



THE INTEGRATED SECURITY APPLIANCE
THE BEST SOLUTION FOR SMALL- TO MID-SIZED
ENTERPRISES

MARCH 2004

THE INTEGRATED SECURITY APPLIANCE

THE BEST SOLUTION FOR SMALL- TO MID-SIZED ENTERPRISES

EXECUTIVE SUMMARY

As a business owner, you know that the network security landscape is growing more sophisticated, and security defenses are becoming more complex to operate and costly to install. What's more, a security attack on your company can mean the difference between staying in business or not. The stakes are high, and the ultimate goal is to deploy security solutions that will protect the stability of your network and the security of your data.

Your small- to mid-sized enterprise (SME) is vulnerable to the same security threats as large enterprises, but you typically don't have the same budget or in-house expertise when preparing your defense. You certainly want to deploy the latest protection against the constant onslaught of emerging threats, but you remain very much concerned about how a security purchase will affect your bottom line.

Today, typical security deployments require you to merge disparate security functions and call on specialized personnel, which can translate to higher costs and leave you less time to focus on your core business.

This paper describes a new approach to protecting your network; an Integrated Security Appliance that delivers the advanced security capabilities small- and mid-sized enterprises need, at a price they can afford.

SME SECURITY CONCERNS

Small- to mid-sized enterprises around the world range from retail and e-commerce storefronts to food distribution, medical suppliers to instructional institutions. They include community colleges and universities, healthcare facilities and hospitals, government agencies and service industries. Regardless of their size or purpose, they must all be concerned about security, and their capacity to deal with it. Common issues include:

- Inadequate budget for purchasing appropriate security solution
- Lack of expertise and focus to keep up with changing security threats
- Lack of time and personnel to maintain a truly secure multi-vendor, multi-layer network defense

As a result, your business may be even more vulnerable than your larger counterparts, because of limitations in the amount of protection you can implement. But network attacks can cripple or destroy a small business that is reliant on Internet connectivity. Downtime caused by an attack almost always results in lost productivity and revenue. You may find yourself liable for failing to comply with security and privacy regulations, which can result in fines or court costs. Finally, cleanup costs can be extremely high, and in some cases lost data is unrecoverable.

Figure 1 outlines the major security concerns of small- to mid-sized businesses as they relate to data integrity, productivity, and policy enforcement.

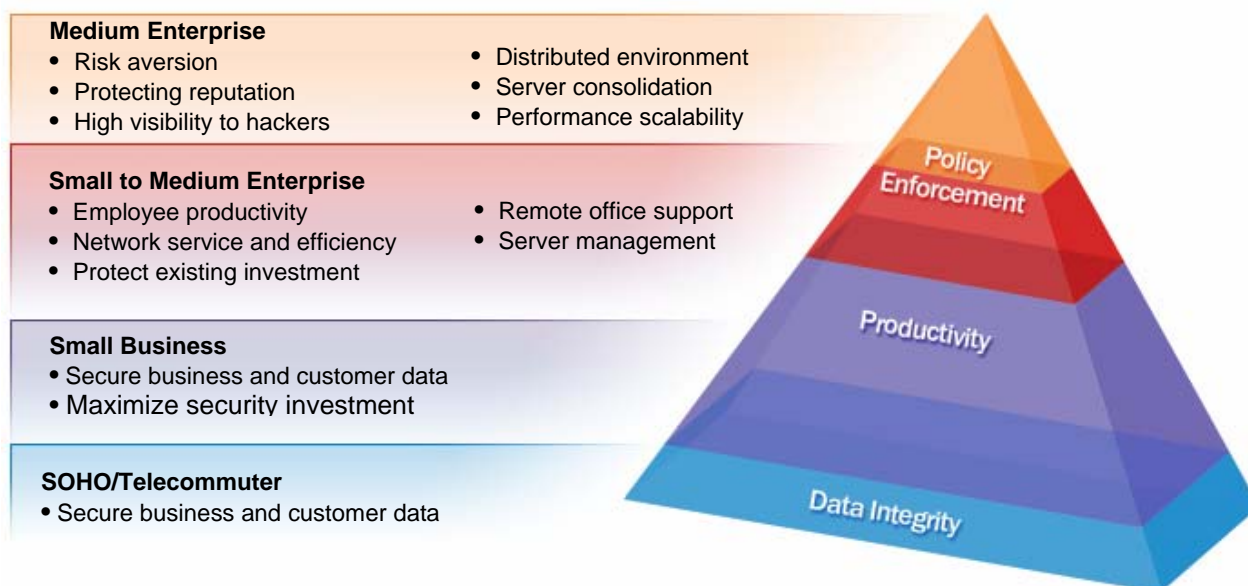


Figure 1. SME security concerns

Any loss of customer confidence can potentially destroy your ability to produce revenue. If your business is attacked and crucial customer data is compromised, you may be less able to compete in your marketplace.

