WHITE PAPER

Internet-Perimeter Security With No Hardware, No Software and No Installation

www.vigilantminds.com

EXECUTIVE SUMMARY

Ideally, Internet security should be "built in" by a company's Internet Service Provider. A company should be able to establish a public Internet presence and secure its information systems and critical data in minutes — with no security hardware, no security devices, no security sensors, no security software, no security consultants and no installation of any of these security solutions. Unfortunately, in the real world, Internet-perimeter security solutions require expensive equipment and time-consuming installation by a team of full-time security experts. These conventional solutions require intensive capital expenditures for equipment and software, as well as significant investments in full-time employees or outside consultants to handle installation, maintenance, and monitoring. Worst of all, conventional perimeter security solutions are typically of limited effectiveness.

Many organizations, especially small and midsize businesses, can afford neither the security products nor the requisite expertise to derive full benefits from them. What they need is an effective perimeter solution that does not require hardware, software or installation. Such a solution is available now for the first time with BufferXone™ — the patent-pending perimeter security solution by VigilantMinds.

THE BUSINESS ISSUES

Internet-perimeter security is a high-wire act in which business owners and executives must balance the price of security versus the risks and costs of failure.

The **price of security** can run into tens of thousands of dollars for capital expenditures (CAPEX) and ongoing investments in:

- **Security hardware** such as firewalls, intrusion detection/prevention devices and sensors that must be installed, monitored and maintained
- **Security software** that must be installed, configured, and managed for updates and patches
- **Full-time employees** to install, monitor and manage the equipment and software "around the clock"

THE COSTS OF SECURITY FAILURES

- **$90,000 —** the *average* cost of recovery per virus outbreak.[1]
- **$400,000 —** the *average* cost of intellectual property theft from a directed attack.[1]
- **$1.4 million —** the *average* cost of recovery from Directed Denial of Service.[1]
- **$100,000 —** the *average* cost of cleaning up after worms.[2]
- **$2,000** per employee **—** the *average* cost of a phishing exploit.[3]

---

[1]Source: 2004 CSI/FBI Computer Crime and Security Survey
[2]Source: ICSA Labs, Herndon, Va.
[3]Source: Nucleus Research, Wellesley, Mass.

- **Consultants** using specialized security expertise to adapt these security solutions to the needs of the business

The **costs of failure** are even more painful and include:

- **Damage to the business** and its networked systems from threats such as worms, viruses, Distributed Denial of Service (DDoS), identity theft, phishing, directed and undirected attacks and unforeseen "zero day" threats
- **Network downtime** resulting in lower operations productivity and reduced employee efficiencies
- **Lost revenue and lost customers** from the interruption in business continuity
- **Damage to corporate brand image and reputation** that could lead to loss of credibility among stakeholders both inside (board of directors, employees) and outside (customers, partners, regulators, media) of the organization
- **Legal consequences** (stiff fines and jail time) stemming from non-compliance with government regulations that require organizations (regardless of size) to protect the privacy and integrity of customer and employee data and other digital assets

To attain and sustain Internet-perimeter security is especially challenging for small and midsize businesses (SMBs). For these companies, achieving levels of security that are comparable to that of a Fortune 500 company may seem unrealistic. The costs of failure, however, are unacceptable — with less margin for error than many larger enterprises have — and include everything from the consequences outlined above to the potential demise of the business. Today, SMBs must work hard to find the right balance of security investment and cyber-risk for their businesses.

What is the typical security profile of an SMB? It depends. SMB security solutions are as varied as the businesses themselves. The SMB market covers a broad spectrum and means different things to different people: SMBs generally are considered to have from 100 to 5,000 employees. Their security setup may be as simple as having a firewall and a network administrator to having an array of equipment and a Network Operations Center (NOC) supporting multiple networks across geographically dispersed locations.

