SUPPLEMENT

UTM - An Evolution or Revolution

October 7, 2008 - NLB Singapore

It's no secret that security threats are on the rise. Everywhere you look; there are reports on new breaches, hacking/phishing attacks, spam, malware, Trojans, botnet attacks and more. Security threats to SMBs (small & medium enterprises) are just as real as they are to enterprise organizations. Unfortunately, the tragedy is that many SMBs are simply unaware of Unified Threat Management (UTM) and how it can combat these threats. After all, secure networks afford businesses the freedom to be productive and operate efficiently.

So what exactly is UTM? Originally coined by IDC, UTM refers to comprehensive network infrastructure devices in which multiple security technologies - often firewall, intrusion prevention, antivirus and spyware - are combined into a single appliance. Because these devices provide a single, integrated interface, UTM aims to simplify network security management. Most UTM devices are firewalls or IPS devices at the core, with other technologies available as optional components or modules. However, did you know that conversely, nearly all modern firewalls have UTM capabilities?

While UTM was initially targeted at SMBs, vendors have been trying to move the technology upstream to larger organizations. But just how successful has this strategy been so far? Do you know what UTM means and does for your company? UTM is definitely an up-and-coming trend in the network security world.

MediaBUZZ Pte Ltd's Half-Day Forum – UTM: An Evolution or Revolution? – explored this technology in detail to find out more about it - its current trends and challenges, and what these mean for both users and vendors' alike. Read all about the findings and core discussion points in the exclusive event supplement.

CONTENTS

The Many Threats of Network Security

During his presentation at MediaBUZZ's UTM event, Corey Nachreiner, senior network analyst, WatchGuard Technologies took us through the various attacks network security face, how Internet threats have changed since 2003 and just why these threats are more dastardly than we think or even know.

Photo: Corey Nachreiner

Nachreiner put the threat landscape humorously and succinctly in an anecdote: We've all been told, "Oooo, if you use the Internet, a malicious hacker might get you." Right? This kind of talk promotes a mental picture like this: Here's the Internet. Here are a bunch of us innocent folks, using the Internet. Here's you, just another Internet user. Some bad guy pops up. He wants some of your money. So he sends you a scam email: "I'm a poor crippled widow in Nigeria who happens to have a gazillion dollars, and I'll give you half of it if you'll just help me get it to the United States. But first I need you to pay some legal fees on my behalf." Ever gotten an email like that? He sends the email. You receive it. You delete it. The bad guy twirls his handlebar mustaches and says, "Curses! Foiled again!" Then he sends you a virus. Your antivirus stops it."

While Nachreiner trivialized the above for humor's sake, this is exactly what the threat to computer users was in 1998.

A lot of us still carry that mental picture today but the fact is, it is ten years later. Some may ask if the Internet has changed much in ten years. Well, YouTube, Skype and social networks were unseen ten years ago.

In 2003, security professionals noticed a change in the quality and purpose of malicious software, which is called "malware" for short. It soon became apparent that organized crime had moved onto the Internet, essentially changing the face of Internet threats and security forever.
While once upon a time, all we had to worry about was computer viruses' worms and maybe some spam or a server attack or two, nowadays, there is a wide range of malicious code directed at us.

For instance:

- Drive-by downloads lie in wait on web sites so that as soon as we browse there, an attacker's code gets pushed onto our computer.
- Phishing and pharming are deception techniques designed to trick us into giving up sensitive information by convincing us that we are dealing with a legitimate site, when it's really a look-alike under the attacker's control.
- SQL injection is an attack on our web applications that allow attackers to gain control of our website's underlying database, and any sensitive data it may contain

What the above shows, is that today's Internet attacks and threats are very diverse, and this is not going to change for the better but instead probably worsen.
Attack code is big business today, and as a result, attackers want to get onto any computer they can. Another anecdote by Nachreiner: Suppose you're an attacker and you know of a security hole in Internet Explorer. Here's what you do. You create malicious web code that can tell if someone visiting a web site runs Internet Explorer.

You sneak your malicious web code on as many legitimate sites as possible, using various techniques. When victims visit the site, your malicious code exploits the security hole in Internet Explorer to gain access to their computers. Did you target a specific person? No. Did you target a company? No. You targeted the vulnerability itself. Once you get your code on a mass of computers, then you can figure out what is on each of them. The point is, it doesn't matter if you're a small company, or that you mean no harm.
Attackers will still come after you if you have vulnerabilities on your network. It's not personal.

Many of today's attacks are automated mass attacks. Attack code wanders all over the Internet looking for victim machines. By comparison, it has become relatively rare for an attacker manually send an individual attack to against a specific computer or company network.

What's happening nowadays in the network security world is that there are structured teams going after innocent computers now, and they are focused on efficiency. Setting aside rare and exceptional cases, there is almost no such thing as you defending yourself against "a single hacker." We are now up against roving armies of well-coded attackers, financed with big money, organized by a highly motivated and skilled team, who will rob us if possible while barely noticing we exist, emphasizes Nachreiner.

He adds that the main driving force of hackers is very straightforward – it's all about money for them. Secondly, hackers/attackers require a lot of computing power and therefore require our computers as resources. "Our computers can help them reach their goals if they have Internet connection, hard drive space so they can stash their files, and

continues on Page 3 - click here

From Page 2 — The Many Threats of Network Security

email (after all why would an attacker spam from his own computer if he can send it from the computers of 20 or 40 or 100 strangers?). This is why attackers are coming after our machines, regardless of who we are.

Some of today's attack trends include:

Application Vulnerabilities

Attackers used to primarily target vulnerabilities in our operating systems and/or servers. However, vendors have fixed many of the most severe OS and server vulnerabilities, and our firewalls do a pretty good job of protecting our perimeter from external attacks. So lately, attackers have been forced to change their focus, and instead exploit vulnerabilities in client applications, like our web browser, media player, or chat client. These attacks come from the inside-out rather than the outside-in, and they target the weakest security link - users.

Web-based attacks

In general, web-based attacks have become more prominent than email-based attacks. Even the least savvy users have figured out that they should avoid email attachments, so the criminals have moved on to greener fields …. the web.

Blitzkrieg attacks

Attackers rarely target single victims anymore as it's too inefficient and unprofitable. Instead attackers try to automate their attacks on a massive scale.

The advent and rise of botnets

Botnets allow attackers to blend many types of malware into one convenient package. Almost every large scale hacking campaign in the past few years has had a botnet behind it.

New technologies

Finally, attackers are quick to leverage trendy new technologies. For instance, they are already attacking VoIP, IM, P2P, Web 2.0, and many mobile technologies. Since attackers quickly adopt these new technologies, they sometimes figure out ways to attack us that we never dream of let alone anticipate.

Types of Attacks include:

Drive by Downloads

Before 2003, we had to be careful when checking our email, but we could surf the web with indiscretion. This is no longer the case. Now we have to remain wary of malicious web sites that silently force malware onto our computers, called drive-by downloads (DbD).

Sometimes the web sites serving these drive-by downloads are operated by attackers. However, lately attackers have even started hijacking **legitimate** sites, and booby-trapped them with malicious code. So, perfectly normal websites that we visit often, could one day get hijacked and force a backdoor onto our computers.

