



# WATCHGUARD AND UNIFIED THREAT MANAGEMENT: A Business Overview

AUGUST 2007

## **DYNAMIC THREAT ENVIRONMENT**

Keeping corporate networks safe is more challenging every year, and network security has become one of the most critical issues facing businesses today. New and ever-changing threats appear with alarming regularity, and no organization is immune from risk.

Every time a new and more sophisticated threat presents itself, it changes the very definition of what a “secure network” really is. According to the IBM Internet Security Systems X-Force Research and Development Team, more than 7,247 new Internet security vulnerabilities were discovered in 2006, and 88.4% of those could be exploited remotely.

When a network is breached by intruders, a Denial of Service (DoS) attack, or a malicious virus, the entire organization becomes vulnerable. This can leave a company’s operational resources, customer data, proprietary tools and technologies, and intellectual capital in danger of being stolen, misused, or vandalized by third parties. Network attacks can take many forms, including:

**Network Intrusion** - In an intrusion scenario, a hacker with no access privileges attempts to penetrate a network remotely for malicious purposes.

**DoS/DDoS Attacks** - In a DoS attack, targeted systems or networks are rendered unusable, often by monopolizing system resources. A Distributed Denial of Service (DDoS) involves many computer systems - possibly hundreds - all sending traffic to a few specific targets.

**Viruses and Worms** - A virus is a computer program that infects other programs with copies of itself, but which is transferred from system to system by some outside mechanism such as e-mail. A virus executes and does its damage when the program it has infected executes. This is distinct from a worm, which is a computer program that is capable of repeatedly copying itself to other computer systems. Worms can carry viral code.

**Adware and Spyware** - Adware is a software application which installs itself, often without the user's permission, and displays advertising banners while the program is running. They may appear as pop-up windows or as a bar that appears on a computer screen. It may also change browser properties such as the home page. Spyware is similar to adware but often does not reveal its presence by pop-ups or other means. It uses code to track a user's personal information and pass it on to third parties without the user's authorization or knowledge.

**Rootkits** - A rootkit embeds itself into an operating system and intercepts commands that other programs use to perform basic functions, like accessing files on the computer's hard drive. It hides between the operating system and the programs that rely on it, controlling what those programs can see and do.

**DNS Poisoning** - Domain Name System (DNS) servers are duped into re-directing traffic originally heading to a benign destination to a malicious Web site instead.

A network can also become vulnerable every time a business experiences growth and change. As networks become more complex and are expected to do more to support and drive business objectives, a simple firewall is not capable of providing the security your network needs. This is where Unified Threat Management (UTM) solutions can be the right solution.

## WHAT IS UNIFIED THREAT MANAGEMENT?

Unified Threat Management is the name for an emerging trend in the appliance security market. Unified Threat Management appliances are an evolution of traditional firewall and VPN appliances into a product that has many additional capabilities such as: URL filtering, spam blocking, spyware protection, intrusion prevention, gateway antivirus, and a centralized management, monitoring, and logging function. These functions were traditionally handled by multiple systems.

## WHY UNIFIED THREAT MANAGEMENT?

### Unified Threat Management Solutions are Cost-effective

Integrating multiple security capabilities into a single appliance mean that you can purchase and use fewer appliances, eliminating the cost of building layered security with separately purchased solutions.

### Stops Attacks at the Network Gateway to Keep Your Business Moving

The multi-functional security approach offered by UTM appliances lets you avert catastrophe by blocking a broad range of network threats before they have the opportunity to enter your network. For example, malicious code will not have the opportunity to disable security at the desktop or server level. Your business-critical files and applications remain available to keep your staff on the job.

### Easy to Set Up and Use

Separate security systems means different management consoles to configure each system. Because the management paradigms of these systems are typically very different, it can be very time consuming to make sure the different security policies on each system work together and provide adequate protection. In addition, log information from each system will be stored in different formats in different locations, making detection and analysis of security events difficult.

Whether you are an IT expert or a security novice, a UTM solution with centralized management, monitoring and logging provides indispensable ease of use for configuring and managing your security. A UTM solution makes it easy to build coherent security policies, simplifies administration tasks such as log file management, auditing, and compliance reporting, and lowers operational costs when compared with the complexity of setting up separate security systems to defend against various specific threats.