You should also consider the management process associated with installing and maintaining a security system. If you are the sole IT resource for your business, or even if you have some IT resources, you probably can't afford the time required to keep a patchwork security system up to date, nor will you want to deal with multiple support contacts if you need assistance. Everyone needs to understand that outdated security is about as effective as no security.

However, like most of today's business owners, you are giving careful thought to your IT purchasing decisions. You want evidence that a security investment will show measurable improvements to your bottom line

TODAY'S SECURITY ENVIRONMENT

TYPES OF THREATS

A wide variety of complex, sophisticated attacks threaten today's business networks, and new attack types continue to emerge almost daily. Some common current threats include:

- **Malicious code** including viruses, worms, and Trojans that are hidden within files or innocuous code. Once they enter a network, they can self-propagate, and are capable of compromising individual workstations or an entire network.
- **Denial and Distributed Denial of Service (DoS, DDoS) attacks** can disable an entire network and severely disrupt the normal daily operations of a business. DoS attacks are hacker attempts to flood a network with illicit traffic, while denying legitimate users access.

- **Internal and external hacking**, or unauthorized access, to critical data and systems for the purpose of theft, duplication, or destruction. Successful hacks can cause downtime, loss of employee productivity, and considerable cleanup and data recovery expense.
- **Blended threats**, such as Nimda and Code Red, often combine the characteristics of worms, viruses, Trojans, and other malicious code to launch rapidly spreading attacks that cause widespread damage. These threats are especially adept at exploiting security technologies that work independently of each other on a network.

LAYERED SECURITY – THE BEST DEFENSE

The best way to protect your network against such a wide variety of threats is with effective, efficient layered security. Layered security uses multiple technologies to set up defenses at each level of your network where vulnerabilities are likely to exist. Much like setting up a variety of defenses around your property, such as guard dogs, automated alarms, motion detectors, and deadbolts, layered security is known in the industry today as a “multiple point security solution.”

TRADITIONAL MULTI-POINT LAYERED SECURITY

Many SMEs try to implement security systems by mixing disparate point solutions from several vendors. These products must all be purchased, installed, managed, and updated separately. This approach generates difficulties with interoperability, incomplete protection, and time-consuming testing and verifying patches across multiple technologies, all of which can slow a network’s response to attacks. Products that aren’t designed to work with each other can impact the performance rates of a network. The costs involved in implementing enough of these products to provide comprehensive protection can, and often do, become prohibitive for a small- to mid-sized enterprise. The complexity of such a design is shown in Figure 2 on the following page.