In fact, Nachreiner says that web-based attacks like drive-by downloads have overtaken old fashioned email viruses. The statistics, he quotes are frightening. For instance, this year alone, over a million legitimate web sites were hijacked by massive automated attacks, and then forced to serve drive-by downloads. In these specific attacks, sites belonging to trusted entities such as Businessweek, Computer Associates, the Miami Dolphins, and many .edu and .gov sites were all hijacked and loaded with DbDs.

To make matters worse, the hacker underground even sells pre-made web attack kits that make it easy for criminals to launch these drive-by downloads attacks. Some of these web attack kits cost a few hundred to a few thousand dollars on undergrounds forums, others you can find for free. Some examples include kits like, Mpack, icepack, and firepack, which were all made and sold by Russian hackers. They are designed to detect the type of browser a web visitor uses and then exploit the vulnerability that is most likely to work against that browser. Some sellers even offer service and support for their web attack kits, updating them with the latest vulnerabilities.

Reflecting just how bad drive-by downloads have actually become, security firm Sophos finds about 6000 new DbDs links everyday.

Web Application Attacks

Today, we expect websites to deliver dynamic content personalized for us.

To do this, websites have become web applications and have been designed so that we can interact with them in ways we never did before. In the past, websites only displayed information. Now they allow users to post information to them as well. Unfortunately, this new level of interaction between users and a websites has opened up a new class of security vulnerabilities—Web application attacks.

Cross-Site Scripting (XSS)

One example of a web application attack is Cross-Site Scripting. If a web designer doesn't program his web application to interact with users securely, he gives attackers the opportunity to inject scripts into his web code.

For a long time, buffer overflows were the most commonly reported vulnerability, and one could argue, was the most exploited vulnerability on the Internet. This is no longer true. Cross-site scripting flaws have now become the most commonly reported vulnerability. Jeremiah Grossman, from WhiteHat Security, claims XSS vulnerabilities can be found in 70 percent of websites.

Cross-site Scripting allows you to do stuff on a victim's computer with the same privileges of some other trusted website. This means attackers can exploit XSS flaws to read the cookies of other websites (among other things). So if a banking site suffers from a XSS flaw, a phisher can leverage that

continues on Page 4 - click here

From Page 3 — The Many Threats of Network Security

flaw to steal the cookie used for you web session to your banking site. In other words, they could log in to your banking site **AS YOU**, and do whatever they wanted. They'd only have to entice you to click on some specially-crafted link for their attack to succeed.

SQL Injection

Most modern websites also rely on a backend SQL database. For instance, when you login to a site that requires authentication, the web application communicates with a database to check your username and password, and uses that to decide what content you should see. Like before, with XSS, if a web designer doesn't code this SQL interaction securely, an attacker can take advantage of flaws in his code to sneak unexpected SQL queries to your database server. This is called a SQL Injection.

There are many evil things attackers can do with SQL injection. They can steal confidential and private date from your database, such as your customer's credit card info, home address, SSN, etc. They can leverage logic tricks within SQL to bypass authentication mechanisms. They can even add, remove, or modify data in your database. For instance, attackers could leverage SQL injections to change the prices of your products on your ecommerce site.

Botnets

Botnets have been around for years. Most IT people first heard of them in 2000, when several thousand coordinated computers all asked to connect to eBay at the same time. That many requests saturates the phone lines and knocks the victim off the Internet. Thus, it is called a "Denial of Service" attack.

Botnets have evolved and matured over the years and are now ranked by every expert as the number one threat on the Internet. One of the biggest, and most infamous, botnets in 2007 was Storm, which some researchers estimated as having up to half a million infected computers all under the control of criminals.

In the Internet's underground economy, hackers trade code, assist each other, and even sell attack code for bots. The result is that evil code is pulling ahead of good guy code. Some of today's malware can be as sophisticated as the expensive commercial software you buy.

And if all this is not scary enough, attackers are always finding new ways to surprise us, targeting new, trendy technologies such as VoIP, SaaS, P2P, Web 2.0, RFID and so on. They also often find unusual vectors of attack that we never thought to consider. For instance, placing a warez server on a printer, or using a Dreamcast game system to sneakily packet sniff on a network. Finally, mobility is really taking off right now. Whether it's smart phones, or USB sticks, or ipods, confidential data is finding its way outside our network in many new ways.

According to Nachreiner, hackers are hard to catch for the following reasons:

Their Botnets protect them. Botmasters use their victim's computer to launch attacks, rather than their own. If authorities trace the attack machine, they end up at grandma's house and still need to find a way to trace the real attacker. Some botnets have multiple technical layers of separation between the botmaster and the computers doing the illegal activity.

In the past, when authorities found malicious phishing or drive-by downloads web sites, they could take them down in a few hours. Now, botnets can keep these malicious sites up for weeks using something called Fast Flux DNS. In short, a botmaster feeds hundreds of his victims' servers the exact same malicious web page. Then, the attacker creates a domain name for his malicious site, for instance, badsite.com. Usually, a domain name like badsite.com would point to only one IP address. However, by exploiting a design flaw in the DNS protocol, attackers can make badsite.com point to a new IP every few minutes. That way, his malicious web site is constantly jumping around to different bots. If the authorities track down one of the bots and shut down it down, the site just moves on to another.

In addition, criminal networks are almost always geographically dispersed. In fact, the individual members of the criminal organization itself may also live in different countries. Depending on the international climate, and your relations with different countries, you can't always get cooperation in prosecuting foreign attacks. In fact, some countries don't even have strong laws against hacking.

Whenever we do find an only attacker, it often tends to be the "campaign managers".

This leaves the big boss to continue his illegal activities with other campaign managers. It's very similar to how hard it is for the authorities to break up real organized crime, like the mob.

In many cases where authorities have found attackers and tried to prosecute them, the legal battles lasted years and cost thousands of dollars. Often loses never get recuperated, and in some cases, the attackers have continued their criminal activity during and after their trials.

So what can be done?

The only completely secure computer is one that is not attached to the Internet. This is a trade-off: if you can use it, then it can't be 100% secure because, by definition, there is a way into your computer, over the network. Security and usability are often like opposite sides of a teeter-totter. One goes up, the other goes down. The trick is to find the balance.

Security experts have therefore introduced the notion of "layered security" to get around this problem. Nachreiner illustrates the concept this way:

continues on Page 5 - click here

From Page 4 — The Many Threats of Network Security

Security professionals use the word "control" to refer to a generic defensive technique, without specifying what technique. So let's say you have a security control but it only stops half of the attacks coming at you.
Behind it, you put a different security control. It only stops half of the attacks coming at it, too. But since the FIRST control already stopped half of the threats, and the second control stopped half of that half, together they are 75% effective against the total threat. If you keep stopping half of the half, if you line up five controls in sequence, you approach 100% effectiveness.

Nachreiner adds that in reality, a security product that's only half effective couldn't survive in the market. On top of this, various "controls" have to be selected carefully to make sure they really do supplement one another and not just repeat each other. Nachreiner points out here that "security vendors are always telling you to buy one more thing," in this sense, they have a point! The answer, he says, is simple – "defend in depth".