## UNIFIED THREAT MANAGEMENT AND ZERO DAY PROTECTION

Most UTMs in the market today rely on signature- (or pattern-) based technologies to deliver key security functions such as URL filtering, spam blocking, spyware protection, intrusion prevention, and gateway antivirus.

### Signatures are only Part of the Solution

Signature-based solutions, for years the mainstay of every network security arsenal, use a database of known signature files to identify and block malicious traffic before it enters a network. They provide protection against threats such as trojans, buffer overflows, arbitrary execution of malicious SQL code, instant messaging and peer-to-peer usage (such as Napster, Gnutella, and Kazaa), and policy violations.

Once an exploit threat has been unleashed and identified however, it can take anywhere from a few hours to a few weeks for corresponding signature files to become available for download. This security “downtime” creates a window of vulnerability during which networks are open to attack:

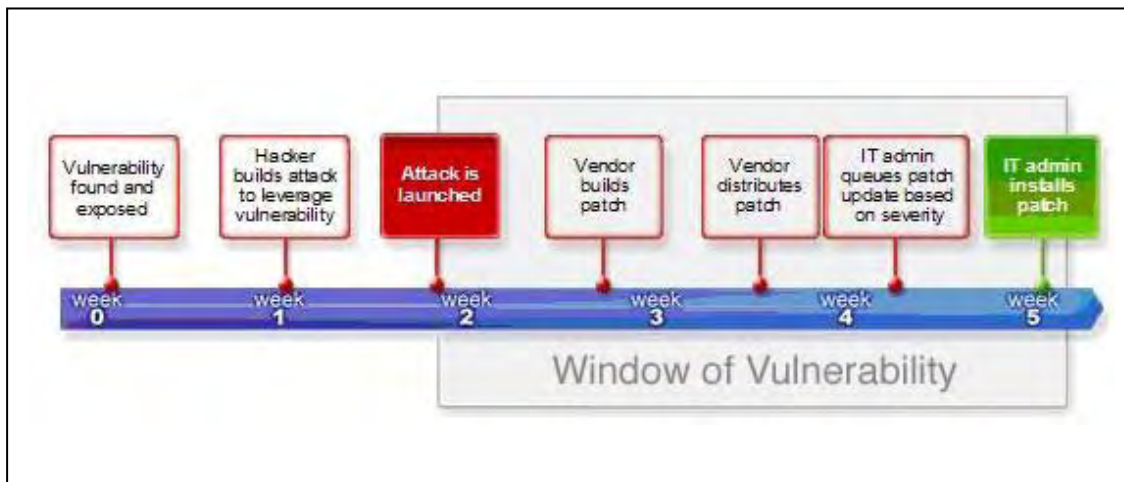


Figure 1: Attack Lifecycle and the Window of Vulnerability

In today's dynamic threat environment, with hundreds of new threats released every year, and worms able to propagate across the world in a few minutes, signatures are often not available soon enough. Protection mechanisms which can defend against new and unknown threats without requiring new signatures or configuration changes are required. This type of protective mechanism is known as Zero Day protection.

# WATCHGUARD UNIFIED THREAT MANAGEMENT

## Zero Day Protection

Although hundreds of new attacks are developed each year, the majority of these attacks fall into a few major classes. WatchGuard® Intelligent Layered Security offers Zero Day protection, as it is designed to protect against these major classes of attacks, and in many cases can offer protection against a brand new attack without requiring any updates or configuration changes.

## Intelligent Layered Security

The Intelligent Layered Security (ILS) engine at the heart of the WatchGuard family of UTM appliances provides powerful protection for growing enterprises, defending against both known and unknown attacks and giving maximum protection while minimizing impact on network performance.