Even with this broad range of SMB security environments, there is still common ground in the security issues with which these businesses must deal. SMBs all have **needs, issues and challenges**, pertaining to computer security that include:

- Security policy set-up, management, and governance
- Vulnerability shielding and patch management
- Security resources, including in-house security expertise (or lack of same)
- The challenge of keeping up to date with infrastructure updates

- The difficulty of staying current on the dynamically changing threat environment
- Validation and remediation of security events
- Regulatory compliance, i.e., the need to satisfy the requirements of governmental regulations such as Sarbanes-Oxley Act of 2002, the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), the Family Educational Rights and Privacy Act (FERPA), the Statement on Auditing Standards (SAS-70), California Senate Bill 1386 (SB1386), ISO 7009 and Canada's Personal Health Information Privacy Act (PHIPA)
- Pressure from various entities, including the company's board, auditors, competitors, media and regulators

CONVENTIONAL SECURITY SOLUTIONS

What choices do SMBs have when it comes to protecting their networked systems from Internet-based threats such as worms and viruses? Historically, small and midsize businesses have had limited "affordable" choices when protecting their information assets, managing threat profiles and safeguarding the full perimeter of their networked systems.

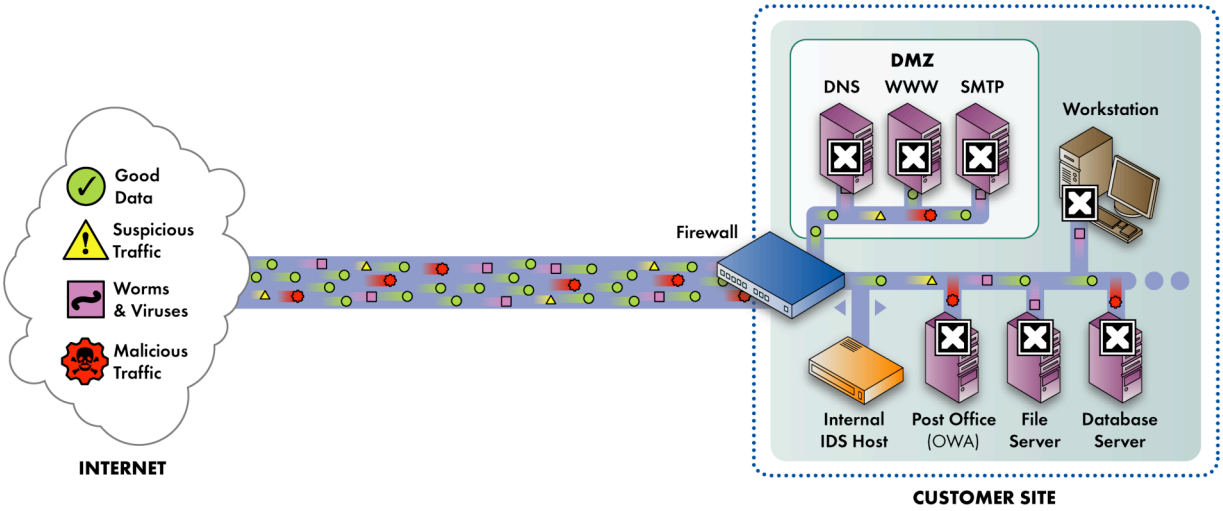
One option, as a starting point, is to conduct a security risk assessment to identify key security issues and vulnerabilities. Based upon the results of this assessment, the company is likely to develop a security plan that includes installing hardware devices in conjunction with security software to protect both their internal and external (public facing) computer systems.

Depending on the company's size, its financial and organizational resources, and how it chooses to prioritize security as a business issue, the security plan may end up as a relatively simple checklist or highly complex security strategy. For example, elements of the plan for perimeter security might include:

- Firewalls
- Intrusion Detection Systems
- Intrusion Prevention Systems
- A demilitarized zone (DMZ)
- Patch and vulnerability management systems

Installation and configuration of such premises-based equipment typically require CAPEX investments of tens of thousands of dollars, plus costly annual charges for maintenance of the equipment.

Additionally, the company needs expertise to understand the security event data, as well as for 24x7 monitoring. Around-the-clock security monitoring typically requires at least five to seven full-time employees who are certified security experts to understand, manage, and respond to security events. The company could pay its Internet Service Provider (ISP) or hire a Managed Security Services Provider (MSSP) to do this monitoring and reporting. For many SMBs, MSSPs make sense because that can provide 24x7 coverage and protection for a fraction of the cost of internal resources. In addition, MSSPs see such a broad range of threats from all over the Internet (for many different clients and geographies), and they have the experience and expertise to act upon that data and prevent emerging threats, including worms and viruses.