Historically, "defense in depth" required a lot of products such as anti-virus, anti-spyware, spam filters, web filtering to block users from malicious or time-wasting sites, virtual private networks for confidential transactions and firewall/intrusion prevention.
This approach has its own new problems, says Nachreiner, including:

- **Different user interfaces to learn**
- **No accountability among vendors**
- **Inconsistent quality**
- **Various updates and patches at random times**

Enter Unified Threat Management (UTM). A UTM appliance puts "defense in depth" all into one intelligent appliance that

- **Gets the defenses off your computers**
- **Runs off one management interface**
- **Gives you one throat to choke** *(i.e. When something goes wrong, the vendor is much less likely to point at the next guy – because he IS the next guy!)*
- **Updates become predictable and routine**
- **Pick the right one, and quality is assured for years**

Nachreiner says UTM was a really nice step forward in the world of security, to reinforce yet simplify a user's defensive posture.
However, recently, UTM devices are starting to become yesterday's news.

Why? Simply because the bad guys didn't stop innovating, and the Internet environment hasn't stayed the same. Now you have worms and malware traveling via Instant Messaging, and over peer-to-peer file sharing. Attackers are targeting Web 2.0 features, and putting spam in the comments on your blog, or trying to do SQL injection against your custom web application. If any of your users visit MySpace or Facebook, there are attacks specifically targeted at those communities. There is also the "insider" problem – i.e. employees who email sensitive data.
Essentially, UTMs were developed before it became normal to have heavy networking uses such as Voice over Internet Protocol, or streaming video.

What can solve an ever-evolving problem? According to WatchGuard, beyond UTM is XTM (extensible threat management). "Blended threats require blended protection. But you want protection that fits your business today, *and* leaves you with attractive options for tomorrow. That's the exciting promise of XTM," concludes Nachreiner.◊

By Shanti Anne Morais

Click here to go back to the contents page

Bringing the "X" Factor to Unified Threat Management

A visionary and pioneer in the security-appliance marketplace since 1996, WatchGuard Technologies today, is recognized as an advanced technology leader of network-security solutions, with over 500,000 award-winning appliances installed in more than 150 countries.

Consistently named by IDC, Infonetics and Frost & Sullivan as a market leader for SME security appliances, WatchGuard is dedicated to protecting SMEs by providing advanced-security features in its appliances at affordable prices – ensuring all solutions are fully upgradeable to accommodate new features and meet new threats as they emerge.

Widely accepted as a strong viable technology provider for secure remote access, the company recently created a stir in the network-security industry with its announcement to introduce next-generation UTM solutions with extensible threat management (XTM) and connectivity capabilities. WatchGuard's increasing market share is evident in its 190 per cent increase in appliance shipments in 2007, most of which were UTMs – confirming the industry's acceptance of UTM solutions and paving the way for the new XTM platform.

Steve Fallin, director, Rapid Response Team WatchGuard Technologies, shares the company's vision and ideas on XTM with ***Asian Channels***.

What exactly is XTM according to WatchGuard?

Extensibility, the "X" in XTM means having the ability to add on to or extend threat-management capabilities.

WatchGuard's XTM vision is built upon the premise that network security solutions fundamentally need to have this quality. XTM appliances must be able to proactively adapt to dynamic network environments, as well as protect against the litany of known and unknown, future threats. With extensible protection, as a business grows, so does its security platform.

WatchGuard's XTM stands for the extensibility needed for best practices in network-security management and control. Network administrators do not have cookie-cutter environments and have to deal with a constant barrage of threats – known and unknown. Each environment is unique and, therefore, has individualized needs and concerns, depending upon the business and the industry. WatchGuard recognizes this and builds extensibility into its network management and user control features, so that administrators can maximize their XTM investments, which are customized to best suit their network and user needs.

WatchGuard's XTM represents extensible choice. Not only do XTM appliances need to fully interoperate and support mixed network infrastructures, but they need the inherent security technology to be flexible, too. This way, administrators can pick and choose the security service that they want from the XTM device. For example, some may want anti-virus (AV) protection provided at a different source other than the gateway. Now, an administrator can turn "off" the AV protection at the XTM appliance, whilst maintaining full firewall, IPS/IDS as well as web content filtering at the network gateway.

With WatchGuard's XTM, the customer has a choice of security services.

XTM thus provides extensible ownership and leads the industry with software upgradeable UTM devices. This allows businesses to maintain high security without having to rip out and replace older devices – giving unmatched asset protection and lowering the total cost of ownership (TCO). WatchGuard will continue to provide this extended life and functionality with its next-generation XTM appliances.

Lastly, the WatchGuard XTM vision opens the door to extensible market opportunities. WatchGuard envisions uptake of a new class of managed security service providers (MSSPs), who wish to provide highly reliable, "in the cloud", managed-security services to their customers. WatchGuard also foresees the possibility of providing a software platform – similar to that of other extensible applications, such as XML – so that third-party developers can create customized security applications that are tailor-made for WatchGuard XTM appliances.

What makes XTM stand out in the network security arena? What are its main benefits?

Extensible security means giving customers' unparalleled security against the next wave of unknown threats, giving customers uncompromised network management and user control, and giving customers unbridled flexibility and choice. Combining these benefits, WatchGuard is uniquely positioned to give businesses around the world the peace of mind of knowing that their networks as well as their employees' work and data is highly secure with our XTM solutions.

WatchGuard's extensible components include:

- Extensible protection to remain secure against the unknown future threats
- Extensible management for easy control in varied environments
- Extensible choice for interoperability and choice of security services, whilst maintaining exceptional standards of protection

continues on Page 7 - click here

From Page 6 — Bringing the "X" Factor to Unified Threat Management

- Extensible ownership through upgradeable devices, thereby offering extended product life and high functionality

Why do you think XTM is so necessary? Do you think XTM will change the face of network security?

By 2007, the UTM market had grown approximately 35 per cent year-over-year, to reach US$1.216 billion. By 2008, industry analysts estimate that sales of UTM appliances will surpass traditional firewall/VPN solutions. By 2010, sales of UTM devices are expected to exceed US $2.5 billion – creating infinite opportunities for the next-generation UTM solutions.

XTM solutions have the capability to change the industry landscape and redefine network security. As discussed above, they address needs not currently met by the prevailing UTM solutions. Although UTMs offer considerable deployment flexibility, the increasingly sophisticated and decreasingly conspicuous threats in an evolving environment require scalable appliances that can be modified, updated and customised so that high security is always maintained. The changing perimeter of the workplace calls for robust security technology to face the "x" factor of unknown threats.

Tell me about WatchGuard and its XTM vision and strategy? How does this strategy tie up with your overall business strategy and vision?

WatchGuard Technologies, a pioneer of firewall technology since 1996, was an early innovator of UTM solutions, and was one of the first to lead the industry with high-performance UTM offerings. XTM is the next generation of UTM technology, predicated upon the substantive expansion of three foundational elements: more security; greater networking capabilities; and more management flexibility.

With threat management being constantly challenged and redefined, XTMs are much-needed security solutions in today's dynamic environment. For business decision makers, XTM offers an ideal cache of reliable security and superior TCO. XTM allows businesses to utilise mobility, consumer technologies, Web 2.0, and other new business applications in a highly secure manner. Because of the inherent flexibility found in XTM, these solutions will help businesses address the needs of regulatory compliance and future changes that are bound to come.

What are the key drivers of this strategy and vision?

Threats are becoming more sophisticated and less conspicuous. This leaves networks vulnerable to extremely targeted attacks that include blended threats, such as phishing e-mails with malware payloads. The challenge is to give businesses threat-management solutions that not only adapt, but can proactively address future and unknown threats so that the highest security is always maintained.

