FortiGuard® Security Services
Applied Security Intelligence

FortiGuard® Security Services

Applied Security Intelligence

FortiGuard Labs

For more than 10 years, Fortinet's dedicated security research team, FortiGuard Labs, has led the industry in innovation, powering all Fortinet top-rated security platforms. This accomplished group is composed of security threat researchers, engineers, and forensic specialists tasked with outsmarting the cybercriminals and delivering cutting-edge protection tools to our global customers, assuring some of the fastest response times in the industry to new vulnerabilities, attacks, viruses, botnets, and other threats. The FortiGuard Labs team collaborates with the world's leading threat monitoring organizations to advise and learn of emerging threats and new trends in the threat landscape. Additionally, the team contributes to the overall security industry by identifying and responsibly reporting vulnerabilities directly to vendors of hardware, operating systems, and applications.

FortiGuard Security Subscription Services

The FortiGuard security subscription services provide 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 multiple threats. These services are designed to optimize performance with maximize protection across Fortinet's security platforms. Since these services are developed and delivered by Fortinet, there is an inherent synergy and integration that further increases their collective effectiveness. FortiGuard services are continuously updated, enabling Fortinet to deliver sophisticated multi-layered security knowledge and provide true zero-day protection from new threats. The FortiGuard Distribution Network (FDN) is a global distribution network that delivers updates to FortiGate®, FortiWiFi™, FortiMail™, FortiAnalyzer™, FortiDDoS™, FortiDB™, FortiWeb™, FortiSandbox™, FortiClient™, and FortiManager™ products.

Quick Facts

FortiGuard Labs operate in North America, Asia Pacific, and Europe.

In a typical week, FortiGuard Labs process over 18,000 TB worth of threat samples, add or update approximately:

- 2 million antivirus signatures
- 18,000 intrusion prevention (IPS) rules
- 250 million URL ratings in 78 categories
- 47,000,000 antispam signatures

In addition, FortiGuard Labs track more than

- 5,800 application control signatures
- 700 database security policies
- 3,000 web application firewall attack signatures

and uncover over 200 zero-day threats

FEATURES

Security Subscription Service	Description	Features and Benefits
Antivirus	Provides fully automated updates to ensure protection against the latest threats. These are delivered via a global high-speed distribution network for fast and reliable access to critical signature updates. Optionally, the FortiGuard Premier Signature Service is available for antivirus that offers guaranteed Service Level Agreements (SLAs) to address severe malware threats.	▪ Automated content updates keep defenses up-to-date with the latest malware and heuristic detection engines. ▪ Proactive threat library provides protection against all known and variants of known threats. ▪ Content Pattern Recognition Language and other new patented code recognition software to create smart detections, designed to pick up a family of threats behind a single variant. ▪ Leading effectiveness validated by Virus Bulletin Testing.
Antispam	Using multiple collection techniques, FortiGuard Labs develop and maintain accurate lists of spammers and spam content. Advanced antispam detection capabilities provide greater protection than standard real-time blacklists.	▪ Dual-pass detection technology reduces the volume of spam email at the perimeter before it enters the corporate network, significantly reducing email attacks, infections, and resource-wasting email. ▪ Flexible configuration allows the ability to set antispam filtering policies. ▪ No-hassle implementation. ▪ Leading effectiveness validated by AV-Comparatives.
Application Control	Protects managed desktops and servers by allowing, denying, and prioritizing network application usage using protection profiles and policies. Enterprise applications, databases, web mail, social networking applications, IM/P2P, file transfer protocols, and custom apps can all be identified accurately by sophisticated detection signatures.	▪ Fortinet is a leader in application control with one of the largest signature datasets, able to identify thousands of apps. ▪ Multiple categories are used to group application signatures, simplifying set up. ▪ Both blacklist and whitelist approaches can be used to allow or deny separately and in combination. ▪ Traffic shaping can be used to prioritize traffic by application on FortiGate. ▪ Flexible policies enable full control of attack detection methods.
Database Security	Cost-effective, automated solution for improving data security within enterprises by eliminating vulnerabilities in passwords, access privileges, configuration settings, and more. Services offer hundreds of policies that cover known exploits, configuration weaknesses, OS issues, lowering operational risks by creating consistent policies across an enterprise.	▪ Hundreds of pre-populated policies come standard to cover known exploits, configuration weaknesses, sensitive data, and operational risks and compliance. ▪ Policy versioning keeps track of predefined policies, allowing you to generate reports with the policy information that existed when the original scan was run. ▪ Easy deployment of activity monitoring and audits across your network via centralized policy management. ▪ Out-of-box deployment includes reporting to cover compliance needs like SOX and PCI DSS.
IP Reputation	Aggregates data from Fortinet's threat sensors, Exodus, the Cyber Threat Alliance, and other global resources to provide real-time updated information about malicious IPs. Protects against large-scale DDoS attacks, centrally-managed botnet attacks, and helps understand the origin of attack sources using Geo IP location.	▪ Protection against malicious sources associated with web attacks. ▪ Block large scale DDoS attacks from known infected sources. ▪ Protect against centrally-managed and automated botnet attacks. ▪ Block access from anonymous and open proxies. ▪ Real-time IP reputation updates. ▪ Analysis tools to help understand origin of attack using Geo IP location.
Intrusion Prevention (IPS)	Arms Fortinet customers with the latest defenses against network-based threats. Fortinet's Global Security Research Team works with worldwide organizations around the clock to shield against the latest application and OS vulnerabilities. Optionally, the FortiGuard Premier Signature Service is available for IPS that offers guaranteed Service Level Agreements (SLAs) for malware threats.	▪ Automated updates keep intrusion detection and prevention defenses current with the latest security content and detection engines. ▪ Comprehensive Intrusion Prevention System (IPS) Library with thousands of signatures. ▪ Flexible policies enable full control of all attack detection methods to suit the most complex security applications. ▪ NSS Labs rating provides proof of high effectiveness on FortiGate.
Vulnerability Scan	The vulnerability scan helps protect your network assets (servers and workstations) by scanning them for security weaknesses. You can scan on-demand or on a scheduled basis. Results can be viewed, or compile a comprehensive report about the network security posture of your critical assets.	▪ Automate regular scanning for compliance requirements at remote locations where FortiGates exist. ▪ Centralized reporting capability for organization-wide visibility.
Web Application Firewall (WAF)	Protects web applications and web services against SQL injection, cross-site scripting and a range of other attacks. The WAF service also includes hundreds of vulnerability scan signatures, hundreds of data-type patterns, web robot patterns, and suspicious URLs.	▪ Automated updates provide regular additions to WAF signatures. ▪ Supports PCI DSS compliance by protecting against OWASP top-10 web application vulnerabilities and using web-application firewall technology to block web-based attacks.

