





 FortiGate-50A

 FortiGate-60

 FortiWiFi-60

 FortiGate-100

 FortiGate-300A

 FortiGate-200

 FortiGate-200A

 FortiGate-300

 FortiGate-300A

 FortiGate-400

 FortiGate-400A

 FortiGate-500

 FortiGate-500A

 FortiGate-800

 FortiGate-800F

 FortiGate-1000

 FortiGate-3000

 FortiGate-3600

 FortiGate-4000

 FortiGate-5020

 FortiGate-5050

 FortiGate-5140

 FortiManager-400

 FortiManager-3000

 FortiLog-100

 FortiLog-400

 FortiLog-800



 FortiReporter



 FortiClient



 FortiProtect



 FortiGuard

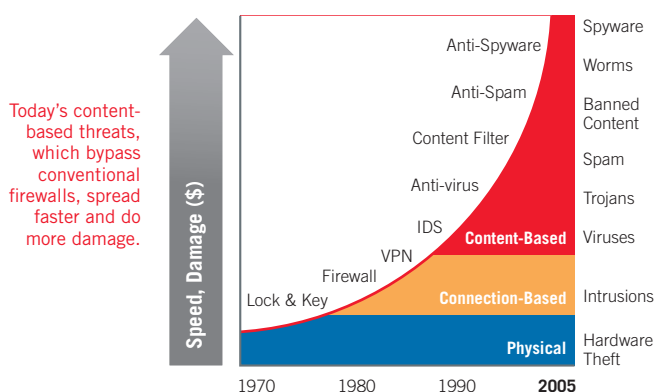


## Who We Are

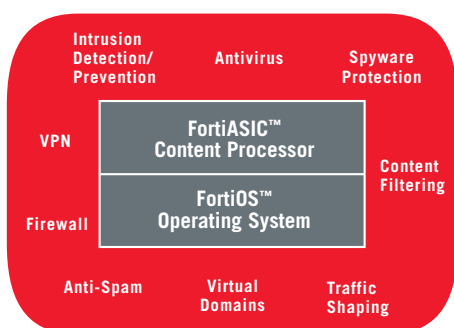
Fortinet was founded in 2000 by Ken Xie, the visionary founder and former president and CEO of NetScreen. The company is privately held and headquartered in Sunnyvale, California, with offices in Australia, Canada, China, France, Germany, Hong Kong, India, Japan, Korea, Malaysia, Singapore, Sweden, Taiwan, Thailand and the UK.

## What We Do

Fortinet's award-winning FortiGate™ series of ASIC-accelerated Antivirus Firewalls are the new generation of real-time unified threat management (UTM) systems. They detect and eliminate the most damaging, content-based threats from email and Web traffic such as viruses, worms, intrusions, inappropriate Web content and more in real-time — without degrading network performance. FortiGate UTM systems deliver a full range of network-level services — stateful firewall, VPN, intrusion detection and prevention and traffic shaping — as well as application-level services such as antivirus, antispyware, and web content filtering, in dedicated, easily managed platforms. A full range of complimentary hardware and software security products are also available for real-time logging, monitoring and network reporting of enterprise managed security service providers and small/medium business networks.



### Capabilities Supported by All FortiGate Antivirus Firewalls



### Worldwide Unified Threat Management Security Appliance and Firewall/VPN Security Appliance Revenue, 2003-2008 (\$M)

	2003	2004	2005	2006	2007	2008	2003-2008 CAGR (%)
UTM Security Appliance	105	225	518	828	1,325	1,987	80.1
Firewall/VPN Security Appliance	1,479	1,668	1,792	1,804	1,623	1,462	-0.2

Source: IDC, 2004

## The Problem We Address: Real Time Network Protection

A growing percentage of so-called “content-based” network attacks, such as viruses, worms and Trojans, are being introduced into organizations via seemingly innocuous activities such as Web browsing. This trend is expected to continue as organizations turn increasingly to real-time communications, like Web applications and instant messaging, as the means to remain responsive and competitive. Unfortunately, conventional network protection systems, such as firewalls and host-based antivirus software, lack the dedicated hardware processing required to perform the deep packet analysis, content reassembly, and application-level screening necessary to detect these threats without imposing unacceptable delays on real-time network applications. As a result, most organizations are dangerously exposed to content-based attacks from real-time web, email and peer to peer traffic.

Fortinet’s FortiGate series of Antivirus Firewalls for the first time provides cost-effective systems that deliver complete network-level and content-level protection at the network edge with real-time performance. Each member of the scalable, flexible FortiGate family is a dedicated, easily managed device that delivers a full suite of best in class capabilities, which include ICSA-certified virus protection and content filtering, along with network-level services including firewall, intrusion detection, intrusion prevention, VPN and traffic shaping functions.