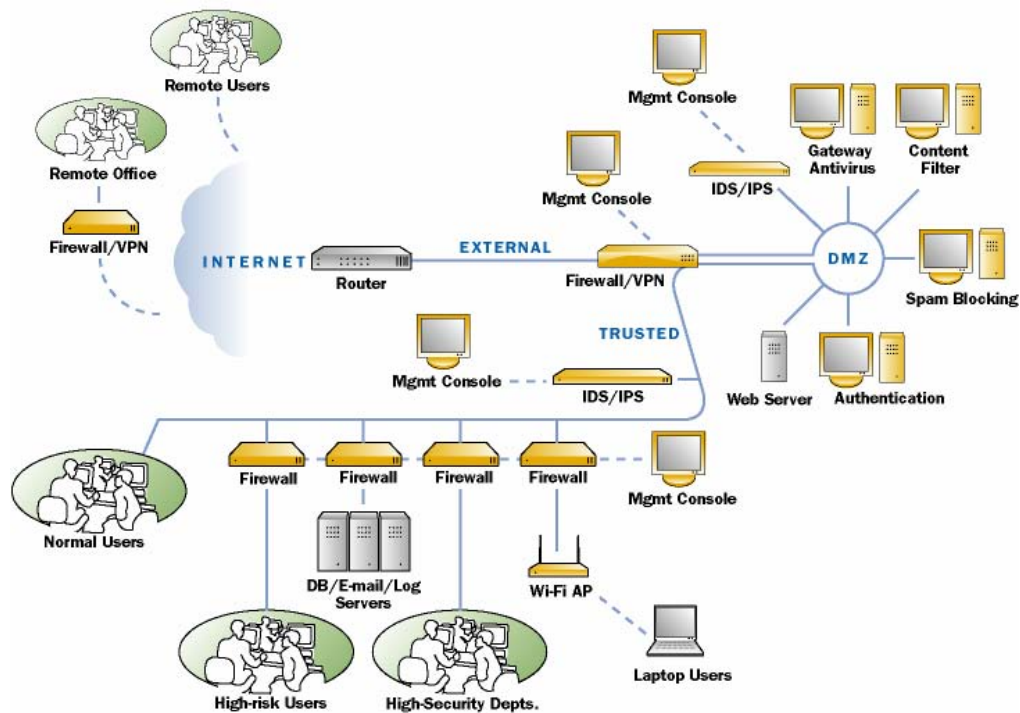


Figure 2. Traditional multi-point security solution

SMEs rarely have the IT infrastructure to maintain and manage such a disparate mix of products, each with their own management stations. What's more, with a multiple point solution, you must also manage multiple support contacts, which can cost even more time and money. Labor costs mount up quickly when you have to re-deploy hardware in the field, revisit a tangled-wire server farm to yank out a box and put in a new one, or learn a new management interface because you outgrew your old firewall and had to change brands. Combining multiple point solutions for layered security is simply too costly and complex for the average SME.

INTEGRATED SECURITY APPLIANCES

The basic concept of an integrated security appliance is not new. It simply means combining multiple security functions into a single solution or appliance. Some security vendors have introduced so-called integrated security appliances in the past. However, these immature solutions have included many shortcomings, especially if function integration is inefficient and poorly implemented. These shortcomings may include:

- **Inadequate performance**
- **Decreased reliability**
- **Limited scalability**
- **Increased management complexity**
- **Insufficient security**

In many cases, vendors have attempted to “integrate” by combining older, complex technologies they may possess through acquisition or licensing. The true integrated security appliance should be built from the ground up to be multifunctional, so that all technologies work together in the most efficient manner. This appliance should have an extensible architecture that allows the new capabilities to be added quickly and easily as the need arises. A true integrated security appliance must provide powerful layered defense against current and future threats, while delivering an economy of scale and scope that can be passed on to the SME customer. In the best of all worlds, the appliance is also model-upgradeable, prolonging the life of the initial hardware investment, and making expanded functionality even easier to implement.

Figure 3 shows a SME security solution managed by a WatchGuard® integrated security appliance, the Firebox® X.

