FORTIGUARD™ SERVICES: REAL TIME RESPONSE TO SECURITY THREAT OUTBREAKS
Contents:

OVERVIEW ................................................................. PAGE 4
EXECUTIVE SUMMARY ............................................. PAGE 4
FORTIGUARD SUBSCRIPTION SERVICES OVERVIEW ...... PAGE 5
FORTIGUARD SERVICE OFFERING COMPONENTS & PROCESSES: A CLOSER LOOK ................................................................. PAGE 6
SECURITY THREAT/RESPONSE LIFECYCLE ................ PAGE 9
SUMMARY: KEY BENEFITS OF FORTINET SOLUTION ...... PAGE 11
ABOUT FORTINET ...................................................... PAGE 12
OVERVIEW
Security personnel must respond quickly and proactively to the increasing num-
ber and severity of threats from viruses, worms and intrusion attacks. Fortinet's FortiGuard services provide a complete, real-time response to the full spectrum of security threats. Combined with Fortinet's ASIC-based FortiGate™ systems that detect and eliminate threats in real-time at the network edge, FortiGuard Services ensure timely, automatic protection and minimize exposure to loss and damage from network-borne attacks.

This paper describes the key elements that make up the four FortiGuard Subscription Services and explains the role of each in ensuring timely protection against fast-moving threats.

EXECUTIVE SUMMARY
Large companies, small and medium sized businesses (SMBs), government agencies and managed security service providers (MSSPs) have been striving to become "real-time enterprises" for several years. With the universal availability of access to the Internet and with applications of all kinds Web-enabled, this dream has finally come true. However, with the continuing increase in the sophistication and propagation speed of security attacks, real-time enterprises need to improve network protection without compromising the performance of their networked applications.

Fortinet's FortiGate™ Antivirus Firewalls have gained rapid acceptance in both key vertical markets and the traditional enterprise market for their ASIC-based architecture and corresponding ability to detect and stop sophisticated content-based attacks at the network edge, before they can reach critical network and computing resources. This paper describes the crucial role played by Fortinet's FortiGuard Infrastructure in the delivery of real-time network protection. By ensuring the rapid identification of new threats and delivery of the latest threat detection information to FortiGate units, FortiGuard Subscription Services are a key enabler of real-time network protection.
FORTIGUARD SERVICES OVERVIEW

The goal of all four Fortinet FortiGuard Services is to ensure that all registered and supported FortiGate systems receive the updates they need to provide complete, timely protection against network-based threats. This is accomplished through the coordinated interplay of the following key components:

- **The globally deployed Threat Response Team (TRT),** which is responsible for identifying new threats, collecting samples, replicating and characterizing attacks, and developing updates for the virus definitions, attack definitions, scanning engines, and other components that enable FortiGate systems to detect and eliminate threats from network traffic streams.

- **The FortiGuard Center (FC),** which provides information to Fortinet customers and partners via a Web-based information portal and subscription-based FortiGuard Bulletin email updates that provide up to date information on the current security threat situation and Fortinet’s response.

- **The FortiGuard Distribution Network (FDN),** which is a series of FortiGuard Distribution Servers (FDS) that communicate with FortiGate units and supply or push updates real-time to FortiGate units.

The following sections provide additional details for each component of each FortiGuard Service offering.
FORTIGUARD SERVICE OFFERING COMPONENTS & PROCESSES: A CLOSER LOOK

THE THREAT RESPONSE TEAM (TRT):
The Threat Response Team members continuously monitor a variety of sources for signs indicating a potential security threat. If an outbreak is detected, the TRT gathers samples of the threat and performs detailed analysis, which involves replicating the threat and characterizing its effects and means of propagation.

Once a threat is identified and characterized, the TRT’s virus and attack researchers develop the appropriate detection signatures, test them to ensure that the signatures will not cause "false positive" indications from legitimate traffic, add the signatures to the FortiGate, FortiMail, and FortiClient Virus and Attack Definition databases as appropriate, and stage the updated databases for distribution to each Fortinet product family via the FortiGuard Update Distribution Network.

As indicated in the following diagram, the Fortinet TRT is deployed on 3 continents, and provides threat response 24x7x365.

GLOBAL THREAT MONITORS
Antivirus and Intrusion Prevention Services Researchers & Signature Developers
The Global Threat Monitors and the AntiVirus and Intrusion Prevention Services Researchers work together to coordinate the response to any attack outbreak. Monitoring is done through several means, including reports to Fortinet’s customer support lines, virus submissions provided to Fortinet (at www.fortinet.com), “honeypots” deployed around the world that detect and retain attacks, and constant interchange with leading virus and intrusion experts worldwide via public and private threat monitoring sites.

