

# Proventia™ Dynamic Threat Protection™ Appliances

*Protection Without Complexity*

## *Executive Summary*

Today, the necessity for secure online transactions has never been greater. Yet, protecting your critical online infrastructure has never been more complex.

The market has long called for protection without complexity. That is, protection delivered through simplified, plug-and-play, multi-function protection appliances. Internet Security Systems has responded by announcing its Proventia™ Dynamic Threat Protection™ appliances.

Built on the industry's leading security intelligence and technologies, Proventia Dynamic Threat Protection appliances identify and stop known and unknown attacks without user intervention. This is achieved through maximized protection, simplified deployment and streamlined management.

Proventia appliances deliver on the long-held hope for customers to discard disparate point security products.

Proventia appliances complement ISS' existing network, server and desktop protection agents - all which are centrally-managed within the SiteProtector™ unified security management system.

This white paper serves to illustrate how Proventia appliances pave the way for a new breed in unified and simplified multi-function protection that protects and prevents without user intervention.

### *Table of Contents*

Executive Summary	1
Today's Security "Solution"	2
Proventia™ Dynamic Threat Protection Appliances	2
Proventia's Foundations	4
> Security Intelligence	
> Technology	
> Protection at a Lower Cost	
> Simplified Deployment	
> Streamlined Management	
> Maximum Protection	
Protection At A Lower Cost	5
Customer Commitment	6
> Hardware	
> Support	
> Maintenance	
Conclusion	6

## *Today's Security "Solution"*

Today's business operations depend on network technologies. From small organizations to multinational conglomerates, securing online transactions continues to be imperative. At the same time, the complexity of protecting your critical online infrastructure continues to be challenging.

When it comes to Internet security, organizations seek one thing: Protection.

However, when it comes to implementing protection, organizations are faced with a complex myriad of solutions requiring complex integration and intricate management. Firewalls. Antivirus. Intrusion Detection. VPN. The list goes on.

Even with all or most of these pieces in place, the protection falls short. As Code Red and SQL Slammer recently illustrated, organizations face serious consequences if they omit any one of these pieces. These malicious exploits painfully illustrated how firewalls and antivirus were incapable of protecting against these very powerful, automated and very intelligent threats.

When organizations simply seek protection, why do they mire themselves in complex solutions requiring integration, multiple vendors and unwanted intricacies? Simple. Because a plug-and-play, multi-function protection appliance has not been available.

## *Proventia Dynamic Threat Protection Appliances*

Introducing Internet Security Systems' Proventia Dynamic Threat Protection Appliances.

Built on the industry's leading security intelligence and technologies, Proventia Dynamic Threat Protection appliances identify and stop known and unknown attacks without user intervention. This is achieved through the unmatched combination of maximized protection, simplified deployment and streamlined management. Proventia appliances deliver on the long-held hope for customers to discard disparate point security products.

As the name suggests, Proventia appliances combine ISS' world-leading security intelligence and technology to protect and prevent.

Proventia appliances complement ISS' existing network, server and desktop protection agents – all which are centrally-managed under the SiteProtector™ unified security management system. Proventia paves the way for a new breed of unified and simplified multi-function protection that protect and prevent without user intervention.

A wide variety of Proventia series and models are designed to meet a range of needs, including:

- √ **A-Series:** comprehensive intrusion protection for aggregate network bandwidth from 200 Mbps to 1200 Mbps on 1 to 4 network segments
- √ **Inline Series:** comprehensive, inline intrusion prevention and protection, married with the world's best intrusion detection
- √ **Multifunction Series:** unified, multi-function protection appliance, eliminating the need for user intervention and stand-alone point solutions such as firewalls, gateway antivirus, Virtual Private Networks (VPN), Intrusion Protection Systems (IPS) and content filtering.

<b>Proventia Appliances</b>	<b>"A" Series</b>	<b>Inline</b>	<b>Multifunction</b>
<b>Appliance Form Factor</b>	X	X	X
One-stop acquisition	X	X	X
Easy deployment	X	X	X
Simple configuration	X	X	X
Redundant power supply	X	X	X
Redundant local storage	X	X	X
<b>Ethernet Network Protection</b>	X	X	X
Performance	1200 mbps	2000 mbps	800 mbps
Maximum Protected Segments	4	1	3
Gigabit Network Access - Copper	X	X	X
Gigabit Network Access - Fiber	X	X	
Inline Network		X	X
Supports Asymmetric Routing	X	X	X
Monitors Full-duplex Segments	X	X	X
<b>Based on RealSecure Technology</b>	X	X	X
Protocol Analysis - Over 95 Protocols	X	X	X
Pattern Matching Algorithms	X	X	X
<b>Unified, Multi-Function Protection</b>			X
Stateful Packet Filter Firewall			X
VPN Gateway			X
IPS	X	X	X
IPS with Inline Blocking		X	X
Layer 7 Application Stream Filter		X	X
DoS Prevention		X	X
Gateway Anti-virus			X
Spam Filter			X
Content Filter			X
DHCP Server			X
Network Address Translation			X
<b>Remote Central Management</b>	X	X	X
Web-based Access			X
<b>MSRP</b>	Starting at \$9,995 US	TBD	TBD
<b>Availability</b>	March 2003	Q3 2003	Q4 2003

## Proventia's Foundations

Proventia Dynamic Threat Protection appliances have been built from the ground up and are based on the world's #1 security intelligence and the world's #1 protection technology.