Adding to this, most network administrators work in mixed-network environments of disparate infrastructure components and solutions. For these administrators, it is imperative to have a flexible and scalable gateway-security appliance that can be modified, updated and customized to meet their particular security profiles and postures. The XTM family will enable customers to choose exactly which security functions they want the device to perform, rather than being forced into buying bundles of capabilities, some of which may not be of interest.

What are your plans for this strategy especially in the Asia Pacific? Are you targeting XTM at certain verticals, sectors and/or markets? Do you think it will be a major attraction to both enterprises as well as SMBs?

WatchGuard's recent vision to introduce next-generation UTM solutions with XTM and connectivity capabilities is keeping the company a step ahead in this competitive marketplace.

Creating and designing network-security solutions – which have the ability to proactively adapt to dynamic network environments and protect against unknown threats – WatchGuard's XTM products ensure maximized productivity, with seamless, robust authentication for identity management and powerful endpoint protection for uncompromised network connections. With vastly expanded security features and functionality, networking capabilities and management flexibility, as well as automated processes, WatchGuard's XTM solutions are suited for SMEs and enterprises alike across varied sectors and verticals – purpose built to thwart attacks from today's smarter malware and botnets.

How do your partners in the Asia Pacific especially fit in with this strategy?

They service organizations that have been asking for some of the capabilities embodied by XTM. APAC buyers are amongst the most discerning in the world. Our two-tiered, partner-centric sales model is designed to attract an expansive network of resellers focused on network-security solutions. Our tier-one distributors carry our full range of products and services to specialised and value-added resellers across the region – increasing our penetra-

continues on Page 8 - click here

From Page 7 — Bringing the "X" Factor to Unified Threat Management

tion in the SME and enterprise marketplace. We are growing our regional revenue at around 20 per cent per year with Hong Kong, India, Indonesia, Malaysia, Thailand and the Philippines as our key Asian markets.
We are currently recruiting more resellers to boost our UTM and XTM sales.
We are particularly interested in adding resellers with strong technical networking capabilities or those with security expertise.

You'll be announcing new products that will build on your XTM vision. Can you please elaborate on this?

Currently, WatchGuard's firmware release for Peak, Core and Edge appliances have built-in extensibility, so users can leverage this innovative technology today! Later this year, WatchGuard plans to release XTM-branded solutions that incorporate more XTM feature sets – addressing extensible threats (the next generation of blended-security threats), having extensible management (improved scalability and greater granular control), offering extensible choice (network interoperability and feature-set customization), and ensuring extensible ownership (network interoperability, total cost of ownership and return on investment). Global markets for security solutions are constantly evolving.
WatchGuard monitors these markets to ensure that we are aware of the optimal time for the introduction of new products and platforms.

What can we expect over the next 1 year from XTM and WatchGuard?

We have established a trajectory that portends more capabilities and more performance. We will be announcing our new XTM-branded products when the time is right.

Are there any major challenges when it comes to XTM in Asia? If yes, how do you think these challenges can be overcome?

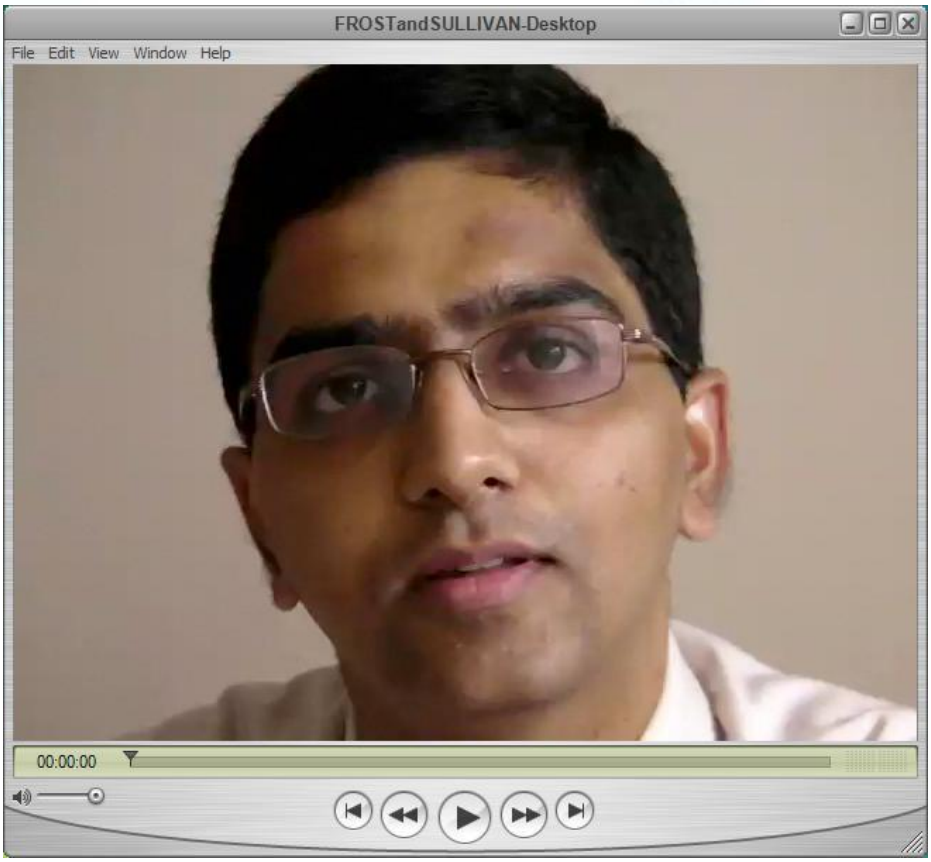
The XTM approach blends seamlessly with the needs of Asian businesses today. For the discerning, skeptical buyer, it provides a sensible and innovative approach to meeting the region's need for flexible, easy-to-use, high-value security solutions. Leading the charge with its pioneering XTM solutions, WatchGuard will continue to create a stir in the Asian network- security market. ◊

By Shanti Anne Morais

Click here to go back to the contents page

Frost & Sullivan: The Possibilities with UTM are Endless

There is no doubt about it, Internet threats are getting bigger, more malicious, smarter and more damaging.
Arun Chandrasekaran, industry manager, Frost & Sullivan points out that the threat landscape has also been undergoing a dramatic shift – from PC viruses that were mainly floppy disk based to Internet viruses that were more email/network based, to malware that was more broadband/website based, to the present day scenario of more targeted attacks, as well as threats that are considered cyber-espionage.
He elaborates that the new security landscape is seeing more covert as well as targeted blended threats, making remediation even more complex.



From Page 8 — Frost & Sullivan: The Possibilities with UTM are Endless

The advent of what Chandrasekaran refers to as "the underground economy" will continue to rise with no signs of abating as the primary motive of such cybercriminals revolves mainly around the motive of financial gain.
Attacks here include phishing, hacking, identity theft, money laundering, bot attacks and the like. In fact, according to him, this shadow Internet economy has been valued at US$105 billion, with this figure looking set to rise even higher.

As a result of all the above and the ensuing challenges in the enterprise ecosystem like disparate systems, little integration as well as high CAPEX & OPEX, Chandrasekaran says that a more holistic view of security that integrates the different dimensions (such as anti-virus, firewall, anti-spam filters, virtual private networks, identity and access control encryption, web security and so on) into a more unified solution is needed – hence the birth of Unified Threat Management – UTM.

