

## VENDOR NEEDS AND STRATEGIES

### Fortinet: Builder and Leader of the Unified Threat Management Security Appliance Market

Sally Hudson

Charles J. Kolodgy

#### IDC OPINION

Complexity is becoming the name of the game for corporate IT organizations. The networks they manage are becoming increasingly complex with higher transmission speeds, more communication protocols, and more users — both inside and outside the firewall. All of that is hard enough, but additionally there are more content-based, network-borne threats. The number of vulnerabilities and those who try to exploit them are on the upswing. To address this complexity, enterprises are turning to security appliances. These devices, which are easy to deploy and manage, offer an island of simplicity while providing high levels of security protection. The most recent development in the security appliance market is the new unified threat management (UTM) security appliance. Devices in this category combine various security technologies, firewall, virtual private networks (VPNs), intrusion detection and prevention (IDP), and gateway antivirus. Regarding security appliances and UTMs in general, IDC believes that:

- ☒ By 2007, 80% of all security solutions will be delivered via a dedicated appliance.
- ☒ UTM appliances provide enterprise, small and medium-sized business, and even service provider customers with considerable deployment flexibility, while at the same time offering a standard management platform. All of the functions of a UTM can be utilized, or the product can be used for a specialized purpose.
- ☒ UTM security appliances originally gained popularity with small and medium-sized enterprises, but with increased ASIC-accelerated platforms, both larger enterprises and service providers are implementing these systems. All of these segments continue to be targeted by conventional security vendors, network equipment providers, and newer security systems like Fortinet because of the large number of potential customers.
- ☒ The security appliance market, including the UTM market, will be extremely competitive. The keys to success in the security appliance market will be product differentiation through improved performance and features.
- ☒ A leading pioneer of the UTM security appliance market is Fortinet Inc. It was one of the first companies to organically develop and combine all of the solutions available in the UTM appliance, and it is the only vendor incorporating dedicated ASICs for real-time antivirus and IDP processing.



## IN THIS STUDY

This IDC study profiles Fortinet Inc., a privately held company participating in the security appliance market and leading the universal threat management market space. Fortinet's FortiGate Antivirus Firewall products consist of a tightly integrated set of security technologies that provide both network and content security with an eye toward speed and performance.

## SITUATION OVERVIEW

Fortinet Inc., headquartered in Sunnyvale, California, is a privately held company founded in 2000. To date, Fortinet has more than 525 employees located in the Americas, Asia, and EMEA. The Fortinet FortiGate Antivirus Firewall systems, FortiClient software, FortiLog systems, and companion products are designed to provide multifaceted security for IT organizations requiring robust security and high performance. Larger enterprises and service providers often leverage Fortinet products for ISCA-certified capabilities, including gateway antivirus, firewall, IDP, and IPSec VPN. These capabilities often complement existing enterprise installation of security products from firewall, VPN, or IDP vendors. Smaller enterprises and home office users use the product set for a comprehensive UTM platform.

---

### **Security Appliances and Unified Threat Management**

IDC defines security appliances as special-purpose devices composed of a combination of hardware, software, and networking technologies whose primary function is to perform specific or multiple security functions. The security appliance consists of hardware with a hardened operating system (OS), a limited applications set, and no user software installation, other than possibly complementary client software for dynamic threat prevention. Security appliances may also include other features, such as security management, logging, policy management, quality of service, load balancing, high availability, and reporting bandwidth management. However, these features are designed only to support the primary security workload.

Fortinet participates in the unified threat management security appliance segment of the above market. IDC defines the UTM market as follows: UTM security appliance products include multiple security features integrated into one box. To be included in this category, as opposed to other segments, the appliance *must* be able to perform network firewalling, network intrusion detection and prevention, and gateway antivirus. All of the capabilities in the appliance need not be utilized concurrently, but the functions must exist inherently in the appliance.

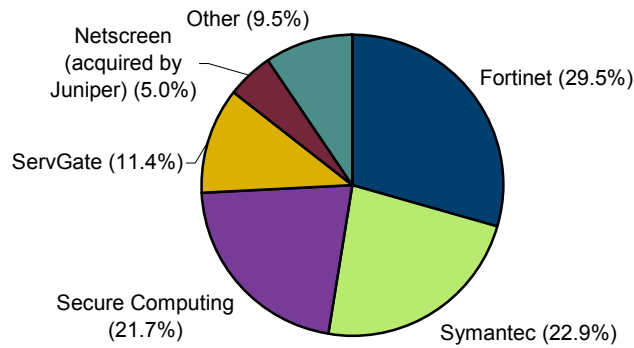
#### ***The Fortinet Approach***

Fortinet's FortiGate antivirus firewall systems and associated product line meets the above criteria and provides both integrated network and content security in an environment guaranteed not to degrade network application performance. The latter claim is based on the vendor's product differentiator in this market: Fortinet is the only

UTM player to incorporate its own ASIC chip technology to significantly accelerate performance of antivirus and other security functions to provide real-time antivirus protection. The company has also internally developed seven 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 integration of integral security features. In 2003, Fortinet was the leading vendor with 30% share of an exploding market (see Figure 1). Market leadership has continued into 2004. According to IDC's Security Appliance Quarterly Tracker, Fortinet has maintained its market leadership with nearly 23% share (see Figure 2).

