SIMPLIFIED | SECURITY

SecurePartner Information Guide

INTERNET SECURITY SYSTEMS™

Introduction

Welcome to **Simplified Security—Your SecurePartner™ Program Sales Information Guide.**

As a busy account executive, you need tools to help you sell effectively. With a little help from Internet Security Systems Channel Marketing Group, this sales information guide will help you achieve your goal.

This guide outlines all the details of Internet Security Systems' new product line. It also provides a better understanding of:

- **What is protection**
- **What needs protection**
- **Why your customers buy protection**
- **How Internet Security Systems' protection products create unique, ongoing sales opportunities**

We prepared this guide with YOU in mind. We've also included detailed "battle cards" which arm you with strategic information to generate WINS! We're excited about this simplified approach to information security. After reading this guide, we hope you will share our excitement, too!

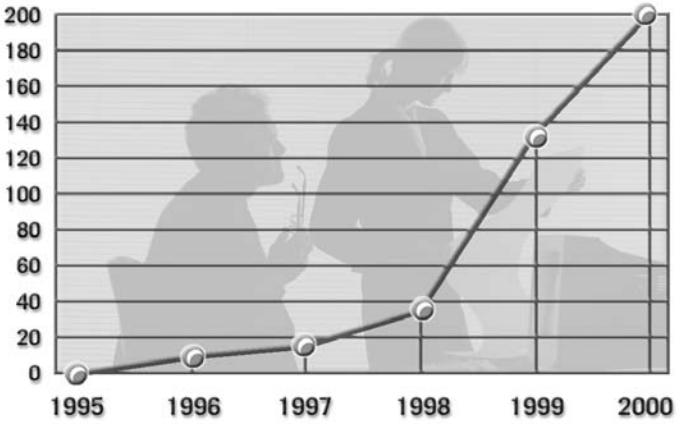
Table of Contents

Facts About ISS

This section provides you with basic information about Internet Security Systems and the latest company performance statistics.

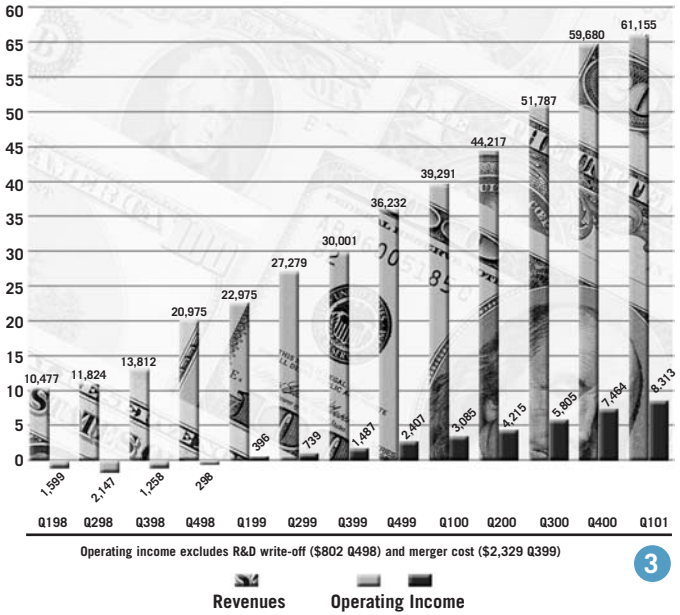
Financial Results FY00
Revenues for fiscal year 2000 were a record $195 million, up 167 percent compared with revenues for fiscal year 1999.

Growth Since Inception



Quarterly Revenue and Profit Trend

Amounts in $000s



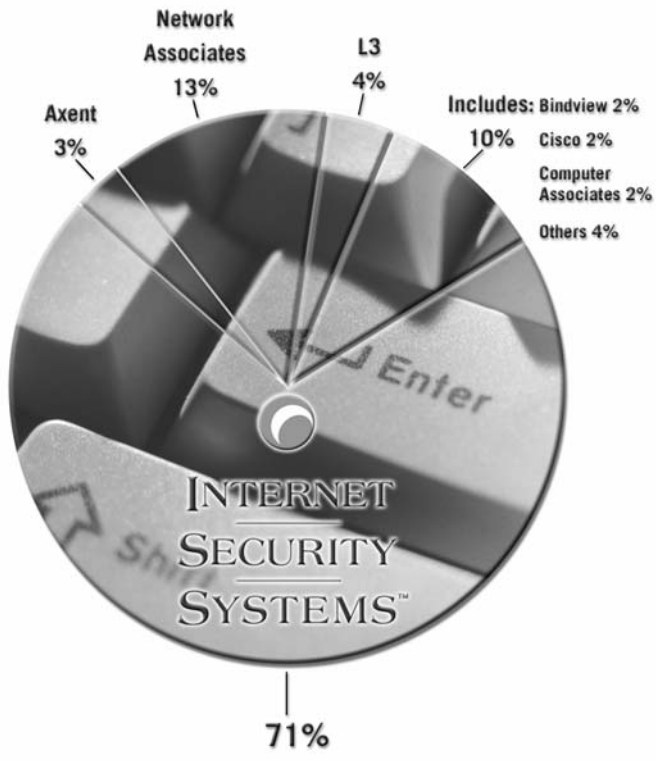
Official Stats

- Pioneer of network security technologies including security assessment, intrusion detection, security management
- 1,500 employees in 22 countries
- 10,000 customers worldwide

What the Industry Says

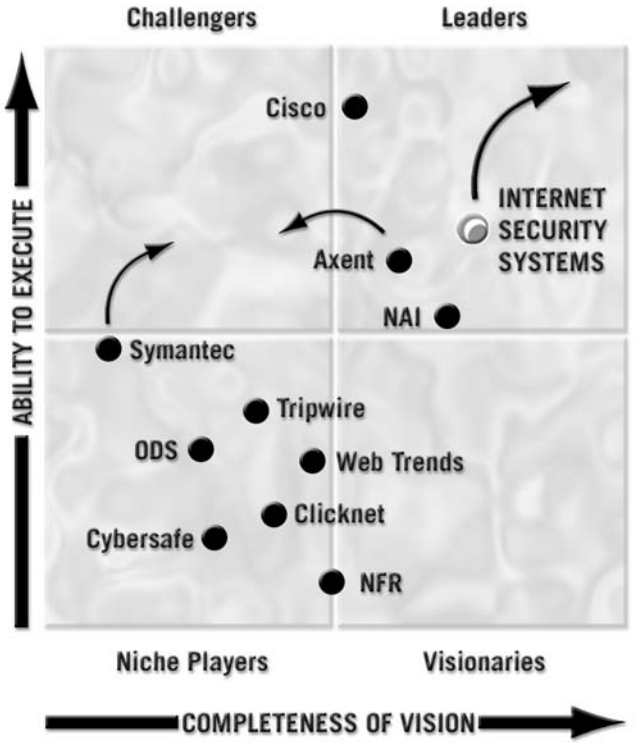
- Rated 5th fastest growing technology company in North America by Deloitte & Touche
- Recognized by Gartner Group in the "Magic Quadrant"
- Ranked by IDC as the market leader worldwide: 71 percent share of combined intrusion detection/vulnerability assessment market

IDC-Worldwide Market Leader in IDnA



Gartner's Magic Quadrant

Source:
Gartner Research



Why ISS Will Succeed

- Profitable, well-managed industry leader
- Innovative, customer-driven
- Delivers superior value
- Solutions focus: making business protection easier to understand, easier to buy and easier to deploy and manage
- Best-of-breed partners

Why SecurePartners Will Succeed

- Access to best-in-class channel programs
- Dedicated sales and technical support team helps drive value and increase sales
- World-class sales and technical training

- Simplified security solutions including products, consulting, education and managed security services
- Technology leader: technical resources like the ISS' X-Force™ team helps bring the best prevention and detection solutions to market faster

The intrusion detection and assessment market has just expanded to include the security mainstream – opportunities are greater than ever!

