



Contact Itplanit 1-877-842-9772

Today for a free estimate



**WatchGuard®
Firebox® X Peak™
e-Series**

Stronger Security, Simply Done™

Security Concerns

Business Concerns

Network uptime
Administrative cost
Maximizing productivity
Safeguarding info
False positives block communication
Web surfing
TCO



IT Concerns

Security
Network uptime
Scalability
Troubleshooting
Setup and deployment
OS updates / readiness
Response time
Complex networks
Mobile users

Security is complex. Budgets are constrained. IT is understaffed.

What is **Unified Threat Management (UTM)**?

Unifying and integrating multiple security features onto a single hardware platform

- Firewall / VPN
- AntiVirus
- Intrusion Prevention Service (IPS)
- URL filtering
- Anti-spam
- Anti-spyware

Why do **UTMs** make sense?

- Comprehensive security that works cooperatively
- Reduced TCO (Total Cost of Ownership)
- Simplified administration
- More efficient technology
- Enables you to spend more time managing your business, not your network security



Firebox® X Peak™ e-Series



Key Advantages

- **Integrated Unified Threat Management solution** delivers the most comprehensive security in its class
- **True Zero Day protection** with Intelligent Layered Security (ILS) eliminates the window of vulnerability
- **Powerful performance and advanced networking features** support complex customer environments
- **Unified, central, intuitive security management** with WatchGuard System Manager
- **Scalable & upgradeable** to protect your investment
- **Industry-leading support** to keep you up and running



Integrated Unified Threat Management (UTM)

Firebox® X: The most comprehensive security in its class

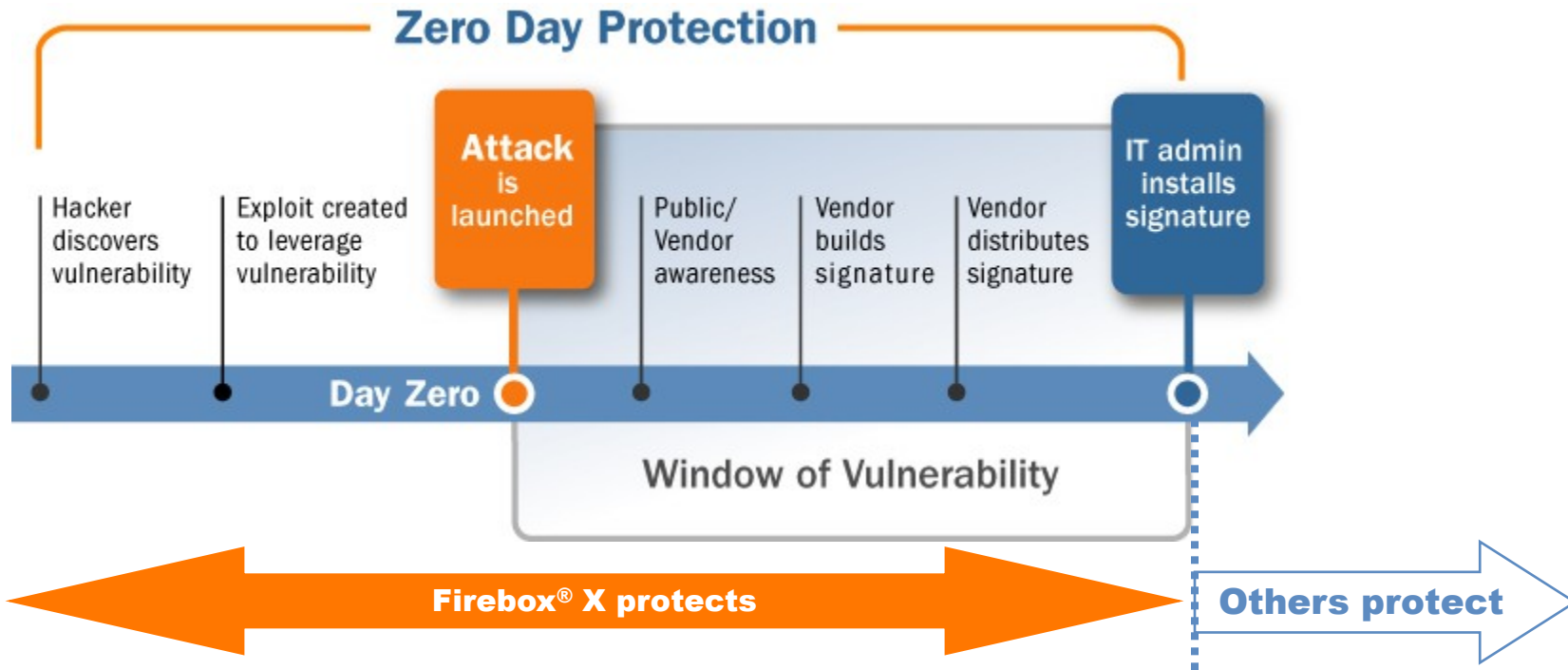
Integrated security capabilities – more than just a firewall!