Conventional Perimeter Security

MINIMAL RESOURCES = MINIMUM SECURITY

But what about SMBs with limited resources? Unfortunately, many small and midsize businesses lack the requisite expertise and cannot afford to outsource security monitoring. These businesses may rely on the network firewall as their primary enforcement point for their security policy. The firewall is intended to both protect the business from malicious, Internet-based activity and to facilitate business with others that are connected to the Internet. The firewall is a necessary component for any organization providing Internet-accessible services and for the safe and secure utilization of these services. A firewall, however, is only the first line of defense in a layered security program.

By definition, if a company is to provide its employees, partners, suppliers and other stakeholders with Internet-accessible services, some “paths” or “doors” to these services must remain open to incoming traffic. As these business services increase and more doors are “unlocked”, firewall systems may become more open than originally intended. Unfortunately, in many cases, the burden of day-to-day network and systems operations does not allow for

regular review and re-evaluation of business services requirements and Internet security policies and practices. In these situations, the firewall can and will become an easily circumvented border on the perimeter of the network.

Although conventional firewalled networks may seem to be protected, many security compromises occur because of misconfigured firewalls or unpatched systems. Indeed, rigorous patch management has emerged as a fundamental driver for ensuring business continuity and network security. In today's environment, the time between recognition of a security vulnerability and exploitation of that vulnerability (via worms, viruses, or hackers) is accelerating to the point that "zero day" threats — that is, exploits occurring on the same day that a vulnerability is discovered — are a real possibility for every business.

Sole reliance on the firewall may leave these businesses exposed to vulnerabilities, undirected attacks, exploits from hackers, worms and viruses. Considering these vulnerabilities, SMBs cannot afford to be without some additional form of perimeter protection to augment the firewall.

THE NEXT GENERATION OF PERIMETER SECURITY

What many businesses need — both large and small — is a fully functional "layer of security" in front of the existing IT security infrastructure. Ideally, this solution would be easy to use and require no changes to the company's network infrastructure. In an ideal world, much of this security could be provided by the business's Internet Service Provider. The ISP could analyze and filter the Internet traffic provided to their clients BEFORE the client sees the threat. Of course, because ISPs are organized and run as "common carriers" of telecommunications services, they are not likely (under their current business model) to "interrupt" or "filter" any of the network traffic that they provide. Thus, the mitigation of Internet-borne threats and risks are left to the individual businesses.

These Internet-connected businesses need the next generation of perimeter security — a "buffer zone" between their networked systems and the Internet to provide the same type of analysis and malicious Internet traffic filtering and blocking that could be performed at their ISP — BEFORE it is sent to their business systems.

This next generation of perimeter security — the buffer zone — should be designed to provide multiple layers of protection that work simultaneously to deliver:

- Protection of information assets through a variety of security safeguards such as intrusion detection and prevention, early worm prevention, and distributed denial of service avoidance — without the need for additional hardware or software purchases
- Automated blocking of malicious traffic and known exploits and worms

- Proactive, vulnerability-shielding capability that blocks unforeseen threats and provides additional time to install critical patches from software vendors
- "Clean" Internet connections for optimized bandwidth
- Anti-virus and spam filtering for e-mail
- URL, content and application filtering
- A central repository for correlation, reporting and auditing of security-related activities (for regulatory compliance and data analysis)
- Simple and rapid implementation for full protection of the perimeter within minutes, rather than in days or weeks
- Real-time access and control to all security information events and response mechanisms, so that business users can maintain ownership of their security
- Scalability to accommodate business growth
- True affordability for small and midsize businesses

The next-generation of perimeter security should be priced so any size organization can afford to be secure. This next generation security solution should also be easy to activate — requiring no hardware to install, no software to configure, no devices to tune, no equipment to maintain, no training to implement and no expertise to operate. In short, the next generation of perimeter security should deliver enterprise-class perimeter security in a simple, affordable and effective manner — one that is particularly "pain free" to the SMBs that have very limited resources — but is scalable for businesses of all sizes.

BUFFERXONE – THE NEXT GENERATION IS HERE

VigilantMinds has responded to the market's need for a "next-generation" solution that truly makes perimeter security simple. VigilantMinds developed **BufferXone**™ (pronounced "buffer zone"), a patent-pending, device-less, installation-free system that provides enterprise security for any size business, government agency, healthcare organization or educational system. BufferXone is the embodiment of next-generation perimeter security.

