



Graphic: Deep Pahwa

Given the rapid rise in blended threats as businesses go online, Unified Threat Management systems (UTM), which perform network firewalling, intrusion detection and prevention, are gaining importance across big and small enterprises alike. Like most other IT products, it is gaining ground in SME and SOHO segments and is no longer just another corporate acquisition.

UTM Integrated Security

As enterprises become increasingly dependent on the Internet, there is a growing trend among firms to open their network infrastructures to key stakeholders, including customers, employees, partners and suppliers. As open access of their network resources is granted, it is only natural that cyber threats grow exponentially.

Whether these threats originate from inside or outside the organization, enterprises are increasingly forced to deal with a variety of potentially devastating attacks and vulnerabilities such as viruses, malicious code, Web defacement, insider abuse and theft of intellectual property. The biggest danger to businesses today comes from the proliferation and growing sophistication of traditional threats such as trojans, viruses and worms.

Inconspicuous attacks

Another emerging threat is targeted attacks. These are cus-

tomized attack vectors developed by organized criminal gangs. They target specific companies to extract confidential or classified information and are more difficult to detect and repel.

Previously, most threats could be countered by detecting their signatures, but now signatures are becoming increasingly difficult to define. This is because they combine attack methods and signatures from different categories such as viruses that are delivered by worms, or spoofed websites containing malicious code.

Today's threats affect all businesses equally, because the worms, viruses and trojans do not discriminate how big or successful a company is before deciding whether or not to infect the systems. Many threats have an ulterior financial motivation as well.

The bigger the target, the larger the reward and the more likely it will be under attack.

Since launching these attacks is inexpensive, any financial reward seems significant enough to motivate.

This means that as businesses go online, the Internet itself becomes an increasingly complex threat vector for hackers, malicious applications and vulnerability exploits. Virus and worm outbreaks, explosive growth in phishing, spyware and keyloggers attack through the Internet is quickly moving up the priority list of corporate information security.

Tackling threats

To combat the growing number of attacks to information security, companies continue to invest heavily in security hardware and software solutions to minimize business risk. Yet, many of these solutions are implemented to address an immediate challenge. For instance a firewall deployment can allow access for legitimate or trusted traffic while

keeping illegitimate or distrusted traffic out.

As various security solutions are deployed, the resulting enterprise network topology becomes a complex, multi-vendor, multi-product environment that is difficult to consistently manage and maintain because it requires proper diligence and care. For most enterprises it is a daunting challenge to keep pace with both new and existing vulnerabilities, frequent technology platform software and hardware changes and security policy changes that impact every function of e-business operations on a day-to-day basis.

Significant capital investments in management technologies, facilities and skilled personnel are required to properly and proactively secure a company's network infrastructure. Therefore many enterprises are turning to third-party providers of managed security services to address these real-world business needs and requirements.

"Enterprises want to maximize their return of investment with regard to their security resources while simultaneously reducing the total cost of ownership for their security infrastructure systems," says Ajit Pillai, Country

Manager, India & SAARC, Watchguard Technologies. "The challenge remains for companies to efficiently manage distributed secure Internetworks. A multitude of security products are integrated over heterogeneous platforms and require frequent upgrades, periodic testing, and reconfigurations as newly identified vulnerabilities arise," he adds.

For survival in a post 9/11 economy, companies are learning to keep pace with changing security technologies and best practices to combat the escalation of threats and vulnerabilities confronting the enterprise. "The industry is moving towards delivering security solutions through multi-functional devices rather than using a firewall plus separate appliances to protect against specific threats such as anti-virus or content filtering," says Antony Chapman, Senior Director, (APAC/MEA), SonicWall.

"There is a movement in the industry towards delivering Unified Threat Management, which is a dynamically updated gateway anti-virus, anti-spyware and intrusion prevention services. This is the only true method of keeping network security protected against new threats as they emerge," he adds.

APPLIANCE MARKET GROWTH

SECURITY MARKET (\$ Millions)	2001	2002	2003	2004	2005	2006	CAGR
Security Hardware	2,937	3,600	4,679	6,009	7,488	8,900	25%
Security Services	8,025	9,727	11,969	4,915	18,649	23,216	24%
Totals for all security spending	16,929	20,310	24,767	30,314	36,950	44,527	21%

Source: IDC & BAS estimates

What, why, where

UTM refers to the aggregation of essential security services into a single hardware platform, i.e. network security appliance. UTM systems help provide comprehensive security services.

According to an IDC classification, UTM security appliances include multiple security features integrated into one box. These appliances are able to perform network firewalling, network intrusion detection and prevention, and gateway anti-virus.

Industry analysts note that the rapid rise in blended threats has greatly contributed to a need for the flexible, highly integrated functionality that UTM delivers. Since UTM is easy to install, use and manage and helps aggregate security functions, network administrators only have to learn one interface instead of a dozen different software packages. This means that even small teams or a single individual can install, manage and maintain a range of security functions.

A single interface also means that the learning curve becomes gentler and administrators can be more productive in a shorter span of time. Deploying UTM devices at choke points makes the maintenance of individual PCs and servers less critical because of the additional filtering done by the UTM appliances.

"UTM is an industry response to customer demand for manageable security solution with unified interface and methodology. In the long run, this should result in a new generation of security solutions which design from ground up to do just that instead of merging and fixing existing solutions," believes Surendra Singh, Head South East Asia and India, Websense.