Industry Partners

Aventail	Netscape
Check Point	Nokia
Compaq	Nortel Networks
Entrust Technologies	Stonesoft
GTE Internetworking	Sun Microsystems
Hewlett Packard	Top Layer
Lucent Technologies	TrendMicro
Marsh	V-One
MCI Worldcom	WatchGuard
Microsoft	Websense
NEC	

Product and Service Descriptions

Following is the current high-level messaging for Internet Security Systems' most important brands, products and services.

Mission

To be our partners' trusted security partner and premier provider of security management solutions for the Internet.

Value Proposition

Make information security simpler, more powerful and more cost effective for a broader range of customers worldwide.

Positioning

ISS approaches Internet security through a complete lifecycle approach, offering a managed solution that covers the full continuum of Internet security needs. This standards-based approach creates a continuous cycle of information security centered on five complementary areas: assessment, design, deployment, management, education and support (ADDME™). By using our customers' business objectives as the starting point for building an information security solution, ISS avoids the trap of a one-size-fits-all approach to Internet security. The result is a risk management solution that is supported and understood by both technical and executive staff, a proper mix of in-house and outsourced security alternatives, and careful attention to creating achievable and enforceable security policy.

ADDME Solution Lifecycle

Yet ISS doesn't stop there. ISS' team of world-class security experts remain steadfastly focused on uncovering, documenting and inoculating against the latest threats. This team of specialists, dubbed the X-Force, understands exactly how to transform the complex technical challenges into a practical and affordable strategy. SecureU™, ISS' comprehensive education services, in turn provides the knowledge transfer necessary to ensure that customers can maximize their investment in an ISS solution.

Tagline

The Power to Protect℠

The Power to Protect translates to:

- Standards-based, business-oriented solutions
- World-renowned research and development
- Market-leading software and services
- Innovative outsourced managed security services
- A successful, financially stable partner

Add it up and ISS delivers. And that confidence in turn gives ISS partners the power to grow. We have invested in this tagline over the years and have a lot of equity in it. The tagline should be used as it is today – always on the same page as the Internet Security Systems logo.

ISS Brands

Internet Security Systems™ – Our company name is our primary brand. Key brand messages about Internet Security Systems include:

- Stable, financially successful partner
- Solves business problems with cost-effective, business-driven solutions
- Rapid, proactive response to customer needs
- Experienced knowledge leader – we have earned our customers' trust
- This is about protecting my business – why rely on anyone but the best?

X-Force™ – ISS' team of world-leading security experts dedicated to counter intelligence against hacker threats. X-Force experts are focused solely on uncovering, documenting and coding the latest black hat tricks. They routinely work with ISS solutions engineers to rapidly update software and be the first to bring to market new prevention and detection solutions. By documenting security risks and developing valuable fix action information, the X-Force created the industry's first and largest on-line information protection center – the X-Force Knowledge Base, available publicly at xforce.iss.net.

RealSecure™ – a powerful, automated, real-time intrusion protection system for computer networks and hosts. RealSecure provides unobtrusive, continuous surveillance, intercepting and responding to security breaches and network abuse before systems are compromised. It also provides effective intrusion protection solutions by offering diversified sensors and management consoles.

RealSecure™ for Nokia – an automated, real-time, intrusion detection solution that manages online risk through cost-effective network surveillance and automated response to suspicious activity. RealSecure network sensor is integrated into Nokia Network Security Platform hardware to quietly monitor network packet traffic for patterns of misuse. This appliance is designed for easy deployment, features a hardened operating system, plug-and-play technology and "hot swappable" components for uninterrupted service.

Internet Scanner™ – provides automated, network-based security assessment and policy compliance evaluation. Internet Scanner performs scheduled or event-driven probes of network communication services, operating systems, routers, e-mail and Web servers, firewalls, and applications, thereby identifying system weaknesses which could result in unauthorized network access. Internet Scanner generates reports ranging from executive-level trend analysis to detailed step-by-step instructions for eliminating security risks, including automatic links to vendor Web sites for software patches.

System Scanner™ – System Scanner is the industry's leading solution for host-based security assessment and policy compliance evaluation. System Scanner Agents leverage ISS' extensive X-Force Security Knowledge base to scan systems automatically, applying a comprehensive set of host-based security vulnerability checks and policy rules to quickly identify security risks. System Scanner includes built-in best practice configuration based on Internet Security Systems' extensive policy management consulting experience. Designed to support the flexibility required by changing e-business and enterprise environments, System Scanner works in either centralized or distributed configurations. Hundreds of servers can be grouped together for ease of management, yet variances can be granted on a single-machine basis.

Database Scanner™ – Database Scanner is the first security assessment solution engineered specifically to provide automated vulnerability assessment and analysis for database applications. Predefined and customizable security policies allow users to quickly tailor security levels and enforcement to the needs of their databases and database-driven applications. Database Scanner automatically identifies potential security exposures in database systems and applications, ranging from weak passwords to Trojan horses. Its built-in knowledge base, directly accessible from easily understood reports, recommends corrective action for violations and noncompliance. Database Scanner supports assessment for Oracle, Microsoft SQL Server and Sybase databases.

ISS Services

For SecurePartners who need assistance selling a total solution, ISS has the answer. Contact your channel account manager to discuss additional options of reselling our Consulting or Educational Services.

Consulting Services – can be resold to extend your total security solution. ISS Consulting Services will work with SecurePartner customers to plan and implement an information security solution that is most appropriate. Our highly experienced consultants design a customized strategy given the organization's online assets, architectural maturity, and industry within the marketplace. Armed with a standards-based solutions methodology and ISS' intellectual capital, our consultants are 100 percent security-focused. All ISS consultants are highly experienced, certified security experts covering major security technologies, operating systems and applications. Our professionals provide proven and reliable security solutions that protect mission-critical networks, hosts, databases and applications. They utilize the knowledge and expertise offered by ISS' X-Force, our world-renowned research and development team, as well as ISS' award-winning security management software, to provide complete solutions for our customers, regardless of size or industry.

Managed Security Services – powerful business solutions that protect critical infrastructure 24 hours a day, 7 days a week, 365 days a year. ISS Managed Security Services work without an extensive investment in staff or technology, for organizations ranging from startups to global enterprises. ISS' MSS programs address two distinctly different market needs. Each managed service is available directly from ISS, or from more than twenty managed security providers. This flexibility allows any business to receive best-of-breed security management, either directly from the industry leader, or as part of a broader offering from a trusted business services provider.

Educational Services – ISS' SecureU provides targeted educational programs to meet the needs of IT security professionals. These programs include courses in the fundamentals of security and networking, vulnerability management, threat management and intrusion detection, public key infrastructures, firewalls, and others. Each course offers the option of certification via standardized examinations and can be resold by SecurePartners that want to offer customers a total security solution. SecureU also offers state-of-the-art computer-based training in intrusion detection which leverages the intellectual capital of our technical developers, the ISS X-Force research team and field engineers to our customers' desktops.

Did You Know?