Intelligent Layered Security performs proactive, in-depth diagnostic searches of the data stream and cooperatively shares information on suspicious traffic among its layers. Zero Day protection is provided through three key mechanisms:

- **Protocol Anomaly Detection** - Internet standards for data traffic are enforced to detect and block non-conforming traffic and isolate threats
- **Behavioral Analysis** - Hosts exhibiting suspicious behaviors are identified and stopped
- **Pattern Matching** - High-risk file types known to propagate viruses or attacks are flagged and deleted before they enter your network

Data flows smoothly while traffic is scanned, and viruses, worms, spyware, trojans, and other malicious attacks are proactively blocked at the edge of your network.

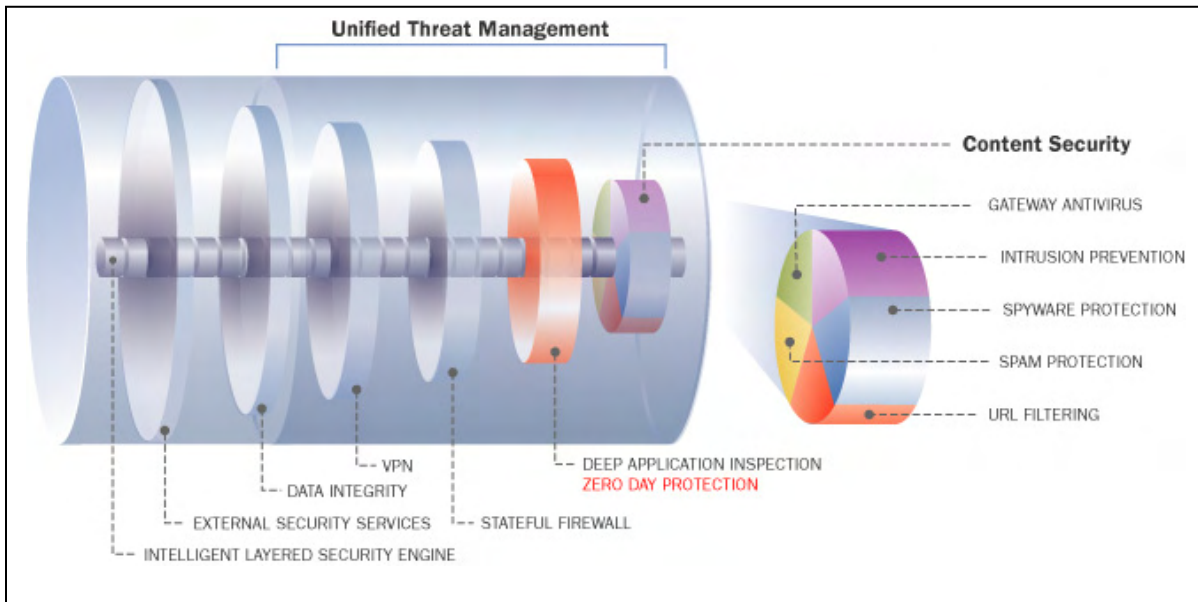


Figure 2: Intelligent Layered Security Architecture and UTM

The WatchGuard ILS architecture consists of six security layers working cooperatively with one another to dynamically detect, block, and report on malicious traffic while passing benign traffic through as efficiently as possible. Each layer performs different security functions:

1. **External security services** provide technologies that extend network protection beyond the firewall
2. **Data integrity** validates the data packet integrity and packet protocol conformance
3. **Virtual Private Networking (VPN)** ensures secure and private external communication
4. **Stateful firewall** restricts traffic to the sources, destinations, and ports allowed by the security policy
5. **Deep application inspection** ensures conformance with application layer protocol standards, rejects dangerous files by pattern or file type, blocks dangerous commands, and modifies data to prevent leakage of critical system information
6. **Content security** analyzes and regulates traffic for appropriate content; examples of this include signature-based technologies, spam blocking services, and URL-based content filtering

More details about the WatchGuard ILS architecture and its Zero Day protection capabilities can be found in our whitepaper titled [\*Introducing the WatchGuard Intelligent Layered Security Architecture: Better Security for the Growing Enterprise.\*](#)

## **Unified Threat Management Services**

WatchGuard offers a number of security services which are designed to augment the Zero Day protection capabilities of ILS. The services currently offered are gateway antivirus, intrusion prevention, anti-spam, URL filtering, and spyware protection.