The core competency of VigilantMinds, as a managed security services provider, is cutting-edge information security expertise. As such, VigilantMinds has a successful history of providing innovative intrusion prevention solutions, real-time monitoring, and response mechanisms for all aspects of information system security issues.

With this experience, VigilantMinds recognized the inherent deficiencies and increased costs of device- and software-based network security systems and developed BufferXone to provide enterprise-class perimeter security for businesses of all sizes.

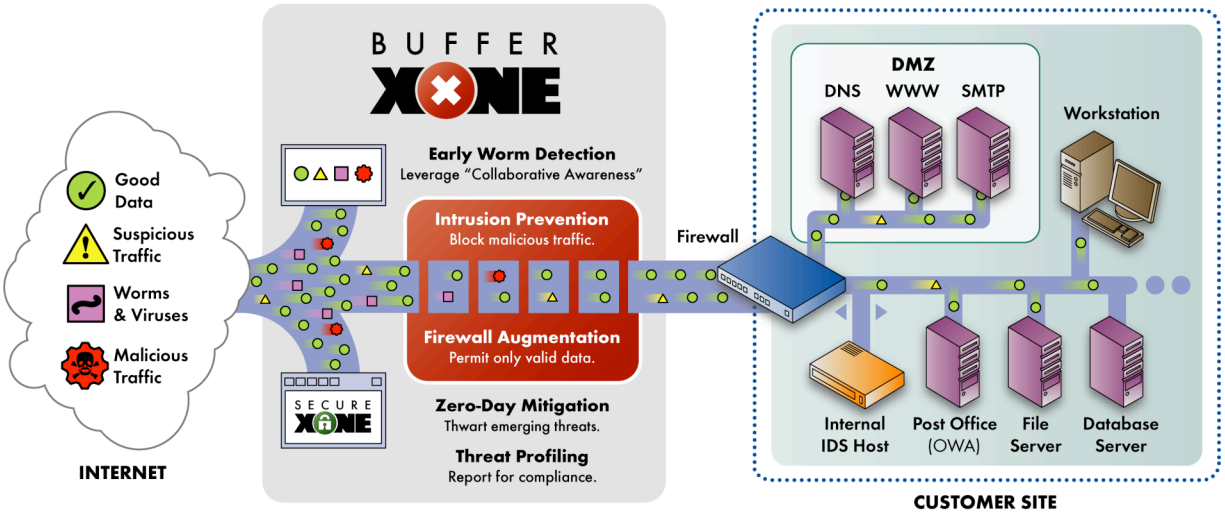
BufferXone is the only comprehensive Internet-perimeter security solution featuring:

- All-in-one protection that includes active blocking of malicious exploits, worms, and viruses
- No hardware to buy, install, and manage
- No software to buy, configure, and maintain
- No sensors or devices to keep up-to-date
- No full-time employees and or high-priced consultants to hire and manage

VigilantMinds hosts the secure data centers where the BufferXone hardware and software that provide this innovative service reside. The company also manages the Secure Operations Center where the professional security experts validate and respond to the latest security developments and vulnerability announcements. By leveraging these resources, BufferXone customers benefit from best-in-class perimeter security — at a reasonable price — while maintaining full access and control of their security data.

HOW IT WORKS

VigilantMinds designed BufferXone to be the most comprehensive Internet-perimeter security solution for enterprises, including small and midsize businesses. It is also the simplest security solution to deploy and utilize for any-size network. BufferXone shields vulnerable corporate hosts from Internet-based threats and provides automatic filtering and blocking of malicious Internet traffic. It does so with imperceptible latency without blocking legitimate business traffic.



After BufferXone: Security Made Simple©

BufferXone provides a multi-layered "zone of security" that protects Internet-based systems and information assets while ensuring business continuity. Incoming network traffic is funneled in a parallel process through multiple filters and protection systems. BufferXone screens data that enters Internet-facing applications and servers for suspicious and malicious payloads that could damage or compromise business-critical information systems. BufferXone proactively 'blocks' bad data sent to these Internet-facing applications (such as Outlook® Web Access [OWA] , FTP servers, Web servers, and e-commerce solutions) and 'alerts' on data that appear to be questionable or suspicious. The customer has the ability via the SecureXone web portal to select when to change from alert (or "learning") mode to automatic blocking mode for each protected Internet server / host.