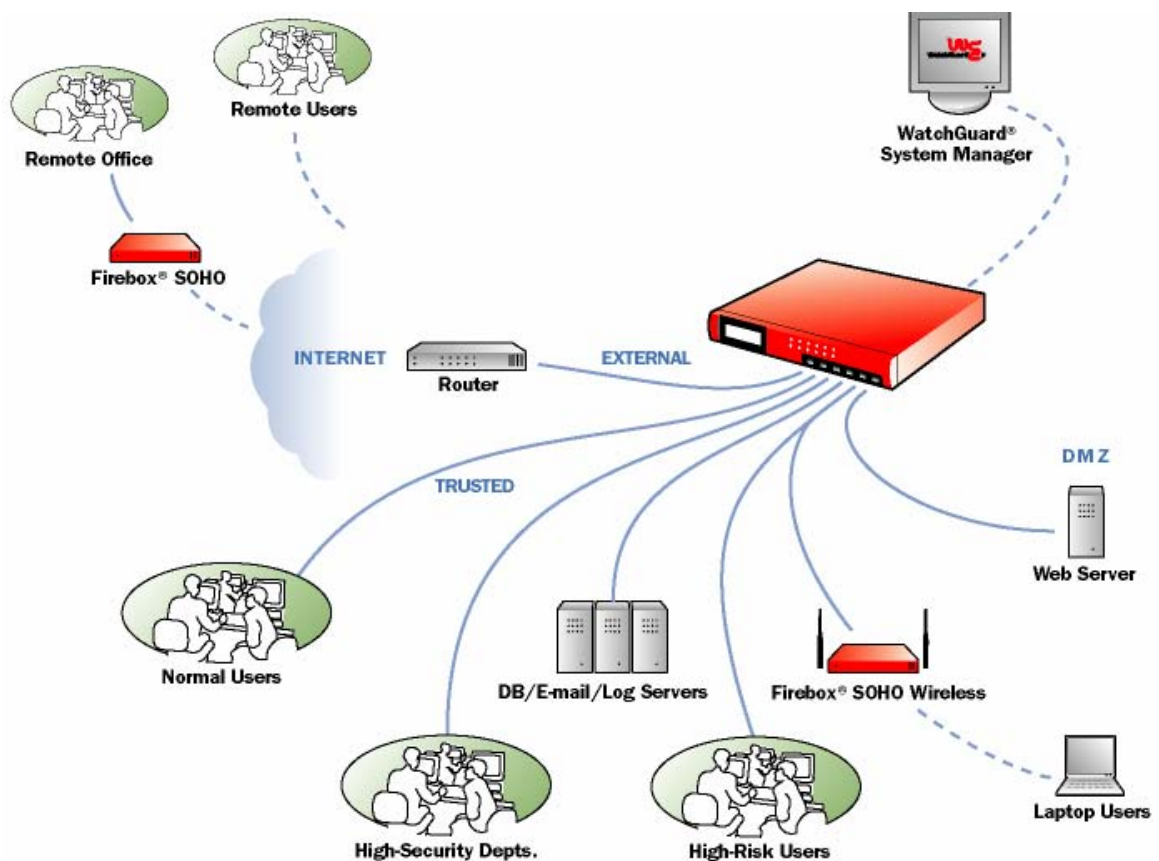
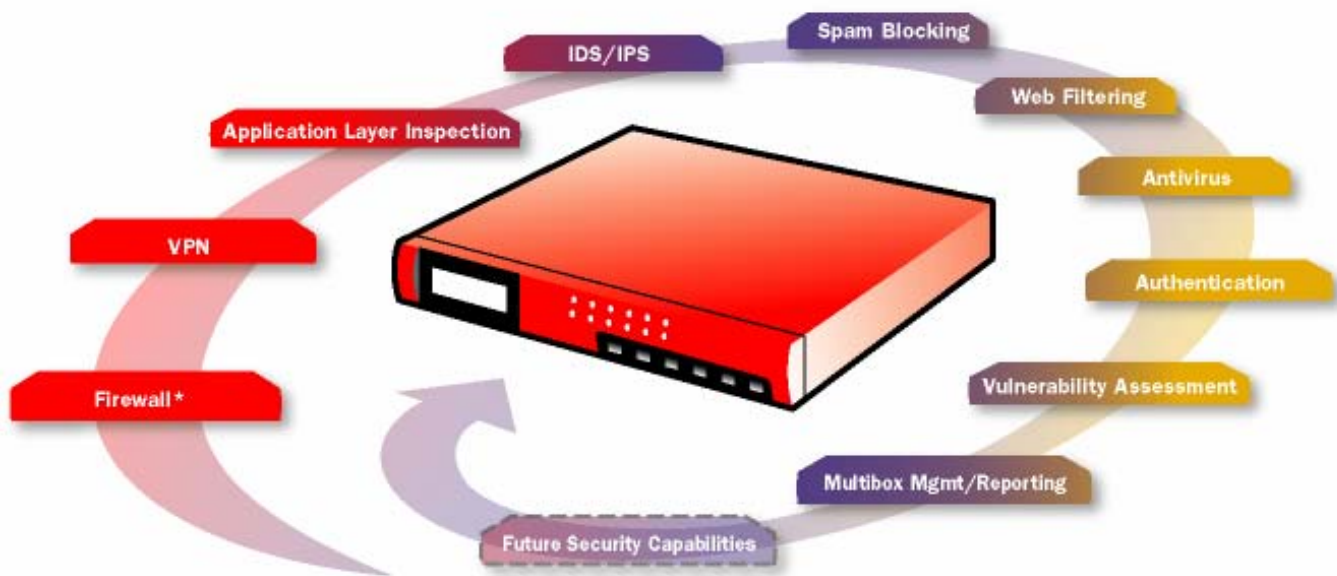


Figure 3. SME security architecture with Firebox® X

WATCHGUARD REDEFINES THE INTEGRATED SECURITY APPLIANCE

INTRODUCING FIREBOX® X

WatchGuard® understands the process of integrating security capabilities in an effective and affordable way. That's why we've been dedicated to the creation of an effective integrated security appliance since 1996. Our latest generation appliance, the Firebox® X, is the first fully Integrated, model-upgradeable security appliance on the market today for the small- to mid-sized enterprise that is designed to be fully expandable. Figure 4 shows integrated security functions available on the Firebox X.



*Perimeter and Interdepartmental

Figure 4. Firebox® X: Integrated Security

The Firebox X delivers enterprise-class protection in an expandable platform that lets you easily unlock features, capabilities, and performance simply by applying a license key to your existing appliance, eliminating the need for costly device replacement or augmentation as your business and security needs change. Figure 5 shows model upgrades for the Firebox X as well as available add-on features and service options.

