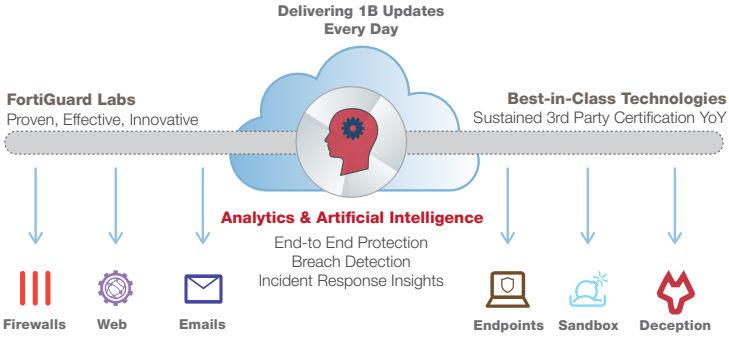
DATA SHEET

FortiGuard Security Services

FortiGuard Labs, the threat intelligence and research organization at Fortinet, develops, innovates, and maintains one of the most recognized and seasoned artificial intelligence and machine learning systems in the industry. We use this to deliver proven unparalleled protection, visibility, and business continuity across the Fortinet Security Fabric, protecting our customers against the wide range of ever changing and sophisticated threats.



Subscribe to FortiGuard to stay protected against the latest threats across all threat vectors and attack surfaces today!

Why FortiGuard?

What sets FortiGuard apart comes down to our advanced and proven analytics and artificial intelligence (AI) platform developed, innovated, and operated by FortiGuard Labs. Our platform ingests and analyzes 100 billion events every day, on average, to deliver over one billion security updates daily to protect our customers against new, unknown threats across all Security Fabric deployments.

Where other vendors measure results in days, weeks, or months, Fortinet can show impressive outcomes by the minute.

Ultimately, the effectiveness of security AI and analytics systems are only as good as the inputs and training that go into them. At Fortinet, our platform is driven by one of the largest and most experienced security research organizations in the industry with over 215 researchers and analysts, spanning 31 countries. Our FortiGuard team contributes 580,000 hours of research annually. Very few, if any, of our competitors can say that!

In fact, FortiGuard is credited with over 841+ zero-day discoveries – a record unmatched by any other security vendor.

Additionally, we feed in millions of events coming from across global Fortinet Security Fabric deployments by customers who join our submissions program and ingest threat intelligence across over 200 Threat Intelligence Ecosystem partners and collaborations. This combination gives Fortinet unparalleled insights and visibility to proactively identify and stop the latest threats around the clock.

FortiGuard Minute

609,000
Hours of Threat Research Globally Per Year

18,000,000
Network Intrusion Attempts Resisted Per Minute

340,800
Malware Programs Neutralized Per Minute

940
Terabytes of Threat Samples

19,000,000
Malicious Website Accesses Blocked Per Minute

19,000,000
Botnet C&C Attempts Thwarted Per Minute

6,400,000
Intrusion Prevention Rules 63 Rules Per Week

841+
Zero Day Threats Discovered

Certifications

Customers can rest assured knowing that our security efficacy is backed by sustained year-over-year certifications and rigorous testing by leading organizations including NSS Labs, ICSA Labs, Common Criteria, Virus Bulletin, Virus Bulletin Spam, Mitre, Oasis, and NASA. This program makes the Fortinet Security Fabric the most certified and proven security solution available in the industry.

Feature Highlights

To benefit from and access the intelligence, expertise, and protection delivered by FortiGuard Labs, customers simply need to add the desired security subscriptions to their Fortinet Security Fabric deployment.

FortiGuard security services are designed to optimize performance and maximize protection across the Fortinet Security Fabric and are available as both individual and bundled subscriptions. Our subscriptions cover every aspect of the attack surface and includes IP reputation updates, intrusion prevention, web filtering, antivirus/anti-spyware, anti-spam, database security, virus outbreak protection service, content disarm and reconstruction, security rating services, and network and web application control capabilities.

Subscription Benefits

- Up-to-the minute threat intelligence in real time to stop the latest threats
- Insight into threats anywhere in the world through a global network of more than three million sensors
- Fast and comprehensive intelligence via automated and advanced analytics (such as machine learning) being applied to cross-discipline information
- High fidelity with mature and rigorous back-end processes
- Prevention of exploitation of new avenues of attack with proactive threat research
- Top-rated effectiveness achieved through the commitment to independent, real-world testing

Subscribe to FortiGuard to stay protected against the latest threat across all threat vectors and attack surfaces today!