Chandrasekaran notes that Frost & Sullivan has also been seeing some major trends and shifts in the UTM market. For one thing, when it first started out, UTM appliances tended to be deployed by mainly small and medium enterprises (SMBs), mainly because it was a great value proposition for them. In the last 12-18 months though, Frost & Sullivan has noticed that more large multinationals are looking into and taking up UTM, mainly for their branch offices. "UTM is definitely becoming more viable as a platform.
For example, it is becoming more scalable. Also, one of the biggest drivers of UTM is its ability to enable the convergence of multiple technologies on a single platform," he elaborates.
He adds that UTM is continuing its trend of climbing up the value chain. "On the services side for example, in the past, there were not many managed security services in UTM but this is now changing especially amongst bigger enterprises and larger managed security services providers," Chandrasekaran states.

With regards to the evolution of UTM, he observes that UTM has already seen a huge shift from its early days (from 2000-2003) when its appliances were predominantly for firewall and anti-virus purposes. Chandrasekaran explains further, "More and more technologies are being added on for example intrusion detection. Now, even web application security is being looked at. In addition, non-security technologies are being considered like WAN acceleration.
The possibilities with UTM are endless and we will definitely see it evolve even more over the next 6-12 months."

While UTM has many merits, he says, such as lower TCO, greater

Photo: Arun Chandrasekaran

centralized management, evolving technology convergence, ease of use and affordability; it also still has its fair share of challenges – what Chandrasekaran refers to in his presentation as "the undelivered promises of UTM". These include scalability issues, lack of "best of breed" capabilities as well as lack of intelligent integration. However, he is quick to add that these challenges are something the key vendors are aware of and are keen to address. "Again, the evolution of UTM will probably iron out a lot of its issues." "Some vendors are already looking beyond UTM",he concludes.◊

By Shanti Anne Morais

Click here to go back to the contents page

MayDay: The Storm Continues – Batten Down the Hatches

How to measure the real cost associated with botnets today that control over a million PCs worldwide and launch more than 100 billion spam messages a day, flooding the mailboxes of unsuspecting recipients?

Cyber dependency has grown to such an extent that cyber vandalism is an issue that needs to be addressed by every computer owner, from large organizations to individuals. The current dynamics of internet crime – its sophisticated technology, boundless scale and massive economic impact – redefine the term internet security.

IBM ISS general manager, Val Rahamani, claims, "The security industry is dead, long live sustainability." Just as new internet security products are launched, new online threats arise. In the endless game of catch up, most industry experts now believe that network security is doing its job if the processes and systems just stay one step ahead of the incessant threats.

Botnets: Top Threat in 2008

Botnets, a collection of compromised computers infected with software robots or bots, continue to figure prominently in the "Top Threats of 2008" by many prominent leaders in the ICT industry. Botmasters, or bot herders, seem to have one purpose in life: launching viruses or worms to infect ordinary-user PCs with malicious applications or bots. Bots on the infected PCs are coded by the operator or botmaster to log onto a designated server – christened the Command and Control (C&C). Access to the network of bots attached to the C&C is then sold to spammers who use the data for monetary gain in a plethora of ways.

From Storm to Kraken and MayDay, now there's Sribzi – botnets have evolved to stunning levels of sophistication at lightning speeds, raking in big bucks for the spammers and botnet operators alike. Since their inception in 1998-1999, when the notorious NetBus and BackOrifice2000 appeared as the first backdoor programs enabling remote administration of infected computers, cyber criminals have been having a field day wreaking havoc across the internet. Trojans worked behind the scenes – without the user's knowledge or consent – performing file operations on remote machines or launching new programs. At that time, to control an infected computer, all a cyber criminal had to do was establish a connection with the infected machine via a LAN-based application on the TCP/IP protocol stack, and exploit the Windows API for control.

Within a year or two, programs advanced to an extent wherein botmasters were able to control several machines simultaneously – operating as network servers, which opened a predefined port and passively waited for the botmaster to connect. Further innovations saw infected computers initiate connections themselves, monitoring every move the unknowing PC user made. This first lot of backdoor administrators was likely hackers, since they used a channel normally used only by hackers – Internet Relay Chat (IRC). They connected to IRC servers on a predefined IRC channel and waited for messages from the botmaster in control of the C&C.

Botnet hijacking soon became the norm as a new generation of malicious users appeared, scanning IRC channels with suspiciously heavy traffic where they could gain entry and hijack the botnet – effectively taking control of the network and reordering the bots to password-protected IRC channels.

These hijackers eventually developed a way by which an unwitting computer on a LAN could connect to an internet server and relinquish control to a botmaster anywhere in the world – bypassing proxy servers and Network Address Translations (NATs). The hijacker could then establish an HTTP connection with the administration server using the client computer's local settings – ensuring accessibility. After that, a simple script could control small computer networks. Enter cyber criminals cashing in by selling botnets to spammers, who, in turn, lined their pockets by sending phishing emails, stealing files, documents or personal information – including passwords and other sensitive data – to launch spam-email campaigns, denial-of-service attacks (DDoS) and online-fraud schemes. In some cases, a large number of computers could even be managed using any internet device – including a mobile phone that supported WAP/GPRS – further raising the cyber-crime bar.

These first botnet networks were vulnerable; they depended on a single C&C and were designed to simultaneously infect computers with different bots connecting to different C&Cs. It was the evolution of peer-to-peer (P2P) botnets, without a C&C, that enabled botnets to become the internet's worst enemy. Newfangled botmasters only had to send a single command to any computer on the network and the subservient bots would spread the command to other computers in the botnet automatically.

230 Dead as Storm Batters Europe

Batter is exactly what it did and not only within Europe. The new-kid-on-the-block took more than 50 million computers by storm worldwide.

continues on Page 11 - click here

From Page 10 — MayDay: The Storm Continues – Batten Down the Hatches

The Storm botnet emerged in January 2007 as a traditional computer worm and quickly morphed into the commander of the internet, luring users with spam hidden in subject lines related to extreme weather.

In the beginning, the malicious program was distributed as an email attachment to spam messages (often seen as PDF files named "ReadMore.exe"). Once opened, the code infected victims' computers, leveraging P2P architecture to spread rapidly – converting into as many as three to five new Storm worms a day. Later, attachments were replaced with links to infected files inserted into spam messages and links to infected web pages and blogs.

It soon became clear that Storm was not yesterday's bot. Developed and distributed by professionals, the bot code mutated on a dedicated computer on the internet, rather than within the program itself – spawning new versions as quickly as once an hour; thus, making antivirus database updates ineffective for many users. The Storm botnet was also programed to protect itself from frequent requests from the same IP address, launching a DDoS attack on any suspicious address to keep network analysts at bay. Meanwhile, the bot tried to remain as inconspicuous as possible, using limited system resources to avoid detection. Notably, instead of communicating with a central server, Storm only connected to a small number of computers on the infected network (typically 85,000 machines, of which only 35,000 were set up to send spam) – making identification of all zombie machines virtually impossible. Finally, the botmaster was constantly changing distribution methods and using sophisticated social-engineering techniques.

