

SERVICE BRIEF

AI-Powered Threat Protection for Small and Midsize Businesses

Overview


Today’s small and midsize businesses (SMBs) are more complex than ever. As organizations increasingly digitize their operations, rapidly add technology into their business processes, and migrate to the cloud, these changes inevitably add complexity to securing the expanding attack surface and opening the door to more cyberattacks. Like larger enterprises, smaller organizations are also at risk of cyberthreats such as exploits, malware, ransomware, zero-day attacks, and emerging AI-based threats that can enable threat actors to gain a foothold and harm business operations.

SMBs need enterprise-grade protection to secure their networks across multiple branches and sites. They need to secure users and their access to applications regardless of location, whether they work in the office or remotely. And organizations need security tools and solutions that are easy to deploy and use to monitor their environments without giving up important features or enterprise-grade capabilities.

AI-Powered Threat Protection

SMBs need the same caliber of protections that enterprises do. FortiGuard AI-Powered Security Services is developed and continually updated with the latest threat intelligence of FortiGuard Labs. Its services counter threats in real-time with AI and machine learning (ML)-powered, coordinated protection, natively integrated into the Fortinet Security Fabric, and enabling fast detection and enforcement across the entire attack surface.

The services give SMBs the confidence that their complex and hybrid environments are secured with the strongest possible protection.



FortiGate Next-Generation Firewalls (NGFWs) and NGFW-based solutions include FortiGuard AI-Powered Security Services. These services are developed and continuously enriched with the latest threat intelligence from FortiGuard Labs, the elite Fortinet threat research team.

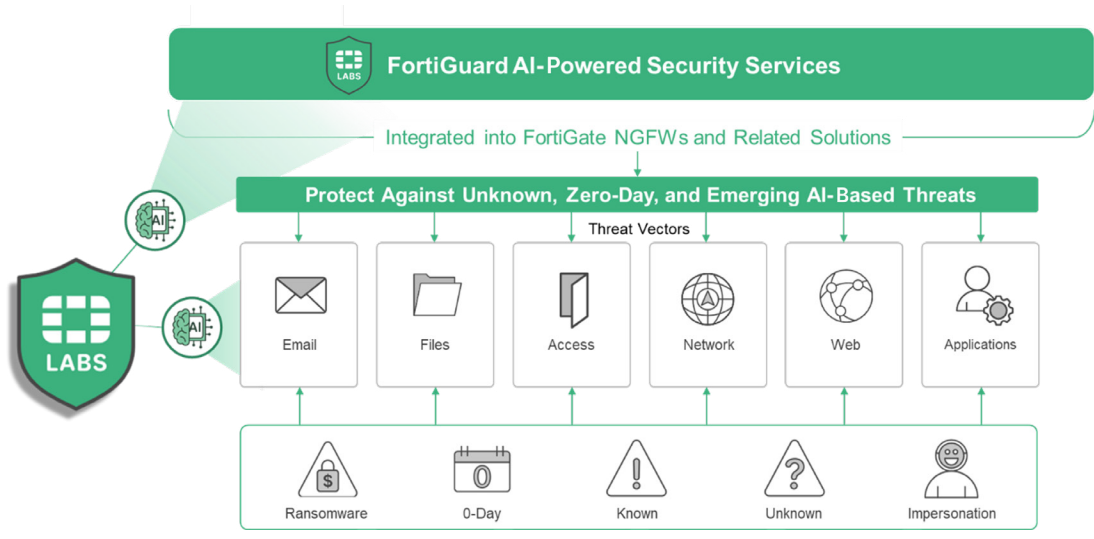


Figure 1: FortiGuard AI-Powered Services for SMBs



Secure Networks, Applications, Data, and Users

FortiGuard AI-Powered Security Services is integrated into Fortinet FortiGate NGFW solutions and helps SMBs address key security and compliance requirements across a number of areas.

Network and file security

The **FortiGuard IPS Service** blocks the latest stealthy network-level threats and network intrusions. It uses a comprehensive intrusion prevention system (IPS) library with thousands of signatures, backed by FortiGuard Labs research, credited with over 1,000 zero-day threat discoveries. The IPS service includes end-to-end updates for IPS administration, including support for finance and other regulated deployments.