Subscription Services

Antivirus

FortiGuard Antivirus delivers automated updates that protect against the latest viruses, spyware, and other content-level threats. It uses industry-leading advanced detection engines to prevent both new and evolving threats from gaining a foothold inside your network and accessing its invaluable content.

Intrusion Prevention (IPS)

FortiGuard automated IPS updates provide latest defenses against network intrusions by detecting and blocking threats before they reach your network devices. You get the latest defenses against stealthy network-level threat, a comprehensive IPS Library with thousands of signatures, flexible policies that enable full control of attack detection methods to suit complex security applications, resistance to evasion techniques proved by NSS Labs, and IPS signature lookup service.

Application Control

Improve security and meet compliance with easy enforcement of your acceptable use policy through unmatched, real-time visibility into the applications your users are running. With FortiGuard Application Control, you can quickly create policies to allow, deny, or restrict access to applications or entire categories of applications.

The sophisticated detection signatures identify Apps, DB applications, web applications and protocols; both Block/Allow List approaches can allow or deny traffic. Traffic shaping can be used to prioritize applications and flexible policies enable full control of attack detection methods.

Security Rating Service

The Security Rating Service is helps guide customers to design, implement, and continually maintain the target Security Fabric security posture suited for their organization. By running Security Rating Service audit checks, security teams will be able to identify critical vulnerabilities and configuration weaknesses in their Security Fabric setup, and implement best practice recommendations.

IoT Service

The IoT service helps customers significantly reduce their attack surface by enabling the Fortinet Security Fabric to automatically discover and segment IoT devices based on FortiGuard intelligence, and enforce appropriate policies against them. With the service, FortiGates can query FortiGuard servers to obtain information about unknown devices and then act accordingly based on policy.

Indicators of Compromise (IOC)

The IOC service is an automated breach defense system that continuously monitors your network for attacks, vulnerabilities, and persistent threats. It provides protection against legitimate threats, guarding customer data and defending against fraudulent access, malware, and breaches. It also helps businesses detect and prevent fraud from compromised devices or accounts.

Vulnerabilitity Scan

Vulnerability scan network assets for security weaknesses, with on demand or scheduled scans. Comprehensive reports on the security posture of your critical assets and automated scanning of remote location FortiGates.

Web Application Firewall (WAF)

Automated WAF signature updates that protect against SQL injection, cross-site scripting, and various other attacks, hundreds of vulnerability scan signatures, data-type and web robot patterns, and suspicious URLs. Supports PCI DSS compliance by protecting against OWASP top 10 vulnerabilities and using WAF technology to block attacks.

Web Filtering

Block and monitor web activities to assist customers with government regulations and enforcement of corporate internet usage policies. FortiGuard's massive web content rating databases power one of the industry's most accurate web filtering services. Granular blocking and filtering provide web categories to allow, log, or block. The comprehensive URL database provides rapid and comprehensive protection. Credential stuffing defense identifies login attempts using credentials that have been compromised using an always up-to-date feed of stolen credentials.

Industrial Control Systems Security

The FortiGuard Industrial Security Service continuously updates signatures to identify and police most of the common ICS/ supervisory control and data acquisition (SCADA) protocols for granular visibility and control. Additional vulnerability protection is provided for applications and devices from the major ICS manufacturers.