Here's the latest information on protection for online assets.

What is protection

In today's market, online protection means that valuable online assets, whether customer records, proprietary trade secrets or access to critical systems, are protected against attack and misuse.

What needs protection

It's simple – basically anything in an enterprise that carries or houses information – like networks, servers, desktops and databases – and allows access points to the network outside the corporate firewall from mobile systems, remote offices to wireless systems.

The goal is to value, prioritize and protect an organization's online presence, wherever or whatever that presence might be. Managing the technology that makes protection happen should be its complement, as inexpensive and unobtrusive as possible.

Why your customers buy protection

Security has become routine in our daily lives. We lock houses and cars, take care no one is looking over our shoulders when we use ATM cards; we even lock sensitive documents in a drawer. Customers need to take the same approach to information security.

As the world becomes increasingly connected, risk rises accordingly. Potential security risks include:

- hackers, both inside and outside an organization
- former and/or disgruntled employees
- vandals
- vendors
- foreign governments
- industry spies
- script kiddies

In response, businesses need a means to manage risk without disrupting normal operations or having to invest more money in a security solution than is necessary.

ISS products/services create sales opportunities

Internet Security Systems' family of products offers customers award-winning Security Assessment and Intrusion Detection solutions. An integrated set of standards-based, best-of-breed security solutions, these offerings provide comprehensive security support – from the initial planning stages of protecting your e-business assets to controlling threats and vulnerabilities and supporting overall analysis and decision-making processes. Our offerings help customers develop sound security strategies that effectively monitor and protect critical online assets, providing continuous status updates and necessary automated security improvements with minimal impact on your network performance and business operations.

Proactive security assessment products include:

- Internet Scanner
- System Scanner
- Database Scanner

The following RealSecure solutions continuously guard and monitor networks and host-based systems:

- Network Sensor
- RealSecure for Nokia
- Server Sensor
- Workgroup Manager Console

Lull-in-conversation facts

The average corporation currently spends more on coffee and soft drinks than on network security. So says Forrester Research. Here's a few more interesting facts and statistics about information security:

- Eighty-five percent of all attacks are carried out by internal users or users trusted by an organization.
- Since April 1, 2001, over 700 sites in the Peoples Republic of China were defaced or taken down by hackers sympathetic to the United States.
- Chinese hackers allegedly attacked and defaced over 2000 U.S. business and government sites.
- The White House was hit by a denial of service attack in May 2001 that significantly slowed access.

- In a February 2000 report, the Yankee Group asserted that denial of service attacks resulted in capitalization losses that exceeded $1 billion on the days of the attacks, and revenue loss of both sales and advertisement revenue was expected to exceed $100 million for the sites, which included eBay, Buy.com, E-Trade and Amazon.com.
- Nearly one-third of US companies, financial institutions, government agencies and universities say outsiders pene trated their computer systems last year. *(1999 Computer Security Institute/FBI Computer Crime Survey)*
- Although 56 percent of companies surveyed say information security is a high priority, only 19 percent have a complete, descriptive policy to monitor security practices and solutions. *(1999 Computer Security Institute/FBI Computer Crime Survey)*
- According to Forrester Research, 48 percent of the Fortune 1000 companies indicated that security is the most significant factor preventing them from using the Internet to transact business.
- E-commerce companies are more likely to be targeted by hackers, according to a survey by Information Security magazine. The rate at which company networks are breached has nearly doubled in the last year, and the average loss was estimated at $256,000.
- The FBI estimates that electronic crime costs US companies $10 billion per year. Hacking incidents are expensive not only because of what's taken, but because of costs associated with cleaning up the mess.
- For the third straight year, financial losses due to computer security breaches mounted to more than $100 million. The most serious financial losses occurred through theft of proprietary information and financial fraud. *(1999 Computer Security Institute/FBI Computer Crime Survey)*

Product Battle Cards

Hot Buttons and Trends

Analysts Frost & Sullivan forecast the intrusion detection and assessment software market to grow to $1.6 billion by 2006. In addition, IDC predicts:

- the size of the security consulting market should more than double to $14.8 billion by 2003 from $6.2 billion in 1999
- worldwide security software market will grow from an estimated $4.2 billion in 1999 and $7.4 billion by 2002

The security market continues to grow, creating tremendous upside potential. Gartner Group points out one stunning reality behind these forecasts: half of small to mid-sized businesses implementing their own security measures will fall prey to cyber crime within the next two years. So, it's clear – companies need help securing digital assets.

Use these Battle Cards to arm yourself with the information you need for selling and positioning Internet Security Systems' products and services. But first, get to know a little more about our customers – the security elite and security mainstream.

Security Elite

Internet Security Systems defines early adopters as security elite – either a "guru" (IT manager) or member of the IT operations staff (security network, systems or database administrators). Although the *security elite* know ISS, messages tailored to their specific objectives will smooth the sales process. Keep in mind:

- Gurus are looking for the next big thing
- Operations staff have to implement the next big thing
- The hand-off from guru to operations begins the transition from security elite to security mainstream

Security elite gurus are often responsible for enterprise-wide purchases. They play on the leading edge, wanting a combination of best technology currently available (even if deployment and integration aren't perfect) and redundant solutions for in-house security information management. Tell gurus:

- ISS provides unmatched breadth, depth and manageability in security management

- ISS will continue our technology leadership
- ISS will continue to drive the market for enterprise configuration, deployment, scalability, management and analysis

Security elite operations staff typically deploy the guru's chosen solution. Since they want backing and strong resources, tell them:

- ISS knows how to make this technology operational
- ISS understands how to manage security across an enterprise
- ISS is experienced, reliable, proactive

Security Mainstream

Customers in this market play it safe; their philosophy is "no one ever got fired for buying IBM!" The *security mainstream* represents *ISS' key growth market.* Here, we have an opportunity for comprehensive coverage wins. In general, *security mainstream* customers are business people needing business solutions – a CIO, CSO, CTO, director of IT or a corporate independent security auditor consultant, for example. Keep in mind, mainstreamers want:

- as complete a solution as possible, not disparate technology
- reference accounts
- comfortable, long-term relationships with vendors they can trust
- self-sufficient technology *(no one delivers this yet)*
- confidence that vendors understand their business needs and will craft programs to fit
- to spend wisely, and only when necessary

Because of this "solution" mindset, mainstreamers prefer a single vendor and/or one with which they have an existing relationship. They tend to make smaller purchases and think about enterprise integration much later. Tell mainstreamers:

- ISS is established, respected, profitable
- ISS offers comprehensive, single-vendor coverage including products, consulting, education and managed security services
- *Any* organization with a network has data at risk
- Our core business is security solutions not simply technology

- Executives already understand digital assets need protection but may not be clear what a solid solution looks like

A Competitive Products Overview

Each Battle Card includes a competitive brief to help position Internet Security Systems products against a variety of competitors. Keep in mind the following tips:

How to Break Down the Competition

- *Understand competitor strengths and weaknesses.* Do your own research and READ competitive reviews.
- *Understand EXACTLY what customers' requirements are.*
  - What problems are they trying to solve?
  - Why are they interested in a competitor?
  - What features do they believe a competitor has that Internet Security Systems does not?

Now use the following Battle Cards to arm yourself with the information you need for selling and positioning Internet Security Systems' products.

- RealSecure – Intrusion detection that continuously guards and monitors networks and host based systems.
- Internet Scanner, Database Scanner and System Scanner – proactive security assessment products.

