VENDOR PROFILE

IBM ISS: Two Years Later

Jon Crotty          Irida Xheneti
Ramasubramoni. R    Andrew J. Hanson

IDC OPINION

While many secure content and threat management (SCTM) vendors are pushed to niche market segments or peripheral product solutions, a select group of major vendors, such as IBM, can expect to thrive and diversify their portfolio within this market. The IBM Internet Security Systems (ISS) products and services family is well positioned to do this with a broad offering that includes threat mitigation solutions, intrusion detection systems (IDS), intrusion prevention systems (IPS), professional services, and managed security services (MSS). IBM's successful foray into the security and vulnerability management (SVM) market and security services market has expanded the company's security solutions portfolio, which already includes a broad range of solutions spanning a variety of technologies, platforms, and markets. Highlights include:

- IBM ISS led the worldwide IPS market in the $100,000+ price band in 2008.
- IBM's acquisition of ISS catapulted IBM to become a leader in the security services market from both a capability and a credibility perspective.
- ISS integrated its software solutions into the Tivoli portfolio and introduced an all-in-one low-cost security appliance for small and medium-sized businesses, an SSL virtual private network (VPN) that caters to large and small customers, and a virtual appliance version of its network intrusion prevention system.

IN THIS VENDOR PROFILE

This IDC Vendor Profile profiles IBM Internet Security Systems (ISS), a leading security services provider and vendor of intrusion detection and prevention systems. IBM's acquisition of ISS has further enhanced IBM's posture in the security market by creating a well rounded portfolio of professional and managed security services. IBM ISS offers a wide range of security products, with the strength of the IBM brand powering its products in a very competitive market.

SITUATION OVERVIEW

Enterprises and end users around the globe are constantly deploying new technologies; employing resources available on the Web; and transforming their IT infrastructure to improve business operations, reduce costs, and increase revenue.
While new cost-cutting technologies such as virtualization, mobility, and green IT are enabling organizations to cut cost and improve customer experiences, they have also become the primary target for the majority of security threats and vulnerabilities. Furthermore, the regulatory environment has become more stringent, requiring organizations to have in place robust corporate risk management programs to prevent instances of data loss exposing companies to serious legal and financial repercussions. Today's constantly connected enterprise has significantly transformed the perception of doing business in a global environment. Increasing instances of information leaks, identity and access management loopholes, and compliance violations are fueling demand for robust security solutions that will address not only the perimeter security challenges but more importantly the internal security vulnerabilities that are increasingly exposing organizations to a number of security vulnerabilities. Periodic security risk assessments, vulnerability assessments, event management, and correlation services coupled with security vulnerability products and services will continue to be in significant demand. While organizations undergo IT budget reductions due to the current economic downturn, organizations are further evaluating innovative cost-cutting technologies and assessing the security impacts to proactively manage risk and meet compliance regulations.

**Security and Vulnerability Management**

The security and vulnerability management software market, which includes policy and compliance, security information and event management, and proactive endpoint risk management, is becoming increasingly important to businesses worldwide, a fact borne out by 19.4% year-over-year growth in 2007 to reach $2.25 billion in total revenue. IDC sees continuing growth potential for the total market and expects that each of the submarkets listed above will individually exceed $1 billion in total revenue in the next three to four years.

Despite significant merger and acquisition activity in 2007, the SVM software market remains large and diverse. It currently consists of over 65 vendors, and not one of them has been able to garner more than 10% market share individually. The consolidation of vendors is constantly balanced by new technologies, start-ups, solutions, and niche vendors that are spawned to address increasing and diversifying threats as well as government and industry regulations. Although there are some leading vendors that provide a large portfolio of SVM solutions, IDC expects the SVM market to remain diverse and open for heated competition.

**Secure Content and Threat Management**

In the secure content and threat management market, IDC expects that over the next few years, the separate desktop antivirus, desktop antispyware, desktop firewall, and host intrusion prevention products will be incorporated into a single, integrated endpoint security product. Unlike endpoint suites that tie disparate products into a single installation, the trend is moving toward a single product that can perform all of the tasks available in the individual products. This trend will gain in popularity among both corporate users and consumers looking for comprehensive security with improved management capabilities and system performance.
Additionally, IDC expects virtualization technologies to see increasing use in the SCTM market. Virtualization allows security administrators to run multiple layers of defense in a single box, reducing the capex and system footprint.

