DATA SHEET

FortiGuard Security Services

New cyber threats emerge every moment of every day. Whether it's ransomware, phishing campaign, or infrastructural vulnerability—organizations must constantly be prepared to defend against something new at all times. Extensive knowledge of the threat landscape, combined with the ability to respond quickly at multiple levels, is the foundation for providing effective security. That's where the threat research and intelligence of FortiGuard Labs is critical to protect your network.

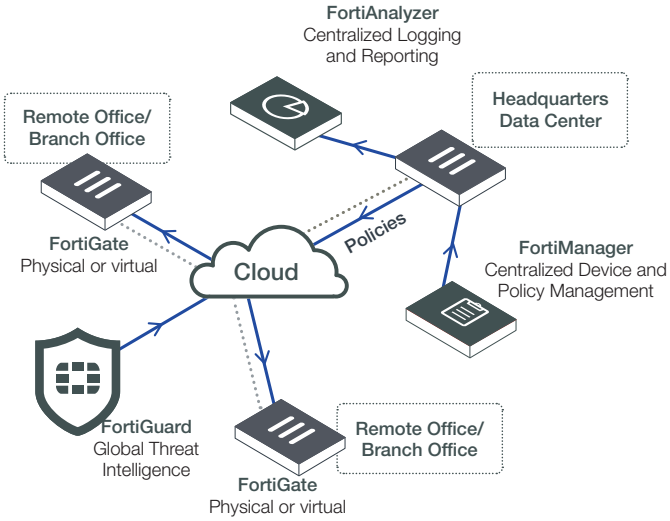
Applied Security Intelligence

FortiGuard's certified & proven security protection provides comprehensive security updates and protection for the full range of Fortinet's Security Fabric solutions. FortiGuard Labs consists of hundreds of research specialists, with an average of over 16 years experience in threat research and response, providing cutting-edge protection to customers and enhancing their cyber security defense. Seemless integration into your SOC/NOC for actionable security operations against today's threats.

Power of FortiGuard Labs

When dealing with an almost invisible adversary, it is important to understand everything that is observable about them. FortiGuard threat intelligence encompasses research performed by FortiGuard analysts in cooperation with extended security industry and law enforcement organizations. Hundreds of FortiGuard researchers scour the cyber landscape to discover emerging threats and develop effective countermeasures to protect organizations around the world. They are the reason FortiGuard is credited with over 650 zero-day discoveries – a record unmatched by any other security vendor. A unique combination of in-house research, information from industry sources, and machine learning, and artificial intelligence technologies is why Fortinet security solutions score so high in real-world security effectiveness tests at places like NSS Labs, Virus Bulletin, ICSA Labs, AV Comparatives, and more.

FortiGuard Labs uses data collected from sensors positioned around the globe to protect more than 300,000 customers every day.



FortiGuard Minute

580,000
Hours of Threat Research Globally Per Year

140,000
Malicious Website Accesses blocked per minute

10,000,000
Network Intrusion Attempts resisted per minute

65,000
Botnet C&C attempts thwarted per minute

35,000
Malware Programs Neutralized Per Minute

22,000
Intrusion Prevention Rules, 63 Rules per Week

860
Terabytes of Threat Samples

681
Zero Day Threats Discovered

Intelligence Illumination

By leveraging global threat data, enterprise organizations will be able to outsmart highly complex attacks. It Is important to understand the capabilities, tactics and procedures of cyber threat actors. With possession of this kind of information, enterprises have enough "illumination" to understand how to better respond to threats that are targeting their organization. It is this information that would ultimately illuminate the path to a **stronger cybersecurity posture** within your organization.

Combat Threats

By combining our threat intelligence feed with local data from your network, such as logs and security events from your infrastructure, you will be able to quickly remediate threats with a surgical precision, lessening the time to respond to threats and saving valuable security personnel time. Threats arise from everywhere on the globe, and a threat that has first appeared in Japan for instance, could be targeting a corporation in Europe tomorrow. By having information about what may happen tomorrow, your organization will be gaining **pro-active, intelligent based protection** to stay ahead of threats.