- **Intelligent Layered Security** proactively protects your network
 - Deep Packet Inspection
 - Protocol Anomaly Detection (PAD)
 - Behavioral Analysis
 - Pattern Matching
 - Shunning
- **Additional security services**
 - Gateway Anti-Virus/Intrusion Prevention Service with anti-spyware capabilities
 - WebBlocker – URL filtering
 - SpamBlocker
- **Unified management platform with WatchGuard System Manager** - provides singular interface for management, logging, and alerting across all security services – *unlike* most competitors



Stronger Security

True Zero Day Protection



Superior, proactive protection against new & unknown threats

- Before a signature or patch is developed and deployed, so no window of vulnerability for the network being attacked
- Proxies thoroughly analyze packets – unlike most competitors
- Proactive approach; more comprehensive than reactive signature-based technologies that rely on fingerprinting each new attack as it emerges

Zero Day protection means stronger security

Real World Examples

WatchGuard Intelligent Layered Security proactively blocks:

E-mail-borne viruses at the gateway – in default configuration:

- Beagle, Nimda, Sober, My Doom, Bable, Netsky.x, Fizzer, and variants

Top 10 spyware programs*:

- PurityScan, N-Case, Gator, CoolWebSearch, Transponder, ISTbar, KeenValue, Internet Optimizer, Perfect Keylogger, TIBS Dialer

Network attacks that do not comply with protocol standards

...all without waiting for signatures

*Reported by Webroot



Performance & Ports

Power up!



Firebox X Peak is the highest-performance line of UTM appliances from WatchGuard, providing the most comprehensive, powerful security in its class.

High Performance Security Appliance

- Up to 2.0 Gbps firewall performance
- Up to 600 Mbps VPN performance

Full Gigabit Ethernet (10/100/1000) Interface Support

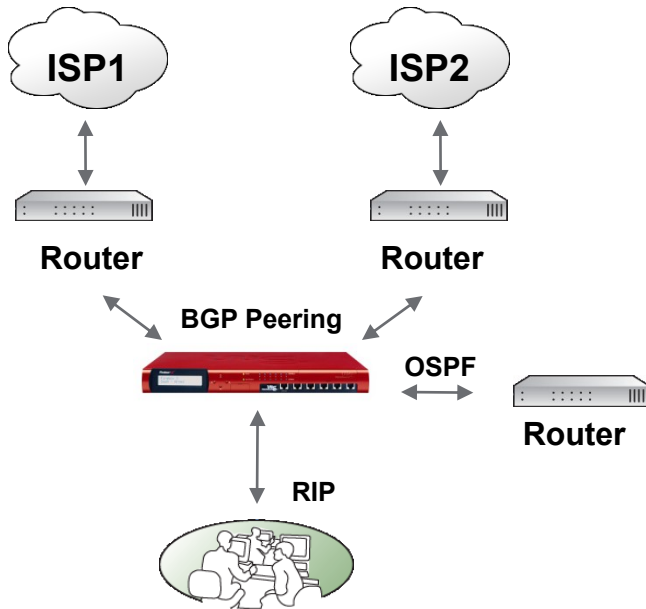
- 8 x GigE (10/100/1000) on all Peak e-series models