"Storm evolved like an ever-shifting malware kaleidoscope," says Scott Pinzon, information security analyst, WatchGuard LiveSecurity, CISSP. "As it grew in size and strength, Storm was called the world's most powerful super computer". From annoying, colossal amounts of spam to the fallout from the debilitating cyber attack on Estonia, the full extent of Storm's reach and ensuing damage will never be known. By year end, the Storm botnet seemed to have dissipated – either broken up into parts and sold or abandoned due to lack of continued profitability.

You Can Call Me Kraken or Bobax or Bobic, or…

Emerging earlier this year, the so-called Kraken botnet, also known as Bobax, took over Storm's claim as the world's largest, most-destructive botnet – boasting between 185,000 to 400,000 hacked computers in its collection. With the capacity to spam about nine billion messages a day, Kraken has been in and out of the news with other aliases including Bobic, Oderoor, Cotmonger and Hacktool.Spammer – and is even disputed to be the same botnet known as MayDay.

Like most botnets, the purpose of Kraken seemed to be the propagation of massive amounts of spam. The Kraken code came in a file that looked like an ordinary image file, such as JPEG or PNG, but with a hidden extension that prevented users from recognizing it as an executable file. Once an innocent user opened the file, it copied itself onto the user's PC and deleted the original copy – erasing all its tracks. Kraken, therefore, presented enormous difficulties for analysts to detect. This malicious botnet caused individual PCs or servers to send as many as 500,000 spam messages in a single day – double the size of Storm. Spotted in at least 50 Fortune 500 companies, it was undetectable in over 80 per cent of machines running antivirus software on Microsoft Windows operating systems. Unlike Storm, the Kraken botnet code included a list of domains anywhere in the world where the C&C server might be located. Once a machine was newly infected, it began sifting through that list to find the current C&C.

If a C&C server was taken down, which happens regularly with large botnets to avoid detection, Kraken's botmaster could simply move the C&C function to another domain instantly – effectively evading even the most robust network security. Until recently, Kraken ruled the internet, causing mayhem and uncountable monetary gain for both spammers and the bot herder.

MayDay: Storm's Little Brother

By late January/early February 2008, MayDay arrived on the scene, appearing as a P2P architecture-based Botnet, more cunning and more sophisticated than Storm. After launching, a bot – connected to the web server specified by the program – registered itself in the server database and received a list of all bots on the infected computer. This established P2P communication, based on ICMP message, with other bots in the zombie network. To avoid detection, MayDay carefully measured how much traffic passed between the C&C and each bot client. In addition, it enforced a short window wherein communication must happen.

However, its non-encrypted, network-communication protocol had not been designed to eclipse antivirus software and it never possessed the same ability to vary itself frequently, unlike Storm. Though it did not compare in size or strength, MayDay is heralded as a serious Botnet with a tidy

continues on Page 12 - click here

From Page 11 — MayDay: The Storm Continues – Batten Down the Hatches

code applicable to Windows and Linux – indicating a skilled development team. Nobody has seen hide nor hair of the MayDay bot for a few months now. Is it still lurking out there waiting for July to surface again?

Srizbi: The Perfect Storm

The latest newcomer topping the botnet charts is Srizbi, accounting for up to 50 per cent of all spam today – weighing in as the single-largest menace on the internet at this time, dwarfing even Storm. Total infection rate to date is around 300,000 PCs across the globe, spewing an estimated 60 billion spam emails per day. All those emails about watches, pens, and male-enhancement pills flooding your mailbox are all probably the work of Srizbi. Even at its height of destruction, Storm only accounted for 20 per cent of worldwide spam. So far, Srizbi is out producing all the other botnets combined. Super botnets have already begun to dominate internet traffic.

It appears as if Srizbi is reproducing itself in the emails it distributes. Though not unique, this feature may be helping the botnet from being detected at this stage and deceiving people by using more sophisticated social engineering. History suggests that Sribzi will fade away, just like Storm, just like Kraken, just like Mayday. However, by then, another new super botnet will probably have taken its place.

Summary

No doubt, botnets today are a key internet disrupter and have proven to be the most powerful and effective cyber-criminal tools to date. From lucrative phishing and fraud scams to extortion and exerting political pressure on governments, today's cyber criminals are an intelligent breed – using social engineering to entice a victim to click a link or open a file, instead of cracking a firewall to penetrate a machine. Additionally, botnet crime is becoming increasingly dangerous owing to its ease of use and availability. The economy supporting these cyber crimes has grown to such an extent that everything from virus-writing kits to spam-spewing zombies are now available for purchase or hire.

Unfortunately, home-users' computers make up a large part of infected zombie machines. A bot master's worth is judged, not by his technical prowess, but by his ability to gain access to networks with millions of compromised machines. The bounty is just too great to expect cyber criminals to go away.

However, internet security experts debate how to control these damaging devils that creep into our machines and then run rampant day and night. Executive Director of National Cybersecurity Alliance, Ron Teixeira, strongly believes that only a combination of network-security tools can prevent botnet attacks in the future. We need to educate the industry and the average computer user about the problem and illustrate easy and practical ways to prevent malware infection. To the industry, he petitions more investment in network-security technology to thwart the attacks at the outset. Lastly, he urges heavy-handed law enforcement to ensure cyber criminals are seriously punished, once caught. ◊

By Corey Nachreiner,
Network Security Analyst,
WatchGuard Technologies

Tips to Banish Botnets Once and for All

- Deploy in-depth defence strategies and multi-layered network security
- Promptly patch and vigilantly download security updates
- Block JavaScripts
- Monitor ports and plan port security to block unauthorised traffic
- Generate user awareness amongst friends and colleagues

Click here to go back to the contents page

Photo: Participants of MediaBUZZ's event on UTM—A Revolution or Evolution, October 7, 2008 NLB

The UTM Story

Over the past 5-6 years, the Unified Threat Management (UTM) market in the Asia Pacific market has been taking off. Anthony Lim, Security & Governance Chapter, SiTF, shares with us the colorful back story of UTM and his perspective on it.

Photo: Anthony Lim

Pre-UTM

The emergence of UTM, says Lim, was fuelled to a large extent by the increasing popularity of appliance security solutions made fashionable by Nokia, NetScreen, WatchGuard Technologies, Cisco Systems and more. "Even the likes of ISS, Symantec and Trend Micro had a tryst with these appliances, though I think some were more successful than the other," he observes.

"Suddenly, everyone wanted an appliance firewall," he adds. Its popularity was driven mainly by its ease of deployment since the appliances were basically plug and play. Secondly, for the most part, these appliances were by default pre-configured to be ready-to-use. Lim elaborates, "These were important attributes because people were by then deploying them in a hurry and by the droves, due to the runaway proliferation of internet services, which were in turn, driven by the mainstream availability and high volume of broadband connectivity back then."

The end result of this was that other security solutions vendors decided to hop onto the appliance bandwagon resulting in the introduction of anti-virus, anti-spam filters, email security, IDS/IPS and so on. "By 2003/2005, it was not difficult to imagine an enterprise Security Operation Center (SOC) buying and stacking boxes, some of which were by then imaginably colorful (and I mean red, yellow, blue and green instead of the usual grey, black or silver)," he says tongue in cheek.

"So, it became logical to think that this wasn't the best idea because you can imagine rackfuls of security appliances, rack-mount servers, patch-boards, hard disks, routers, switches and all the spaghetti in between – you get the idea!" Lim continues.

