FORTINET

Applied Security Intelligence

FortiGuard Security Services

Trusted and actionable security intelligence from FortiGuard Labs

Certified & Proven Security Protection

Comprehensive security updates and protection for the full range of Fortinet's Security Fabric solutions

FortiGuard Labs Research

Hundreds of research specialists, with over 16 years experience in threat research and response, providing cutting-edge protection to customers and enhancing their cyber security defense.

SOC-Integrated

Seemless integration into your SOC/NOC for actionable security operations against today's threats

Services

Intrusion Protection, Application Control, Web Filtering, Web Security, Anti-Virus, Anti-Botnet, Anti-Spam, Endpoint Vulnerability, Industrial Security

FortiGuard Minute

as of 2017 Q3

450,000
Hours of Threat Research Globally Per Year

200,000
Malicious Website Accesses blocked per minute

1,900,000
Network Intrusion Attempts resisted per minute

32,000
Botnet C&C attempts thwarted per minute

60,000
Malware Programs Neutralized Per Minute

20,000
Intrusion Prevention Rules, 100 Rules per Week

381
Terabytes of Threat Samples

500
Zero Day Threats Discovered

FortiGuard Security Services
www.fortiguard.com

FortiCare Worldwide 24/7 support
support.fortinet.com

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 430 **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 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.

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.

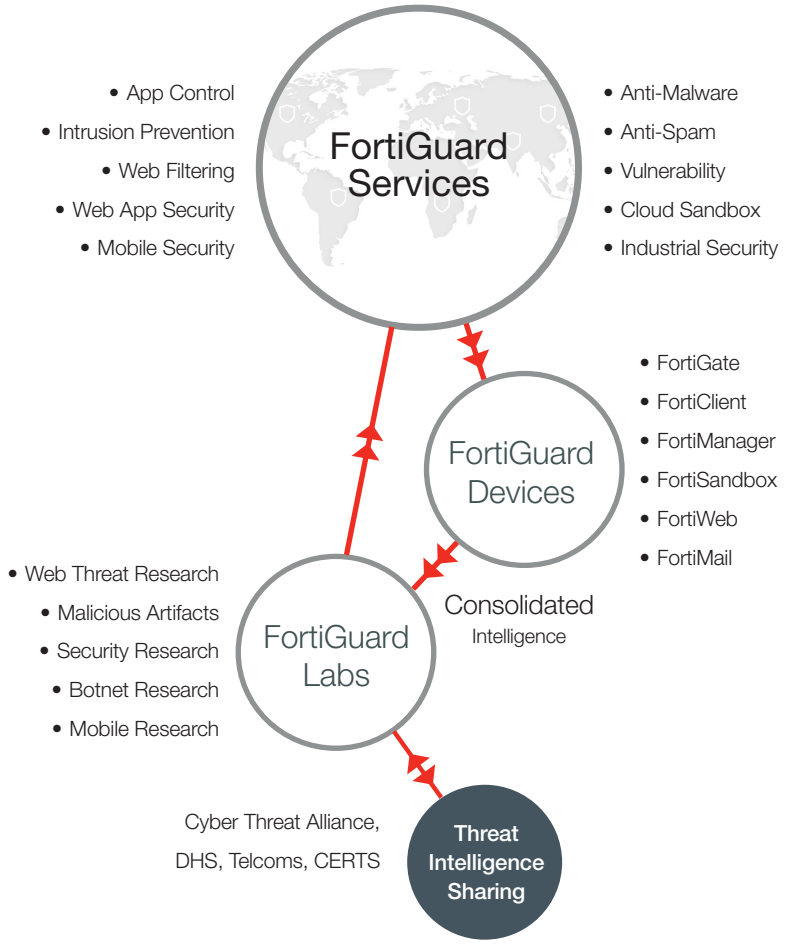
Combat Threats

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.

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.

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, and network and web application control capabilities to enable unified protection against today's threats.



Feature Highlights

Intrusion Prevention (IPS)

- Automated updates provide latest defenses against network-based threats.
- latest defenses against stealthy network-level threats
- **Comprehensive IPS Library** with thousands of signatures.
- Flexible policies enable full control of attack detection methods to suit complex security applications.
- Resistance to evasion techniques **proved by NSS Labs**
- IPS signature lookup" service

Vulnerability Scan

- Vulnerability scan network assets for security weaknesses
- On-demand or scheduled scans.
- **Comprehensive reports** on the security posture of your critical assets.
- Automated scanning of remote location FortiGates for compliance requirements

Application Control

- Protects managed assets by controlling network application usage
- **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
- Flexible policies enable full control of attack detection methods

IP Reputation

- Aggregates real-time threat data from Fortinet's threat sensors, Cyber Threat Alliance, and other global resources
- Protection against malicious web and botnet attacks.
- **Block large scale DDoS attacks** from known infected sources.
- Block 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
- Guaranteed SLAs to address severe malware threats

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.