Fiber Interface Model (Firebox 8500e-F)

- 4 RJ-45 copper GigE (10/100/1000) interfaces
- 4 SPF GBIC fiber optic interfaces

Advanced Appliance Software

Fireware® Pro



Superior Dynamic Routing

✓ *New Fireware 9.0 advanced networking features!*

• Fireware Pro serves complex networks and includes:

- **VPN Enhancements** – Improves network redundancy
 - ✓ VPN failover
 - ✓ IKE 3rd party certificates
 - ✓ Drag-N-Drop VPN tunnel management Integrated with High Availability
 - ✓ Drag & Drop VPN tunnels w/Firewall rules
- **Traffic Shaping** – Optimizes your network and cut costs
 - ✓ VLAN
 - ✓ Policy based routing
 - ✓ Multi-WAN
 - ✓ QoS
 - ✓ Load balancing
- **Dynamic Routing (BGP, OSPF, RIP)** - Maximizes network flexibility, redundancy, and efficiency by dynamically updating routing tables
 - **High Availability (Active/Passive)** - Offers hardware redundancy to a standby appliance
- **Traffic Management and Prioritization** - Ensures business-critical applications get the bandwidth they need
- **Multi-Wan Failover** – Provides back-up to keep you up and running

WatchGuard® System Manager

Intuitive, easy-to-use management software

Intuitive graphical interface

- Easy to learn; easy to use

Unified management console

- Centrally manage your entire network of Edge, Core and Peak e-Series appliances
- No need to maintain separate software for multiple point solutions

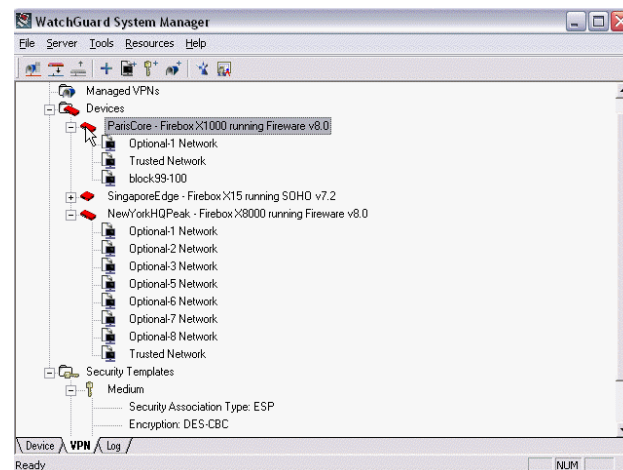
Interactive real-time monitoring

- Immediately see and understand what's happening in your network

Drag-and-drop VPN

- Create secure branch office VPN tunnels quickly and easily
- ✓ With support for High Availability and firewall rules

Secure, flexible logging and comprehensive reporting



Real-time VPN creation

"WatchGuard has possibly the best monitoring and reporting packages available." - InfoWorld, March 2006

- ✓ *New Fireware 9.0 advanced networking features!*



Scalable & Upgradeable

Protects your investment – Grows with you

All available through convenient, downloadable license keys:

Model Upgrades

- Upgrade within the product line as your performance requirements increase, extending your investment

Service Upgrades

- Add additional security functions to combat new and emerging threats quickly and easily

Advanced Appliance Software Upgrade

- Firewall Pro upgrade provides the feature requirements needed in more demanding networks environments



LiveSecurity® Service

Expert Guidance and Support

Security Broadcasts – alert you to threats

- Dedicated group of network security experts monitors the Internet to identify emerging threats
- Timely broadcasts alert you to new vulnerabilities

Software Updates – ensure you have the latest enhancements

- Functional enhancements
- Updates to address specific threats when they occur

Technical Support – gives you timely expert advice

- Highly-trained team of support representatives
- 4-hour targeted maximum response time; 1 hour for Gold Level
- Responsive expertise to support mission-critical systems

Training, Tutorials, and Self-Help Resources

Remote Code Execution Flaw Afflicts Microsoft Publisher

Severity: **High**

12 September, 2006

Summary: ([Audio version](#))

Today, Microsoft released a security bulletin describing a vulnerability in Microsoft Publisher, a component of their Office suite of applications. By enticing one of your users into opening a specially malformed Publisher document (.PUB), an attacker could exploit this flaw to execute code with the victim's privileges, potentially gaining control of your user's computer. If you use Office in your network, you should download, test, and deploy the appropriate patch as soon as possible.

