

Leadership in Intrusion Prevention as Demonstrated by IBM

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMATM) White Paper
Prepared for IBM

January 2010

Table of Contents

| | |
|--------------------------------|---|
| Executive Summary | 1 |
| Competitive Landscape | 1 |
| Pitfalls to Avoid | 2 |
| Evaluating Effectiveness | 4 |
| IBM Differentiators | 5 |
| EMA Perspective..... | 6 |
| About IBM | 7 |

Executive Summary

It is difficult to ignore the vast importance of IPS technology in nearly every enterprise IT security strategy. In most cases, IPS technology is the cornerstone for protecting governments, enterprises, and Small-to-Medium Businesses (SMBs) against threats to IT applications and infrastructure. The significance of IPS in all of these arenas truly cannot be overstated.

Aside from providing protection against security threats, IPS is utilized as the primary visibility point for most security teams. Costly incidents ranging from virus outbreaks to misconfigurations are all noted in IPS alerts, and in fact are often the first sign of trouble for security teams. Without these alerts, security teams and network operations would largely be blind to the issues their infrastructure is experiencing. It is therefore imperative that an IPS prevents as many attacks as possible.

Of course, this means that the underlying IPS engine must be sophisticated enough to determine the intentions of malicious users and automated programs. This is certainly no easy task. Furthermore, making the determination of what an advanced IPS engine looks like is convoluted by the highly volatile and competitive IPS marketplace that has seen players such as Cisco, IBM, Juniper, McAfee, Sourcefire, and TippingPoint all weighing in with their thoughts. While the marketplace has seen a number of high quality solutions, there are specific competitive differentiators that make particular IPS products better than others.

There are specific competitive differentiators that make particular IPS products better than others.

Unfortunately, as the IPS market continues to mature, end users are becoming less and less aware of these competitive differentiators. Users have become less reliant on power user features in IPS and have instead elected to rely heavily on the automated features. This has allowed market competitors to flood user communities with marketing FUD (fear, uncertainty and doubt) and beautiful graphical user interfaces that, although pretty, do not address security-related issues. The IPS market is in fact so muddied with misinformation that leading analyst firms have even produced ranking reports where so-called leaders and visionaries seem to have vast gaps in capabilities, when in fact they are utilizing the same IPS engine. These reports further damage the market by failing to recognize the underlying technology that truly separates the leaders from the up-and-comers.

This ENTERPRISE MANAGEMENT ASSOCIATES[®] (EMA[™]) whitepaper explores the IPS market and how to determine what constitutes an industry leader. Professionals will gain insight into the specific attributes that make an IPS engine strong or weak, and will be able to determine common pitfalls that should be avoided when considering IPS products. The qualities of a leader such as IBM are examined as IBM Internet Security Systems (ISS) reflects leadership in IPS technology through a strong underlying IPS model and useful integrations within the IBM portfolio.

Competitive Landscape

The IPS landscape is highly competitive. In its earliest inception, the IPS market was predicated on advanced users searching for avant-garde capabilities in infrastructure protection. For the most part, these users understood then-current IPS products inside and out. Many were also willing to invest resources in researching the underlying capabilities of these products in order to determine the best solution for their needs.

This environment has of course changed over the past few years. As the IPS market continues to mature and products have become easier to deploy and use, IPS technology has become increasingly familiar to less technical professionals. In part, this can be attributed to IPS having largely become a commodity technology and an integral aspect of commonly accepted security practices. The increased maturity and commoditization of this market has led to a situation where tight competition leads vendors to seek any advantage they can. In order to gain a competitive edge, for example, a vendor may adopt a more elegant user interface and focus on ease-of-use. Such tactics may, however, have an unfortunate side effect of leading users to become distanced from deep familiarity with the underlying capabilities of IPS technology. When these tactics mask deficiencies in IPS effectiveness relative to other competitors, they open the door for market FUD and mud slinging, particularly when slick marketing may move more product than the product's ability to block attacks and maintain a secure posture in the face of more advanced threats, with each different side in this competitive battle having its adherents.

Possibly the most unfortunate outcome of the current competitive landscape is the increasing ignorance of so-called IPS knowledge leaders. On the one hand, analysts may be more focused on “signature quality,” user interface, and integration points as opposed to engine quality. On the other, end users may become more concerned with automation and simplicity as opposed to power-user capabilities and real effectiveness. Unfortunately, the general acceptance of simplified interfaces and excessive focus on ease-of-use has led too many users to either forget or to never fully research the underlying capabilities of IPS technologies.