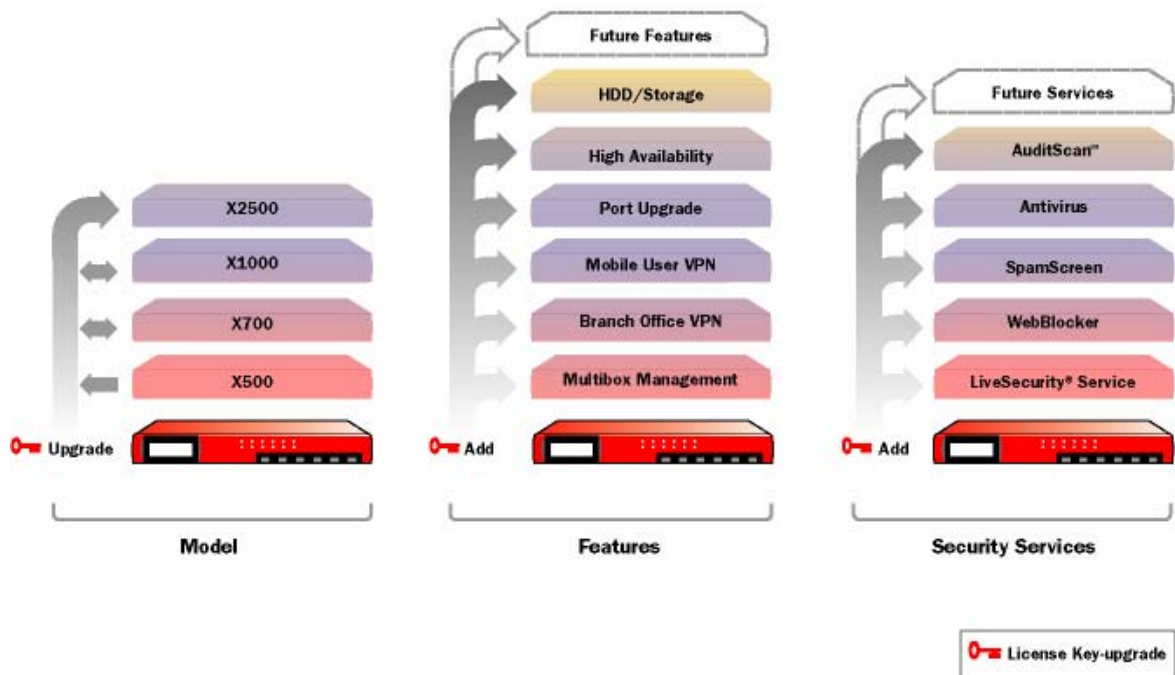


Figure 5. Firebox[®] X platform expandability

INTELLIGENT LAYERED SECURITY ARCHITECTURE

Our innovative Intelligent Layered Security (ILS) architecture provides security at all levels of your network. Multiple technologies work together to eradicate damaging traffic in the most efficient and effective manner. This architecture protects multiple network layers, and is overseen by the Intelligent Layered Security engine that monitors and directs actions across multiple layers for optimum protection and performance. The ILS layers are:

- **External Security Services** such as vulnerability assessment
- **Data Integrity** validates data packet integrity and protocol conformance
- **Virtual Private Networking (VPN)** ensures secure and private external communications
- **Stateful Firewall Filter** ensures that traffic passing through the firewall is benign
- **Application Security** validates traffic against known threats and policies
- **Content Security** analyzes and regulates traffic for appropriate content

Although the ILS architecture only shows six layers, each layer contains multiple security functions, which all adds up to numerous integrated capabilities.