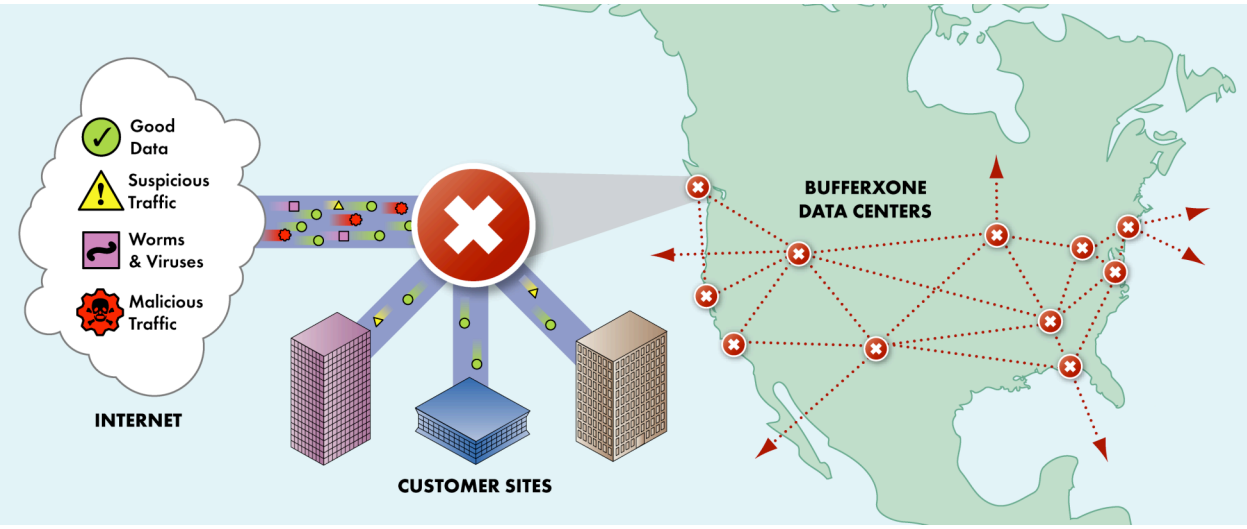
THE BUFFERXONE ARCHITECTURE

BufferXone delivers results for customer organizations through its patent-pending technology, innovative systems architecture and multi-mode traffic analysis and management processes. These parallel processes ensure imperceptible network latency and optimized security through simultaneous engagement of:

- The SecureXone™ Security Event Management Web portal for actionable intelligence and control and customization of network security events and security processes
- Intrusion detection for monitoring suspicious network activity and threat profiling
- Intrusion prevention for real-time blocking of threats, exploits, and Internet-based worms
- Added firewall functionality to ensure that only traffic analyzed and validated by BufferXone reaches the client firewall and desired system services
- Proactive vulnerability shielding that provides protection from "zero day" attacks
- Early worm detection and prevention via VigilantMinds proprietary network anomaly analytics
- An architecture designed for avoidance of Distributed Denial of Service (DDoS) attacks

BUFFERXONE NETWORK OF DISTRIBUTED DATA CENTERS

To ensure the availability of protected systems, VigilantMinds operates multiple fully redundant, geographically dispersed and carrier-diverse data centers with multiple power backup and failover capabilities. The customer's DNS server routes all traffic requests to the BufferXone data centers. Protected — cleaned and filtered — traffic is then routed to the appropriate customer server and host destinations.



Each day, the VigilantMinds network of distributed data centers processes millions of requests. By correlating and analyzing this volume of traffic, BufferXone is able to proactively detect and prevent new attacks and attempted exploits – including new worms – very early in their lifespan on the Internet.

BufferXone processes more network traffic in a day from more geographically diverse places on the Internet than most corporate hosts see in a year. The intelligence provided from this unique vantage point is fed through the VigilantMinds SNARE (Statistical Network Anomaly Reporting Engine) mechanism on a continuous basis. As a result, BufferXone customers are protected from new and emerging attacks before they can be launched or directed at their companies' networked systems.