The Advent of UTM

What happened next was that security vendors endeavored to reduce the number of boxes at the SOC by trying to increase the number of security solutions within the given box (appliance), hence the UTM idea was born.

Notably, the first commercially known attempt at a UTM appliance was probably by Crossbeam Systems. "Here, I don't mean the bar refrigerator size server, $100,000 super-fast, industry product/solution," says Lim.

In 2003, Crossbeam Systems introduced the "C" series—a rather large appliance with a Check Point firewall, Trend Micro antivirus and ISS' IDS all in the same box. Over the next few years, Crossbeam introduced different sizes and variances of the "C" series. "Not to be outdone, Check Point, ISS and Nokia were soon apparently accusing one another of trying to eliminate the other by introducing firewalls with IDS in the same box or vice versa. Again, you get the idea!" remarks Lim.

"Symantec soon decided their appliance was way too difficult to develop and deal with, preferring to focus instead on merging with Veritas. In the meantime though, WatchGuard, SonicWall, Fortinet, F5 Networks and the rest, proceeded to solder on and eventually formed the UTM market that we know today. It is interesting to note that they all began with different single application appliances," he expands.

"Today," he adds, "Check Point has re-introduced a new set of appliances, while Nokia has decided to put their security appliance division up for sale."

The Current UTM Market

According to Lim, the present day UTM market in the Asia Pacific looks set to grow and is healthy because of a number of reasons:

It is convenient to deploy – especially important amongst SMBs where it is often hard to hire experienced IT security professionals – and can be done both quickly as well as effectively.

UTM saves users the trouble of trying to decide a) which anti-virus, anti-spam or IDS solutions they want; b) what solution users may need that they may have forgotten and c) saves users the trouble of a human resource management issue in case different engineers on your staff prefer different brands or best of breed.

A challenge that Lim feels the UTM market will face is the fact that there may be an attempt to put too many applications into one appliance, in which case, users may end up facing a performance or software management issue.

"In addition, the question of what permutation of applications users will have in which UTM appliance might also arise," he shares.◊

By Shanti Anne Morais

click here to go back to the contents page

UTM: Bent on Creating a Storm

WatchGuard's Norbert Kiss gives us the lowdown on Unified Threat Management, the company's strategy and vision on it and its key drivers in the region.

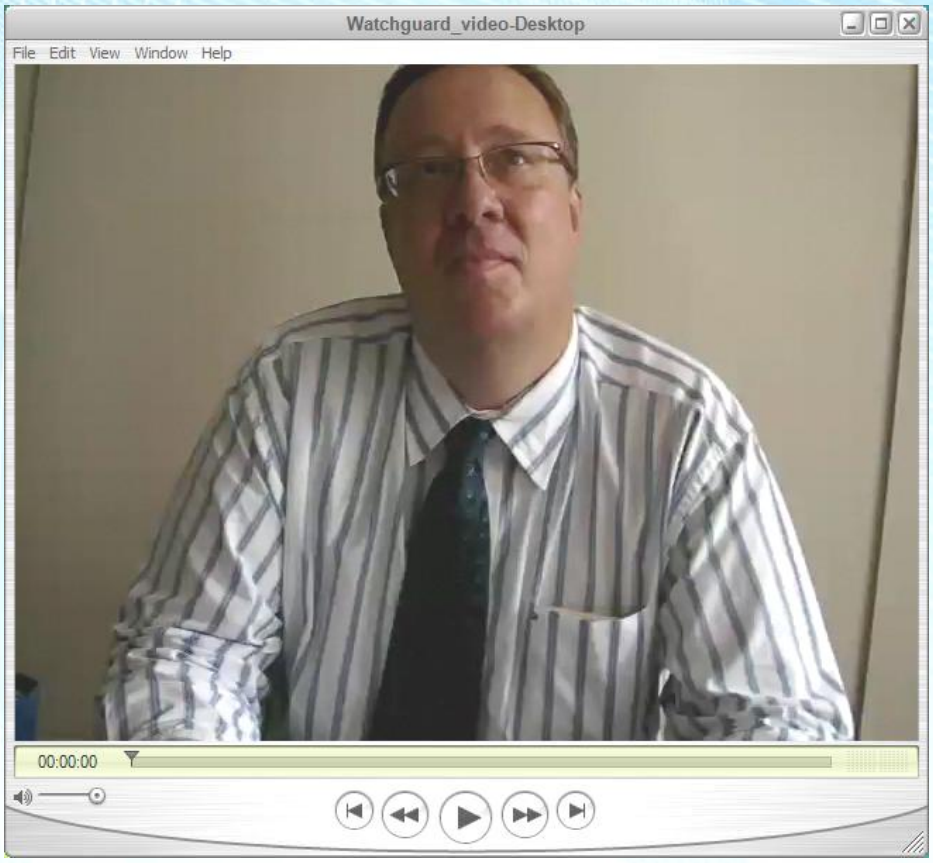
What's your definition of UTM? Is this definition different from the standard in any way? If yes, why?

Unified Threat Management, which stormed the ICT world in 2005, was created due to customer demand for a better way of managing network security for companies of all sizes. Coined by IDC as UTM, 'Unified' signifies that a single device can manage multiple threats, including blended threats – a one-stop shop for customers to manage their network security needs.

Our definition of UTM is the same as that of industry practitioners. However we execute this definition very differently from others within the industry. An example of this is our proxy-based architecture that thoroughly inspects everything that enters the network for threats, providing our customers TRUE Zero Day Protection – compared to most vendors who have packet inspection, thereby checking only a part of the contents. UTM is a gateway technology as opposed to a client technology, so it successfully prevents threats from entering the network. Client-based security only protects the network from threats that have already invaded the network. In spite of working under the same UTM umbrella, the delivery of the WatchGuard offering surpasses industry standards and practices.

Tell me about WatchGuard's vision and strategy when it comes to UTM?

WatchGuard Technologies, a pioneer of firewall technology since 1996, was an early innovator of UTM solutions, and was one of the first to lead the industry with high-performance UTM offerings.



Our vision is to provide customers of all sizes – SMBs or enterprises, with a single device, which is easy to deploy and manage, delivers a quick ROI and adapts well to changing threats.

Our strategy to achieve this is to integrate best-of-breed network-security technology into our UTM devices through innovation and partnerships with leading providers of technologies. The changing perimeter of the workspace, coupled with the "x" factor of unknown threats, has created an opportunity for future UTMs – XTM solutions with next-generation extensible- threat-management technology – which will change the industry landscape and redefine network security. We, as providers of this technology, continue to be evangelists in the market by demonstrating to customers and partners, that UTM and XTM have scaled newer heights to provide greater security technology than the traditional point solutions. We continue to provide our partners with leading channel programmes, education and incentives to ensure they bank on WatchGuard products whilst offering solutions to their customers.

What do you feel makes WatchGuard stand out in UTM market and from your competitors?

There are multiple reasons for WatchGuard's leadership in the network-security industry today. Firstly, WatchGuard's products have distinct technology advantages over our competitors. Being a pioneer of appliance-based network security since 1996, these include Proxy technology, logging and reporting features and more. Secondly, WatchGuard's long-standing reputation as a leading provider of network-security solutions gives us an edge in this crowded industry. With over 500,000 devices around the world protecting networks at this very moment, our technology speaks for itself. Thirdly, our sales model relies highly on our partners, who have successfully helped to build our brand in the market.

continues on Page 15 - click here

From Page 14 — UTM: Bent on Creating a Storm

We continue to provide them with superior products at competitive pricing, coupled with education and incentives, so they can, in turn, offer the best available technology to their customers.