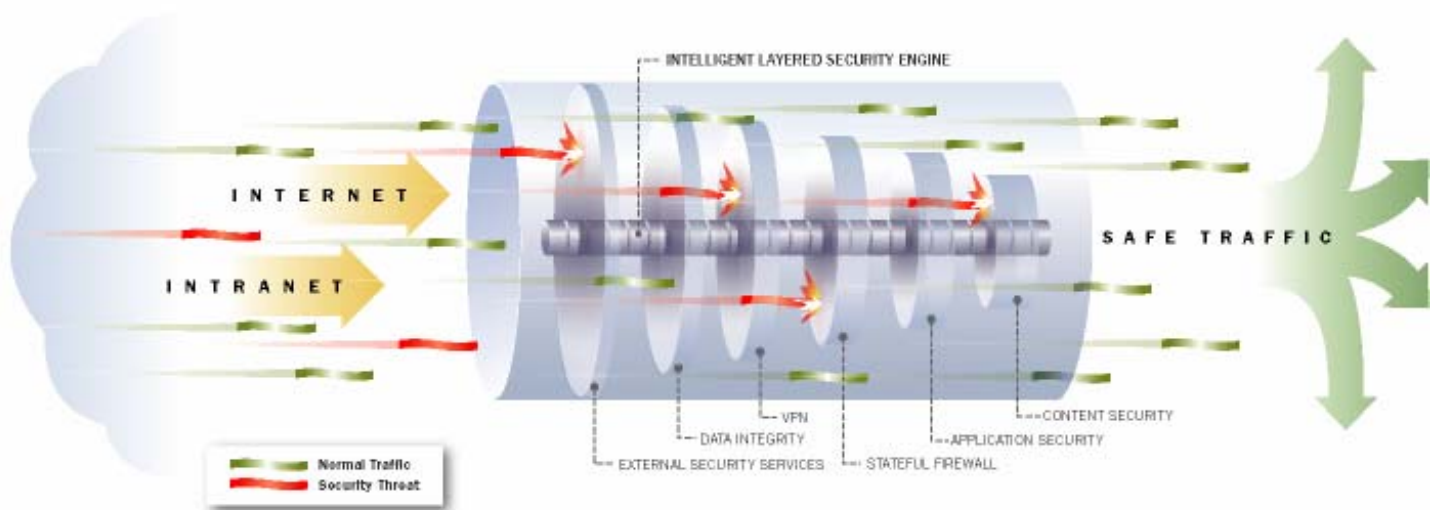


Figure 6. Intelligent layered security

Figure 6 shows how layered security becomes more effective and efficient with the WatchGuard® Intelligent Layered Security engine. The engine acts as a central nervous system running between all protection layers, monitoring and directing traffic to the most efficient layer for processing. This architecture is specifically designed to easily accept new technologies over time as more sophisticated threats emerge.

MANAGEMENT SHOULD BE AN INTUITIVE USER EXPERIENCE

Management of every service and function that Firebox® X delivers is built into a single, intuitive interface that makes installation and maintenance of your entire security system simple and secure. Firebox X is offered at a very economical initial price, with a projected TCO that is much lower than competitive offerings. Right out of the carton, Firebox X smart defaults protect you the minute you install it in your network. Fully and easily configurable, Firebox X lets you quickly design a security policy that best fits your needs.

The Firebox X management interface also gives you real-time views of the network activity throughout your entire system. New features or services automatically appear in the interface when you add them to your appliance.

You also have access to powerful reporting tools that can be configured in a variety of ways at whatever level of detail you require.

In addition, no other security solution available manages VPN tunnel creation with the ease and elegance of Firebox X. Establish new VPN connections with an easy drag-and-drop process. No painful configuring of appliances at either end, or having to remember multiple IP addresses. The Firebox X does it all for you, simply and securely.

Figure 7 shows the components of the Firebox X user interface that contribute to an intuitive user experience over the normal life cycle of the product.