FLIP THE SWITCH

All it takes to activate BufferXone is the flip of a DNS switch[1] — to flip the DNS record to route traffic through the VigilantMinds data centers. BufferXone issues the customer a new, protected Internet Protocol (IP) address that serves as the re-routing mechanism. Once the DNS record is updated with this new protected IP address, Internet traffic is directed to BufferXone's bank of filters, IPS and IDS systems, and anomaly detection engines. BufferXone screens incoming traffic to protect the customer's original IP address and then forwards only the "clean" traffic to the customer. The customer will also re-configure their firewall to accept only traffic that has been validated by VigilantMinds so that undirected traffic (malicious or not) is unable to enter the customer's system from the Internet.

[1] Although most organizations will quickly take advantage of BufferXone by flipping their DNS records, it is important to note that any Internet host with available services can take advantage of BufferXone's protection by directing new connections to the BufferXone IP address. You do not need DNS for BufferXone to work!

MAINTAIN ACCESS AND CONTROL

BufferXone customers use the Web portal to review, investigate, and report on the network traffic that has been deemed malicious. Customers can easily use a Web browser to review suspicious and malicious traffic that has been flagged and/or blocked (depending on the policy setting chosen by the customer) or view trending reports at any time. Customers maintain full access and control of all of their security processes and incident response mechanisms — and thereby maintain true ownership of their security programs.

In order to fill the security needs of businesses of all sizes, VigilantMinds also offers the SecureXone Web portal. SecureXone can provide access to critical security information about intrusion events, wireless and wired networks, a variety of commercial security devices, and control over security and incident response processes and procedures. SecureXone automatically aggregates the security-related information assets of an entire enterprise by centralizing, synchronizing and analyzing data in order to provide actionable intelligence and real-time response on a 24x7 basis.

ATTAIN REGULATORY COMPLIANCE

Working together, BufferXone and SecureXone promote business continuity, risk management and regulatory compliance with the requirements outlined in the Sarbanes-Oxley Act of 2002, the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), the Family Educational Rights and Privacy Act (FERPA), the Statement on Auditing Standards (SAS-70), California Senate Bill 1386 (SB1386), ISO 7009 and Canada's Personal Health Information Privacy Act (PHIPA).

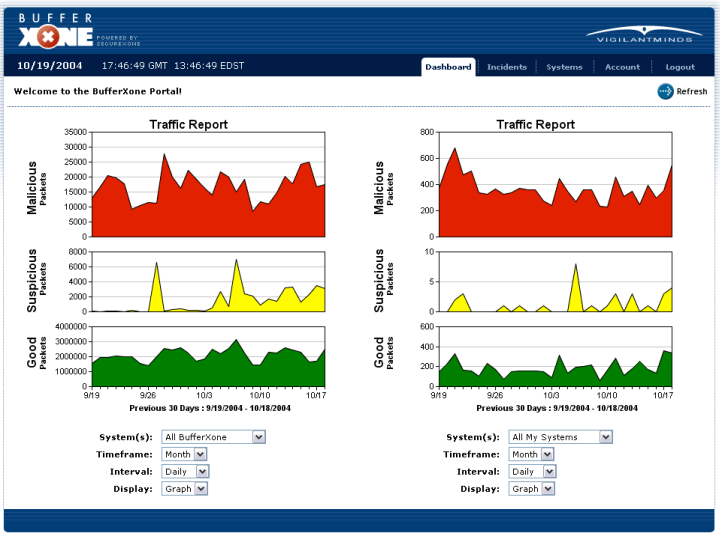
VigilantMinds SecureXone and BufferXone solutions provide customers with an audit trail of the company's employed security processes and the supporting management information to verify these processes are being managed appropriately. These reports are used to verify that viable business measures have been put in place to ensure the integrity of the protected hosts and associated data.

REPORT GENERATION

BufferXone makes it easy to generate reports to satisfy the requirements of government regulations. BufferXone offers three main types of reports, based upon the chosen level of service.