THE FORTIGUARD CENTER (FC):
The online FortiGuard Center, available at www.fortinet.com/FortiGuardCenter, provides a complete overview of current network threats, information about specific viruses and vulnerabilities, online tools to track the detailed definitions of the threats covered by the latest FortiGate virus and attack definition databases.
The resources of the FortiGuard Center portal are a click away, and provide access to a wealth of additional information. Antispam and Web content filtering details and online tools are also available for real-time network security updates. The FortiGuard Center information portal is updated daily - and in the case of a virus outbreak, continuously - with information about threats and the status of Fortinet’s response.

Fortinet’s website also notes an application-focused FortiGuard section under "products" and convenient links to the FortiGuard Center section with an easy-to-read visual display that summarizes the current threat status. From the home page, the vast network security resources of the FortiGuard Center portal are a click away, and provide access to a wealth of additional information:

FORTIGUARD ANTIVIRUS

• **Hot Viruses & Spyware** - The Hot Viruses & Spyware page lists the latest virus and spyware threats and provides a brief explanation of each. At a glance, it provides basic information on those threats that demand immediate attention and those that have been of most concern over the past several days or weeks.

• **Virus Encyclopedia** - The searchable Virus Encyclopedia contains detailed descriptions of the viruses, worms, trojans, and other threats currently active in the wild. A summary of virus information tells the threat level, date of discovery, mode of operation and visible symptoms, and the FortiGate Virus Definition Database Versions that provide protection against each virus or worm.

• **Online Virus Scanner** - The Online Virus Scanner allows customers to scan and test files on their local systems to see if they are infected. Files are scanned against Fortinet’s latest signature and threat databases to ensure that even the newest viruses are detected.

• **Submit Virus Sample** - Describes how to send virus samples to the Fortinet Threat Response Team for analysis.
FORTIGUARD INTRUSION PREVENTION

• **Hot Vulnerabilities** - Using FortiGuard Subscription Services prevents both new and yet unknown threats and vulnerabilities from gaining access to your network and its valuable applications or data assets by preventing and responding to today’s fast-spreading attacks. The Hot Vulnerabilities page summarizes the latest network intrusion threats circulating around the globe and give critical information in each threat and its impact.

• **Attack Encyclopedia** - The searchable Attack Encyclopedia contains detailed descriptions of common attacks that have the ability to infect networked computer systems. In-depth analysis of each attack includes a description, the impact of the attack, the vulnerability exploited by the attack, references, recommended actions, and the FortiGate Attack Definition Database Versions that provide protection against the attack.

• **Security Advisories** - FortiGuard IPS service provides information on the latest security advisories from key sources to give IT and security professions a consolidated web portal for all their security research needs.

FORTIGUARD WEB CONTENT FILTERING

• **Summary** - Fortinet understands the need for timely and thorough malicious webpage listings. Our FortiGuard Web Content Filtering subscription service offers more than 25 million rated domains categorized into 56 unique content categories for best in class user settings. Like the three other FortiGuard subscription services offerings, Fortinet’s Web Content Filtering updates offer the industry’s fastest response and global updates via the FortiGuard global distribution network. URL Lookup: As part of the service, FortiGuard Web Filtering provides a URL Lookup service to allow customers to see ratings for specific web pages and URLs. Improperly rated sites can be submitted to Fortinet’s TRT team for validation and recertification.

FORTIGUARD ANTISPAM

• **Antispam** - Fortinet understands the need for timely and thorough blocking of unwanted email and domains. To achieve up-to-date real-time spam identification with a high degree of accuracy, Fortinet’s FortiGuard Antispam service provides a dual pass inspection technology using several spam source identifiers. Leveraging resources from its globally distributed spam probes (e.g. honey pots) that receive upward of one million spam messages per day, each message is processed through a multiple layers of identification processes to produce an up to date list of spam origins. Fortinet also offers a dedicated secure email appliance called FortiMail that offers both FortiGuard Antispam and Antivirus subscription updates to provide dedicated spam detection, email archiving, and antivirus services for electronic messaging.
In addition to the FortiGuard Center portal, FortiGuard Services include a subscription-based email newsletter called the FortiGuard Bulletin. The Bulletin is issued weekly, and may be issued more frequently in the event of a serious outbreak. In addition to providing a timely update on the current status of security threats worldwide, the Bulletin also alerts customers to actions that can be taken while an outbreak is in process.