**Managed Security Services**

Given the increasing complexity of the threat landscape, budget constraints, government and industry regulations, and the need for improved business operations, the managed security services market continues its dynamic growth trajectory. IDC expects the U.S. managed security services market to grow by a compound annual growth rate of over 15.7% to reach $2.8 billion by 2012. The pace of today’s technology is evolving rapidly and is creating a significant IT infrastructure overhaul. As organizations continue to grow and strive to become more competitive, they add more remote employees, further extend their partnerships, and collaborate with suppliers and customers. This interconnectivity between organizations has led companies to implement and integrate the appropriate technologies to increase the productivity of their employees and enable more efficient collaboration with partners, suppliers, and customers. While new technology initiatives such as virtualization, mobility, and green IT initiatives empower organizations to decrease cost and greater growth opportunities, they have also become the source of many IT security vulnerabilities. To address these security vulnerabilities, organizations have moved away from deploying point products to building a comprehensive security architecture that utilizes a combination of security products and services to develop a comprehensive risk management strategy. Clearly, standalone security systems can no longer keep up with the sophisticated threat landscape, and IT security skills and expertise seem to be inadequate to address monitoring, management, and event analytics types of challenges. IDC believes that managed security services are a very attractive option for enterprises of all sizes.

**Company Overview**

IBM Internet Security Systems provides security products and services that protect organizations against security vulnerabilities and threats. IBM ISS solutions include intrusion detection and prevention systems as well as professional and managed security services. The company has been on the vanguard of intrusion prevention solutions, and it continues to develop its security products offering to provide a comprehensive security architecture for businesses of all sizes.

ISS, headquartered in Atlanta, Georgia, was founded in 1994 and in the same year unveiled its flagship product, the Internet Scanner, but would soon expand its portfolio with additional security software such as the Network Sensor and Server Sensor. In 1998, the company made its initial public offering on the Nasdaq. Along the way, ISS acquired March Information Systems, a United Kingdom–based company whose Security Manager product was rebranded as System Scanner. Other acquisitions include Network ICE's BlackICE technology and a database security solution, Database Scanner, that came from the acquisition of DbSecure. In addition, ISS acquired Netrex Secure Solutions for its managed security services capabilities and Germany-based Cobion AG, which provided ISS with enhanced spam/URL/content filtering capabilities.
In August 2006, IBM acquired ISS in a deal valued at about $1.3 billion. The acquisition strengthened IBM's security solutions portfolio with security services capabilities, intrusion prevention products, security software, and hardware appliances. Furthermore, ISS provided IBM with a foothold in the managed security services market, a good complement to IBM's other service offerings and an area that is primed for significant growth in the future. After the acquisition, ISS continues to operate as an integrated business unit within IBM's global technology services organization, while ISS' software products were integrated with the IBM Tivoli line, so that all future development of the ISS products are in sync with Tivoli to ensure tight integration and compatibility. The acquisition also gave IBM the security research and intelligence information continually collected by the IBM X-Force security research team, which is known around the world for its capabilities. X-Force is beneficial not only for its research capabilities but also for helping IBM bring new security technologies to market while continually translating the threat data it collects into preemptive protection for clients. IBM is working to leverage the products, services, security intelligence, and capabilities acquired with Internet Security Systems to embed security into other IBM offerings.

Company Strategy

IBM ISS is best known for its managed security services capabilities; security software products such as Proventia, its intrusion protection system; and RealSecure, its intrusion detection system. However, the primary attraction for IBM in its takeover of ISS in 2006 was the company's managed security services. IBM stated that its intention behind the acquisition was to bolster its own managed security services; to move its range of hardware, software, managed services, and consulting solutions into a set of automated, repeatable services that can be sold through its partners; and to launch itself into security services. The deal provided ISS the backing of IBM's resources, technology partnerships, and customer service channels to encourage transition to the new model. Today, IBM ISS provides a full suite of security solutions, including professional services and managed security services targeted primarily at enterprise-level customers and some scalable solutions that are also able to reach the SMB segment. The current strategy allows IBM ISS to wrap services around all its security product capabilities to provide customers with a breadth of scalable security solutions. In addition to managing the IBM security products, IBM also manages many other vendor security products to allow customers to take advantage of this flexible service delivery model. Currently, IBM ISS provides security monitoring and management services for firewall, network IDS/IPS, server IDS/IPS, desktop IDS/IPS. IBM also offers UTM, IAM, event and log management, vulnerability scanning, and email and Web security.

