WatchGuard®

PRODUCT DATASHEET

Zero Day Protection

- **Robust, proactive network security**
- **Protects you from new and unknown threats**
- **Closes the window of vulnerability**
- **Far better security than signature-only products**

The Most Powerful Asset in Your Network Defense System

WatchGuard® provides true Zero Day protection through the Intelligent Layered Security capabilities of its Firebox® X Unified Threat Management appliances, shutting down many new and unknown attacks without the need for a signature.

What "Zero Day" Is All About

There's a lot of buzz in the security industry about "Zero Day" attack protection, but vendors differ substantially in the protection they really provide.

- Zero Day threats are new or unknown attacks for which a patch or signature has not been written
- Zero Day protection, therefore, means being protected against a new and unknown threat before the vulnerability is discovered and the exploit is created and launched

True Zero Day Protection Is Built into the Firebox® X Architecture

The Intelligent Layered Security of the Firebox X combines key security capabilities able to defend against classes of attacks and to protect against variants even before they are known. Some of these capabilities include:

- **Protocol anomaly detection** blocks malicious traffic that does not conform to established protocol standards
- **Pattern matching** flags and removes high-risk files, such as .exe and scripting files, viruses, spyware, and trojans from the system by fully inspecting the entire packet
- **Behavior analysis** identifies and stops traffic from hosts exhibiting suspicious behaviors, including DoS and DDoS attacks, port scans, and address scans

What Signatures Bring to a Security Solution

Some vendors make Zero Day claims but in reality their security solutions rely solely on signature-based scanning.

Signature-based security technologies fingerprint each new attack after it emerges, so protection comes when this fingerprint, or signature, is added to the system. This is not Zero Day protection. By their nature, signatures are reactive; they cannot protect against new and unknown attacks without an update.

Signature-based scanning provides a granular layer of protection against spyware, viruses, worms, trojans, and blended threats by identifying known malicious code within business-critical traffic and files. But this technique is only one piece of a comprehensive Unified Threat Management solution.

22 of the 30 most significant viruses and their variants released in 2003 to 2006 were blocked by default on the Firebox®, protecting our customers before signatures were made available.*

The Window of Vulnerability

Signature-based solutions block what has already been identified. Your network is still exposed from the time a new exploit has been launched until a signature or patch is developed and then deployed.

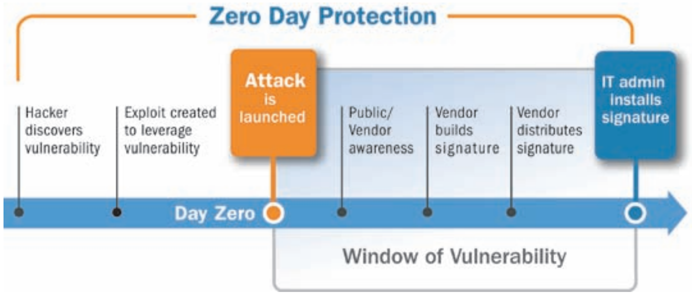
Considering the speed and destructiveness of today's attacks, even a few minutes without protection can be devastating. The reality is, it can sometimes be hours, days, even weeks before a signature or patch is developed and deployed, making this window of vulnerability every IT manager's nightmare.

Robust, Up-front Protection

True Zero Day protection that's in place even before the vulnerability is known is at the heart of our Firebox X security solutions. Get it working for you – visit **www.watchguard.com**

*Based on most commonly used method of propagation (SMTP)

WatchGuard protects you in the window of vulnerability


Zero Day Protection
Hacker discovers vulnerability
Exploit created to leverage vulnerability
Attack is launched
Public/ Vendor awareness
Vendor builds signature
Vendor distributes signature
IT admin installs signature
Day Zero
Window of Vulnerability

Zero Day protection means being protected against a new and unknown threat during the window of vulnerability.