The FortiGuard Bulletin provides updates summarizing the status of threat outbreaks and the actions that can be taken by customers.

THE FORTIGUARD DISTRIBUTION NETWORK (FDN):
The FDN is a multi-tiered server infrastructure that provides fast, reliable updates and filtering services for Fortinet’s four FortiGuard subscription services worldwide.

The FDN consists of a top level FortiGuard Distribution Center (FDC) and multiple, subordinate FDCs in a tiered, redundant architecture. Each FDC contains multiple redundant FortiGuard Distribution Servers (FDSs) with redundant links to the Internet for high-performance service with great resiliency to failure. Fortinet product families that use the FDN network are updated with the latest list of FDN servers and work with the FDN to calculate their quickest update and service paths to each of the FDN Centers located around the globe.

The FDN servers interact with entitlement databases which are used to verify the eligibility of each FortiGate or FortiMail systems for updates and filtering services. The entitlement databases also contain the data required to enable FDSs to "push" updates to FortiGate units between scheduled updates when warranted.

Fortinet’s FortiGuard Operations Personnel Utilize the FortiGuard Distribution Server Console to Initiate an Emergency "Push" Update in the Event of a critical outbreak. In extreme circumstances, such as Level 5 threats that are not yet fully characterized, FortiGate Antivirus Firewalls can be set to block vulnerable file types at the network edge without having to completely shut down all net-
A single configuration change to a FortiGate unit at the edge of a network can block potentially infected files entirely, even before a specific signature is available for host-based antivirus applications.

work connections. Once an updated Virus Definition database is available, FDSs can push the update to all FortiGate Antivirus Firewalls, reducing both the time and amount of disruption of normal network traffic.

This is one of the key benefits of a gateway-based approach to network protection. A single configuration change to a FortiGate unit at the edge of a network can block potentially infected files entirely, even before a specific signature is available for host-based antivirus applications. This type of antivirus and response system adds a new layer of threat protection to give customers a proactive approach in defending themselves against ever changing threats.

SECURITY THREAT/RESPONSE LIFECYCLE

The primary goal of FortiGuard Services is to provide fast response to threat outbreaks. Fortinet continuously monitors the performance of FortiGuard Services by evaluating our performance at each step in the Security Threat/Response Lifecycle, shown below.

As shown in the figure above, the goal is zero response time to new threats. The focus on this goal is what drives Fortinet’s continuous process improvement program. As one example of the FortiGuard update services, each step in the FortiGuard AntiVirus update cycle is described below:

- **Attack launched**: An outbreak starts with the launch of an attack. The attack can initiate anywhere and the hacker typically can hide his identity and mask the source of the outbreak.

- **Attack reported**: Once an attack has been successfully launched, infected networks and computing systems will show symptoms such as performance degradation, inaccessibility (as in the case of denial-of-service attacks), loss of data, unanticipated system behavior, etc. Customers with affected networks are typically the first to detect and report the outbreak. For example, Fortinet provides resources on the FortiGuard Center portal that make it easy for customers to report unusual activity and to send samples of suspicious messages and files. In addition, a number of organizations, such as the CERT coordination center (a major reporting center for Internet security problems), have staff that closely mon-
itor network health worldwide around the clock and keep in close contact with network administrators at a wide variety of organizations. Further supplementing these resources, Fortinet maintains a series of so-called "honeypots" around the world that are designed to attract and capture a variety of attacks. Using data from these and other sources, outbreaks can typically be detected and reported within an hour of launch. Of course, the time can be more or less depending on the nature, point (or points) of origin and the target (or targets) of the attack.

- Sample obtained: In many cases, the report of an attack includes a sample of an infected file. Sample sources include customers, partners, and peer virus and intrusion attack researchers. With presence and customers in all major world regions, Fortinet is well positioned to collect attack samples. In most cases, Fortinet has samples in hand within 30 minutes after an attack has been reported.

- Replication/Characterization: For viruses and worms, which spread either automatically or with user intervention, the first step is to replicate the samples and to study the characteristics of the attack. This process can be complex for several reasons. For example, certain attacks may actually be launched with multiple variants, and in some cases the variants may change at each replication. In addition, so-called "blended attacks" can contain elements of viruses, worms, and intrusions all in a single threat. With sufficient samples and analysis of the attributes of the attack, the precise code that executes the attack can be isolated. Fortinet’s virus research labs operate in multiple locations in parallel, and contain sophisticated tools that automate sample replication and analysis. FortiGuard Service Offering 14 Replication and characterization typically takes between 10 and 30 minutes depending on the complexity of the attack.