Several key differentiators for IBM ISS have catapulted the company to a leading position in the security services market. Bolstering eight global security operations centers, IBM ISS can provide 24 x 7 monitoring and management services to its customers on a global basis. Furthermore, the acquisition of ISS took IBM back into the network security market, which it had exited years earlier, and expanded the company's reach into the security space. With the addition of UTM appliances and other threat protection solutions that complement its range of identity management, application management, and systems management solutions, IBM was able to
develop a new stream of revenue with a comprehensive portfolio to target the threat protection market.

IBM ISS expects the next generation of threat protection to be one where the vast majority of solutions are delivered as services over an extensible, open platform, with security appliances and software becoming the enabling technologies. The strategy at ISS is to move away from single-function, point products; reduce costs; and reduce complexity associated with security solutions. As of November 2007, IBM has committed to investing $1.5 billion to strengthen its security arm by empowering IBM ISS to provide the enterprise market with end-to-end security solutions that are baked into business processes. IBM recognizes exceptional growth potential in the managed security services and is positioning IBM ISS to be a leading security solutions provider as the market matures.

**Product Architecture**

IBM ISS provides security software and services that offer monitoring, detection, and response capabilities to protect networks, servers, and desktops. Its products recognize and respond to intrusions, assess vulnerabilities, collect and analyze data, and provide centralized security management. The company also offers a growing portfolio of managed security services, including security assessment, intrusion detection, firewalls, virtual private networks, and virus filtering.

In September 2008, the company announced new security services and products that help businesses manage operation and IT risk as part of an initiative to help conform to growing compliance requirements. Key elements of the announcement were:

- A new release of its unified threat management (UTM) solution tailored for small businesses, including an SSL VPN
- A virtual appliance version of its network intrusion prevention system (with plans to offer a virtual appliance version of its UTM offering)
- An update to its network enterprise vulnerability scanner
- An IPS controller to aggregate IPS appliances
- A new release of Proventia Management SiteProtector, IBM’s security management console
- A solution to help clients achieve compliance with all 12 requirements of the Payment Card Industry Data Security Standard (PCI DSS)

**Proventia Enterprise Security Platform**

Proventia Enterprise Security Platform (ESP) offers enterprise-wide protection that is tightly integrated with existing IT business processes to improve IT performance, system availability, and risk control. The products within the Proventia Enterprise Security Platform include:

- Proventia Intrusion Prevention Appliance provides transparent, in-line network protection to preemptively block attacks while allowing legitimate traffic to flow unhindered.
Proventia Multi-Function Security Appliances are IBM ISS' UTM line, providing intrusion prevention technology combined with VPN/firewall, antivirus, Web filtering, and mail security in a unified, easy-to-manage device.

Proventia Desktop Endpoint Security provides comprehensive protection in a single product, from a single vendor. Designed for easy integration with a customer's existing infrastructure, the solution combines a personal firewall, intrusion prevention, buffer overflow exploit prevention, application protection, and virus prevention in a single agent. This multilayered protection includes a combination of technologies including virus prevention system (VPS), buffer-overflow exploit prevention, vulnerability-centric intrusion prevention, antivirus and antispyware signatures, personal firewall, and application control.

In March 2009, IBM announced the release of IBM Proventia Endpoint Secure Control (ESC). The new offering provides best-of-breed desktop security management designed to address two major problems in the industry today: the escalating cost of security and the growing complexity of desktop security management. It balances customer needs with a single security management interface and flexible choice of security solutions to address those needs.

Proventia Server Intrusion Prevention System (IPS) offers multilayered protection for Windows and Linux servers, designed to keep customer data and applications reliable, available, and confidential. To combat threats from all angles, Proventia Server IPS combines several protection technologies into a single multilayered agent. Proventia Server IPS guards business-critical data from attacks from the outside and from within, helping customers meet compliance standards.