These factors have produced an IPS landscape where current market leaders such as Cisco, IBM, McAfee, Sourcefire, and TippingPoint are constantly jockeying for a leadership role.

Pitfalls to Avoid

One specific arena in which the intensity of this tight competition has been evident is in the realm of marketing and business tactics. The clever marketing of these competitors has in some cases allowed less capable products and research teams to assert themselves into the limelight. Vendors in the IPS space have gone to great lengths to assert their superiority through interesting ad campaigns that in some cases involved cartoon-like mascots and action figures or have leveraged social networking to create IPS-focused communities. Unfortunately, while these marketing techniques are interesting and enjoyable, they distract end users from the most important question of all: Who has the strongest engine?

This is the first of several pitfalls that those weighing an IPS product must avoid. If a purchaser is not careful, falling for clever marketing will lead them to adopt a technology that may not ultimately be the right fit for their needs, and to overlook competitive offerings that might serve them better.

Another pitfall on the way to making an IPS choice is subscribing to the notion of “good enough” security models that too often are neither good nor enough. For example, many organizations purchase IPS products as part of an enterprise purchasing relationship with a broad portfolio vendor. This places the customer

Another pitfall on the way to making an IPS choice is subscribing to the notion of “good enough” security models that too often are neither good nor enough.

at risk of favoring the package pricing—or simply the “one throat to choke”—of a sole supplier over choosing the best-of-breed. This can be a critical issue in security if it places the organization at risk of adopting less effective defenses against increasingly sophisticated threats. Many buyers will view this type of IPS solution as “good enough” to serve their needs. In other words, they realize that the product they are purchasing is not the best product on the market; however, because the price or the vendor relationship is right, they are willing to bend on effectiveness. The pitfall of this attitude is that the organization runs the risk of incurring unplanned costs resulting from unchecked incidents due to gaps in effectiveness, and the time and effort required to respond.

Put in more simple terms, “good enough” products expose the business to the risk that they will fail to properly address more challenging threats that can negatively affect businesses in the form of lost credibility, productivity, revenue, or other costs. It is essential to recognize that the only “good enough” security model is the one that leverages security products that are best suited to address real-world threats to the business’s bottom line—and that bottom line may be affected by more than just the costs of purchasing from a preferred supplier.

Yet another pitfall is evaluating an IPS supplier on the basis of their investment in their business. On the surface, this might seem to be a reflection of intelligent strategy—but the question must be asked: investment in *what*? If more is spent on marketing than fundamental research, what is the vendor’s prospect for long-term viability as a provider of realistic defense? If simply to close competitive gaps and shore up deficiencies rather than making a leadership stake in effectiveness, what are the vendor’s prospects for continued success? These questions suggest how important it is to understand which competitors have the capability to attain and sustain leadership in product effectiveness. The vendor that makes investments into creating a long-term sustainable model that seizes opportunities for integration is often a better solution for buyers in the long run—and it is in the long run that many enterprises would prefer to see a sustainable relationship with their preferred providers.

Finally, after buyers have avoided pitfalls of clever marketing, “good enough” snares, and confusion between investment and capability, they must also avoid being misled by confusing ranking reports. In some cases, a vendor may score highly in a ranking report but poorly in a lab assessment, and vice versa. Both reports cannot be right—or can they?

Buyers should keep in mind that different types of vendor reports may have very different evaluation criteria. Some analyst and market reports may be targeted more for investors than for potential buyers of a company’s product. It is therefore imperative to find a report that specifically addresses the buyer’s needs. Those for whom product effectiveness is a top priority will therefore want to look for evaluations that focus on capabilities such as engine quality and system performance, for example.

Buyers should keep in mind that different types of vendor reports may have very different evaluation criteria.

Evaluating Effectiveness

When weighing the effectiveness of an IPS product, buyers should consider a number of capabilities. These include:

- **Ability to adapt to emerging threats:** A static IPS that does not evolve rapidly with the threat landscape is an IPS that is ultimately doomed to fail. Preferred IPS solutions are capable of addressing advancing sophistication through dynamic product expansion and high quality detection.
- **High performance:** In order for IPS to be most effective, solutions must operate inline in a production environment. As a result, high performance and throughput are essential attributes of a preferred IPS solution. There are two primary aspects to performance and throughput that are essential in IPS. The first is the total throughput an appliance can process, which may include unprotected traffic. The second is the throughput of protected traffic. The combination of the two provides buyers with metrics on the amount of traffic an appliance can handle without degrading network throughput or a minimum threshold of protection. A preferred solution will perform at high levels in both.
- **Actionable alerting:** Sometimes this is mistakenly referred to as “signature quality.” However, the important part is not the “quality” of individual signatures, but rather the efficiency of the process that one or more signatures may set in motion. This is especially true in polymorphic malware outbreaks where patterns of anomalous alerts are more indicative of an issue than any single “quality” signature could ever feasibly detect. In these cases, signatures do not necessarily have to be complex or in some cases even accurate to produce a result that addresses a serious security threat. In such a situation, the quality of any individual signature is less significant than the ability of the *entire* IPS system to raise proper alerts that more accurately identify an incident.
- **Advanced research and development:** One critical aspect of an IPS solution is the research and development capabilities of the vendor. New attacks and new methods for attack are created every day. In order to stay ahead of emerging threats, it is crucial that a vendor be able to quickly recognize new methods and create capabilities for mitigating the threat.
- **Reduced Total Cost of Ownership (TCO):** Properly securing an IT infrastructure with IPS technology can quickly lead to large expenses. Beyond the expense of implementation and maintenance, costs of administration, monitoring, and integrating with existing infrastructure may add up quickly. In order to curb these costs and reduce TCO it is important to select a product that requires less administration and maintenance without sacrificing on fundamental capability. Solutions that more transparently recognize and enable normal business traffic, for example, while recognizing a wide range of threats may further add to the value of a preferred IPS product.

IBM Differentiators

IBM addresses each one of these characteristics of a preferred IPS solution through a marriage of sophisticated technology and industry leading research and development. IBM begins by using top-tier appliance form factors in the Proventia line of products. The focus on higher capacity appliances means better performance, which in turn means better business enablement.

IBM addresses each one of these characteristics of a preferred IPS solution through a marriage of sophisticated technology and industry leading research and development.

IBM offers a highly effective IPS engine in its Protocol Analysis Module (PAM). PAM leverages industry leading stateful detection technology to alert customers of malicious behaviors. These alerts are primarily based on pattern matching through signatures whose sophistication is well beyond the regular expression matching utilized by some competitors.

Interestingly enough, the higher level of sophistication of the PAM engine does not result in network latency when combined with the specially purposed Proventia appliances. Furthermore, the ability of PAM to detect behaviors simplifies alert data, creating more actionable information. This simplification, however, has not been without controversy. In creating actionable information IBM will sometimes produce more alerts for a singular event. While to some this creates a very simple metric (more alerts is the equivalent to more noise) to the more sophisticated assessor, the extra alerts means better information.

For example, if a vulnerability scan is run against a host protected by an IBM IPS solution, the IPS will detect the individual attacks of each vulnerability check, but will simplify the combination of all of those alerts with an extra alert stating, “Vulnerability Scan Detected.” This prevents security teams from wasting valuable resources in an effort to determine what occurred through the manual correlation. Many other IPS solutions offer no such simplification, forcing those monitoring the IPS solution to research several thousand alerts in order to determine exactly what occurred. This capability speaks directly to another key advantage of the IBM team: the ISS X-Force, part of IBM’s recognized focus on R&D.

The X-Force has long been one of the research pillars of the security community. Today, the X-Force still remains a magnet for top-level IT security talent. Within IBM, the X-Force also enjoys increased collaboration between other IBM lab teams such as the IBM Rational research group of researchers from the former Watchfire and Ounce Labs. The combination of all three teams clearly shows IBM’s continued investment into industry leading threat research.

With regards to the IPS product itself, the insight of the X-Force delivers higher capabilities often well before competitors. One excellent example of where X-Force R&D in combination with other related IBM security labs has created key competitive differentiators can be seen in the realm of Web applications. Currently IBM’s IPS product line does well at protecting Web applications from several of the popular Web application attack methodologies including SQL injection and cross-site scripting. This capability came directly from a collaborative effort between the X-Force and IBM Rational’s security research team. Collaborative efforts such as these which combine IPS blocking with IBM’s application security scanning and access control capabilities allows IBM to create an application centric model that market competitors find extremely difficult to rival.

Sadly, many other vendors lack the ability to address issues in this cross-functional manner. Here again, popular Web application attack methodologies serve as an excellent example. Other IPS leaders have done so poorly in this realm that some Website vulnerability assessment vendors have independently begun developing signatures for IPS systems that do not fare as well in defending Web applications. While this may be adequate for some customers, it is not a sufficient long-term model for enterprises to continue to hope that other vendors will produce necessary components for an IPS without a truly durable long-term relationship. While partnerships may help other vendors close such gaps, it must be noted that IBM has the ability to leverage internal products and knowledge to produce better capabilities.