RealSecure™ Battle Card

Product Positioning

Here's a quick reference of the most common questions your customers might raise.

We already have a firewall, why do we need RealSecure?

- Firewalls and RealSecure use similar technologies to accomplish different things. Firewalls are controlling entities, enforcing general entry and exit rules for an entire network but unable to look for attack patterns. RealSecure does not interfere with the network traffic streams. Rather, it allows traffic to go by while quietly watching for signs of unauthorized activity. RealSecure's definition of "unauthorized activity" is a sophisticated and customizable database of attack signatures.
- Firewalls must guarantee some degree of access which may allow for vulnerability probing.
- Firewall policies may lag behind environmental changes which leaves room for possible entry and attack.
- Firewalls do not prevent the use of unauthorized or unsecured modems as a means to enter or leave a network.
- Firewalls do not operate at speeds conducive to intranet deployment.

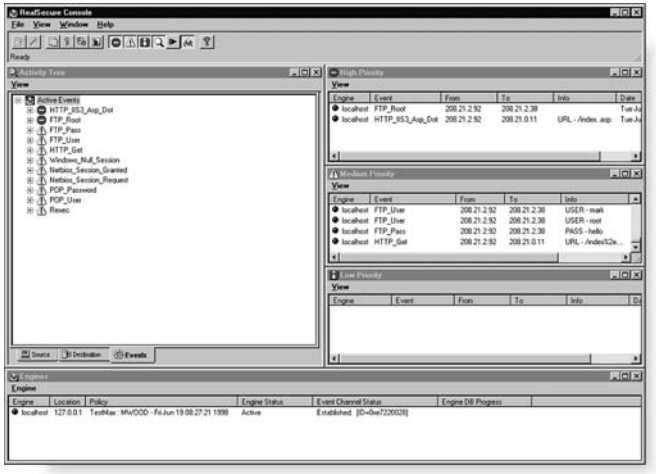
Do I need firewalls if I have RealSecure?

- Absolutely. RealSecure is an essential addition to, but not replacement for, firewall security.
- Even when firewalls are properly configured, they keep out most undesired traffic but still have tunnels, like FTP, that can be exploited by would-be attackers. A firewall will not stop an attack like gaining root access to the FTP server. By monitoring the traffic stream on the network behind the firewall, RealSecure can detect and terminate attempts to gain root access on the FTP server.
- Remember: firewalls have tunnels that allow packets through; firewalls are frequently misconfigured and firewalls can be compromised by an external attacker.

Position RealSecure as a *comprehensive intrusion detection product family* offering a diversified sensor grid – network-based IDS (Network Sensor), host-based IDS (Server Sensor), Network IDS appliance (RealSecure for Nokia), and a single integrated management console (Workgroup Manager) with a command line interface. *None of our competitors offer this type of a complete solution in an integrated family.*

Product Definition

Because Internet Security Systems' RealSecure is an enterprise threat management system, it provides end-to-end protection from internal and external threats against network assets. With RealSecure, networks can be opened to enhance online business operations while significantly improving security and accountability. RealSecure detection components monitor network and server activity for signs of malicious intent, such as denial of service attacks, unauthorized access attempts, and pre-attack reconnaissance probes. When RealSecure detects such activity, the system can respond in a variety of ways, including recording the event, notifying the network administrator immediately, and terminating the attack automatically. By providing a flexible variety of detection and response modules, as well as a sophisticated, centralized management console, RealSecure offers the most advanced threat management for enterprise networks available.



Suspicious activity on the RealSecure Workgroup Manager console.

An enterprise threat management system should form the framework to manage risk without disrupting normal operations and without forcing investment in more security solution technology than necessary. RealSecure meets this requirement through a distributed client-server architecture, with components that fall into two functional categories:

- *Sensors* – a class of modules that provide automated detection and response to threats. These modules are installed at strategic locations throughout the enterprise network and include: a *network sensor* that monitors network traffic in real-time for signs of malicious intent and responds automatically; a *server sensor* that monitors inbound and outbound network traffic directed at a single host as well as the operating system log entries and key system files for indications of intrusion or authorized activity.
- *Workgroup Manager* – a powerful, flexible management console that provides for configuration of the sensors, as well as detailed management and storage of threat data generated by sensors. All RealSecure sensor management is accomplished across secure communication channels. Workgroup Manager modules include: *a console* that allows for centralized control of remote sensors and provides for centralized display of alerts and reporting; *event collectors* which collect data from many sensors in real-time and send data to the enterprise database and console; *an enterprise database* that stores the sensors' event data; and, *an asset database* that contains information about assets including event collectors and sensors.

Internet Security Systems' RealSecure application is a powerful, automated, real-time intrusion detection system for computer networks and hosts, providing customers with end-to-end protection from internal and external threats against network assets.

Key Advantages

The key advantages of RealSecure include:

- Easily adapts to any network environment through flexible sensor options and a scalable, centralized management console
- Intrusion protection with real-time response to improper activity
- Flexible design, which quickly adjusts for different network needs
- Automatic product updates make the latest network security information available and active
- Fast, easily managed reporting system saves time and money by accelerating the monitoring and review process
- Detailed online help system allows RealSecure to be used by less experienced operators thereby reducing cost of ownership and training
- Minimal impact on network traffic and host systems means RealSecure unobtrusively monitors network traffic enabling enhanced security coverage without affecting performance of the network and critical systems
- Self-installing X-Press Update product enhancements, developed with research from the ISS X-Force, ensure the latest network security information is available and active

End result – a flexible, scalable approach to security management with minimal impact on network performance; fortified with the latest network security protection information; cost-effective and easily managed, freeing up time for other critical IT tasks.

Where to Aim

Target customers who want or need to:

- reduce the impact of both internal and external threats
- want a second line of defense
- protect strategic network segments with servers that house critical information and services (finance, human resources, R&D)
- unobtrusively control inter-networking activity across the WAN in support of business-to-business connectivity

Getting the Sale Started

Emphasize these key points when pitching to Security Elite:

- Show how the product can capture valuable forensic information to protect against abuse
- Stop hackers in their tracks...eliminate unauthorized network activity
- Stress fast update capability...protects the IT infrastructure from a growing number of Internet-based attacks
- Emphasize subtlety of security...quietly monitors networks which support emerging e-business initiatives

Accentuate these key points when pitching to Security Mainstreamers:

- Emphasize real-time enforcement of the security policy…ISS combines the latest findings of its X-Force research and development team with RealSecure's real-time notification to deliver most current attack signature updates in the industry
- Stress time savings…comprehensive reporting and management tools eliminate the need for tedious log analysis
- Stress flexibility…the system is easy to customize for real-time response to diverse forms of internal and external threats
- Stress improved service availability…customer networks will be available for business when they need to be
- Emphasize how the product eliminates the need for costly recovery…by responding to threats in real-time

Competitive Market — IDS

Here's how competitive IDS products stack up to RealSecure.

Cisco

Cisco Secure IDS is the former NetRanger.

- *Strengths:* Cisco usually has an established relationship with network managers in companies. They push hard to sell embedded IDS in router and switch blade.
- *Weaknesses:* Current embedded IDS in routers have shown slow performance and support a limited number of attack signatures. Cisco has no host-based IDS solution. In addition, Cisco is NOT a security company – they have no research team like the ISS X-Force – and can be slow to offer attack signature updates to their products.