## How We Do It

With 11 patents pending, FortiGate Antivirus Firewalls leverage breakthroughs in chip design, networking, security and content analysis. The unique, ASIC-based architecture analyzes network content and behavior in real-time, enabling all key network services — including real-time Web applications — to be screened for both network and content-level threats without impacting network performance.

## Fortinet Product Advantages

### Better Value

Fortinet’s security systems, management and reporting products offer best in class choices for seven key security components. Fortinet’s award-winning security solutions are the only security products that are certified in four ICSA Lab categories — Firewall, VPN, IPS, and Antivirus. In September 2004, IDC named Fortinet’s technology as the worldwide leader in the Unified Threat Management (UTM) security category with more than 29% market share. And in April 2004, Gartner named Fortinet’s technology as Visionary in their Enterprise Firewall Magic Quadrant. By offering enterprises the ability to

eliminate multiple security devices and collapse them into an inline network capability, Fortinet decreases a company’s Capital Expenditure (CAPEX) and Operating Expenditure (OPEX) costs. With Fortinet’s simple “per box” licensing, ongoing maintenance, support, and product update costs are greatly reduced compared to competing products licensed on a “per user” basis.

### Leading Edge Technology

Fortinet security platforms offer unparalleled security and performance in each of its products. To provide strong security without performance penalties, Fortinet developed a high-performance security ASIC (FortiASIC) and patent pending Content Pattern Recognition Language (CPRL) specifically designed to speed up the computationally intensive routines commonly associated with complete content protection. This technology goes beyond the Deep Packet Inspection capabilities that many competing firewalls are just starting to implement. FortiGate’s ability to perform stateful firewalling, antivirus inspection, and intrusion detection leverages new security algorithms and behavior-based heuristics to take advantage of the shared information between its security components — giving FortiGate the ability to stop malicious threats that are non-signature based and previously unknown. This technology allows Fortinet to increase its detection capabilities against modern, zero-day attacks that are designed to bypass traditional security defenses such as stateful firewalls and intrusion detection systems.

### Complete Security Solution

Fortinet understands the importance of a complete solution and offers customers robust logging and reporting through its FortiLog and FortiReporter products, automated updates with FortiProtect Services, real-time Web Content Filtering with FortiGuard, and coordinated central management with FortiManager. To provide an additional layer of protection for hosts at the edge of the network (either in the office or away from the office), FortiClient software provides client-based antivirus, spyware detection and removal, personal firewall, and VPN capabilities. All FortiGate security solutions are ICSA Labs certified for Firewall, Antivirus, Intrusion Detection & Prevention, and IPSec VPN — guaranteeing industry recognized standard-based protection and compliance. Passing additional IPS testing with the world renowned NSS Labs further attests to Fortinet’s leading edge technology and its ability to fully detect and stop modern network threats. With ICSA certification and NSS IPS testing, customers are assured that high industry standards are met and can feel confident about the security solution they have chosen to implement in their corporate networks.

## Scalable Security Solutions

### ENTERPRISE

Many larger corporations realize a single line of defense is no longer sufficient for protecting valuable ecommerce transactions, intellectual property and partner data exchange. Defense in-depth is what's needed to prevent network compromise through a combination of new technologies and approaches. The enterprise can leverage Fortinet's Complete Content Protection to detect, log and effectively eliminate a variety of threats, including inappropriate Web content, email spam, and spyware or grayware. All size enterprise networks benefit with Complete Content Protection against increasingly network-borne security threats from a constantly changing perimeter. Today's enterprise networks extend wirelessly internally and with business travel, outwards using partner extranets, internally with employee intranets and all points in between. Pairing with existing host-based antivirus systems, single function firewalls or stand-alone IDP devices, Fortinet's systems dramatically increase a company's dynamic threat prevention capabilities for defense in depth.

#### Fortinet Advantage:

- Best in class ISCA-certified capabilities for all size enterprise networks, wired or wireless and up to multi-gigabit speed throughput for Antivirus gateways, IDP, VPN and firewalls
- Transparent mode functionality for pairing Fortinet security functionality seamlessly with existing security products in the enterprise
- A choice of leading edge ISCA-certified network security feature sets in FortiGate Antivirus Firewalls accelerated by its FortiASIC and Patent Pending CPRL technology
- Scalable security system offerings using consistent management interface for any size enterprise, regardless of the number of central or branch office clients connected to the network
- Attractive per-box licensing eliminates costly per user licensing charged by numerous competitors that can add 4-5x the capital purchase price to the annual operation budget

### MSSP

Damaging attacks to small and medium enterprise businesses by worldwide attacks have grown from \$3.3 billion in 1997 to more than \$12 billion. Fortinet works with all size MSSPs to limit the frequency, severity and sophistication of cyber-attacks for its customer's networks. In the U.S., there is growing recognition that the Gramm-Leach-Bliley Act (GLBA) and the Health Insurance Portability and Accountability Act (HIPAA) apply to a wide range of companies, large and small, who handle consumer financial or health care data. UK-based banks will need to meet the Basel II accord which goes into effect in 2006, requiring them to have three years of auditable data. FortiGate Antivirus firewalls helps MSSPs rapidly deliver one or many high-value security services provisioned from a single platform to SME/SMB customers as well as large enterprise customers.