Mobile Security

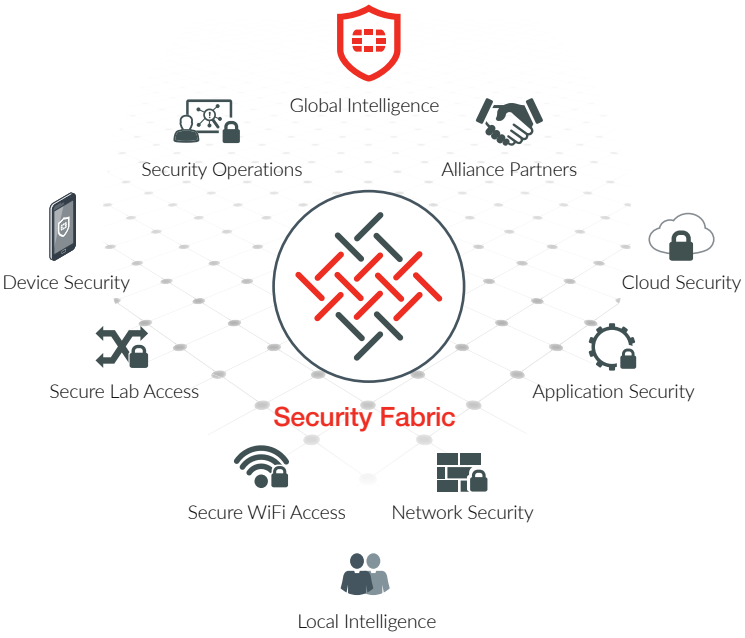
- **Fully-automated updates** protect against the latest threats targeting mobile platforms.
- Employs advanced virus, spyware, and heuristic detection techniques to thwart new and evolving mobile threats.

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.



Fortinet Appliances — Secured by FortiGuard

	APP. CONTROL	IPS	ANTIVIRUS	IP REPUTATION	WEB FILTERING	ANTISPAM	VULN. SCAN	MOBILE SECURITY	WAF
FortiGate	✓	✓	✓	✓	✓	✓	✓	✓	
FortiSandbox		✓	✓	✓	✓			✓	
FortiClient	✓		✓		✓		✓		
FortiCache			✓		✓				
FortiMail			✓			✓			
FortiWeb			✓	✓					✓
FortiADC D/F-Series				✓					✓
FortiADC E-Series				✓					
FortiDDoS				✓					
FortiAP S Series	✓	✓	✓		✓				

Fortinet Developer Network (FNDN)

FNDN is a subscription-based community to help administrators and developers enhance and increase the effectiveness of Fortinet products. The Fortinet Developer Network provides the 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.

FortiGuard Private Label Service

The FortiGuard Private Label Service provides a RESTful Web services API for integrating FortiGuard content with your existing systems to create custom applications. The API makes it possible to seamlessly incorporate FortiGuard's extensive technical resources into your organization's existing knowledge base. The standard FortiGuard Private Label Service included with Site Toolkit allows for streamlined access to the detailed descriptions of the AV, IPS, and Application entries in the FortiGuard Encyclopedia.

Indicators of Compromise
Threat illumination

FortiGuard Services and Bundles

FortiGuard Service Bundles are available individually, or in service bundles that combine critical services into a simple and cost-effective subscription license for organizations of every size.

PRODUCT	DESCRIPTION
FortiGate Enterprise Bundle	Designed to address today's advanced threat landscape, the Enterprise Bundle delivers all FortiGuard security services available for the FortiGate including: NGFW Application Control and IPS, Web Filtering, FortiSandbox Cloud, AntiVirus, Mobile Security, AntiSpam, core FortiCare security services, and a choice of 8x5 or 24x7 support.
FortiGate Threat Protection Bundle	24X7 Comprehensive Support, Advanced Hardware Replacement (NBD), Firmware and General Upgrades, VPN, Traffic Management, Threat Protection Bundle (Application Control, IPS and AV Services) (24x7 FortiCare plus IPS and AV)
FortiGate UTM Bundle	This traditional UTM security services bundle includes NGFW Application Control and IPS, Web Filtering, AntiVirus, AntiSpam, IP & Domain Reputation, and core FortiCare security services, along with a choice of 8x5 or 24x7 support.
FortiGate NGFW (App Control & IPS)	Classic Next-Generation Firewall security with Application Control and IPS updates.
FORTIGUARD A LA CARTE SERVICES	
Anti-Virus	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
IP/Domain Reputation Security	Aggregates malicious source IP data, from Fortinet threat sensors, to deliver up-to-date threat intelligence
AntiSpam	Multi-layered approach to detect and filter spam at the perimeter, giving you unmatched control of email attacks and infections
FNDN LICENSE SKUS	
FC-10-FNDN1-139-02-12	FNDN Personal Toolkit – FNDN access for single user. Includes premium tools and licenses for developers and advanced users of Fortinet products
FC-10-FNDN2-139-02-12	FNDN Site Toolkit – FNDN access for up to 15 users. Includes premium tools, licenses and Premium FortiGuard service including the FortiGuard CTI Feed for developers and advanced users of Fortinet products
ADDITIONAL SERVICE PACKAGES	
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.
FortiCache	Intelligence from AntiVirus, Web Filtering, Content Analysis, and FortiCare services.
FortiMail	Intelligence from AntiVirus, AntiSpam, FortiSandbox Cloud, FortiGuard Virus Outbreak Protection Service, Dynamic Adult Image Analysis Service and FortiCare services.
FortiWeb	Intelligence from Web Application Security, AntiVirus, IP Reputation, Vulnerability Scan, FortiGuard Credential Stuffing Defense, and FortiCare services.
FortiAnalyzer	Subscription license for the FortiGuard Indicator of Compromise (IOC)
FortiADC	Intelligence from 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)

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
Valbonne 06560
Alpes-Maritimes, France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6395.2788

LATIN AMERICA SALES OFFICE
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
United States
Tel: +1.954.368.9990

FST-PROD-DS-FGD

FGD-DAT-R11-201711