FEATURES

Security Subscription Service	Description	Features and Benefits
Web Filtering	Enables Fortinet products to block and monitor web activities to assist customers with government regulations enforcement of corporate internet usage policies. The massive web-content rating databases of FortiGuard power one of the industry's most accurate web-filtering service.	▪ Granular blocking and filtering provide web categories to allow, log, or block. ▪ Comprehensive URL database with many categories with high accuracy provide rapid and comprehensive protection.

FortiGuard Premier Services

With the FortiGuard Premier Signature Service, customers can submit requests for custom AV or IPS signatures. This service includes a service-level agreement with a contractual warranty for response time. Existing FortiCare™ support and FortiGuard AV or IPS service contracts are required on all units that are being covered under this service.

- Proactive alert notification of possible new outbreaks
- Flexible pricing options for 3 or 7 submissions per month
- Monthly virus and IPS activity reports
- Global support for regional service with personal attention to your security ecosystem needs
- For the AV service, Fortinet will provide custom virus signatures or query response to customers within 4 hours
- For the IPS service, Fortinet provides an initial response to a query in 4 hours, a detailed response in 12 hours, and deeper analysis in 48 hours.

Security Subscription Service	Description
Level 1 FortiGuard Premier Signature Service — 3 Incidents	AV, IPS, App Control updates (up to 3 incidents for each per month)
Level 2 FortiGuard Premier Signature Service — 7 Incidents	AV, IPS, App Control updates (up to 7 incidents for each per month)
Level 3 FortiGuard Premier Signature Service — 7 Incidents	AV, IPS, App Control updates (up to 7 incidents for each per month) and IPS signature lookup
Premier Web Service	URL rating services for enterprises, carrier and MSSP. Maximum 20,000 URL per year with a daily cap of 1,000 per day

Fortinet Appliances — Secured by FortiGuard

	App. Control	IPS	Antivirus	IP Reputation	Web Filtering	Antispam	Vuln. Scan	WAF	DB Security
FortiGate	•	•	•	•	•	•	•		
FortISandbox		•	•	•	•				
FortiClient	•		•		•		•		
FortiCache			•		•				
FortMail			•			•			
FortiWeb			•	•				•	
FortiADC D-Series				•				•	
FortiADC E-Series				•					
FortIDDoS				•					
FortIDB									•