- Ability to provision more than one security service per platform, helps significantly reduce both capital and operational expenses for the Managed Security Service Provider
- Superior management capabilities with proactive reporting and logging options for thousands of individual customer premise equipment devices without forcing the MSSP to become a system integrator of multiple product or management platforms
- No company-sponsored, competing security service providers unlike other competitors who have invested in this market bringing an inherent conflict of interest
- Multiple gigabit throughput to integrated customer premise equipment including the Fortigate 100 at the customer site
- Unified Threat Management enables the MSSP to differentiate itself with best-in-class services while increasing service revenue and reducing operating costs

### SMB

Branch corporate offices or smaller businesses require turnkey security solutions. Often these facilities leverage Managed Security Service Provider connectivity and benefit from an integrated Customer Premise Equipment solution found in FortiGate Antivirus Firewalls. These integrated platforms give small businesses the greatest flexibility and protection available in a modern security platform. Fortinet's award-winning technology is consistent across its entire family of products and provides the same leading edge protection regardless of company size (SoHo to SME to large enterprise to service provider).

- Full advantage of best in class enterprise security feature sets in a comprehensive branch office/small office platform that is intuitive, easy to deploy and use
- Products manageability helps small businesses who often don't have the big IT staffs prevalent in larger companies
- ISCA-certified security feature set ensures the smaller office network leverages similar technology usually found only in larger point product enterprise security product
- Unified Threat Management offers smaller businesses a complete security feature set to defend their networks against all vulnerabilities
- No hidden costs as Fortinet offers an attractive per box licensing eliminating costly per user licensing



## Industry-leading Functionality

### Antivirus Gateway



Detects and eliminates viruses, worms and spyware, in real-time. Scans incoming and outgoing email attachments (SMTP, POP3, IMAP) and all FTP and HTTP traffic including web-based email — without degrading Web performance. Antivirus gateways close the vulnerability window by stopping viruses and worms before they enter

the network. Fortinet's worldwide antivirus staff "follows the sun" and offers customer base real-time virus signatures updates using global FortiProtect update network. Wildlist.org co-founder Joe Wells is Fortinet's Chief Antivirus Scientist and helped define integrated FortiOS and FortiASIC leverage for Antivirus capabilities.

### Firewall



Powerful complete content inspection firewall offers certified protection, maximum performance and scalability. Fortinet goes beyond Stateful Inspection host-based firewalls that provide accurate albeit non-content specific packet inspection. Network firewalls typically guard internal computer networks (intranet)

against malicious access from the outside; however, network firewalls may also be configured to limit access to the outside from internal users. Fortinet's FortiASIC accelerates FortiGate systems' firewall capabilities allowing multi-gigabit speed performance for inline network deployment.

### Intrusion Detection and Prevention



Provides alerts based on a customizable database of more than 1,300+ known attack signatures. FortiGate stops attacks that evade conventional host-based antivirus systems, with real-time response to fast spreading threats. Fortinet's worldwide antivirus and IDP staff "follows the sun" and offers customer base real-time virus and attack signatures. Using global

FortiProtect update, FortiOS stops the most damaging attacks at the network perimeter regardless of whether the network is wired, wireless, partner extranet or branch office network connection. FortiASIC also supports behavior-based learning and heuristics adding valuable recognition capabilities beyond simply matching content against known signatures.

### VPN



Industry standard IPSec, PPTP, and L2TP-based VPN support provides secure communication tunnels between networks and clients. Fortinet's ASIC-accelerated VPN capabilities allow enterprises to use the Internet as the public infrastructure and a variety of specialized protocols to support private communications through the Internet. FortiClient VPN authenticate users, encrypt data, and otherwise

manage sessions. Unlike host-based VPN servers, FortiGate VPNs offer gigabit server-to-server connection with no latency to easily extend the intranet or extranet across multiple networks. FortiGate system VPNs lower network connectivity costs compared to alternatives like traditional leased lines or remote access servers.