Proventia Network Enterprise Scanner is a proactive tool that accelerates time to risk reduction by prioritizing vulnerability remediation tasks. It eliminates manual steps by allowing continuous automated scanning across multiple network segments from a single appliance. Enterprise Scanner detects over 1,500 device types and over 3,400 service types to accurately identify the components of a network.

Proventia Web Filter software has more than 9 billion Web objects cataloged to selectively block unwanted Web content.

Proventia Mail Filter software conducts a detailed 10-step analysis of all inbound and outbound email.

SiteProtector Management System offers scalable, centralized management for the Proventia product family.

**Managed Security Services**

IBM ISS' Managed Security Services provide 24 x 7 protection and real-time security management, including system monitoring, emergency response, security consulting services, and regulatory compliance.
IBM ISS' Managed Security Services complement the Proventia Enterprise Security Platform by offering event monitoring and device management. These services protect enterprises against the Internet's most critical threats and enable organizations to minimize risk, mitigate security costs, and establish due diligence. IBM ISS backs its managed services with money-back, guaranteed service-level agreements (SLAs) that provide a warranty against security breaches and pay customers $50,000 if a security breach occurs.

**Professional Security Services**

IBM ISS' Professional Security Services provide a comprehensive security assessment, design, and deployment service that help enterprises achieve regulatory compliance, maintain business continuity, and reduce overall risk to critical business assets. These consulting methods are based on ISO 17799 and ISO 27002 security best practices and use advanced tools, the latest threat intelligence, and advanced countermeasures. These services include security governance, threat mitigation, identity and access management, data security, and physical security.

Complementing the features listed above, IBM ISS' X-Force research and development team, which collaborates with government agencies, industry consortiums, and software developers, is dedicated to discovering, researching, and testing software vulnerabilities.

The X-Force Threat Analysis Service, which is part of IBM Security Governance Services, helps companies evaluate existing security practices in the context of their requirements and future objectives, including technical and business considerations. This service includes risk management, security architecture design and management, regulatory and standards compliance, privacy, and education and training.

IBM ISS' Threat Mitigation Services are backed by the latest vulnerability and threat intelligence from the IBM ISS X-Force research and development team. It includes software, hardware, professional, and managed security services designed to prevent internal and external IT threats. The solution suite includes network protection, endpoint system protection, application security, and vulnerability management.

**Market Position**

In the past year, which has seen a roller coaster of performance in the global economy, IBM ISS has continued to prove its importance to businesses by returning solid growth every quarter. In the quarters since 1Q07, IBM ISS has continued to show revenue growth from its security appliance products by at least 2% quarter over quarter (see Figure 1). Despite significant slowdowns in the economy at the end of 2007, there has been steady growth in revenue every quarter, none more significant than the 25% growth in the last quarter of 2008. IBM ISS led the $100,000+ price band for IPS appliances in 2008, beating McAfee, Cisco, and TippingPoint (see Figure 2).
The intrusion detection and prevention appliance market, in which IBM ISS plays, totaled $1.47 billion in revenue in 2008. The higher-end appliances, those that fall into the $25,000+ price band, account for just under one-third of the total market ($458 million) for 2008. It is in this segment that IBM ISS has found its niche with its IPS products.

**FIGURE 1**

IBM ISS Security Appliance Factory Revenue, 1Q07–4Q08

![Graph showing IBM ISS Security Appliance Factory Revenue, 1Q07–4Q08](Image)

Source: IDC's Security Server Appliance Tracker, 2008
FIGURE 2

IPS Security Appliances Annual Factory Revenue Share for $100,000+ Price Band, 2007 and 2008

2007

Total = $112.26M

2008

Total = $157.52M

Source: IDC's Security Server Appliance Tracker, 2008
FUTURE OUTLOOK

Given that the concept of integration of storage, security, and system management (3S) is relatively new, IDC expects exploration and education, followed by real product sets and enterprise adoption of the concept in the near future. To utilize this new trend, vulnerability management systems will need to address parts of the 3S infrastructure that have previously been underserved. Key segments to address will be databases and storage systems, especially those that, to date, have been completely ignored, such as printers.