- **Traffic Reports** indicate the number and volume of packets that were blocked, flagged as suspicious, and identified as clean. These reports are viewable over various time periods, in both graphical and tabular format. In addition, customer-specific security event data can be compared to industry category or "total BufferXone" data to assess threat levels across similar businesses or across the Internet. In this way, BufferXone provides a panoramic view for "collaborative awareness" of malicious activity from the Internet, so that users can compare their threats with other BufferXone protected servers.

COLLABORATIVE AWARENESS REPORTS



BufferXone makes it easy to generate traffic reports for regulatory compliance and for "collaborative awareness" — data used for comparison with the security posture of other organizations.

- "**Top Ten" Reports** provide information about the leading malicious attacks and top source IP addresses for malicious traffic.
- **Compliance Reports** customized reports help customers satisfy the requirements of regulations such as Sarbanes-Oxley, GLBA, HIPAA and Canada's PHIPA.

VigilantMinds also provides security alerts tailored to the customer's business needs, as well as vulnerability scanning management solutions for ongoing threat profile analysis of internal and external systems. VigilantMinds certified information security experts generate the security alerts at the company's sophisticated SAS-70 standard Security Operations Center (SOC) and Network Operations Center (NOC), both of which are staffed 24/7/365. Vulnerability reports are available online via the SecureXone Web portal, including patch prioritization and other pertinent vulnerability information.

BIDIRECTIONAL PROTECTION

BufferXone's position as a buffer between protected systems and the Internet creates an intrusion-free zone providing bidirectional protection for Internet-based services. BufferXone filters and blocks all the malicious traffic before routing it to the customer's protected systems. When the protected system responds to these traffic requests, the internally generated response is automatically directed back to BufferXone — and is therefore ALSO filtered. Thus, BufferXone ALSO validates all Internet-originating traffic going into or out of the company's Internet-facing servers.

CONCLUSION

BufferXone is the next generation of perimeter security solutions. BufferXone provides full perimeter protection — including firewall augmentation, intrusion detection and prevention, early worm prevention, and distributed denial of service avoidance — without the need for client-based hardware, software or even installation. As an experienced managed security services provider, VigilantMinds hosts the secure data centers where the BufferXone hardware and software reside, along with the company's Secure Operations Center and staff of professional security experts. By leveraging these resources, BufferXone customers benefit from best-in-class perimeter security that is also very affordable.

BufferXone requires no hardware, no software, and no "installation" within the customer's networks and systems. Unlike device- and software-dependent security systems, users do not require specialized training or expertise. BufferXone is implemented without modifying any of a company's existing networks or systems. Thus, BufferXone can be fully implemented within minutes for any business, anywhere in the world.

Not only can BufferXone be implemented easily, it is extremely cost-effective: It requires no capital expenditure (CAPEX) for hardware or software; no need to hire full-time employees or outside consultants; and no contracts for equipment maintenance. BufferXone is offered as part of a monthly hosting model that makes it as attractive to small and midsize businesses as it is to larger enterprises.

BufferXone provides next generation Internet security today without high-cost hardware, software or maintenance services. By providing network-perimeter protection from Internet-based threats, BufferXone minimizes risks, saves money, and provides a more secure environment for any Internet-connected enterprise.

ABOUT VIGILANTMINDS INC.

VigilantMinds maintains information security for financial services firms, health care organizations, educational systems, government agencies, and businesses with operations worldwide, as well as small and midsize businesses. Our client base is diverse in function and global in reach.

Headquartered in Pittsburgh, Pa., VigilantMinds provides managed security services, wireless information security, enterprise security audits, and proprietary security software and Internet-based solutions. VigilantMinds provides 24x7 operations for full monitoring and management of enterprise security systems, software, and devices such as network- and host-based Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), firewall design, monitoring and management, and host event monitoring for critical network devices. Every day, our experts see new threats on the horizon and create solutions to thwart attacks that haven't yet happened. No other vendor matches VigilantMinds for this one-step-ahead approach to ensuring information security and regulatory compliance.

VigilantMinds Inc.
4736 Penn Avenue, Pittsburgh, Pa 15224
412-661-5700
F: 412-661-5684

Canada
Toronto

Midwest
Cleveland
Detroit

United Kingdom
London

Learn more about VigilantMinds:

www.vigilantminds.com
info@vigilantminds.com

Learn more about BufferXone or sign up for a free trial:

www.bufferxone.com
info@bufferxone.com