Exposure:

Microsoft Publisher is a desktop publishing application that ships with Microsoft Office. According to Microsoft's [security bulletin](#), Publisher doesn't perform sufficient data validation when parsing the contents of a Publisher document (.PUB). Opening a maliciously crafted Publisher document could trigger this flaw and corrupt memory in a way that allows an attacker to inject and execute code. In other words, if an attacker can trick one of your users into opening a malicious Publisher document, he could exploit this flaw to execute code with your user's privileges. If your users have local administrative privileges, the attacker could exploit this flaw to gain full control of their machines.

Solution Path

Microsoft has released patches to correct this vulnerability. Download, test, and deploy the appropriate patch as soon as possible.

- [Office 2003](#)
- [Office XP](#)
- [Office 2000](#)

For Firebox SOHO and Firebox X Edge Users:



Comprehensive Protection for Today's Threats

A Powerful UTM Solution

Security Services

Content-based attacks

Trojans within business critical file-types	Suspicious login attempts
Buffer overflows	Web messenger activity/traffic
Cross-site scripting attacks	P2P activity/traffic
SQL Injections	Viruses embedded in business critical files (i.e., .PDFs, .DOCs, etc.)
HTML injections	HTML injections from malicious URL's
Remote Code Execution	Spyware
Privilege Elevation	
Protocol command decoding	

Out of the Box Protection: Firebox® X Core™

Content-based attacks

Fingerprinting
Protocol Anomalies
Malformed packets
Suspicious attachment types
Malicious Active X code
Spyware/Adware

Rate-based attacks

SynFlood
DoS, DDoS
Buffer overflows
Fragmentation attacks

Behavior-based attacks

Port-Scans
Address space probes
Spoofing attacks

Policy-based attacks

TCP hijacking
State-based attacks
ICMP attacks (Ping of Death)

Why WatchGuard®

- **Experts focused on network security for more than a decade**
- **Profitable, private company focused on your network security needs**
- **A recognized leader for the SMB security market**
- **Proven innovators**
 - The first to introduce security appliances to the marketplace
 - Over a dozen patents
- **Trusted allies for small and mid-sized businesses worldwide**



Our Customers Say It Best



“Gigabit-capable firewalls aren’t rare anymore, but, as we found, easy to manage, affordable, scalable gigabit firewalls certainly are. The WatchGuard appliance was the only one we found that met our specific needs and requirements.”

Kendall Miller, CIO of
Benelogic

“The central management feature of the WatchGuard appliances has not only cut down the time necessitated for monitoring and change management, but has enabled us to reduce our traditional spending by 48% per year.”

Charles Parris, Network
Administrator at Boys &
Girls Club of King County
(Washington)

To find out more about our security solutions,
visit us online at www.watchguard.com

The WatchGuard® Advantage



Stronger Security

The most comprehensive Unified Threat Management security solution available on the market today.

Simply Done

Easy to use security management console for all Firebox X appliances and security services.





Thank You!

Stronger Security, Simply Done™

ADDITIONAL SLIDES



What is **Unified Threat Management**?

Unifying and integrating multiple security features onto a single hardware platform

