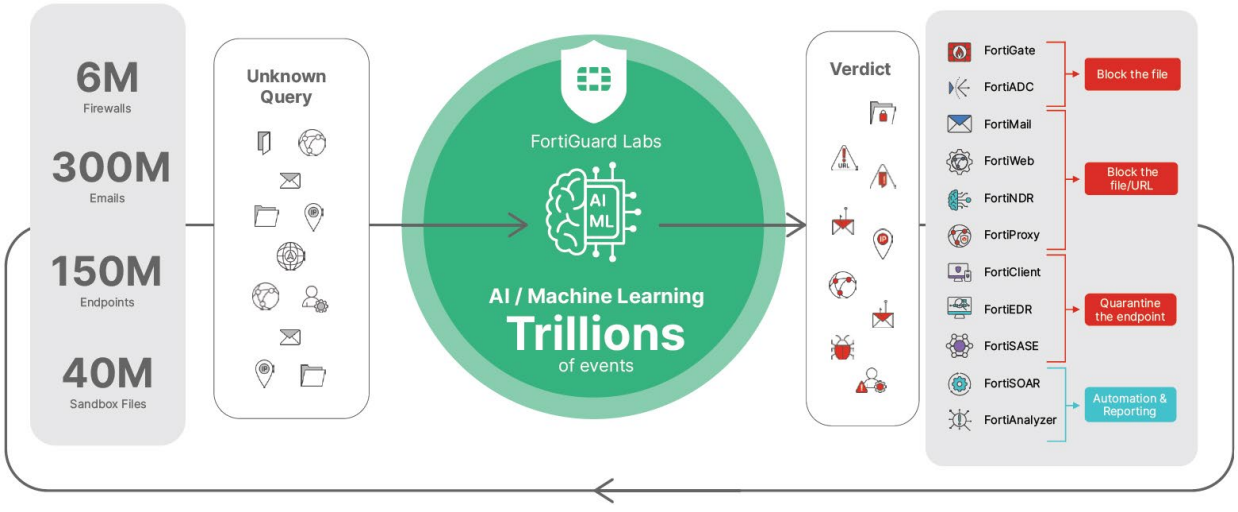

Figure 1: FortiGuard Labs Threat Intelligence

Proactive, Real-Time Protection across the Security Fabric

FortiGuard AI-Powered Security Services, along with real-time threat intelligence from FortiGuard Labs, is seamlessly integrated into the Fortinet Security Fabric. This integration ensures continuous, real-time protection across all Fortinet Security Fabric solutions.

The Security Fabric is built on the FortiOS operating system, common industry standards, and open APIs, allowing you to easily connect and maximize the value of your existing investments. This unified framework also enables a proactive security posture, ensuring your defenses are always aligned and responsive to emerging threats.

Key integrations within the Fortinet Security Fabric include:

Fortinet Security Fabric Integrations

Key FortiGuard AI-Powered Security Services

URL and video filtering

FortiGuard's AI-driven, cloud-delivered web filtering service offers comprehensive protection against a wide range of threats, including ransomware, credential theft, phishing, and other web-based attacks. By utilizing AI-powered behavioral analysis and threat correlation, it instantly blocks unknown malicious URLs with minimal false positives. Additionally, it provides granular control over web and video categories, enabling detailed filtering, logging, and blocking to ensure both rapid protection and regulatory compliance.

DNS filtering

The FortiGuard DNS Filtering Service offers robust defense against sophisticated DNS-based threats, including DNS tunneling, protocol abuse, DNS infiltration, command-and-control (C2) server identification, and domain generation algorithms. It provides complete visibility into DNS traffic, blocking high-risk domains such as newly registered and parked domains, enhancing network security at the DNS layer.

Intrusion prevention system (IPS)

The FortiGuard IPS Service blocks advanced network-level threats and intrusions with a comprehensive IPS library, featuring thousands of signatures supported by FortiGuard research. Embedded in context-aware policies, it allows full control over attack detection methods, enabling effective defense against complex security challenges and evasion techniques. The IPS service, specifically trained on Cobalt Strike data, ensures more accurate detection and blocking of Cobalt Strike–related intrusion attempts.