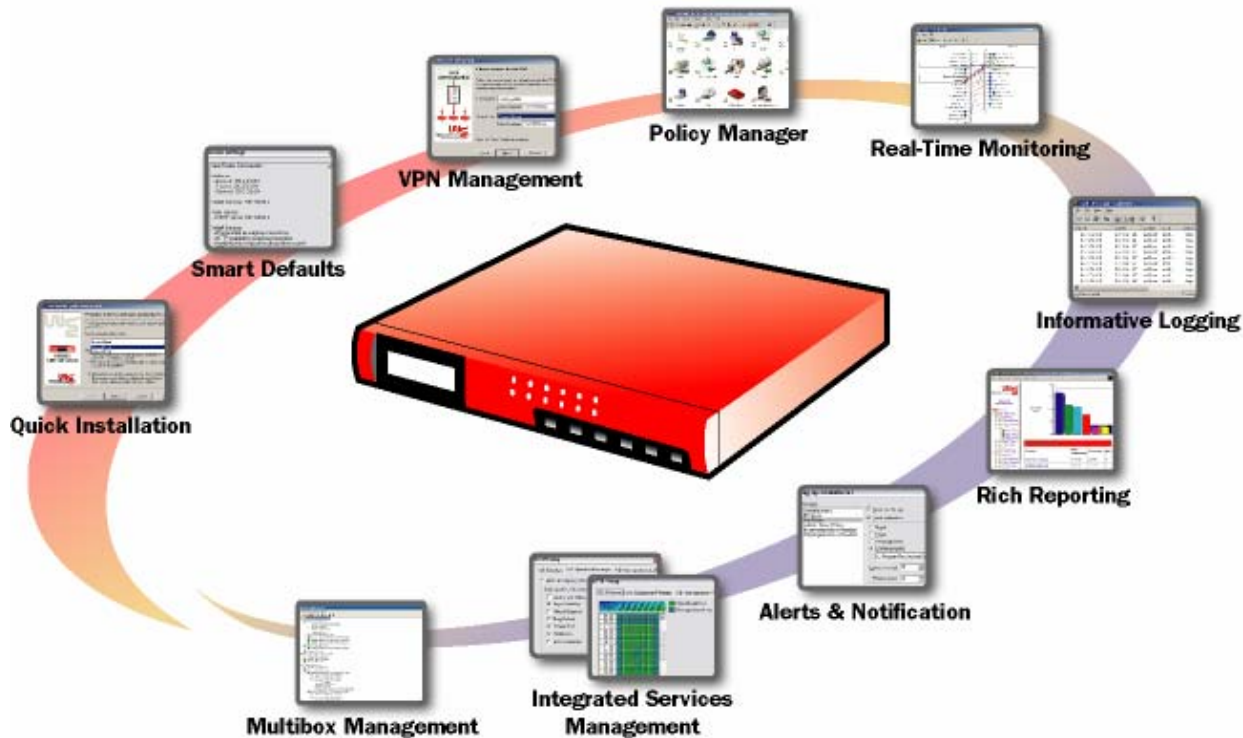


Figure 7. Intuitive user experience

ERADICATING TRADITIONAL SHORTCOMINGS

Remember those shortcomings we described in the previous section: performance, reliability, scalability, and management complexity? The following sections describe exactly how the Firebox[®] X eliminates each of them:

- **Performance rates**

The biggest hit on performance rates of many so-called integrated appliances comes from the implementation of “deep packet inspection”, or application layer (content) filtering, which requires significantly more processing power than packet level (header) filtering. WatchGuard[®] has been using this technology since 1997, so we know how to perform application layer security with less performance degradation than other solutions. The Firebox X is packed with plenty of horsepower so it can handle even the busiest network.

- **System reliability**

As more functionality is added to a single device, there is an increased worry that if that device fails, the network will be vulnerable. To lessen this concern, WatchGuard uses the highest quality

components and the most advanced system designs for long-term reliability and trouble free operation. With the 3 to 6 port and High Availability upgrade option all Firebox® X appliances can be placed in a redundant high-availability configuration so that if one device fails, the secondary device takes over operations seamlessly.

- **Scalability**

If you want an integrated appliance that can accept heavier loads and new applications, you will be happy to know that the Firebox X was designed from the start with scalability and expandability in mind, to allow for expansion of hardware, performance, and add-on security services. All devices are equipped with a high-performance Intel CPU and ample memory; so new capabilities and features can be unlocked, and you can upgrade any to any higher model, simply by activating a license key for your existing appliance. You won't need to add expensive hardware to get the functionality you need.

- **Management Complexity**

Traditional security solutions, even so-called integrated solutions, can be a management nightmare. Each function may come with its own management software and often the management systems are unable to communicate, or can't be viewed simultaneously. Upgrades and patches for so many management systems are nearly impossible to keep updated, especially for smaller businesses with limited IT resources.

With Firebox X, the management of every security function is built into a single, intuitive user interface that gives you a single view of your entire security system from a central management console. Management sessions are encrypted and secure, so they can be generated from anywhere at any time. WatchGuard reporting and logging features are superior in their flexibility and ease of use. WatchGuard Firebox System Management software tells you what is happening all over your network at any time. And you can configure it to any level of detail you need.

DELIVERING BETTER TOTAL COST OF OWNERSHIP (TCO)

In addition to your initial investment in a security product, you should take into account ongoing costs for security improvements, maintenance contracts, and operations. As your business grows, your security needs will grow, requiring additional software functions, features, and performance upgrades to keep your security current.

As Figure 8 shows, The Firebox X offers a lower initial *and* extended TCO than other competitive offerings on the market today. Notice that the difference between the TCO of Firebox X and the nearest competitor is substantial. This is due in large part to having more integrated capabilities built in, a more affordable service and renewal pricing model, and bundled management and reporting. This chart shows the relative TCO for WatchGuard and four competitors over a 4-year time spread.

Even without accounting for the operational efficiencies, business impact and reduced need for appliance replacements, the Firebox X is clearly more affordable to own and maintain than competitive offerings.