### Anti-spam

Blacklisting of websites & domains, keyword scanning of emails each configurable on a per user basis and the ability to leverage a dynamic scoring system using a number of criteria. Pending Blacklist and Whitelist support in the FortiOS classifies domains support, IP addresses, and email addresses that can be blocked or added to the whitelist — maintained and updated on a per user basis or on a corporate basis along with additional pending Fortinet updates services. Additional Fortinet technology under development includes Bayesian Algorithms

that can be personalized to each user and adapt automatically to changes in spam. Bayesian analysis compares words or phrases in the email in question to the frequency of the same words or phrases in the intended recipient's previous emails (both legitimate and spam). Content filtering synergies with the FortiGuard URL filtering network facilitates fingerprinting techniques looking specifically at the URLs contained in a message and compare them against URLs previously identified as spam propagators.

### Traffic Shaping

Fortinet's traffic shaping helps user control network traffic in order to optimize or guarantee performance, low-latency, and/or bandwidth. The FortiOS firmware offers packet classification, queue disciplines, enforcing policies, congestion management, quality of service (QoS), and fairness. Since network bandwidth

is a limited resource, traffic shaping helps businesses prioritize and manage costly network services. Intelligently managed, traffic shaping improves your latency, service availability and bandwidth utilization without any drawback due to lower priority bandwidth intensive multimedia or peer to peer network traffic.

### Web Filtering

Processes all Web content against known malicious URLs to block inappropriate material and malicious scripts from Java Applet, Cookies, Active X scripts entering the network. Fortinet categorizes more than 15 million domains and over billions of web pages to ensure its customers steer clear of malware on the Internet. Fortinet's FortiGuard web filtering works dynamically with FortiGate systems providing automated updates

with any newly categorized content in more than 56 categories. FortiGuard services are also user-customizable to allow corporate network URL additions to prevent access to additional undesirable sites including phishing-target websites. Web content filtering assures improved productivity for enterprise and regulatory compliance for CIPA-compliant educational institutions.

# Unified Threat Management

## Enterprise

Fortinet is the only Unified Threat Management (UTM) vendor to incorporate its own ASIC chip technology to significantly accelerate performance of antivirus and other security functions in order to provide real-time network protection. The company is also a pioneer in internally developing seven (7) important UTM feature sets to match this ASIC — antivirus, VPN, firewall, IDP, content filtering, antispam and traffic shaping. Fortinet has played a key role in pioneering the UTM category with its strategy of ASIC development and integration of integral security features. In 2004, International Data Corporation, a leading market research firm, named Fortinet the leading vendor with 30 percent market share of an expanding global market.

Another enterprise distinction is Fortinet's Complete Content Protection (CCP) that offers a sophisticated approach dynamically updated with Fortinet's global update network for antivirus and IDP signatures called FortiProtect and a URL filtering service called FortiGuard. CCP technology differs from conventional security methods by its ability to reassemble packet level payloads in real-time at gigabit network speeds into application-level objects, such as files and documents. Using CCP technology, the reassembled objects are scanned and analyzed against a dynamically updated list of thousands of wild list viruses and worms. New, zero-day security threats are also halted when clients reconnect to the network with FortiOS istics and behavior-based analysis. CCP is also useful in detecting a variety of threats, including inappropriate Web content, email spam, spyware, and phishing attempts.

## Managed Security Service Providers

Theft of intellectual property, concern over liability from network misuse and regulatory compliance are driving businesses to seek the necessary solutions for protecting their networks. The worldwide damage from network attacks has grown, and is estimated to be \$12 billion. To meet and exceed exacting service provider managed security service needs, FortiGate platforms leverage both the FortiASIC and general purpose processors to ensure optimal application support for one or many UTM security features.

Larger capacity platforms, such as the new ATCA-compliant FortiGate 5000 chassis series offer multi-gigabit throughput for in-demand security services including gateway antivirus, IDP and managed firewall. MSSP small medium enterprise customers deploying competitive products attempting to cobble together UTM solutions from OEM relationships built on traditional server and networking systems have discovered dramatically reduced performance across their networks when compared to Fortinet products. Both MSSPs and their customers also save hundreds to thousands of dollars on per user licensing fees since the FortiGate Antivirus Firewalls offer a more attractive per box licensing strategy.

In all, Fortinet's FortiGate and related hardware/software product suite including FortiManager and FortiLog for best manageability, logging, and reporting provides a unified set of technologies developed from the ground up to provide both network and content security with an eye towards speed and performance.

## Branch Office, Small Office and Home Office

UTM security systems originally gained popularity with small and medium-sized enterprises, but with increased ASIC-accelerated platforms both larger enterprises and service providers are implementing as well. IDC defines UTM security systems as a combination of hardware, software, and networking technologies whose primary function is to perform specific or multiple security functions.