Antivirus

The FortiGuard Antivirus Service delivers automated, real-time updates to protect against evolving threats, including polymorphic attacks, ransomware, viruses, spyware, and other content-based malware. Using industry-leading detection engines, it prevents new and sophisticated threats from infiltrating your network, endpoints, and cloud environments, safeguarding valuable resources from compromise.

AI-based inline malware prevention

The FortiGuard AI-Based Inline Malware Prevention Service offers real-time blocking of previously unknown threats. By leveraging advanced AI and ML at cloud speed, it holds potentially malicious files in a queue until a final verdict is made. FortiOS ensures rapid prevention with optimized queueing and hardware acceleration, with inline protection available via FortiSandbox and FortiGuard AI-driven malware prevention.

Data loss prevention (DLP)

The FortiGuard Data Loss Prevention Service delivers a consistent, comprehensive DLP pattern database, enabling integration with various Fortinet security solutions. This service helps businesses safeguard their data, preventing costly loss or breaches by enforcing policies designed to protect sensitive information across the network.

Inline and API cloud access security broker (CASB)

The FortiGuard CASB Service provides visibility and granular control over SaaS applications used within the organization. This service enables FortiGate Next-Generation Firewalls (NGFWs) and SASE integration, working with the FortiClient Fabric Agent to enable inline zero-trust network access (ZTNA) traffic inspection and posture checks, enhancing secure access to cloud applications.

OT Security Service

The FortiGuard OT Security Service offers deep visibility and control for over a hundred ICS/SCADA protocols and industrial equipment, protecting critical OT infrastructure with thousands of OT-specific vulnerability and application signatures. The service also includes device and OS detection, IoT hardware MAC address vendor mapping, and vulnerability correlation, providing protection against industrial and IoT-based threats.

Attack surface security service

This service continuously assesses and rates the security infrastructure, offering real-time query, segmentation, and enforcement for IoT devices. Automated discovery and vulnerability correlation help reduce attack surfaces, providing visibility into potential risks and improving security posture.

Indicators of compromise (IOC) and outbreak detection

FortiGuard's automated breach defense system monitors your network for ongoing attacks, vulnerabilities, and persistent threats. It continuously protects against fraudulent access, malware, and breaches, with detailed outbreak alerts that provide updates and insights for SOC teams. This enables proactive threat hunting and rapid response, reducing time spent on research and increasing readiness.

AntiSpam

The FortiGuard AntiSpam Service works in conjunction with FortiMail to minimize spam at the network perimeter, providing greater control over email threats and significantly reducing the risk of infections. It offers superior protection compared to standard blocklists, enhancing email security for organizations.

Antibot and C2

The FortiGuard Anti-botnet and C2 Service blocks unauthorized attempts to establish communication with compromised remote servers, preventing malicious C2 communications and data exfiltration.

MITRE ATT&CK–based reporting and investigation tools

FortiGuard leverages AI-powered static and dynamic malware analysis to detect and respond to evolving threats, including ransomware and crypto-malware, across a broad attack surface. It provides real-time actionable intelligence, automating the detection and response to advanced zero-day malware, improving overall threat mitigation and incident response.

Additional capabilities

FortiOS also includes capabilities for mobile malware protection, credential security, content disarm and reconstruction, and virus outbreak prevention, further strengthening the security posture and resilience of the network.

Purchasing Options

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

- A la carte
- Three bundles optimized for use cases
- Enterprise Agreement

FortiGuard AI-Powered Services: A Proactive, Layered Defense

FortiGuard AI-Powered Services, driven by FortiGuard Labs, delivers a proactive and layered defense to organizations across all environments, at any time. This always-on suite utilizes advanced AI and real-time threat intelligence to detect, protect against, and respond to a wide array of evolving cyberthreats. Fully integrated into the Fortinet Security Fabric, these services strengthen NGFWs and provide comprehensive protection across your entire attack surface—whenever and wherever it's needed.

August 18, 2025 1:01 PM / MKTG-1712-0-0-EN