### World's #1 Security Intelligence from the X-Force

In-depth security research is - and always has been - the core of Internet Security Systems and the foundation of all ISS products and services. No other organization can match ISS' X-Force™ security intelligence team in global breadth, depth or rapid response. X-Force is unparalleled in its research efforts and is the world number one in security advisories, representing 45% of all vulnerabilities discovered by commercial research entities - 3 times more than any other entity. X-Force threat research and analysis establishes the intellectual capital that underpins the Proventia Dynamic Threat Protection appliances. In addition, centrally-deployed X-Press Update™ product enhancements deliver the latest X-Force information quickly and automatically. This ensures that Proventia customers have a first-to-know, first-to-protect advantage that no other security appliance can match.

### World's #1 Security Technology via ISS' Protection Engine

Internet Security Systems' Protection Engine is the underlying technology that drives all ISS Intrusion Protection and Vulnerability Assessment agents - and is the core technology behind all Proventia appliances. Based on the technology utilized in ISS' market-leading RealSecure® intrusion protection solutions, the Protection Engine is the world's first universal technology engine that spans networks, servers, desktops and applications to detect, prevent and respond to known and unknown attacks.

**Detect:** To be the world's best prevention and protection appliance provider, you first must be the best in detection. It is the combined employment of multiple detection techniques that makes ISS the world leader - no single detection technique is effective on its own.

Through ISS' world-leading security intelligence and the optimal combination of these detection techniques, the Protection Engine quickly and accurately identifies threats that other solutions miss. Detection techniques include state-based seven-layer protocol analysis, pattern matching, behavioral analysis, application layer pre-processing, heuristics, TCP reassembly and custom signatures, along with vulnerability assessment to detect known and unknown threats. The result is unparalleled detection capabilities that extend across 95 network and application protocols to detect over 1,700 known vulnerabilities and countless unknown exploits. No other offerings on the market even come close to this breadth and depth of protection.

**Prevent:** Once the Protection Engine detects malicious behavior, preventative measures are then initiated. A variety of proactive preventative mechanisms are available from the Proventia appliances. These include inline packet filtering and blocking, active blocking and instant vulnerability remediation through a unique Virtual Patch™ capability.

**Respond:** Once an attack is detected or prevented, the Protection Engine responds using an array of built-in and user-defined mechanisms. Built-in actions include event, packet and evidence logging, TCP resets, real-time attack verification, event correlation, aggregation and firewall or router reconfiguration. A variety of notification responses are also available, which include console alerts, email and pager notification and SNMP traps.



Looking forward, the Protection Engine will be further enhanced to drive unified multi-function protection appliances.

### ***Protection At A Lower Cost***

While based on ISS' world-leading security intelligence and technology, Proventia appliances offer much more in terms of value, functionality and support. Namely, simplified deployment, streamlined management and maximized protection.

#### **Simplified Deployment**

Proventia is a true plug-and-protect appliance. Proventia appliances reduce the time required to acquire, deploy and protect to mere minutes. These single-vendor appliances deploy quickly and easily across multiple geographic locations and require minimal configuration. Simply plug the Proventia appliance into a standard 1U or 2U rack mount, plug in the network segment to be protected, turn it on and the protection solution is in place and functional.

#### **Streamlined Management**

Proventia Dynamic Threat Protection appliances are centrally-deployed, managed and updated through ISS' unified management system, SiteProtector. SiteProtector is the world's only management platform that provides centralized control, command and event management for network, server and desktop protection agents.

SiteProtector simplifies and streamlines Proventia management - from appliance updates to advanced data correlation tasks. Each Proventia appliance or RealSecure protection agent reports to SiteProtector, with data correlation being applied at every level of the process to minimize excess network traffic and maximize the ability of administrators to quickly and easily focus on the most critical security issues.

The SiteProtector SecurityFusion™ module enhances and extends SiteProtector's correlation capabilities by adding two automated and advanced correlation techniques: Attack Impact Analysis and Attack Pattern Recognition. Fusion immediately estimates the impact of attacks by correlating the target's known vulnerabilities and operating system to the attack, automatically alerting users to real attacks, while de-emphasizing failed attacks and eliminating false alarms. Fusion also automatically correlates attack activity over time to link seemingly disparate events or incidents - whether occurring now or in the past - into a single, significant incident.

#### **Maximized Protection**

An easy-to-use, simple-to-deploy protection appliance is worthless if it doesn't deliver maximum protection. Proventia Dynamic Threat Protection appliances can boldly boast unparalleled protection through building on the aforementioned world-leading security intelligence and world-leading protection technology.

Proventia appliances take protection a step further by offering a variety of options listed in the Proventia™ Dynamic Threat Protection Appliances section. Items of note include:

- √ Multi-segment protection
- √ Inline prevention married with the world's best detection
- √ Multi-function protection

## **Customer Commitment**

Proventia enjoys the same level of quality in its hardware, support and maintenance as it does in its technology and security intelligence.

### **Hardware**

Proventia appliances are premium quality systems based on Intel equipment and are built to Internet Security Systems specifications. The Proventia appliance form factor features include one-stop acquisition, easy deployment, simple configuration, redundant power supply and redundant local storage.

### **Support**

World-class customer support offering:

- √ 24/7/365 global technical support for both software and hardware issues
- √ Unlimited contact with Internet Security Systems engineers
- √ Access to the comprehensive online support knowledgebase

### **Maintenance**

Proventia's maintenance program comprises:

- √ Security Intelligence: regular X-Press Update product enhancements to ensure that appliances are up-to-date with the latest threat protection information and other security developments
- √ Hardware: advanced exchange warranty

## **Conclusion**

Protecting online infrastructure is no longer an expensive, complex task. Proventia Dynamic Threat Protection appliances deliver maximized protection, simplified deployment and streamlined management.

Built on Internet Security Systems' world-leading security intelligence and technologies, Proventia appliances pave the way for simplified multi-function protection appliances that identify and stop known and unknown attacks without user intervention.