Antispam

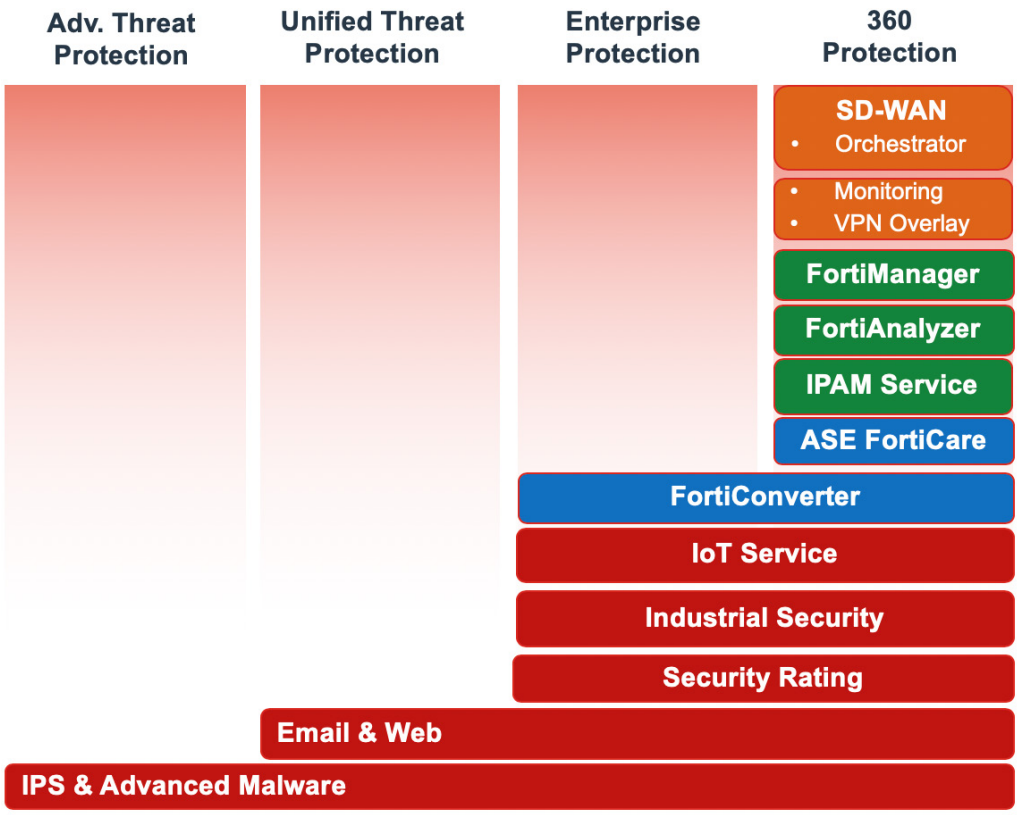
FortiGuard Antispam provides a comprehensive and multi-layered approach to detect and filter spam processed by organizations. Dual-pass detection technology can dramatically reduce spam volume at the perimeter, giving you unmatched control of email attacks and infections. Advanced anti-spam detection capabilities provide greater protection than standard real-time blacklists.

Cloud Sandbox

FortiCloud Sandbox Service is an advanced threat detection solution that performs dynamic analysis to identify previously unknown malware. Actionable intelligence generated by FortiCloud Sandbox is fed back into preventive controls within your network—disarming the threat. FortiSandbox is NSS Labs Recommended for breach detection and breach prevention, and ICSA Labs certified for advanced threat defense.

FortiGuard Subscription Bundles

FortiGuard Labs delivers a number of security intelligence services to augment your core security component. You can easily optimize the protection capabilities of your security solution by either selecting individual services or logical security and support service bundles, like our Enterprise Bundle, which offers greater flexibility and savings.



Which Bundle Is Right for Me?

Our FortiGuard Bundles are sized to help arm Fortinet's customers with all the services needed to readily achieve their desired outcomes and get the most of out their Fortinet Security Fabrics.

USE CASE	ADVANCED THREAT PROTECTION (ATP)	UNIFIED PROTECTION (UTP)	ENTERPRISE PROTECTION (ENT)	360 PROTECTION
Next Generation Firewall	✓	✓	✓	✓
Secure Web Gateway		✓	✓	✓
Compliance and benchmarking			✓	✓
SD-WAN[1,2]				✓

[1] SD-WAN Core capabilities of FortiGate and FortiOS do NOT require any additional license or bundle
[2] SD-WAN recommended but optional capabilities like "SDWAN Cloud Monitoring and SDWAN Orchestrator" are offered as part of the 360 Protection bundle

Additional Deployment Use Cases

FortiGuard security subscriptions works optimally with the Fortinet Security Fabric to protect all deployment use case needs. To learn more, visit https://www.fortinet.com/support/support-services/fortiguard-security-subscriptions.html for more.

- Next-generation Firewall (NGFW)
- Secure SD-WAN
- Intrusion Prevention (IPS)
- Intent-based Segmentation
- Secure Web Gateway (SWG)
- Management and Analytics
- Advanced Threats
- Email
- Public Cloud
- Private Cloud
- Web Application Firewall
- Application Delivery Controller
- Endpoint Protection
- SIEM