Symantec/Axent — NetProwler and Intruder Alert

- *Strengths:* Large platform support on host side, remote update capability, and many options to customize.
- *Weaknesses:* NetProwler requires too much configuration to operate and performance is poor, GUI is hard to understand; Intruder Alert historically has been slow to update – possibly because they support too many platforms. Intruder Alert is considerably hard to configure and customize.

Dragon — Network Security Wizards

- *Strengths:* Web interface, good attack recognition.
- *Weaknesses:* Dragon is difficult to set up and manage without extensive Unix experience. This product runs only in a Unix environment, there is no NT solution. Weak reporting – uses line graph outputs. Very small and young company.

Network Flight Recorder — NFR

- *Strengths:* Allows user to create custom attack signatures, runs on several flavors of Unix and NT.
- *Weaknesses:* NFR is not easy to use; poor reporting, lack of attack signatures, weak technical support.

Clicknet entercept

- *Strengths:* Host-based sensor targeted for small- to medium-sized businesses. Clicknet touts "protection" versus "detection"; Version 1.0 product runs on NT and Solaris.
- *Weaknesses:* "Blue Screen of Death" can be expected when running this product; about 100 attack signatures that are not high risk level; system call filtering non-trivial and very difficult to strike balance between security and functionality; company originally focused on network mapping and documentation, has small resources on security knowledge.

References and Resources

ISS competitive analysts continuously research the marketplace for potential competitive threats and have a clear vision of how to position ISS products to win deals. For additional competitive data, contact your channel account manager who can engage a local ISS sales engineer in your efforts.

Internet Scanner™ Battle Card

Product Positioning

Here's a quick reference of the most common questions your customers might raise.

We already have a firewall, why do we need Internet Scanner?
Firewalls are designed to enforce access control. A misconfiguration can easily allow outsiders to break into the network despite the firewall's presence. The International Computer Security Association (ICSA) uses Internet Scanner to *certify* firewalls to ensure that attackers cannot exploit bugs in the firewall to bypass access controls. Thousands of customers worldwide use Internet Scanner with firewalls to ensure that attackers cannot exploit misconfigurations in the firewall

Can Internet Scanner execute from outside the firewall on devices inside the firewall? Should scans start from inside or outside the firewall?
Firewall scans should attempt to reach at least one address on the opposite side of the firewall in order to test both the firewall itself and traffic it allows through. Assuming Internet Scanner can penetrate the firewall from the outside, it will simulate an attack on all devices authorized with an IP address defined in the key. Inside the firewall, scans identify vulnerabilities on network devices behind the firewall. Internal scans are especially important since roughly 85 percent of all security breaches occur from inside a corporate backbone.

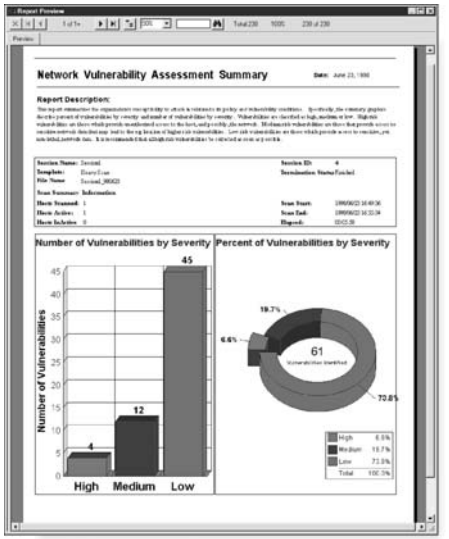
This test can be accomplished, however, only if the firewall will allow packets from the scanner to route through to machines and services behind the firewall. If they cannot, then it is NOT recommended that firewall configurations be changed simply to run a scan!

Why do I need to scan my entire network?
There are many different ways to compromise a network. Scanning the entire network provides a definitive understanding of all available devices and services, and renders a road map of the potential exposure. For example, low-value computers (e.g. desktop workstations) can be compromised with any of a large number of "back door" programs like NetBus or BackOrifice. These systems can then be used to attack more important computers, such as database servers. Regular scanning of desktop computers helps protect important assets.

Product Definition

Internet Scanner provides automated, network-based security assessment and policy compliance evaluation. Internet Scanner performs scheduled or event-driven probes of network communication services, operating systems, routers, e-mail and Web servers, firewalls, and applications, thereby identifying system weaknesses which could result in unauthorized network access. Internet Scanner generates reports ranging from executive-level trend analysis to detailed step-by-step instructions for eliminating security risks, including automatic links to vendor Web sites for software patches.

Internet Scanner's reports produce detailed technical, operational and management information presented in a logical, easily understood format. Each report provides access to instructions for corrective action and vendor sites for security patches.



Key Advantages

- Provides prioritized actions to reduce the risk of exposure for an organization's most critical online assets
- Increases staff efficiency by automating analysis and reporting
- Features the most comprehensive list of vulnerability checks in the industry to greatly reduce risk and develop enforceable network security practices even relatively inexperienced administrators can manage
- Tightly integrated with Database Scanner to identify new database resources on a network and automatically execute risk assessment scans

- Fast, easily managed graphical reporting system saves time and money by accelerating the auditing process
- Scalable and grows with an organization from small networks to enterprise installations
- Self-installing X-Press Update product enhancements, developed with research from the ISS X-Force, ensure the latest network security information is available and active

Where to Aim

Target customers who want or need to:

- identify the need to measure, understand and improve their current level of security
- uncover specific vulnerabilities related to network communication services, operating systems, routers, e-mail and Web servers, firewalls, and applications
- bring their organization into security compliance with government regulation

Getting the Sale Started

Emphasize these key points when pitching to Security Elite:

- Show how someone can hack the Web server and by-pass policy controls…clearly demonstrates what points of vulnerability currently exist
- Emphasize ability to prioritize work…Internet Scanner helps security administrators work on the most critical problems first
- Stress reduced risk exposure…measures whether security risk is being managed properly
- Stress ability to track trends and harden policies…with quantifiable matrix on active internal and external threats

Accentuate these key points when pitching to Security Mainstreamers:

- Emphasize the importance of configuring firewalls correctly…with misconfigured firewalls, security is not effective and still leaves an organization open and vulnerable
- Stress the importance of knowing what's on the network… modems, RAS servers, links to external organizations
- Emphasize cost-savings…Internet Scanner can save time in producing reports which translates to cost-savings for customers

- Stress time-savings…consultants and auditors can better spend time on more important jobs
- Improved profitability…audits are faster, more accurate and more comprehensive which helps boost profitability
- Justifies expense for firewall…nets-out effect of installing firewall and explains how you perform due diligence
- Builds case for new headcount or technology for security… by tracking trends on active internal and external threats

Competitive Market — Vulnerability Assessment

Here's how competitive products compare to Internet Scanner.

CyberCop Scanner

- *Strengths:* Supports Visual Basic scripting; 3D Network Map for qualifying network devices and connections; there is Autofix for registry checks, however, there is no way to undo fixes; also uses CASL (custom attack scripting language) for user-defined checks.
- *Weaknesses:* Slow, unreliable; infrequent updates; Autofix capabilities are limited to registry changes; Autofix lacks "undo" and doesn't track which machines had a fix applied.

NetRecon

- *Strengths:* Uses Crystal Reports for reporting; inexpensive and NetRecon will give the product away to sell more ESM; simple key. "Ultra-scanning", continued scanning, 3-D graphics.
- *Weaknesses:* Poor reports; poor product integration; no policy editor; also lacks highly publicized checks. Cannot perform scans via automatic scheduling; no IP range restrictions or trend analysis; weak technical support.