- Signature development and test: Once the attack’s operating code has been isolated and its method of operation has been completely characterized, Fortinet’s virus and attack researchers develop "signatures" that enable to network intrusion detection system (NIDS) and/or antivirus engine to detect and eliminate the attack.

The challenge in this step is to ensure that any signature(s) are highly specific and will identify threats without triggering false alarms from legitimate traffic. Rigorous testing using highly automated tools is required to quickly refine signatures to eliminate both "false positive" and "false negative" detections. This process can require 30 minutes or more depending on the complexity of the attack, and is key area of Fortinet’s research and investment in new tools to further automate the process.
• Signature database upload to FDN: Once a signature has been produced, it is added to the latest virus and/or attack definitions database(s) so that they can be downloaded to protect the various Fortinet products using the FortiGuard Subscription Services. The new databases are then staged to the primary FortiGuard Distribution Servers. This process requires less than 5 minutes.

• Signature database "Pushed" to FortiGate AV firewalls: Until this step, Fortinet handles the outbreak lifecycle in a manner similar to other AV/IDS vendors. However, at this point, Fortinet is able to leverage the unique position of FortiGate units at the edge of customer networks to greatly reduce outbreak response time and provide more effective network protection, especially for the most dangerous, fast-moving threats.

With conventional, host-based antivirus software, a customer's network will not be protected until every host requests a download of the updated signature database. This may take several hours or more depending on the rate at which update requests are scheduled in each host's antivirus software. With Fortinet, if the Threat Response Team determines that the current outbreak is sufficiently severe, the FortiGuard Distribution Network will be commanded to initiate a "push" update. In this case, the FortiGuard Distribution Servers worldwide will check their registration databases and will identify all FortiGate units that are eligible for and have requested reception of push updates. Within 5 minutes, all properly registered and enabled FortiGate units worldwide will receive their updates and will shield all of the hosts "behind" them from the new threat.

At several points in the outbreak life cycle, users are kept informed of the progress of the attack and of the availability of a Fortinet response via the FortiGuard Center portal and FortiGuard Bulletins. Depending on the outbreak, the entire process can take as little as one hour, and requires barely a fraction of the effort typically required of system administrators to ensure that all hosts have updated antivirus signatures. Even with this rapid response, FortiGate remains committed to continually reducing the "time to protection" to the goal of Zero Response Time.

SUMMARY: KEY BENEFITS OF FORTINET SOLUTION

The trend towards the "real-time enterprise" has brought significant challenges to information security for organizations of all types. The speed and complexity of attacks has increased - as has the resulting damage - at the same time that the tolerance for security-related delays diminished.

Fortinet's ASIC-accelerated FortiGate Antivirus Firewalls, FortiMail Secure Messaging platforms, and FortiClient host-based security application meet the challenge of real-time network protection by providing application-level processing at the network edge and host that enables the detection and prevention
of viruses, worms, intrusions banned content, spam and other threats in real time. The FortiGate units are complemented by Fortinet’s FortiGuard Services, which ensure that Fortinet customers worldwide are continuously protected in the shortest possible time against the never-ending stream of new, fast-moving threats.

Through a combination of industry-leading personnel and innovative technology, the FortiGuard Services address every step across outbreak lifecycle, with a solution that provides improved protection while reducing the burden on security and systems administrators. The responsiveness, protection, and ease of administration of the Fortinet solution is unmatched by conventional antivirus offerings, and underscores Fortinet’s commitment to providing the world’s most effective, real-time network protection for real-time organizations.

ABOUT FORTINET (WWW.FORTINET.COM)
Fortinet is the confirmed leader of the Unified Threat Management market. The company’s award-winning FortiGate™ series of ASIC-accelerated antivirus firewalls, winner of the 2004 Security Product of the Year Award from Network Computing and the 2003 Networking Industry Awards Firewall Product of the Year, are the new generation of real-time network protection systems. They detect and eliminate the most damaging, content-based threats from e-mail and Web traffic such as viruses, worms, intrusions, inappropriate Web content and more in real time - without degrading network performance. FortiGate systems are the only security products that are quadruple-certified by the ICSA (antivirus, firewall, IPSec, NIDS), and deliver a full range of network-level and application-level services in integrated, easily managed platforms. Named to the Red Herring Top 100 Private Companies, Fortinet is privately held and based in Sunnyvale, California.

SALES
Please contact us through fortinet.com/sales or phone toll-free in the U.S. (866) 868-3678 or +1(408) 235-7700.

POTENTIAL PARTNERS
Please contact us at partners@fortinet.com or visit us at www.fortinet.com.