Fortinet UTM security systems are ideally suited to the branch office where IT resources are scarce. These systems consist of hardware with a hardened operating system (OS), a limited applications set, and no user software installation other than possibly complementary client software for host based threat prevention. Security systems may also include other features, such as security management, logging, policy management, quality of service, load balancing, high availability, and reporting bandwidth management.



## Worldwide Update Distribution Network

### FortiProtect and FortiGuard

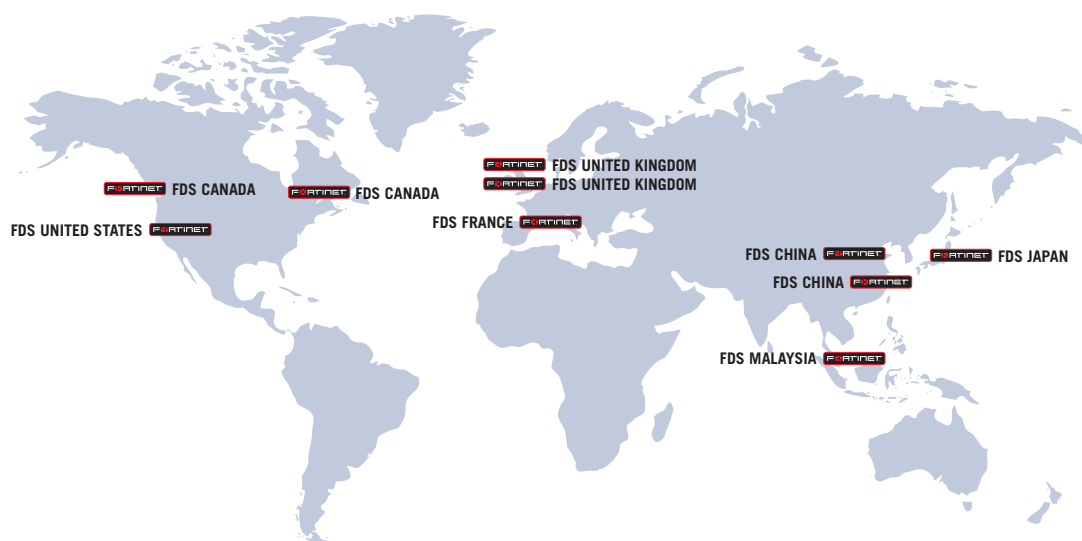
Fortinet's FortiProtect services provide customers with the latest security updates in real-time, 24 x 7, no matter where customers are located around the world. With more than 10 data centers located in secure high availability locations throughout the world, Fortinet security platforms are guaranteed to receive the latest Antivirus, Intrusion Detection & Prevention (IDP), and Anti-Spam signatures and updates as soon as they appear. By allowing customers to select Push, Pull, or customized updates, Fortinet security platforms are constantly updated to provide the highest level of detection for both known and unknown threats. This approach greatly increases the level of defenses against viruses, worms, trojans, spyware, and malicious network attacks at the network perimeter — before threats can enter into the corporate network and cause problems.

FortiGuard offers an automated web URL filtering service that secures customers from unauthorized Internet access. With legal action and government regulations increasing over Internet access, controlling inappropriate or unauthorized Internet activity can address the following issues:

- Lost productivity
- Network congestion
- Need to upgrade Internet link
- Legal liability
- Copyright infringement
- Loss of information
- Negative publicity

FortiGuard simplifies web content management by removing the daunting task of manually controlling access lists for Internet access. By providing more than 56 categories of Internet application types and having one of the world's largest rating databases, customers can setup Internet access policies to allow, block, or monitor Internet traffic to comply with their corporate usage policies in just a few minutes. Like the FortiProtect service, FortiGuard's rating databases are constantly updated with new site ratings. With more than 15 million rated domains and several billion rated URLs, FortiGuard offers superior accuracy and application range to outperform traditional web filtering technologies.

As the new attacks are using more web based content and malicious web sites, the need to automate security defenses is becoming very clear. Solutions that rely on manual updates will not provide the latest defenses against this new breed of fast spreading attacks. Fortinet's FortiProtect and FortiGuard services coupled with a global infrastructure offer the latest security defense signatures and updates 24 x 7 to shield and protect customers.



# Complete Security Solutions

## FortiManager

The FortiManager System is an integrated management and monitoring tool that enables enterprises and service providers to easily manage up to 5,000 FortiGate Antivirus Firewalls. It establishes a central point for monitoring and maintaining security policies across multiple, dispersed FortiGate installations. The FortiManager Server appliance and the Java-based FortiManager Console scales to support multiple system administrators and hundreds of FortiGate units.