Cisco — Secure Scanner (formerly NetSonar)

- *Strengths:* Offers network mapping, security vulnerability assessment, decision support, risk management, and security policies validation. Runs on Windows NT, Solaris SPARC and Solaris x86 and has 24-hour tech support.
- *Weaknesses:* Shallow, unsophisticated checks – no depth or breadth. Poor and limited quality fix information. Poor scanning performance – slow and inefficient. Zero checks for firewalls, LDAP, and IOS. Infrequent updates and is not responsive to security threats.

Web Trends — Security Analyzer

- *Strengths:* Attractive reporting interface; integrates with other Web Trends enterprise information management solutions. Automatic updates using WebTrends' Autosync feature.
- *Weaknesses:* AutoSync feature automatically grabs new checks (this can be a fault for elite users, but a strength for mainstreamers); scans are known to run slowly; Web Trends is slow to offer updates to their product and has limited security expertise compared with ISS' X-Force.

Nessus Security Scanner

- *Strengths:* Delivers vulnerability information, automated assessment focusing in the Unix space. This product's check code is readable in plain text in the source and offers total freedom of use, with no restrictions on IP addresses being scanned.
- *Weaknesses:* Very high total cost of ownership. Product requires significant amount of Unix and security expertise to install and use; no policy capabilities; limited report filtering; no documentation or support. Nessus commercial scanners have been know to be overpriced, buggy and inefficient, largely because commercial concerns promoted time-to-market over quality. Checks are written in a custom-built scripting language, so the open source may not be easily readable and verifiable. In addition, many customers have no interest in reading the source code, but would prefer to simply get the checks from a trusted security advisor, such as ISS.

eEye Digital Security — Retina

- *Strengths:* Inexpensive, well-designed GUI for viewing results. Claims to have team of security experts actively researching new vulnerabilities on a 24 x 7 basis. Autofix can fix registry and file permission vulnerabilities.
- *Weaknesses:* Scans are slow and inefficient. No pre-defined policies; weak reporting; unreliable checks; auto-fix is limited. No real automation and is impossible to integrate with other solutions. No browser or backdoor checks and lots of false positives

References and Resources

ISS has competitive analysts continuously researching the marketplace for potential competitive threats and have a clear vision of how to position ISS products to win deals. For additional competitive data, contact your channel account manager who can engage a local ISS sales engineer in your efforts.

System Scanner™ Battle Card

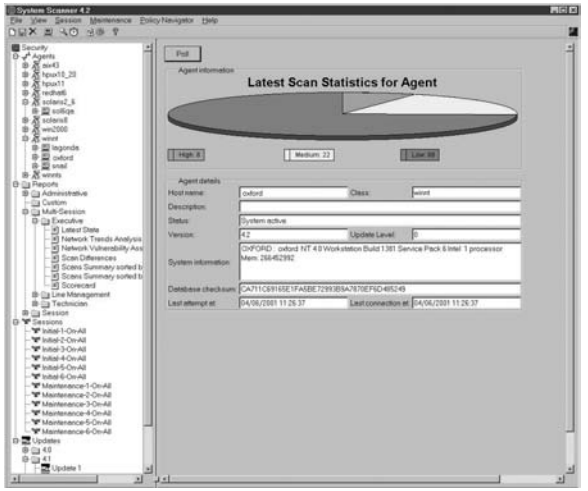
Product Positioning

Here's a quick reference of the most common questions your customers might raise.

How does System Scanner help?
System Scanner helps the user manage the security gap. The gap is the difference between actual security management practice and the desired level of security or requirements of the enterprise security policy has been identified by ISS as a typical situation in many enterprise environments. System Scanner has been designed to help our customers to "Close the Security Gap" and then to ensure maintenance of the "closed gap" by the provision of many security management features.

I have heard that System Scanner is very difficult to install and configure.
NO. System Scanner is very simple to install with Install Shield Wizards on Windows and friendly scripts on UNIX. A typical 'localhost' installation should take no more than 20 minutes.

Agents are available for Windows and Popular UNIX platforms.



Product Definition

System Scanner searches deep into online operations to provide a host-based security assessment that targets

security weaknesses undetectable through network scanning. While Internet Scanner determines vulnerabilities by scanning devices at the network level, System Scanner detects internal vulnerabilities at the system level through a wide variety of cross platform agents that reside on each system. These agents allow a security policy to be implemented, managed, and controlled across an entire enterprise from a centralized point. System Scanner prioritizes security risk based on relative severity, and having secured the system, it locks down the configuration with a digital fingerprint – making it easier to detect unauthorized tampering.

Key Advantages

- Mitigates risks on the most important information assets in any organization – the servers
- Dramatically reduces auditing workload with standard reports
- Adjusts checks and policies to match requirements of company security policy to ensure compliance with policy requirements
- Customizable checks can be easily added to supplement this product's large number of built-in vulnerability, misconfiguration and other tests
- Reduces work for technical support teams and help desks
- Self-installing X-Press Update product enhancements, developed with research from the ISS X-Force, ensure the latest network security information is available and active

Where to Aim

Target customers who want or need to:

- develop a security baseline for multiple system configurations
- ensure compliance with the security policy across the enterprise
- know exactly how effective current security measures are
- enhance the efficiency of system administration staff by automating large portions of security policy management and implementation
- enforce user-based access controls
- rapidly deploy new servers (especially Windows NT/2000)
- better understand vulnerabilities on the network and already use Internet Scanner
- establish an intrusion recovery plan for quickly addressing network incidences and restoring key business services

Getting the Sale Started

Emphasize these key points when pitching to Security Elite:

- Show how someone can by-pass policy controls and become a bigger threat
- Show how the product can validate the integrity of user accounts
- Emphasize validation…System Scanner can quickly validate whether security policies are properly enforced
- Deploy new technologies…to protect confidential customer information in support of new or emerging business practices like e-commerce

Accentuate these key points when pitching to Security Mainstreamers:

- Emphasize how System Scanner can detect if users are running network packet analysis or using bad passwords… it can reveal both internal threats and vulnerable users
- Stress the importance of knowing whether a hacker can break into a system…to demonstrate potential exposure and points of vulnerability
- Stress time-savings…this product can reduce the reporting workload
- Improved security controls…establishes and maintains a security baseline
- Emphasize ability to reduce business impact…by stopping unauthorized activity

Competitive Market — Vulnerability Assessment

Here's how competitive products compare to System Scanner.

Tripwire

- *Strengths:* Multiple platform coverage. Good at "file integrity assessment." Performs system baseline and will report any deviations against it. Large customer base since the product was originally free.
- *Weaknesses:* Does only about 20 percent of what ISS' System Scanner does – does not perform vulnerability assessment, just file integrity assessment. Not scalable, can't configure just one system and roll that policy out

to the enterprise. Weak online help; there is no guidance on what files should be or consequences of modifying those files.

Symantec/Axent — ESM

- *Strengths:* ESM allows for selective automatic updating of agents. The reporting feature provides a user interface to drill down and see the status of an agent and its corresponding policy violations. Product updates – tune-up pack – is available on CD or via Internet.
- *Weaknesses:* Updating agents is not automated as it appears when looking at the ESM Enterprise Console. In order to automatically update an agent; it is necessary to manually upgrade the console first and then manually upgrade the manager. ESM product updates have been known to be limited and infrequent.

References and Resources

ISS has competitive analysts continuously researching the marketplace for potential competitive threats and have a clear vision of how to position ISS products to win deals. For additional competitive data, contact your channel account manager who can engage a local ISS sales engineer in your efforts.