Certifications

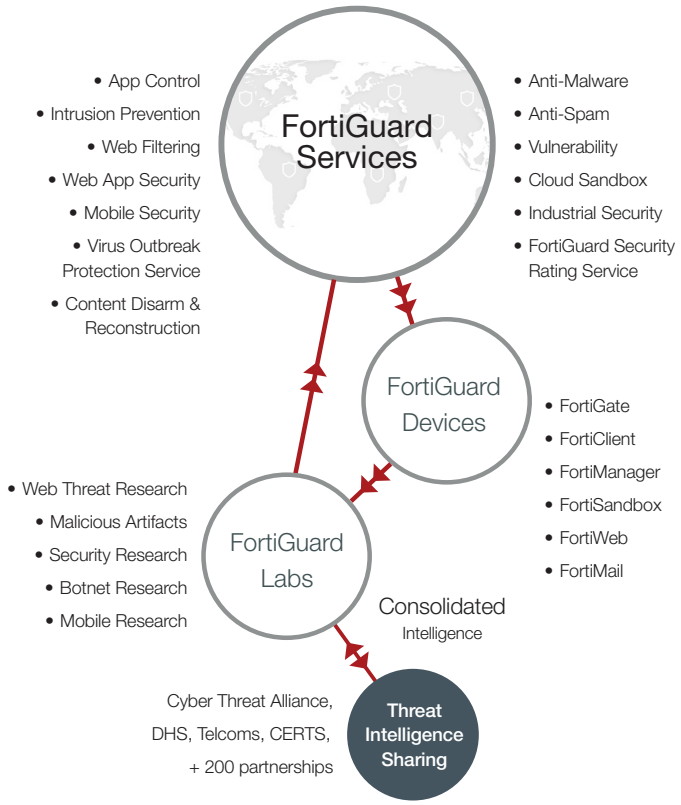
FortiGuard technologies earned its certifications through rigorous testing across a broad spectrum of performance indicators, conducted by independent organizations with industry-wide standards, including: NSS Labs, ICSA Labs, Common Criteria, Virus Bulletin, Virus Bulletin Spam, Mitre, Oasis and NASA.

FortiGuard Security Services

Cyber threats and cyber crime are on the rise. Criminals are exploiting the complexity of our expanding networks to infect, steal data, and hold systems to ransom. **Extensive research and knowledge of the threat landscape**, combined with the ability to respond quickly at multiple levels, is imperative for providing effective security.

Powered by AI

FortiGuard security services are designed to optimize performance and maximize protection across Fortinet's security platforms and are available as subscription feeds for the FortiGate Next-Generation Firewall / IPS platforms, the FortiMail secure email gateway, the FortiClient endpoint protection software, FortiSandbox, FortiCache, and the FortiWeb web application firewall. This includes IP reputation updates, intrusion prevention, web filtering, antivirus/anti-spyware, anti-spam, database security, , virus outbreak protection service, content disarm & reconstruction, security rating services and network and web application control capabilities to enable unified protection against today's threats.



FortiGuard Security Services
www.fortiguard.com

FortiCare Worldwide 24/7 support
support.fortinet.com

Feature Highlights

Intrusion Prevention (IPS)

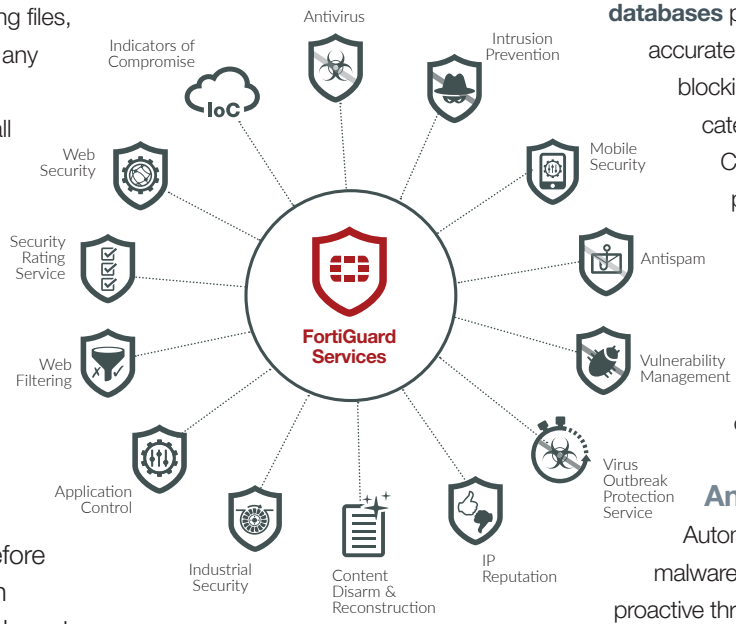
FortiGuards Automated updates provide latest defenses against network-based threats. You get the latest defenses against stealthy network-level threat, a **comprehensive IPS Library** with thousands of signatures, flexible policies that enable full control of attack detection methods to suit complex security applications, resistance to evasion techniques **proved by NSS Labs and the** IPS signature lookup service.