### Key Features

- Real-time status and event monitoring speeds identification and response to system outages or attacks
- Powerful Role-based administration enables different administrators to be restricted to specific management domains and specific functions
- Policy Manager enables administrators to create policies and rules to be applied to multiple FortiGate devices or groups automatically
- Scheduled or manual peer back-up capabilities provides FortiManager database redundancy

## FortiLog

The FortiLog family of logging and reporting appliances and the FortiReporter Security Analyzer software package are dedicated solutions that securely aggregate and analyze log data from multiple FortiGate Antivirus Firewalls. The systems provide network administrators with a comprehensive view of network usage and security information, disparately located throughout the enterprise. They minimize the effort required to monitor and maintain acceptable use policies, to identify attack patterns and prosecute attackers, and to comply with governmental regulations regarding privacy and disclosure of security breaches.

### Key Features

- Scalable capacity with logging for up to 100 FortiGate Antivirus Firewalls in a single FortiLog unit
- Network capacity and utilization data enables network administrators to plan and manage networks more effectively
- Supports compliance with HIPAA and other data/customer privacy regulations

## FortiClient

To combat today's latest security threats, defenses must be applied at all different layers of the network. FortiClient offers mobile users, telecommuters, and home offices a solid solution with three security functions — IPSec VPN Client, Personal Firewall, and Antivirus with Spyware detection and blocking. Designed to be extremely easy to use, FortiClient provides the latest security technology without requiring complex user involvement. VPN policies can be centrally managed and pushed out to each client to simplify user setup and connectivity.

### Key Features

- Personal Firewall and Antivirus components provide application monitoring, zoning, and registry monitoring to detect known and unknown threats
- Protects mobile users when they can't be protected by corporate security resources
- High value solution with IPSec VPN

## FortiReporter

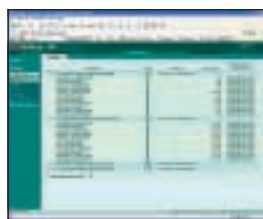
Security managers/administrators and IT administrators need a comprehensive understanding of their Internet and network activities, such as network bandwidth usage, virus and intrusion attack activity, application/protocol usage as well as employee Internet use. FortiReporter Security Analyzer is a cost-effective, HTML browser-based, analysis, reporting and monitoring solution that generates easy-to-understand proactive reports from syslog messages across all FortiGate platforms. FortiReporter's hundreds of easily accessed reports cover virus and worm activity, bandwidth usage, network attacks, Web usage, and protocol usage on any system running Microsoft Windows NT, 2000, XP, or 2003.

### Key Features

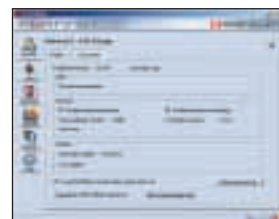
- Analyze and understand virus and worm activity
- Identify attack type and source, analyze event severity and port of attack
- Understand protocol usage by user and department, analyze incoming and outgoing traffic/bandwidth patterns including inappropriate Internet usage by employees
- Understand bandwidth utilization by department, IP address and protocol



 FORTIMANAGER.



 FORTILOG.

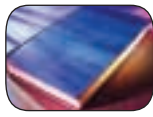


 FORTICLIENT.



 FORTIREPORTER.

## Vertical Market Solutions



### Education

The Internet has increased students' exposure to many valuable and useful sources of information; unfortunately, however, it has also made it easy to access inappropriate or illegal content and to utilize campus networks for non-educational pursuits. Education customers look to Fortinet to reduce inappropriate content and exposure to potential liability; intrusions into academic record and exam data-stores; utilization of campus networks for illegal content sharing; rapid propagation of viruses, worms and other content-based threats. While numerous security products are available today, the cost of procuring and managing multiple, independent systems stretches the budget limitations of most educational institutions.



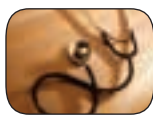
### Financial

Any organization handling consumer financial data have the additional challenge of being compliant with security and privacy regulations imposed by the Gramm-Leach-Bliley Act (GLBA) and UK Basel II Accord. Companies that handle such data — accountants, auto dealers and travel agents — may not be aware that these and other country-specific regulations, previously applicable to traditional financial institutions, apply to them as well. Many financial institutions are turning to Unified Threat Management security products with best in class security applications, including FortiGate Antivirus Firewalls. These ASIC-accelerated systems protect the corporate network at its continually changing perimeter, while identifying and preventing malicious blended security threats coming from both external and internal sources.