THE INTEGRATED SECURITY APPLIANCE: THE BEST SOLUTION FOR SMALL- TO MID-SIZED ENTERPRISES

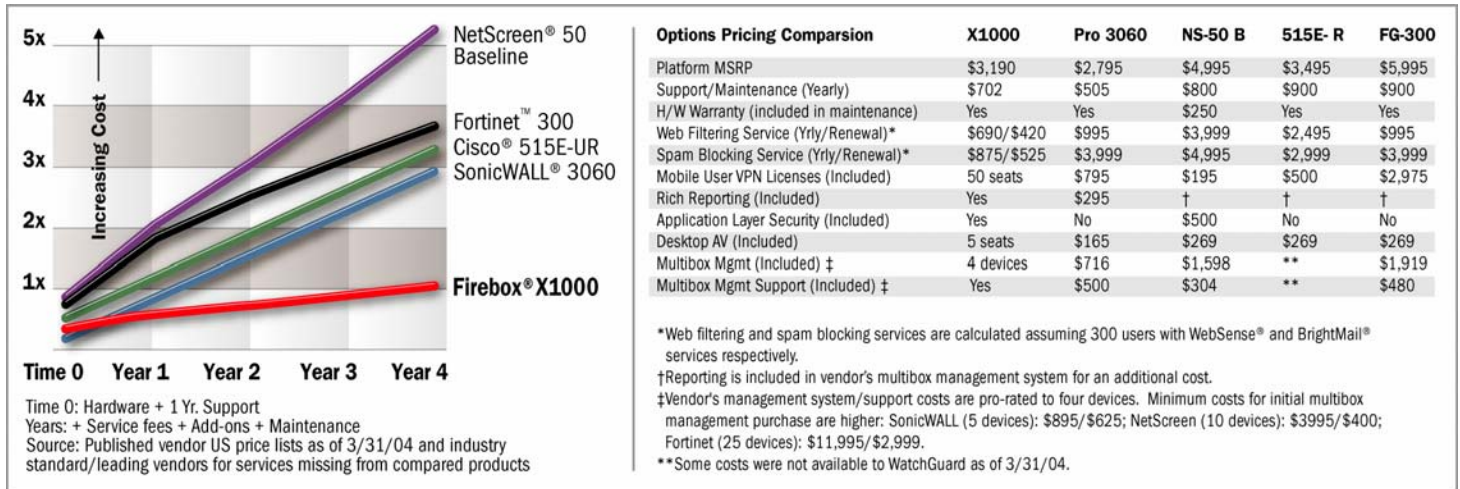


Figure 8. Firebox® X delivers a lower TCO*.

FIREBOX® X: EXPERT SERVICE AND SUPPORT

All Firebox® X products are backed by our LiveSecurity® Service program, giving you expert guidance and support to keep you informed and your security up to date.

LiveSecurity® Service is unique in the industry as the most comprehensive support program available. What other vendors call premium, and charge extra for, we consider to be standard support that you are entitled to as a WatchGuard® customer. With your standard support subscription (an initial period of service is included with the purchase of any standard WatchGuard product) you will receive:

- **Vulnerability alerts** help you see threats coming before they hit you. Emailed alerts arrive directly in your inbox, making you among the first to learn of new threats. Alert text is easy to understand, and you'll know within four sentences whether the threat affects you.
- **Hotfixes and feature enhancements** keep your defenses tuned. Software updates are a great value, because they include the types of new capabilities and full-rev upgrades that other vendors charge extra for.
- **Expert guidance** helps you know what to do. Industry experts provide articles for every level of security expertise, from "none" to "advanced." Security changes so rapidly that if you stop learning; you run the risk of becoming obsolete. LiveSecurity Service editorials help keep you informed.
- **Superior customer care.** Our standard targeted response times are 4 hours, period, unlike competitors who charge extra for response times less than 24 hours. Our technical support team members are certified on all WatchGuard products and technologies, and are easy to access. We give our customers a single contact number that can connect them to support personnel in every time zone around the globe. We can be contacted by phone, the Web, or through your reseller.

* For detailed comparison costs by vendor, please contact your reseller, or WatchGuard Inside Sales at 1.800.734.9905.

SUMMARY

Network threats aren't going to disappear; they will simply become faster and more dangerous. Companies of all sizes rely heavily on the Internet and on network connectivity to conduct their business. Since the threats are the same for all, small- to mid-sized enterprises need sophisticated network security just as much as large enterprises. WatchGuard® is committed to providing truly effective security solutions for the SME market, solutions that incorporate the latest technology, at an affordable price. Expandable by design, the model-upgradeable Firebox® X Integrated Security Appliance is the right solution today, and will continue to be the right solution well into the future.

ADDRESS:

505 Fifth Avenue South
Suite 500
Seattle, WA 98104

WEB:

www.watchguard.com

E-MAIL:

information@watchguard.com

U.S. SALES:

+1.800.734.9905

INTERNATIONAL SALES:

+1.206.613.0895

FAX:

+1.206.521.8342

ABOUT WATCHGUARD

WatchGuard network security solutions provide small- to mid-sized enterprises worldwide with effective, affordable security. Our Firebox line of extendable, integrated security appliances is designed to be fully upgradeable as an organization grows, and to deliver the industry's best combination of security, performance, intuitive interface, and value. WatchGuard Intelligent Layered Security architecture protects against emerging threats effectively and efficiently, and provides the flexibility to integrate additional security functionality and services offered through WatchGuard. Every WatchGuard product comes with an initial LiveSecurity Service subscription to help customers stay on top of security with vulnerability alerts, software updates, expert security instruction, and superior customer care.

FOR MORE INFORMATION: Please visit us at www.watchguard.com or contact your reseller for more information.

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.

©2004 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, the WatchGuard Logo, Firebox, and LiveSecurity are either registered trademarks or 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. WGCE65979_0304