Content Disarm & Reconstruction (CDR)

strips active content from files in real-time, creating a sanitized file and active content is treated as suspect and removed. CDR processes incoming files, deconstructs them, and removes any possibility of malicious content in your files that do not match firewall policies, fortifying your zero-day protection strategy.

Virus Outbreak Protection Service (VOS)

closes the gap between antivirus updates with FortiCloud Sandbox analysis to detect and stop malware threats discovered between signature updates before they can spread throughout an organization, with real-time look-up to our Global Threat Intelligence database, providing you with the latest in malware protection.



Security Rating Service

Stay on track of your Security Roadmap and Target Security Maturity level with measurable and meaningful feedback in the form of actionable Configuration Recommendations, and Key Performance/Risk Indicators. Build Senior Management Confidence by demonstrating effective business asset protection and compliance with regulatory requirements.

For more information on Fortinet's Security Rating Service, please visit the FortiGuard website:
https://fortiguard.com/security-best-practices

IP Reputation

Aggregates real-time threat data from Fortinet's threat sensors, Cyber Threat Alliance, and other global resources. Provides protection against malicious web and botnet attacks, b**locks large scale DDoS attacks** from known infected sources and blocks access from anonymous and open proxies. **Real-time IP reputation updates** and analysis tools with Geo IP origin of attack.

Web Filtering

Block and monitor web activities to assist customers with government regulations 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 Comprehensive URL database provides rapid and comprehensive protection. Fortinet's **Credential Stuffing Defense** identifies login attempts using credentials that have been compromised using an always up-to-date feed of stolen credentials.

Antivirus

Automated content updates & latest malware and heuristic detection engines, proactive threat library protects against all known threats and variants, Content Pattern Recognition Language and **new patented code recognition software** protects against unknown variants and guaranteed SLAs to address severe malware threats.

Application Control

FortiGuard's App Control protects managed assets by controlling network application usage. The **sophisticated detection signatures** identify Apps, DB applications, web applications and protocols, both blacklist and white 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.

Vulnerability 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 for compliance requirements.

Feature Highlights

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.

Web Application Firewall (WAF)

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

Industrial Security

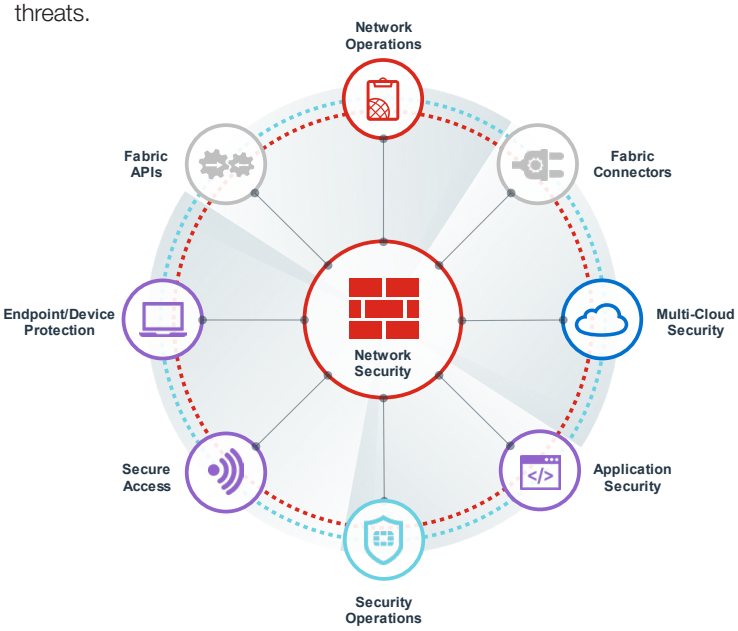
Protects ICS and SCADA of OT organization better by blocking or restricting access to risky industrial protocols. Gives you visibility and control of hundreds of industrial applications and lets you add custom applications. Provides real-time threat intelligence updates to battle advanced cyber threats. Supports major ICS manufactures to provide vulnerability protection.

