

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



Earth-friendly technology

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 (UTM) 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 means being protected against a new and unknown threat during the window of vulnerability.



Stronger Security. Simply Done™