Implementing UTM devices often appears to be less challenging than installing software. This is because administrators do not need to wrestle with the complexities of operating systems, such as tuning the kernel parameters, or ensuring that certain patch levels of software are installed for the OS.

Implementing UTM devices is typically just connecting it to a network and launching a browser to begin configuration.

"UTM will become the future of network security, because the benefits of an easily managed product providing essential security services will become obvious to many IT managers and network administrators before long," feels Vishak Raman, Country Manger, Fortinet.

International perspective

A few months ago, security vendor Secure Computing Corporation announced the results of an independent survey documenting the attitudes of enterprise IT managers toward UTM security appliances. Titled 'Unified Threat Management Appliances: Ready to Take Off?', the study was conducted by TheInfoPro, Inc and surveyed 102 enterprise IT managers across a broad variety of industries in April 2005.

The survey found that almost 50% of interviewees indicated 'more' or 'much more' interest in multi-function security appliances compared to 12 months previously. More than 60% were seriously considering using a security appliance for multiple security functions while another 10% already did or planned to in the next 12 months.

The UTM market is expected to boom over the next few years, according to research firm IDC. In 2003, the total sales in this category were \$105 million, but that is expected to grow to \$3.5 billion by 2008.

According to the study, IT managers said that they want best-of-breed security functions from multiple vendors on a single platform. A majority of interviewees (55%) indicated a preference that functions on a single security appliance are from more than one vendor; another 14% were neutral.



"Enterprises want to maximize their return of investment with regard to their security resources while simultaneously reducing the total cost of ownership for their security infrastructure systems"

AJIT PILLAI
Country Manager, India & SAARC, Watchguard Technologies

challenge is to find the right UTM solution that excels in every aspect while maintaining the highest level of availability," says Surendra Singh of Websense.

"The adaptability and scalability of these systems varies from product to product. UTM solutions would ideally appeal to businesses, which have limited resources and expertise in security threat management and help reduce the resources and expertise in support, managing and deploying such solution," he adds. With SOHOs and smaller businesses becoming increasingly aware of the need for integrated security solutions, vendors need to provide solutions that are comprehensive and cost-effective. Many Indian enterprises prefer a single vendor providing comprehensive solutions, rather than multiple vendors providing point solutions.

The performance of the UTM, add-on services available, effectiveness of the services bundled and the value for money is very critical for customers to buy these solutions. Vendors and their partners need to provide their SMB customers, UTM solutions that ensure a low cost of ownership and

low cost of license renewals. It should have a single point management and lower administrative overheads so that there is no requirement of multiple specialists to handle multiple products.

Making demo units available, providing the required market

"UTM is a dynamically updated gateway anti-virus, anti-spyware and intrusion prevention services. This is the only true method of keeping network security protected against new threats as they emerge"

ANTONY CHAPMAN
Senior Director, (APAC/MEA), SonicWall



"UTM will become the future of network security, because the benefits of an easily managed product providing essential security services will become obvious to many IT managers and network administrators before long"

VISHAK RAMAN
Country Manger, Fortinet

Estimated at \$30 million in 2004 (Security Appliance Market Total), the revenue is likely to grow at an excess of 50%, because UTM is getting across quickly to the users," says Vishak.

With security appearing to be the only IT spending that has been rising year after year, despite the economic trend, the market opportunities are growing bigger. "India is a big market with a comparatively large population of highly educated and technically aware computer users. As such, it is a market with huge potential. More Internet security innovation would be coming directly from India as the market grows," feels Antony.

"Earlier, security and storage were treated as two different streams. Both were trying to garner the market place separately. The merger of Symantec and Veritas has shown that secure computing and more storage is the way going forward. More such consolidations are likely in the future," believes Ajit.

In essence therefore, the continued growth of the international IT outsourcing market in India, including software development and call centers will make it imperative for all Indian businesses to maintain the same robust network security as their counterparts in other parts of the globe. UTM solutions will be preferred over solutions in isolation and integrated appliances. They include all the aspects of security, all the parameters of security like Firewall VPN, Gateway Anti-virus, Intrusion Prevention System (IPS), Span prevention and URL filtering bundled into one, will be most sought after.

SUBBALAKSHMI BM
(subbalakshmi@cybermedia.co.in)

SOME STATISTICS

- 90% of companies use anti-virus software; 78% of them were hit by viruses, worms etc - 2004 CSII/FBI Computer Crime and Security Survey
- A survey of three million corporate computers found 82 million instances of spyware - Gartner Group, September 2004
- 70% of employees admit to viewing or sending adult-oriented personal e-mail at work - NFO Worldwide
- Up to 40% of Internet use in the work place is not business related - International Data Corp
- 60% of IT managers considering security appliances prefer UTM vendors who offer best of breed on a single appliance
- More than 60% of the surveyed companies were seriously considering using a security appliance for multiple security functions; another 10% already do or plan to in the next 12 months
- In 2003, the total sales in UTM category were \$105 million, but that is expected to grow to \$3.5 billion by 2008

Source: 'Unified Threat Management Appliances: Ready to Take Off?', a survey by TheInfoPro, Inc

Challenges of implementation

Not all customers find it easy to manage multiple isolated security products. Sometimes this would mean more than just a management headache given the security gaps in-between. "The