### Government

Under the many world government Information Security Management Act, all systems, including records management systems, must be assessed for risk, and certified and accredited. Further, the US E-Government Act requires agencies to develop privacy impact assessments for new or modified IT systems. Fortinet's award-winning line of FortiGate™ Antivirus Firewall products either currently meet or are in the process of obtaining the following certifications: Federal Information Processing Standards (FIPS) 140-2; Common Criteria: EAL 4 for firewall and EAL 4 for antivirus; ICSA: Firewall, VPN (IPSec), antivirus, and intrusion detection.



### Healthcare

Healthcare organizations and their business partners are required to invest in the security systems and processes that ensure the integrity of their patients' private data. Several requirements beyond adequate protection at a reasonable cost need to be addressed, including: Patient records are stored and transmitted in an encrypted form; Healthcare organization's internal IT systems cannot be

easily compromised by network intruders; and IT infrastructure intrusions can be completely logged, reported and acted upon quickly. Fortinet FortiGate Antivirus Firewalls secure private connections to healthcare provider partner firms including medical offices, insurance partners and remote clinics.



### Manufacturing

As global companies increasingly rely on e-business to gain competitive advantage, they are driven to rely on networked supply-chain management and Internet trading communities. Numerous manufacturing firms have large numbers of mobile (laptop) network users who constantly have their systems infected with viruses while traveling, making it difficult to keep virus definitions up to date. As a result, manufacturer's internal systems become infected whenever these users connected to a corporate network. Fortinet helps each remote site support VPN tunnels to the central site, and the content carried via each VPN tunnel is scanned for viruses, worms and other harmful threats.