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

The **FortiGuard Application Control Service** lets you quickly create policies to allow, deny, or restrict access to entire categories of applications. Application control helps keep malicious, risky, and unwanted applications out of the network through control points at the perimeter, in the data center, and internally between network segments.

Web/DNS security

The **FortiGuard DNS Filtering Service** provides consistent protection against sophisticated DNS-based threats, including DNS tunneling, DNS protocol abuse, DNS infiltration, command-and-control (C2) server identification, and domain generation algorithms. DNS filtering provides complete visibility into DNS traffic while blocking high-risk domains, including malicious newly registered and parked domains.

The **FortiGuard URL Filtering Service** provides comprehensive threat protection to address various threats, including ransomware, credential theft, phishing, and other web-borne attacks. It leverages AI-driven behavioral analysis and threat correlation to block unknown malicious URLs with near-zero false negatives.

The **FortiGuard Anti-Botnet and C2 Service** blocks unauthorized attempts to communicate with compromised remote servers to receive malicious C2 information or send out extracted information. It protects against malicious sources associated with web attacks, phishing activity, web scanning, and scraping.

SaaS and data security

The **FortiGuard CASB Service** (inline) secures SaaS applications in use, providing broad visibility and granular control over SaaS access, usage, and data.

The **FortiGuard Attack Surface Security Service** is integrated into FortiGate NGFWs and continuously monitors and assesses the organization's assets and security controls to provide an overall security posture rating.

Because SMBs often face tough challenges in hiring and retaining security personnel, it can be especially hard to remain more proactive. This is where attack surface management can be especially beneficial for them.

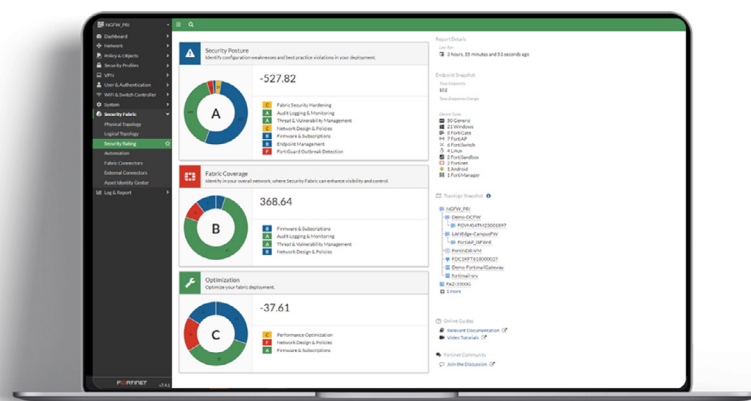


Figure 2: FortiGuard Attack Surface Security Service



The FortiGuard Attack Surface Security Service is a lightweight cyber asset attack surface management or CAASM tool for identifying assets across the environment, assessing any risk they might pose, and scoring the organization's overall security posture.

The automated service identifies and evaluates assets and existing security infrastructure for potential vulnerabilities, misconfigurations, less-than-optimal settings, and other areas of potential risk. For leaders, the service provides comprehensive visibility into risk, and analysts and administrators can drill down all the way to the individual asset level. The service also guides remediating potential risk areas, which help raise the organization's overall score.

Service Availability

All services are available as part of the FortiGuard Unified Threat Protection Bundle, except the FortiGuard Attack Surface Security Service, which is available as part of the Enterprise Protection Bundle or a la carte.

Services to Meet SMB Needs

SMBs face many of the same challenges that larger organizations face regarding cyberthreats. However, unlike their larger counterparts, smaller organizations cannot weather the costs associated with a breach and can find their businesses severely impacted or even put out of business. As a result, SMBs need enterprise-grade threat protection.

Fortinet FortiGuard AI-Powered Security Services provides advanced AI-powered threat protection against a wide range of threats, keeping SMB networks, applications, files, email, employees, and web usage secure.



www.fortinet.com