- Firewall
- VPN
- Anti-virus
- IPS
- URL filtering
- Anti-spam
- Anti-spyware

WatchGuard's Unified Threat Management



WatchGuard's Unified Threat Management

Investment protection

Expert guidance and support with LiveSecurity®

Zero Day attack protection

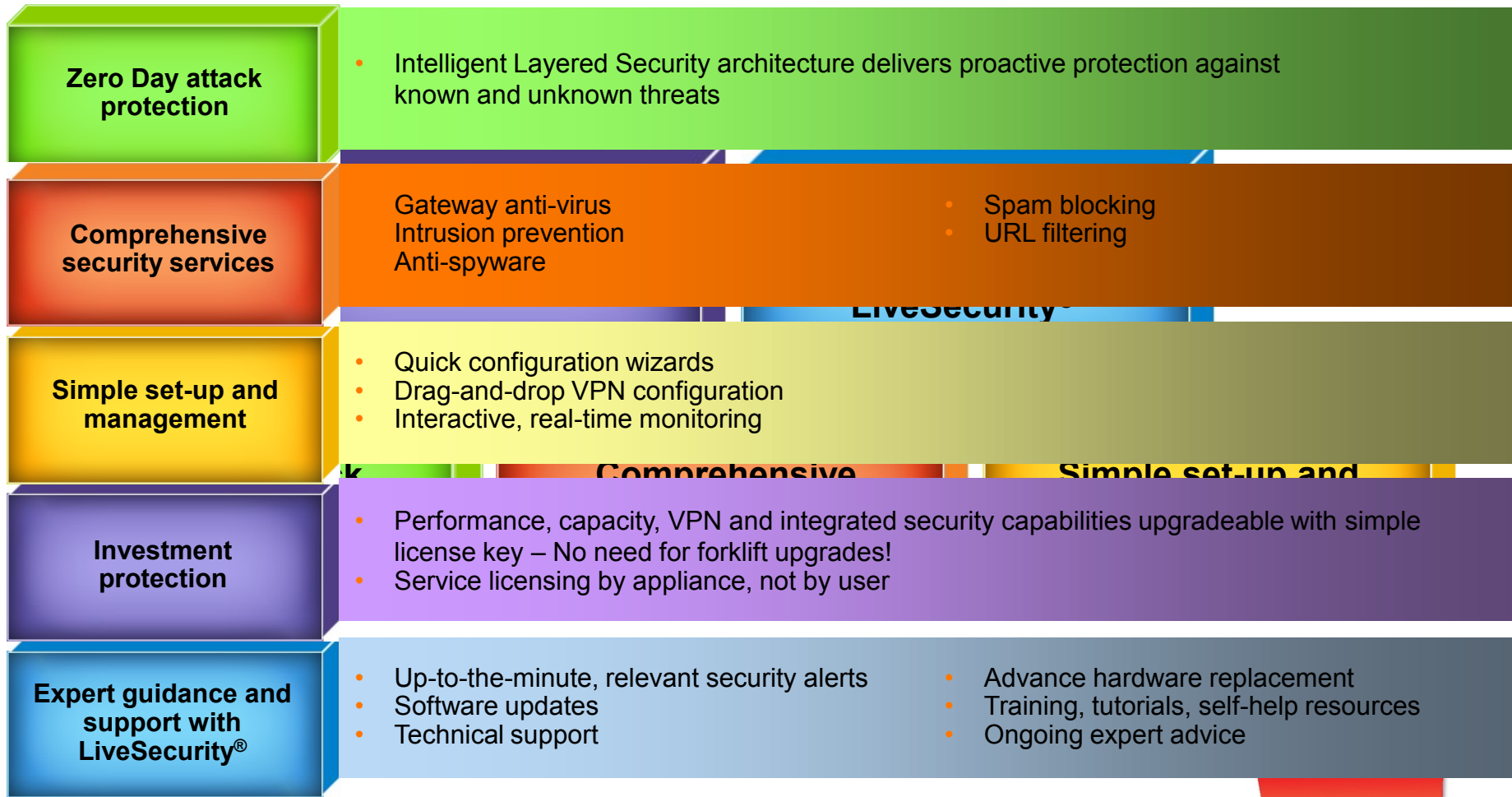
Comprehensive security services

Simple set-up and management

WatchGuard...offers solid default settings, efficient scrutiny of network packet streams, improved intrusion prevention and built-in malware defenses against both known and unknown viruses and spyware.

- Charles Kolodgy, IDC

WatchGuard's Unified Threat Management Advantages





Contact Itplanit 1-877-842-9772

Today for a free estimate



Thank You!

Stronger Security, Simply Done™