From your experience, do you see any UTM trends that are particular to the Asia Pacific? Are you seeing a shift in trends in any way when it comes to UTM?

The face of the network security market is changing continuously due to increased internationalisation and globalisation, coupled with dynamically-changing and highly sophisticated internet threats. Even SMBs are finding they must maximise productivity for their remote and mobile users, whilst ensuring a highly secure network. With SMB networks expanding at an ever-increasing pace, UTMs play an important role in addressing these changing trends. UTM as a technology is standard across the world. We haven't seen any specific requirements by geography, apart from local language requirements and the need to manage and block local social-networking sites and chat rooms. However, we have seen a significant difference in the speed of adoption of this technology. I would say that mature IT markets such as Australia, Hong Kong and Singapore have a high level of acceptance for UTM and penetration continues to grow in these markets. Japan, although a technologically advanced country, has been slow to accept the UTM technology, but we are currently seeing growing adoption there now. Other parts of the region have just begun to realise the varied benefits of UTM and the importance of network security in an increasingly mobile world, which represents a significant opportunity for us to tap into these fast-growing markets.

What are the key drivers of UTM? Do you think there are any underlying factors in the security landscape that are in particular, driving UTM?

All organisations, irrespective of their size, are exposed to the same set of security threats. However, SMBs today have limited budgets for internal or completely outsourced security for technology infrastructure management. They seek security solutions that ensure increased productivity, lower cost of ownership, compliance assurance or ease of deployment and management, as well as resource scalability and availability. Constantly evolving network-security threats that can cause immeasurable inconvenience, affect a company's reputation and result in unpredicted support costs – forcing SMB management to address these needs. Traditional remote-access-security solutions are no longer viable solutions for SMBs that require uncompromised network connections, so SMBs are turning rapidly to UTM solutions. WatchGuard's UTM appliances are purpose-built, not only to meet enterprise needs, but SMB needs as well.

Many regard UTM as a technology for SMBs. What's your take on this? Do you think the enterprise also benefits from UTM? Do you think the enterprise is ready for UTM?

It's true that UTM has been primarily focused towards SMBs. This was due to the fact that large enterprises had large IT budgets, multiple staff and would often roll out specific point solutions for specific security threats. This is changing rapidly in these more challenging economic times. The benefits of UTM, including improved threat management and performance are opening new opportunities for UTM in the enterprise space.

We can see clear evidence of this as enterprises often take advantage of UTM in their branch offices and remote locations where having multiple point solutions is just not viable. UTM in the enterprise space offers significant benefits to the customers.

"Performance is one of the biggest gotchas in UTM"? Do you agree with this and what is WatchGuard doing in the area of UTM performance?

This has been an unfair perception of UTM for some time. If a customer buys a separate unit for SPAM and separate unit for Web blocking, a separate unit for IPS, etc. and then switches them all on, they will naturally see a slowdown in network traffic. The same is true with a UTM device. If you turn everything on, it will slow down the network. So the issue is not just true for UTMs, but for any network-security solution.

However, there are areas that can be improved. Multiple levels of hardware can improve the performance, giving customers the choice to move up the product chain to gain higher performance levels. Also, the UTM hardware itself has become much faster, with dramatic improvements in UTM performance over the past 12 months – a trend one will continue to see. In spite of this, UTM solutions have been widely accepted by customers, and the UTM market has seen enormous growth with vendor revenue of US$100 million in 2004 to US$1.3 billion in 2007. Sales are forecasted to exceed $2.5 billion in 2010*. UTM solutions have typically dominated the network-security arena essentially containing a firewall, network-intrusion detection and prevention, and gateway anti-virus capabilities.

continues on Page 16 - click here

From Page 15 — UTM: Bent on Creating a Storm

WatchGuard created a stir in the market when it announced its plan to introduce next generation UTM solutions called extensible threat management. Can you tell me more about your XTM vision and how you are paving the way for your XTM solutions? What are the benefits of XTM, why do you think it is so crucial to businesses and what types of companies do you think will benefit the most from it?

Yes, XTM is a very exciting new direction for UTM indeed and we are focused on XTM research and development. WatchGuard is the first network-security vendor to provide a vision on what Chris Kolodgy, IDC Industry Analyst, defines as "the next generation of Unified Threat Management (UTM), integrated network-security appliances," called Extensible Threat Management (XTM). Fundamentally, XTM is the new UTM and is extensible in its ability to protect existing and future unknown threats. We announced our XTM direction a few months back and expect to have the first products hitting the shelves in Q1 2009. These 10GB throughput products will offer best-of-breed, robust and comprehensive network protection, in-house management, using an intuitive, centralised console, options to for CLI -based management, along with local-language support and localisation. Customers across the board, from SMBs to large enterprises, will benefit from WatchGuard's new XTM technology. WatchGuard's XTM-branded solutions incorporate XTM feature sets – addressing extensible threats (the next generation of blended-security threats), having extensible management (improved scalability and greater granular control), offering extensible choice (network interoperability *and* feature-set customisation), and ensuring extensible ownership (network interoperability, total cost of ownership and return on investment), which without a doubt are essential and beneficial to any global organisation.

Primarily, XTMs offer enhancements in security, networking and management capabilities. In addition, XTMs will manage security threats from new emerging areas, such as VoIP and HTTPS and provide enhanced SSL security – which is unique to XTM. In the area of network capabilities, XTMs will offer features such as high throughput and high availability, clustering technology – what can be provided with UTM today. On the management side, there will be significant enhancements in visual reporting and connectivity to enterprise-management software such an Openview, Tivoli, etc.

Do you think XTM will change the face of network security? How?

Yes, XTM is on its way to becoming the new standard. XTM solutions have the capability to change the industry landscape and redefine network security. It is the next logical progression to UTM and it will mean that we can adapt faster to new threats, work in much larger networking environments and ensure ease-of-use in terms of management. There is a lot of talk about "cloud computing" and "application hosting" and many companies are now adopting these technologies, which open entirely new security threats – which is exactly what XTM is designed to address. XTMs address needs not currently met by the prevailing UTM solutions. The changing perimeter of the workplace calls for robust security technology to face the "x" factor of unknown threats, and XTMs have the ability to proactively adapt to dynamic network environments and protect against unknown threats.

When can we expect to see WatchGuard's XTM solutions in Asia?

Currently, WatchGuard's firmware release for our Peak, Core and Edge appliances have built-in extensibility, so users can leverage this innovative technology today! Early next year, WatchGuard plans to release XTM-branded solutions (XTM-1050 will be the first one in Q1 2009) that incorporate more purpose-built XTM feature sets – addressing extensible threats, having extensible management, offering extensible choice, and ensuring extensible ownership. Global markets for security solutions are constantly evolving. WatchGuard monitors these markets to ensure that we are aware of the optimal time for the introduction of new products and platforms. We are putting a lot of development effort into XTM and XTM will be the basis of our strategy and products in 2009.◊

By Shanti Anne Morais

click here to go back to the contents page