Order Information

FortiGuard a la carte Services	
Anti-Virus, Botnet IP/Domain, and Mobile Malware Service	Protects against the latest viruses, spyware, and other content-level threats.
Web Filtering	First line of defense against web-based attacks, monitor, control, or block access to risky or malicious websites
Cloud Sandbox	Advanced threat detection solution that performs dynamic analysis to identify previously unknown malware. Includes: Virus Outbreak Protection Service and Content Disarm & Reconstruction Service
Virus Outbreak Protection	Protects against emerging threats discovered between signature updates
Indicator of Compromise	Provides a continually updated list of known bad threat elements for prevention and detection capabilities
Security Rating Service	Identifies security fabric configuration weaknesses, provides ranking against industry peers, and automates best practice recommendation
IoT Service	Automatically identifies, segment, and enforces policies against IoT devices using FortiGuard intelligence
Industrial Security Service	Provides in-line protection, proactive filtering of malicious and unauthorized network traffic, enforce security policies tailored to industrial environments, protocols and equipment
IPS Service	Provides real-time threat intelligence updates to block and prevent advanced cyber threats
AntiSpam	Multi-layered approach to detect and filter spam at the perimeter, giving you unmatched control of email attacks and infections
Advanced Malware Protection	FortiGuard Advanced Malware Protection is a robust service providing core technologies needed for security protection for known threats and emerging threats. and includes: Antivirus, Botnet IP/Domain Service, Mobile Malware Security, FortiSandbox Cloud, Virus Outbreak Protection Service and Content Disarm & Reconstruct.
Penetration Testing Service	FortiGuard Pentest Team conducts a series of technical assessments on your organization's security controls to determine the weakness on computer hardware infrastructure and software application, apply commercial automated tools to discover unintended services made publicly available by your network and also apply real-world attackers' methodologies to discover unknown vulnerabilities on the given target.
FortiCare SKUs	
FC-10-#####-247-02-DD	FortiCare 24x7 -- In addition to 24x7 phone and email support, this SKU covers automatic updates following databases: Application Control DB, Internet Service DB, Client ID DB, IP Geography DB, Malicious URL DB, and URL Whitelist DB.
FC-10-#####-280-02-DD	FortiCare 360 Contract (24x7 FortiCare plus Advanced Support ticket handling & Health Check Monthly Reports; Collector included with Setup & Administration)
FNDN License SKUs	
FC-10-FNDN1-651-02-12	FNDN Develop Toolkit – FNDN access for single user. Includes Develop tools and licenses
FC-10-FNDN1-652-02-12	FNDN Deploy Toolkit - FNDN access for single user. Includes Deploy tools and licenses
FC-10-FNDN2-139-02-12	FNDN Site Toolkit – FNDN access for up to 15 users. Includes premium tools and licenses for developers and advanced users of Fortinet products
Additional Services	
FortiAnalyzer	Subscription license for the FortiGuard Indicator of Compromise (IOC)
FortiSandbox	Intelligence from IPS, AntiVirus, IP Reputation, Web Filtering, and FortiCare services.
FortiClient	Intelligence from Application Control, AntiVirus, Web Filtering, Vulnerability Scan, and FortiCare services.
FortiProxy	Intelligence from AntiVirus, Web Filtering, IPS, DLP, Appication Control, DNS Filtering, AntiSpam, Vulnerability Scan and FortiCare Service
FortiMail	Intelligence from AntiVirus, AntiSpam, FortiSandbox Cloud, Virus Outbreak Protection Service, Dynamic Adult Image Analysis Service, FortiCare services
FortiWeb	Intelligence from Web Application Security, AntiVirus, IP Reputation, Vulnerability Scan, FortiGuard Credential Stuffing Defense, FortiCare services.
FortiADC	Intelligence from AntiVirus, IP Reputation Web Application Security, FortiGuard Web Filtering Service, and FortiCare services.
FortiDDoS	Intelligence from IP Reputation and FortiCare services.
FortiSIEM	Subscription license for the FortiGuard Indicator of Compromise (IOC)
FortiCASB	Provide visibility and control for data stored in the cloud.
FortiManager Cloud	Cloud-based Orchestration Service (1yr subscription)
FortiAnalyzer Cloud	Cloud-based Security and Event Management Service (1yr subscription)
SD-WAN Cloud Assisted Monitoring	SD-WAN Bandwidth & Quality Monitoring Service
SD-WAN Overlay Controller VPN Service	Cloud-based VPN Overlay Service & Portal
SD-WAN Orchestrator	Enables SD-WAN orchestrator functionality in FortiManager to simplify SD-WAN orchestration with zero-touch provisioning
IPAM Service	IP Address Management (IPAM) is a cloud service to help customers better and more efficiently manage DNS and DHCP
FortiConverter Service	Policy Migration and Optimization Service

FORTINET

www.fortinet.com