Database Scanner™ Battle Card

Product Positioning

Here's a quick reference of the most common questions your customers might raise.

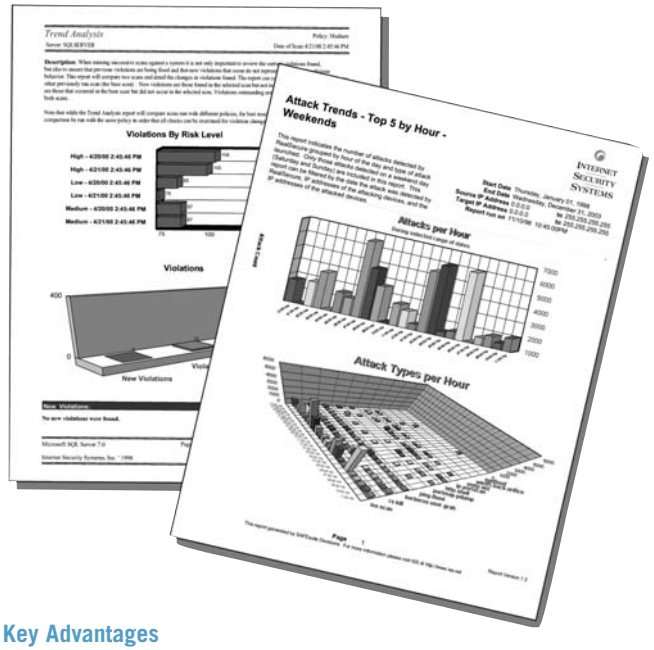
Why is database security important?
Relational databases frequently hold the most critical information assets of an organization. Examples of the types of valuable information assets stored in databases include company financial records, customer information including credit card and account information, proprietary engineering details, medical information, technical assets, etc. It is extremely difficult for even the most experienced database administrator (DBA) to be aware of all database security issues, detect every attack or suspicious activity on a server, and verify that all configuration options are set correctly. Within minutes, Database Scanner can detect what would take security officers, consultants or DBAs days or weeks to research. Database Scanner then provides information to help patch security risks immediately.

How is Database Scanner different from standard database security tools?
Database Scanner provides security checks that are not available in the standard security mechanisms of most relational databases. Database Scanner detects weak passwords, checks password aging (expiration), detects login attacks, disables stale logins (old unused accounts), and tracks login hour restrictions. Regular testing of password strength on every login account is crucial to data integrity and security. Passwords are the first line of defense in accessing a database system. If the passwords aren't routinely checked to meet certain basic criteria such as length, not being easily guessed, and not a word in the dictionary, the contents of a database could be compromised very quickly. Most relational database systems don't require users to have *any* password, let alone one that is difficult to guess, and the lack of other security features combined with this makes the implications even more serious.

Product Definition

Database Scanner is the first security assessment product engineered specifically for protecting database applications through security policy creation, compliance, and enforcement. Database Scanner automatically identifies potential security exposures in database systems – ranging from weak passwords to Trojan horses. Its built-in knowledgebase is directly accessible from user-friendly reports that recommend corrective actions for violations and non-compliance. Available for Oracle, Microsoft SQL Server, and Sybase databases, Database Scanner facilitates ongoing database assessment and security improvement within ISS' easy-to-use Security Management framework.

Easy to read reports contain a detailed graphical analysis with recommended fixes for known violations.



Key Advantages

- Automates the performance of a wide range of vulnerability checks; policy editor speeds and simplifies the creation of scanning policies so users can easily match security practices with needs of business and database applications
- Captures security knowledge in an easy-to-use form for database administrators
- Provides a secure database platform for use in e-commerce applications
- Integration with Internet Scanner allows Internet Scanner to initiate a database scan upon detection of a database on a host
- Fast and easily managed graphical reporting system saves time and money by accelerating the auditing and enforcement process
- Self-installing X-Press Update product enhancements, developed with research from the ISS X-Force, ensure the latest network security information is available and active

Where to Aim

Target customers who want or need to:

- protect access to the organization's most critical information and digital assets stored in databases (financial information, customer records, personnel files, engineering data and product specifications, etc.)
- administer and secure complex systems like databases
- use databases as the foundation of new ERP, e-commerce and extranet business systems

Getting the Sale Started

Emphasize these key points when pitching to Security Elite:

- Emphasize how Database Scanner can help lend familiarity to every setting in the database management system…to ensure if all settings that affect database security are correct
- Show how administrators can know if a database has been compromised
- Stress the importance of knowing all potential security holes in the DBMS…this audit tool outlines vulnerabilities for proper corrective action
- Broadens knowledge-base…this product provides access to best practices, recommendations and corrective actions in database security and builds awareness of potential back doors into the DBMS that could affect the enterprise
- Emphasize ability to mitigate business risk…by controlling e-commerce applications

Accentuate these key points when pitching to Security Mainstreamers:

- Outline how this product helps protect the database from disgruntled employees and ensure passwords are being used correctly

- Emphasize time-savings…Database Scanner can quickly and easily develop, implement and maintain appropriate database security and automate the database security audit and analysis process
- Stress increased confidence…business partners will know databases are secure
- Improve security of company, partner and customer data…databases are scanned to verify security policies and outline what corrective measures may need to be taken
- Stress ability to track trends and harden policies…with quantifiable matrix on active internal and external threats

Competitive Market — Vulnerability Assessment

Here's how competitive products compare to Database Scanner.

Pentasafe — Database Security Administrator

- *Strengths*: Centralized security auditing; monitoring and alerting notifies administrators of database activity and possible security events; password policy enforcement through password manager.
- *Weaknesses:* Complex to configure. Security Manager requires extensive database administration expertise to install and configure. Higher total cost of ownership due to difficult deployment, configuration and management. Slow to update product on the latest vulnerability checks.

Symantec/Axent — ESM for Oracle

- *Strengths:* Sub-module check for vulnerabilities in different areas including access, accounts, auditing and passwords. Integrated with Axent ESM.
- *Weaknesses:* Not certified by Oracle which has resulted in limited Oracle checks. Host based requires installing an agent on every database to be scanned. No command line functionality.

References and Resources

ISS has competitive analysts continuously researching the marketplace for potential competitive threats and have a clear vision of how to position ISS products to win deals. For additional competitive data, contact your channel account manager who can engage a local ISS sales engineer in your efforts.

What's New At ISS?

We recently completed the acquisition of privately-held Network ICE Corporation, a leading developer of desktop intrusion protection technology and highly scalable security management systems. Network ICE was founded in 1998 by a team of network analysis and security experts to solve the problem of intrusion detection and defense for high-speed networks and VPN deployments. Their solutions include enterprise and consumer turnkey intrusion protection and security policy management which use patent-pending technology to protect networks and systems from hackers by detecting and blocking the attack, tracing the identity of the intruder and reporting the details of the attack.

This acquisition broadens our overall market opportunity and enhances our strategy of offering information protection solutions that actively prevent and detect security risks at every potential point of compromise on desktops, servers and networks.

Network ICE's desktop applications and security management solutions complement our leading network and server-based security management software and service solutions by extending our expertise to protect mobile, remote and corporate desktops.

Here's a list of the Network ICE products currently available to our partners:

BlackICE Agent for Workstations – Intrusion protection and personal firewall solution for managed, corporate desktop systems. Available for Windows 95/98/ME, Windows NT, and Windows 2000.