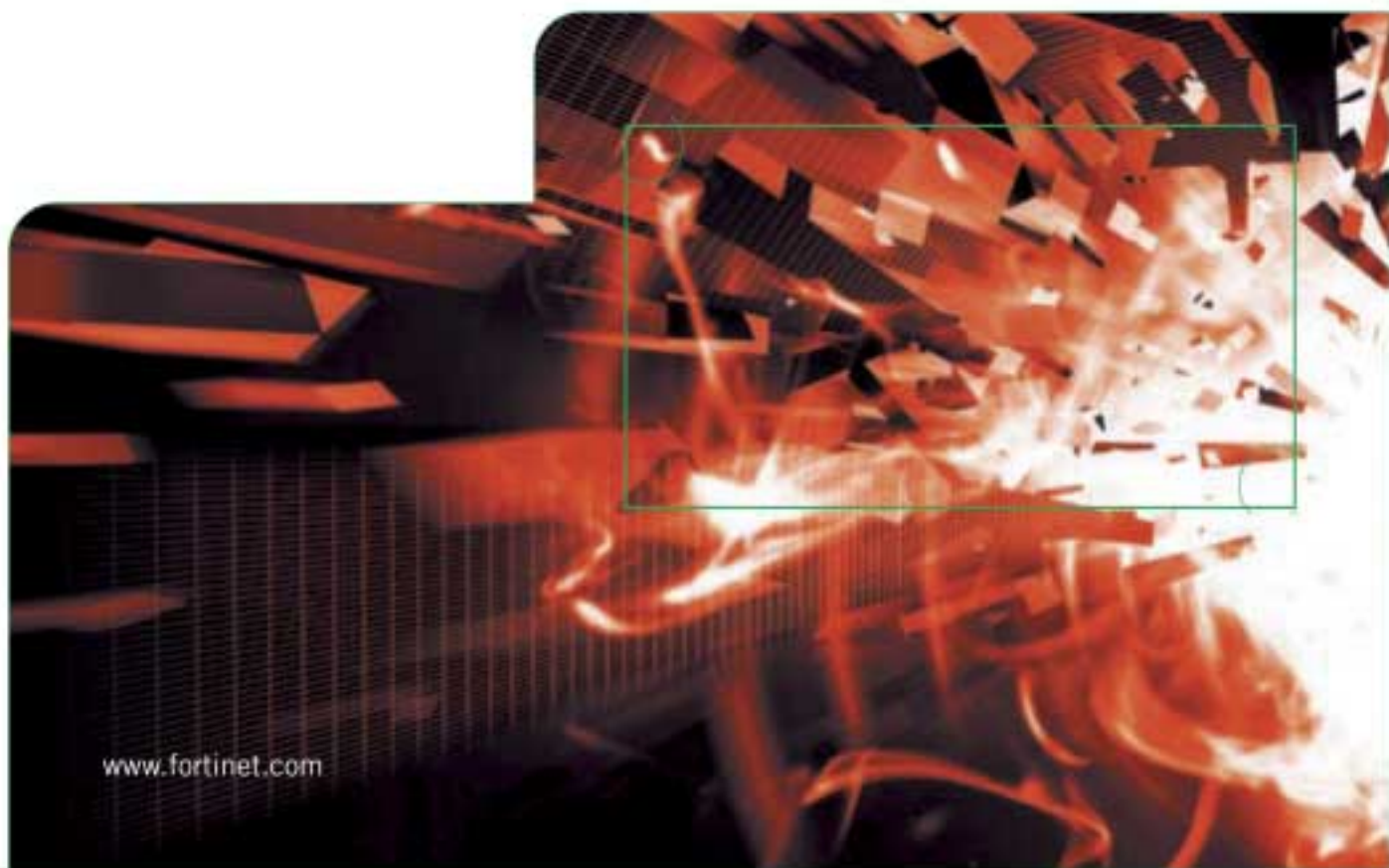
### Wireless

Wireless LANs provide a tremendous amount of freedom and flexibility and support the increasing desire for always-on, always-available connectivity. However, wireless LANs also break down the notion of a definable "network edge," and bring significant new challenges for maintaining network security. The FortiGate platform uniquely protects wireless LANs in the enterprise with strong 802.11 data security 802.1x authentication, and all of the FortiGate antivirus firewall security features. Fortinet's wireless solutions offer unparalleled security defenses for small to medium sized wireless LAN deployments.



### Retail

Retail business operations increasingly rely on the network as the backbone of key operations. The problem in securing retail networks is usually a lack of IT staff, geographic support, and costly downtime on a per minute basis. Retail networks are no longer an option, today's independent stores have increased competition from both their brick-and-mortar competitors and from online services. To remain competitive, retail networks are expanding to multiple store sites with support for self-help kiosks, inventory control and POS (point of sale) applications that network customer financial transaction information. Networked information gathered from wired cash registers, wireless point of purchase displays and other devices needs robust security and protection 24 hours a day/7 days a week.





A GLOBAL NETWORK TO SERVE YOU

**Australia**

Level 17, 201 Miller St  
North Sydney 2060  
Australia  
Tel: +61-2-8923-2555  
Fax: +61-2-8923-2525

**Canada**

Suite 400, 4710 Kingsway  
Burnaby, BC V5H 4M2  
Canada  
Sales: 1-888-825-5996  
Tech Support: +1-866-648-4638  
Tel: +1-604-430-1297  
Fax: +1-604-430-1296

**China**

Cyber Tower, Suite B-903  
2 Zhongguancun South Ave.  
Beijing 100086, China  
Tel: +(8610) 8251-2622  
Fax: +(8610) 8251-2630

**France**

4 Place de la Defense  
92974 Paris La Defense Cedex  
France  
Sales Support: +33-4-9300-8710  
Tech Support: +33-4-9300-8810  
Sales: +33-1-5858-2864  
Fax: +33-1-5858-002

**Germany**

Feringapark  
Feringastrasse 6  
85774 München-Unterföhring  
Germany  
Tel: +49-89-99216-300  
Fax: +49-89-99216-200

**Hong Kong**

Room 3206, 32/F  
Convention Plaza – Office Tower  
1 Harbour Road, WanChai  
Hong Kong  
Tel: +852-3171-3000  
Fax: +852-3171-3008

**Japan**

Kokusai Tameike Building 6F  
2-12-10 Akasaka, Minato-ku  
Tokyo, 107-0052  
Japan  
Tel: +81-3-5549-1640  
Fax: +81-3-5549-1641

**Korea**

27th fl. Korea World Trade Center  
159 Samsung-Dong, Kangnam-Ku  
Seoul 135-729, Korea  
Tel: +82-2-6007-2007  
Fax: +82-2-6007-2703

**Taiwan**

18F-1, 460 SEC.4  
Xin-Yi Road  
Taipei, Taiwan, R.O.C.  
Tel: +886-2-8786-0966  
Fax: +886-2-8786-0968

**United Kingdom**

Fortinet (UK) Ltd.  
1 Farnham Road  
Guildford, Surrey GU2 4RG  
United Kingdom  
Tel: +44-(0)-1483-549061  
Fax: +44-(0)-1483-549165

**United States**

920 Stewart Drive  
Sunnyvale, CA 94085  
USA  
Sales: +1-866-868-3678  
Tech Support: +1-866-648-4638  
Tel: +1-408-235-7700  
Fax: +1-408-235-7737

Your Local Contact

[WWW.FORTINET.COM](http://WWW.FORTINET.COM)

© 2005 Fortinet, Inc. All rights reserved. Fortinet, FortiGate, FortiOS, FortiASIC, FortiLog, FortiVoIP, APSecure, FortiResponse, FortiManager, FortiWiFi, FortiProtect, FortiGuard, FortiClient, and FortiReporter are registered trademarks of Fortinet Corporation in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners. BRO1010412