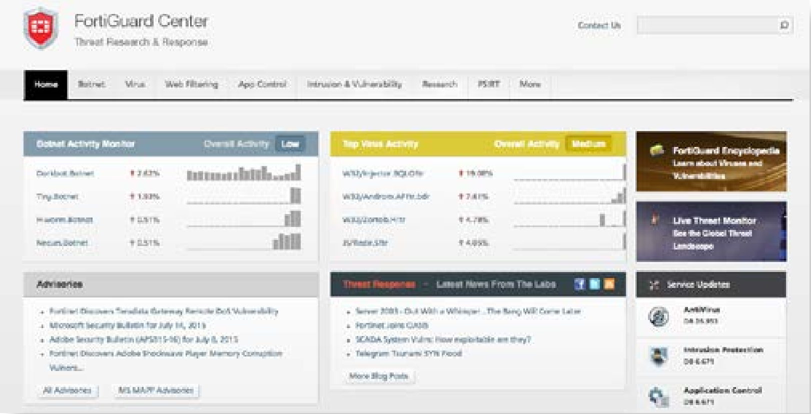
FortiGuard Labs provide the backbone of Fortinet's top-rated security platform. The data stream from Fortinet threat sensors blends with information provided by strategic partnerships with Exodus, OASIS, and the Cyber Trust Alliance, and is further enriched with threat information from global CERTs, MITRE, government information-sharing initiatives. Over 190 terabytes of security information is analyzed with patented machine learning and analytics, as well as human research, to create one of the fastest, most secure platforms available.

FEATURES

FortiGuard Center — Online Security Portal

The FortiGuard Center is an online resource providing a rich security knowledge base and technical resources including:

- Latest threats listing, news, and advisories
- Encyclopedia that provides detailed descriptions of known threats with remediation/protection advice
- Technical resources for mobile threats index, spyware terms and classifications, web-filtering categories and classification, and information about the filtering techniques used for the antispam service
- Online virus file scanner and submission portal
- URL/IP Rating Lookup



Advisories

- Fortinet Discovers Teradata Gateway Remote DoS Vulnerability
- Microsoft Security Bulletin for July 14, 2015
- Adobe Security Bulletin (APSB15-16) for July 8, 2015
- Fortinet Discovers Adobe Shockwave Player Memory Corruption Vulners...

Threat Response – Latest News From The Labs

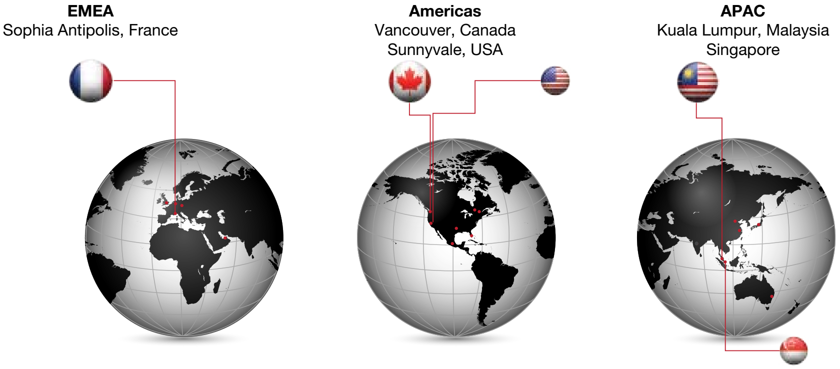
- Server 2003 - Out With a Whimper ...The Bang Will Come Later
- Fortinet Joins CIASB
- SCADA System Vulns: How exploitable are they?
- Telegram Tsunami SYN Flood

FORTINET
POWERED BY FORTIGUARD
Legend
Execution
Memory
Link
DoS
ATTACK TYPE
ATTACK LOCATION
CoDeSys.SCADA.Remote.Code.Execution
Mozilla.Products.Code.Execution.and.Security.Bypass
MS.SharePoint.InfoPath.Logging.DoS

FortiGuard Interactive Threat Map

Fortinet's threat map demonstrates IPS data in action across our network of threat sensors. The map illustrates how data is flowing between sensor and attacker, showing C&C communication or files being sent, the severity or attack rating, and the type of attack, all delineated by colors and animation style.

Access the FortiGuard Center at: www.fortiguard.com and Threat Map at : http://threatmap.fortiguard.com



FortiGuard Distribution Network

The FortiGuard Distribution Network has data centers around the world located in secure, high-availability locations that automatically deliver updates to the Fortinet security platforms. With the FortiGuard subscription services enabled, customers can rest assured that their Fortinet security platforms are performing optimally and protecting corporate assets with the latest security technology.

FORTINET

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

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA SALES OFFICE
Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel: 011-52-(55) 5524-8480