Antispam

Dual-pass detection technology reduces spam at the network perimeter. Flexible configuration and no-hassle implementation. Allows anti-spam filtering policies. **Advanced anti-spam detection capabilities** provide greater protection than standard real-time blacklists.

Mobile Security

Fully-automated updates protect against the latest threats targeting mobile platforms. Employs advanced virus, spyware, and heuristic detection techniques to thwart new and evolving mobile threats.



Fortinet Appliances - Secured by FortiGuard

	APP CTRL	WAF	WEB FILTERING	ANTI-SPAM	IPS	VUL-SCAN	ANTI-VIRUS	IP REP	MOBILE SECURITY	IOC	VIRUS OUTBREAK PROTECTION SERVICE	CONTENT DISARM & RECONSTRUCT	SECURITY RATING UPDATE
Product													
FortiGate	✓		✓	✓	✓	✓	✓	✓	✓		✓	✓	✓
FortiSandbox			✓		✓		✓	✓	✓				
FortiClient	✓		✓			✓	✓						
FortiProxy	✓	✓	✓	✓	✓	✓	✓	✓			✓		
FortiMail				✓			✓				✓		
FortiWeb		✓					✓	✓					
FortiADC		✓	✓				✓	✓					
FortiDDoS								✓					
FortiAP S Series	✓		✓		✓		✓						
FortiCloud Sandbox											✓	✓	
FortiAnalyzer										✓			
FortiSIEM										✓			

Fortinet Developer Network (FNDN)

FNDN subscription-based community helps administrators and developers enhance and increase the effectiveness of Fortinet products, by providing official documentation and advanced tools for developing custom solutions using Fortinet products, like customer web portals, automated deployment and provisioning systems, and CLI scripting.

Benefits

- Developer Toolbox - Exclusive access to advanced tools, scripts/utilities and example code
- Documentation and How-Tos - Latest API documentation and how-to content for customization and automation
- Connect with Experts - Communicate and collaborate with advanced users and interact directly with Fortinet experts

Subscription Levels

- Basic - Free access to documentation, Forums, and basic tools
- Personal Toolkit - Full access for single user, Premium tools and licenses
- Site Toolkit - Full access for up to 15 users, Premium tools and licenses, FortiGuard services

FortiGuard Premier Signature Lookup

The FNDN Site Toolkit includes a number of advanced FortiGuard services that allows you to access FortiGuard's comprehensive security resources. Organizations around the world use the FortiGuard IPS and application control capabilities in the FortiGate platform to block network intrusions and manage thousands of different applications. The FortiGuard Premier Signature Lookup Service provides viewing of IPS and application control signatures with source code. You can search for signatures by ID or name to look up information on released IPS and application control signatures.

FNDN Global Servers

FortiGuard Services and 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.

	ADVANCED MALWARE PROTECTION	THREAT PROTECTION BUNDLE	UTM PROTECTION BUNDLE	ENTERPRISE PROTECTION BUNDLE	360 PROTECTION BUNDLE	A-LA CARTE ONLY	FORTICARE CONTRACT
Components/ Services							
Application Control Database, Internet Service Database, Client ID Database, IP Geography Database, Malicious URL Database, URL Whitelist Database		✓	✓	✓	✓		✓
Botnet domain Database, IP Reputation Database	✓	✓	✓	✓	✓	✓	
AV Database (multiple) Flow AV Database, Mobile AV Database	✓	✓	✓	✓	✓	✓	
FortiCloud Sandbox	✓	✓	✓	✓	✓	✓	
IPS Database		✓	✓	✓	✓	✓	
Content Disarm & Reconstruct Feature	✓	✓	✓	✓	✓	✓	
Virus Outbreak Protection Query	✓	✓	✓	✓	✓	✓	
Web Filtering Query Secure DNS Query			✓	✓	✓	✓	
Anti-Spam Query			✓	✓	✓		
Security Rating Database				✓	✓	✓	
Industrial Database (IPS and Application Control) Signatures				✓	✓	✓	
FortiCASB				✓	✓	✓	
FortiManager Cloud					✓		
FortiAnalyzer Cloud					✓		
SD-WAN Cloud Assisted Monitoring					✓		
SD-WAN Overlay Controller VPN					✓		
FortiConverter Service					✓		

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
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
FortiConverter Service	Policy Migration and Optimization Service

FORTINET

www.fortinet.com