BlackICE Agent for Servers – Intrusion protection and firewall solution for corporate servers. Available for Windows NT, Windows 2000, and Solaris servers.

BlackICE Sentry – Intrusion protection solution for half-duplex 10/100 Ethernet network segments. BlackICE Sentry runs on Windows NT platforms.

BlackICE Sentry Full-Duplex – Intrusion protection solution for full-duplex 10/100 Ethernet network segments. BlackICE Sentry Full-Diplex runs on Windows NT platforms.

BlackICE Gigabit Sentry – Intrusion protection solution for Gigabit Ethernet network segments. BlackICE Gigabit Sentry runs on Windows NT platforms.

BlackICE Guard – Inline intrusion protection solution for legacy assets (such as mainframes) as well as critical network segments. BlackICE Guard comes with a bypass fail-over unit and runs on Windows NT platforms.

ICEcap Manager – Management console for BlackICE Agent for Workstations, BlackICE Agent for Servers, BlackICE Sentry, BlackICE Gigabit Sentry, and BlackICE Guard.

Roadmap

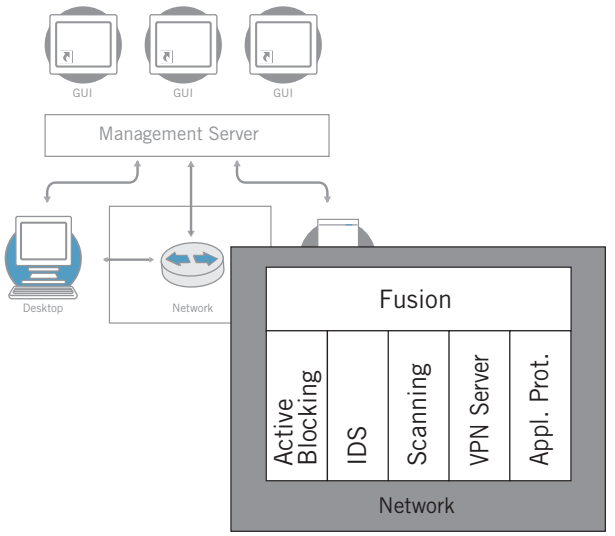
Integration of Network ICE's desktop applications and security management solutions began when the acquisition closed on June 5, 2001. Integration efforts will take place in several stages with the probability that full and complete integration of the product lines will not be complete until the end of 2002.

Ultimately, our products will become one with Network ICE's, which means:

- RealSecure Network Sensor and BlackICE Sentry will be integrated to create a single sensor for 10/100 Ethernet segments.
- RealSecure Server Sensor and BlackICE Agent for Servers will be integrated to create a single sensor for Windows NT and Windows 2000 servers.
- The capabilities of RealSecure Workgroup Manager and ICEcap Manager will be integrated into RealSecure Site Protector, ISS' unified management console initiative.

Our future product strategy involves restructuring our technology to map to the way businesses operate. The ISS roadmap includes:

RealSecure Protection Systems for Networks provides comprehensive security services across networks ranging from standalone installations to complex enterprise operations.

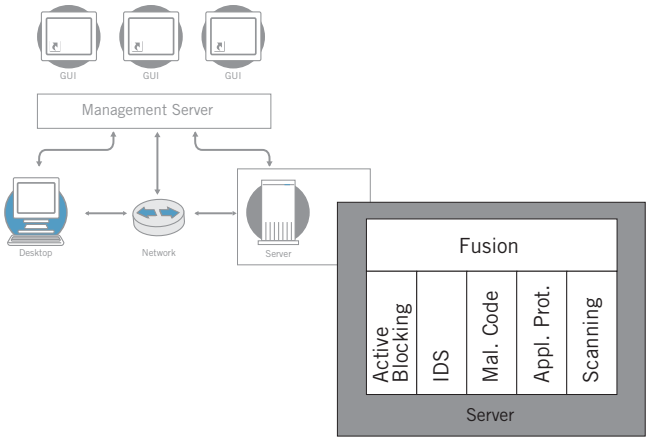


RealSecure™ Protection Systems for Networks – provides a wide range of essential security services, all tightly integrated into a centralized operational and management framework. These components include firewall protection at both the network perimeter and on internal segments, VPN server capabilities, comprehensive high-speed intrusion detection and response, vulnerability assessment and network resource identification, and malicious code elimination.

Corporate networks connect businesses to users, customers, vendors and partners. They also provide the primary conduit for online theft, vandalism and misuse of corporate resources. Key messages to keep in mind for RealSecure Protection Systems for Networks include:

- network security is flexible and sufficiently self-contained
- handles protection tasks with minimal administration
- doesn't interfere with network performance

RealSecure Protection Systems for Servers augments an already comprehensive set of security services with protection for critical server-based applications.



RealSecure™ Protection Systems for Servers – combines sophisticated, distributed firewall capabilities, host-based intrusion detection and response, security policy distribution and compliance, malicious code elimination, and specialized defensive measures for applications running at the server level. All Server operations are tightly integrated with each other, and report to a central console for simplified configuration and management.

Key messages for RealSecure Protection Systems for Servers include:

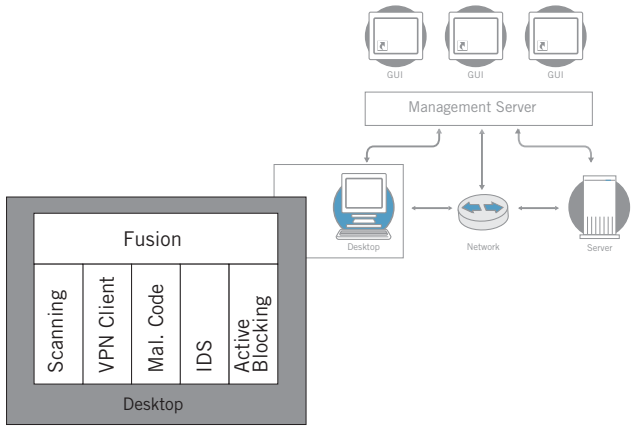
- server security system defends both the server and applications running on that server
- solution is transparent and constantly available, having as little impact on server's daily operations as possible

RealSecure™ Protection Systems for Desktops – hardens individual desktops against mis-configuration and malicious code, provides localized firewall capabilities, establishes Virtual Private Network (VPN) connections inside the corporate firewall and detects and responds to attacks against the local system. These operations take place with minimal effect on end users, while maintaining constant, secure communications with a central management console for oversight by security or IT staff.

ISS recognizes the desktop is any organization's first opportunity to prevent misuse or theft of online corporate assets. Key messages for RealSecure Protection Systems for Desktops include:

- establishes security at the desktop, which is becoming increasingly critical as remote workers, home workers and mobile workers extend access to corporate resources outside traditional enterprise defenses
- these tightly integrated offerings are centrally distributed, configured and managed
- scalable up to thousands of individual users

RealSecure Protection Systems for Desktops includes vulnerability assessment, VPN client services, malicious code control, intrusion detection and response, access control/active blocking, and security data correlation to harden desktops against attack and misuse.



INTERNET
SECURITY
SYSTEMS™

About Internet Security Systems (ISS)
Internet Security Systems, Inc. (ISS) (Nasdaq: ISSX) is the leading global provider of security management solutions for the Internet. ISS protects critical information and network resources from attack and misuse. By combining best of breed software products, market-leading managed security services, aggressive research and development, and comprehensive educational and consulting services, ISS is the trusted security provider for thousands of customers around the world.