**FIGURE 1**

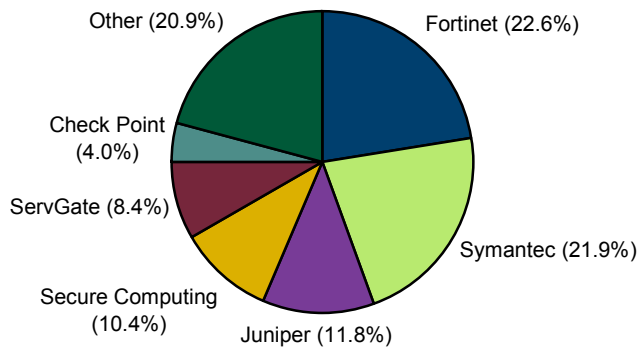
Worldwide Unified Threat Management Appliance Revenue Share by Vendor, 2003



Source: IDC, 2004

**FIGURE 2**

Worldwide Unified Threat Management Appliance Revenue Share by Vendor, 1H04



Source: IDC, 2004

Fortinet offers customers a complete set of network security features accelerated by its FortiASIC. Fortinet refers to its offering as "Complete Content Protection (CCP)," as it offers real-time protection of network-borne threats up and down the OSI network stack. This approach goes beyond both the standard firewall inspection technologies — stateful inspection (which examines data packet headers) and deep packet inspection (a second-generation alternative to stateful packet inspection that offers additional inspection).

CCP offers a more sophisticated approach that is dynamically updated with Fortinet's global update network for antivirus and IDP signatures, called FortiProtect, and URL filtering update network, called FortiGuard. What differentiates the CCP technology from the other methods is 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 with FortiOS heuristics and behavior-based analysis. CCP is also useful in detecting a variety of threats, including inappropriate Web content, email spam, spyware, and phishing attempts.

CCP is, of course, more processor and DRAM memory intensive. The technology can require from 100–1,000 times more processing per packet than either stateful or deep packet inspections. To meet and exceed these needs, FortiGate platforms leverage both the FortiASIC and a general-purpose processor to ensure optimal application support for one or many UTM security features. Larger-capacity platforms, such as the new FortiGate 5000 chassis series, use larger amounts of DRAM for security in larger enterprises and service providers than the smaller FortiGate systems for small office users. IT users deploying competitive products attempting to cobble together CCP solutions from OEM relationships built on traditional server and networking systems have discovered dramatically reduced performance across their networks.

#### **FortiGate Appliances: FortiASIC and FortiOS**

To circumvent this problem, Fortinet developed its own hardware and software architecture specifically for a CCP environment. FortiGate appliances are based on an integrated hardware and software architecture specifically designed to accommodate high-performance, application-level content processing placed directly in line within the network's core or perimeter to provide real-time security functions. Fortinet believes that its technology is the only platform currently on the market that can deliver application-layer services (e.g., virus detection and content filtering) at real-time multigigabit/second data rates.

A key component of the more than 15 different FortiGate products is the FortiASIC chip. This proprietary chip incorporates a hardware scanning engine, hardware encryption, and real-time content analysis processing capabilities. The FortiASIC chip provides acceleration for firewall, encryption/decryption, signature and heuristic packet scanning, and traffic shaping via counting packets and measuring flows.

Further, the vendor has developed a custom operating system, FortiOS, that offers high performance for firewall and content security inspection capabilities within a single platform. The product is designed to constantly thwart new and existing

blended attacks by combining antivirus, antispam, VPN, firewall, and intrusion prevention and intrusion detection capabilities with a unique combination of software, ASIC, and dynamic updates.

### **FortiProtect Infrastructure Services**

Fortinet provides its customers with an array of support services, including:

- ☒ FortiProtect Center, available at the company's Web site and via daily HTML push email, is a real-time information portal with information about viruses, worms, and other current network threats. Automatic updates to FortiOS are designed to reach all FortiGate units worldwide in less than five minutes.
- ☒ FortiProtect Threat Response Teams are comprised of worldwide expert network security specialists that collect and analyze virus samples and develop virus signatures to update the current list of Fortinet antivirus definitions. The team also develops network vulnerability signatures and updates Fortinet's network intrusion and spyware or Grayware detection systems.
- ☒ FortiProtect Distribution Network, working in conjunction with the worldwide Threat Response Team, provides automated, timely updates regardless of time zone or geography for the FortiGate products.

In all, Fortinet's FortiGate and its related hardware/software product suite provide a unified set of technologies developed from the ground up to provide both network and content security with an eye toward speed and performance. From best-in-class usage for the enterprise or service provider to comprehensive solutions for small businesses, Fortinet offers a UTM benchmark for IT security users.