IDC believes that efforts by NAC vendors to minimize the overall complexity and costs of integrating NAC into existing network infrastructures will continue to succeed at an accelerated pace. As these integration issues become secondary concerns, IDC forecasts a broadening of NAC’s appeal across a wider range of enterprises. Widespread use of NAC as a critical component to policy checking and the use of SVM as the agent for managing those security policies and the remediation of any issues associated with them highlight a clear correlation between NAC and SVM. SVM vendors need to ensure interoperability with NAC solutions and assess how their product set fits with NAC. Vendors will also need to expand the coverage of their security management offerings to address the emerging 3S and NAC infrastructures that will grow in the next five years.

IDC expects to see continued M&A activity in the SVM market. While most of the acquisitions so far have been on the security management side, IDC expects to see some action on the vulnerabilities management side from the larger vendors. At the same time, there would be start-ups that create innovative technologies and advance the capabilities of SVM solutions. The mixture of consolidation and innovation will create new product suites that offer comprehensive solutions for enterprises of all sizes.

IDC believes vendors should develop SVM solutions that will be able to provide a more aggressive and proactive security model. Instead of just event response, SVM vendors should offer solutions that will analyze vulnerabilities in a fashion that will provide an explanation of the danger and a priority for remediation.

SVM software vendors should also dedicate solutions to the SMB segment because, thus far, it has been undervalued by SVM products. With government requirements for security and privacy proliferating, the SMB segment would also be concerned about compliance and risk. Small and medium-sized enterprises need simple, easy-to-use, and affordable products for policy compliance and risk management. Vendors that recognize the opportunity and address it early will reap the rewards.

As vendors in the MSS market look to provide more value to their customers, strategic mergers and acquisitions will continue. As of 2007, firewall management services constitute the largest share of the managed security services market, followed by endpoint security management services and IAM. However, as these systems reach maturity and UTM adoption surpasses all other network security segments, IDC anticipates a significant uptake in UTM managed security services. A limited number of leading business services vendors are already moving to address the opportunity, but IDC expects other companies will soon follow.
ESSENTIAL GUIDANCE

Advice for IBM ISS

The diversity of the vendors in the SVM market should encourage IBM ISS to maintain its strong channel sales, which have traditionally accounted for over 65% of the company's total revenue. Channel partnerships will be critical in bringing IBM ISS solutions to the SMB market, which has been deterred from SVM solutions because of price restraints, both direct and overhead, associated with vulnerability assessment and other SVM segments.

Being part of IBM's diverse security portfolio that includes IAM, MSS, security management, intrusion prevention, and threat management, IBM ISS would be wise to accelerate the integration of various components of IBM's security portfolio. IBM ISS' portfolio and integrated services platform will provide a natural launching point for expanding security capabilities along specific strategic lines and focus areas. IBM has an opportunity to offer strong security to enterprises as part of its overall management software and managed service offerings. Furthermore, there is an increasing trend among enterprises to opt for an integrated network management and security solution to streamline both costs and management requirements, which could be a key opportunity for IBM ISS to target with its security-as-a-service (SaaS) solutions portfolio.

There remains a gap between the potential offered by virtualization security solutions and the product options on the market today. While IBM has grown into a major player in the security arena, covering areas such as application security, identity management, and network security solutions, its X-Force and "Phantom" efforts look like the next major initiative in the virtualization security space. IBM ISS is well positioned to bring X-Force features to the growing market.

In terms of product acquisitions, a network-based anomaly detection solution would add to IBM ISS' portfolio, which interestingly was one of ISS' attempts in its pre-IBM days, when it was looking to acquire Arbor.

LEARN MORE

Related Research


©2009 IDC #217829


- **Worldwide Secure Content and Threat Management 2007–2011 Forecast and 2006 Vendor Shares: 1 + 1 = 4** (IDC #207523, June 2007)

---

**Copyright Notice**

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, telebriefings, and conferences. Visit www.idc.com to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit www.idc.com/offices. Please contact the IDC Hotline at 800.343.4952, ext. 7988 (or +1.508.988.7988) or sales@idc.com for information on applying the price of this document toward the purchase of an IDC service or for information on additional copies or Web rights.

Copyright 2009 IDC. Reproduction is forbidden unless authorized. All rights reserved.