Another aspect of the comprehensive IBM portfolio that supports ISS capabilities comes in the form IBM Security Operations Centers. In tribute to IBM's real world performance and capabilities—and unlike some others—IBM uses their own products in administering the security operations of its customers. Currently IBM Security Operations Centers (SOCs) support both public and private sector organizations of all types and sizes. In an effort to deliver the best possible security capabilities in these realms, IBM utilizes its own IPS products. It would be easy to assert that this highlights IBM's continued confidence in its investment in this product line, but it should not be overlooked that it also exposes IBM directly to very vocal and objective critics. The fact that IBM's security services operations succeed with these customers by using ISS IPS products relates directly back to IBM's ability to produce a well differentiated and quality product.

EMA Perspective

Since its acquisition of ISS, IBM has assumed the ISS mantle of being the quintessential network security and advanced IT threat protection company. While the external perception of the company may be quickly changing from the hacker rock star elan for which ISS was once known, the quality and capabilities of its IPS product have not changed. IBM still produces one of the leading IPS products in the industry. The experience of EMA analysts with IPS products and capabilities consistently highlights IBM Proventia G as one of the best performers on the market.

IBM may not have the most polished marketing engine in the competitive landscape, however, and EMA must note that its IPS console is well overdue for some beautification. It is clear that the SiteProtector product is an engineering-driven solution as the GUI bells and whistles are minimalistic. However, the look of the solution is a minor aspect when compared to the strength of the detection and prevention engine. The look is even less significant when compared to the quality of the threat analysis and response team that supports the product itself. In this realm, the IBM IPS team and the X-Force research that backs it is second to none.

The X-Force team has been sufficiently successful that some of its current members and alumni are well recognized within the security community. The fact that some of these members have since moved on should not dampen one of the X-Force's key competitive differentiators: it is a *team* of talented individuals. While some attrition is to be expected when a dynamic pure play is acquired by a major portfolio vendor, the X-Force has been able to replace that talent with new members that are passionate for security. It is the notoriety of the X-Force brand and the shared passion among its members that continues to make the X-Force one of the biggest draws for security talent in the industry today.

**IBM still produces one of
the leading IPS products
in the industry.**

EMA security analysts have on several occasions stuck their neck out for the IBM team and its IPS product, and this paper is certainly no exception. However, EMA feels very strongly that the IBM Proventia G product is one of the most under-appreciated and misunderstood security products on the market today. Anecdotally, EMA analysts have a long and positive history of working hands-on with IBM's IPS products, and have seen firsthand the product family's successes and failures—and still, there are few security products that EMA would assert deserve more trust or favor than the IBM Internet Security Systems IPS product line.

Of course, security is a domain in constant flux, and today's leaders can become tomorrow's laggards if they fail to see where threats are headed, and how the enterprise chooses to respond. The fact that IBM is viewed favorably should not diminish the fact that the company does have strong competitors in IPS when it comes to engine and capabilities. However, should IBM continue to invest the necessary resources to continue to evolve and integrate the IPS product and maintain one of the strongest R&D capabilities in the industry, EMA will continue to have no issue in viewing the product in a positive light.

About IBM

Through world-class solutions that address risk across each aspect of a customer's business, IBM can help customers build a strong security posture that helps reduce costs, improve service, and manage risk in dynamic infrastructures, helping cost-effectively embrace change and innovation without compromising security. IBM Internet Security Systems is part of IBM's robust portfolio of security solutions. To learn more about IBM security solutions, please visit: <http://www-03.ibm.com/security/>.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that specializes in going “beyond the surface” to provide deep insight across the full spectrum of IT management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help its clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise IT professionals and IT vendors at www.enterprisemanagement.com or follow [EMA on Twitter](#).

This report in whole or in part may not be duplicated, reproduced, stored in a retrieval system or retransmitted without prior written permission of Enterprise Management Associates, Inc. All opinions and estimates herein constitute our judgement as of this date and are subject to change without notice. Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. “EMA” and “Enterprise Management Associates” are trademarks of Enterprise Management Associates, Inc. in the United States and other countries.

©2009 Enterprise Management Associates, Inc. All Rights Reserved. EMA™, ENTERPRISE MANAGEMENT ASSOCIATES®, and the mobius symbol are registered trademarks or common-law trademarks of Enterprise Management Associates, Inc.

Corporate Headquarters:
5777 Central Avenue, Suite 105
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com



2025.012910