## **FUTURE OUTLOOK**

Use of Internet technology is a given for businesses today. Another given is that technology is also abused by hackers, criminals, and other miscreants. The threats to enterprises and service providers of all sizes continue to grow and become more complex. Although many security technologies have been deployed to protect these environments, hackers have increasingly focused on blended threats, a combination of malicious code keyed to exploit specific vulnerabilities. These blended attacks are specifically designed to circumvent point security mechanisms such as independent VPN, firewall, and antivirus products.

The blended threats work against point solutions, but they have a high probability of failure when the security solutions are unified. IDC believes that the development and deployment of the UTM security appliances provides flexible best practices security solutions for the future. IDC is forecasting a meteoric rise for the UTM market, at the expense of existing point firewall/VPN security appliances. The contrasting growth forecasts for UTM and firewall/VPN security appliances are presented in Table 1. By the end of the forecast period, IDC expects the UTM segment to be larger than the established firewall/VPN market segment.

**TABLE 1**

## 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

Note: For key forecast assumptions, see *Worldwide Threat Management Security Appliances 2004–2008 Forecast Update and 2003 Vendor Shares: The Rise of the Unified Threat Management Security Appliance* (IDC #31840, September 2004) and *Worldwide Firewall/VPN Software 2004–2008 Forecast Update and 2003 Vendor Shares: Desktop Firewalls on the Move* (IDC #31839, September 2004).

Source: IDC, 2004

The rise of UTM to segment leadership in five years is predicated on the following factors:

- ☒ UTM appliances like Fortinet's FortiGate antivirus firewalls will be able to provide performance greater than or at least equal to that of single application appliances in enterprise, service provider, or small and medium-sized business settings.
- ☒ UTM appliances provide customers with considerable flexibility to customize their security approach. All of the functions of a UTM can be utilized, or the product can be used for a best-in-class specialized purpose.
- ☒ UTM appliances will have comprehensive management, reporting, and logging platforms that enable the management of all security features, including signature updates and reporting.
- ☒ UTM security appliances have previously been a staple security product for small and medium-sized enterprises, but now offer an attractive high-performance addition to existing enterprise and service provider point security systems. There is considerable growth potential from these markets.

IDC believes that the keys to success for UTM security appliance vendors will be product differentiation through improved performance, pricing, and feature sets. Vendors need to stand out in the marketplace by improving on leading supplier benchmarks. This can be done in a number of ways: price, performance, the mix of security functions incorporated in the device, improved manageability, security knowledge services, or security certification. Interestingly, Fortinet has been emphasizing all of these differentiation strategies. One prime example is Fortinet's antivirus and IDP per-box pricing strategy, as opposed to other vendors who require per-user licenses. This differentiation alone can lead to savings for larger enterprises and service providers choosing FortiGate systems.

## ESSENTIAL GUIDANCE

The new UTM security appliance market, which incorporates all 15-plus FortiGate systems appliances, is becoming a very competitive market. In 2003, there were seven vendors that could be identified as selling UTM products. By the end of 2004, there should be at least 16 vendors. The vendors include those best known for network security, others that are leading antivirus vendors, and a number of small appliance vendors in Europe and Asia.

Fortinet has been a pioneer in the development of the UTM segment. It was the first company to offer all of the solutions available in the UTM appliance. IDC believes that Fortinet's market leadership is the result of it being the only vendor that incorporates dedicated ASICs for the antivirus processing, along with its wide range of products that can meet the needs of any potential customer. The vendor's product set ranges from the SOHO FortiGate 50A to the multigigabit carrier-class FortiGate 5000 series and all points in between for enterprise customers.

For IT customers requiring fast, reliable, and very comprehensive security appliance technology, Fortinet should be on the short list of vendors to consider.

## LEARN MORE

---

### Related Research

- ☒ *Worldwide Threat Management Security Appliances 2004–2008 Forecast Update and 2003 Vendor Shares: The Rise of the Unified Threat Management Security Appliance* (IDC #31840, September 2004)
- ☒ *Worldwide Firewall/VPN Software 2004–2008 Forecast Update and 2003 Vendor Shares: Desktop Firewalls on the Move* (IDC #31839, September 2004)
- ☒ *Worldwide Secure Content Management 2004–2008 Forecast Update and 2003 Vendor Shares: A Holistic View of Antivirus, Web Filtering, and Messaging Security* (IDC #31598, August 2004)
- ☒ *IDC's Software Taxonomy, 2004* (IDC #30838, February 2004)
- ☒ *IDC's Enterprise Security Survey, 2003* (IDC #30653, December 2003)

---

## **Copyright Notice**

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, telebriefings, and conferences. Visit [www.idc.com](http://www.idc.com) to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit [www.idc.com/offices](http://www.idc.com/offices). Please contact the IDC Hotline at 800.343.4952, ext. 7988 (or +1.508.988.7988) or [sales@idc.com](mailto:sales@idc.com) for information on applying the price of this document toward the purchase of an IDC service or for information on additional copies or Web rights.

Copyright 2004 IDC. Reproduction is forbidden unless authorized. All rights reserved.

---

**Published Under Services:** Security Products; Firewalls and Security Appliances