### ***Gateway Antivirus and Intrusion Prevention Service***

This service combines two key capabilities; let's look at each one in turn.

#### **Gateway AntiVirus Capabilities**

Identifies and blocks worms, spyware, and trojans within e-mail attachments, therefore blocking threats from entering your network and executing dangerous payloads. The integration of Gateway AntiVirus (AV) with other security layers in ILS provides some important benefits, namely:

- **Efficiency** - The Gateway AV service only scans files not blocked by the ILS pattern matching capabilities, greatly reducing the number of files which need to be scanned
- **More granular control** - Gateway AV finds viruses in file types which you may choose to allow into your network such as .zip, .doc, etc.

The WatchGuard antivirus database contains thousands of virus, spyware, worm, and Trojan signatures, including both Wildlist and "zoo" viruses. A broad range of compression/decompression algorithms is supported, including ZIP, RAR 2.0, TAR, GZIP, ARC, and CAB files. Signature delivery is automatic, and signature update checks can be programmed for any desired interval. The targeted threat response time is 8 hours, which is significantly better than industry average.

## **Intrusion Prevention Capabilities**

WatchGuard Intrusion Prevention Service (IPS) provides in-line protection from attacks that comply with protocol standards but carry malicious content. It is a signature-based service designed to protect against a broad range of attacks including cross-site scripting, buffer overflows, and SQL injections.

The IPS can selectively block IM services, such as AIM, Yahoo, IRC, and MSN Messenger. This protects against IM-based security threats, including exploits which allow the attacker to gain control of a machine running an IM client, and infections by viruses transferred in files over IM.

Peer-to-Peer (P2P) applications such as Napster, GnuTella, Kazaa, Morpheus, BitTorrent, eDonkey2000, and Phatbot can also be blocked. Peer-to-Peer presents two problems. First, it uses up valuable bandwidth that is better used for business purposes. Second, it is a well-known vector for transmitting spyware (Kazaa in particular). By blocking P2P, we solve both of these problems.

The IPS can also detect and block outbound spyware communication to malicious hosts, preventing sensitive data from being sent out by spyware programs. This activity can be logged or alerted on so that the system administrator can identify and remediate infected machines.

The WatchGuard proprietary intrusion prevention engine integrates tightly with other ILS functions, reducing false positives and speeding execution while producing comprehensive log information.

## **Anti-Spam Service**

Spam accounts for more than 63% of all e-mail today, and represents a major problem for most companies. The WatchGuard spamBlocker service utilizes [CommTouch®](#) Recurrent Pattern Detection (RPD™) technology for real-time anti-spam detection that provides powerful protection from spam attacks. Rather than evaluating keywords and content, this technology analyzes large volumes of Internet traffic in real time to identify the repetitive components, or DNA, of each outbreak as soon as they emerge. Close to 500 million messages per day are sampled, and advanced algorithms detect, identify, and classify new outbreaks - typically within 1-2 minutes. These algorithms are also capable of distinguishing solicited bulk e-mail from spam. spamBlocker utilizes this technology to give you up-to-the-minute protection from spam attacks by comparing suspected spam directly with the CommTouch® Detection Center (which has approximately 20,000,000 spam classifications) in real time. This technology provides four key benefits:

- **Extremely fast response** to new outbreaks
- **Near zero false positives** make it the best service in the industry at distinguishing legitimate communication from spam attacks
- **High spam detection rate** protects networks from 97% of unwanted e-mails
- **Language agnostic** to block spam regardless of the language, content, or format of the message

## **URL Filtering Service**

The WatchGuard WebBlocker URL filtering capability enables you to configure not only who gets Web access and who doesn't, but also what type of Web access is available. Using an intuitive set of controls, you can quickly select which categories of Web pages users get access to, and what time of day they get access. WebBlocker utilizes site database and engines from the global Web-filtering leader, [SurfControl™](#), to ensure the most accurate categorization and complete coverage. WebBlocker uses numerous categories to help you block content you don't want to allow on your network. For example, blocking pornography can assist in enforcing company policy on sexual harassment in the workplace, and blocking sports content may increase workplace productivity. With the WebBlocker customizable exceptions lists, per-person authentication, and