WatchGuard

Stronger Security, Simply Done™

WatchGuard®
PRODUCT DATASHEET

Unified Threat Management

- **Fully integrated, multifaceted protection**
- **Most complete security in its class**
- **Includes built-in Zero Day attack prevention**
- **Powerful security services add even more protection in critical attack areas**
- **Unified management, monitoring, and logging capabilities**

WatchGuard
Stronger Security, Simply Done™

Powerful Security with True Zero Day Protection

WatchGuard's Firebox® X Unified Threat Management solutions provide the most comprehensive security in their class – for fully integrated, multifaceted protection from network threats, including:

- ✔ **Spyware**
- ✔ **Trojans**
- ✔ **Worms**
- ✔ **Bots**
- ✔ **Viruses**
- ✔ **Spam**
- ✔ **Blended threats**
- ✔ **Web-based exploits**
- ✔ **SQL injections**
- ✔ **Buffer overflows**
- ✔ **DoS/DDoS attacks**
- ✔ **Policy violations**

What is Unified Threat Management?

Unified Threat Management (UTM) is an emerging trend in the network security market. UTM appliances have evolved from traditional firewall and VPN appliances into a solution that has many additional capabilities, including URL filtering, spam blocking, spyware protection, intrusion prevention, and gateway antivirus, as well as integrated management, monitoring, and logging capabilities – all functions previously handled by multiple systems.

Built-in Zero Day Protection is the Foundation

We start with powerful security. The Intelligent Layered Security (ILS) in the Firebox X offers true Zero Day protection right out of the box. It protects against new and unknown threats before the vulnerability is discovered and the exploit is created and launched. Many vendors only provide signature-based protection. These reactive solutions actually leave their customers exposed to new types of threats until the exploit becomes known, a signature is written, and the signature update deployed.

Layers of Powerful Defenses Working Together

Unlike many UTM appliances on the market today, with ILS in the Firebox X the security layers work together to strengthen overall security. With software capabilities coordinated, each component can lend support to the overall security structure. For example, when Intrusion Prevention Service identifies an attack, it can tell the firewall what to do about it.

Cooperative communication between layers reduces and fine tunes the processing required by the security functions. The result – you get the protection you need to stay safe while optimizing performance.

Powerful Security Services to Boost Defenses

Our flexible solutions allow you to easily add any of our security services to enhance protection in critical attack areas, and manage them from one integrated management console.

Security services include:

- ***spamBlocker:*** Best service in the industry at distinguishing legitimate communications from spam attacks in real time, blocking up to 97% of unwanted e-mails, with incredibly low false positives.
- ***Gateway AV/IPS:*** Robust, signature-based protection at the gateway against known viruses, spyware, trojans, and Web-based exploits.
- ***WebBlocker:*** Increase productivity and decrease security risks by blocking access to malicious Web content and managing your users' Web surfing.

The Role of Integrated Management

Whether you are an IT expert or a security novice, you'll find the integrated management, interactive real-time monitoring, and logging capabilities of our UTM solutions provide indispensable ease of use when configuring and managing your security.

- Manage multiple appliances from a central location
- Easily create and implement security policies globally, making it simple to build coherent policies
- Rely on interactive real-time monitoring and logging
- Use just one intuitive interface to install and manage all your security capabilities, including security services

Important Scalability and Cost Advantages

Running multiple software and security appliances introduces time and budget costs to your IT overhead. Other UTM solutions may charge per-user licensing fees or require you to pay for centralized logging and reporting capabilities. WatchGuard UTM solutions have no per-user or management software costs, and only have one graphical user interface to learn. Each integrated, centrally managed security capability provides network-wide protection for all users configured behind your Firebox X.

You're only limited by your traffic capacity. When you reach that capacity, you simply activate a model-upgrade license key to a higher model to unlock additional throughput and capacity. This is the least labor-intensive and most cost-effective way to protect your network security investment.

ADDRESS: 505 Fifth Avenue South, Suite 500, Seattle, WA 98104 · WEB: www.watchguard.com
U.S. SALES: 1.800.734.9905 · INTERNATIONAL SALES: +1.206.613.0895

No express or implied warranties are provided for herein. All specifications are subject to change and any expected future products, features or functionality will be provided on an if and when available basis. ©2006 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, the WatchGuard Logo, Firebox, Fireware, LiveSecurity, and Stronger Security, Simply Done are either trademarks or registered trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries. All other trademarks and tradenames are the property of their respective owners. Part No. WGCE66355_0506