

### Contents

|   |   |
|---|---|
| Introduction .....                        | 1 |
| The New Reality .....                     | 1 |
| Where Intrusion Prevention Comes In ..... | 2 |
| Real World IPS Insights .....             | 3 |
| In-Band Solutions.....                    | 3 |
| Blocking Malicious Traffic.....           | 4 |
| Staying Ahead of the Threat.....          | 5 |
| Ease of Use .....                         | 6 |
| Real World Wrap Up.....                   | 7 |
| Summary .....                             | 7 |

### Introduction

This white paper addresses three primary areas that organizations must consider when formulating network security strategies and evaluating possible solutions for intrusion prevention.

1. First, what are the key network security challenges facing enterprises today and how have they evolved over the past few years?
2. Second, what are the criteria for an effective IPS solution within the context of a new security reality?
3. Third, what insights can be gained from the experience of enterprises already deploying IPS solutions in the real world?

This paper will explore what organizations can do to apply best practices and make the most of security budgets and resources.

### The New Reality

In an age where e-commerce and business critical applications are quickly becoming “Webified,” security threats are morphing faster than ever and the membership and skill of the global hacking community are rising. Sophisticated scanning, penetrating and obfuscating tools and techniques are also more widely available. Worst of all, hackers are now highly motivated to penetrate networks, applications and databases to steal information that can be sold for profit. It’s the modern bank robbery and many can easily become successful

criminals by stealing and selling information. To compound the problem further, the risk of being caught is low. For example, how is a Botnet attack traced crafted by a Romanian teenager using a machine in Bolivia to attack a bank server in the United States? Even if the attack could be traced, law enforcement agencies are unlikely to understand the nature of the crime. In the meantime, organizations may end up on the front page of the *Wall Street Journal* or *Financial Times* for less than positive reasons.

So what should organizations do? It’s a complex problem and most organizations do not have endless staff and budget to adequately protect their networks. In fact, whatever an organization’s revenue is, odds are that nearly five percent of that will be spent on IT and eight percent of the IT budget will be spent on network and information security. Yet, there is an ocean of point products positioned as the latest quick fix. IT security faces a vexing challenge: how to wisely spend precious budget to provide maximum business assurance against an ever-changing threat landscape. It comes down to one simple principle: automate everything associated with attack detection and enforcement within reason, thereby leveraging precious IT security staff and budget for other projects. It may seem obvious, but full security automation is much easier said than done. IT security decision makers must have clear requirements that guide them to smart security investments and

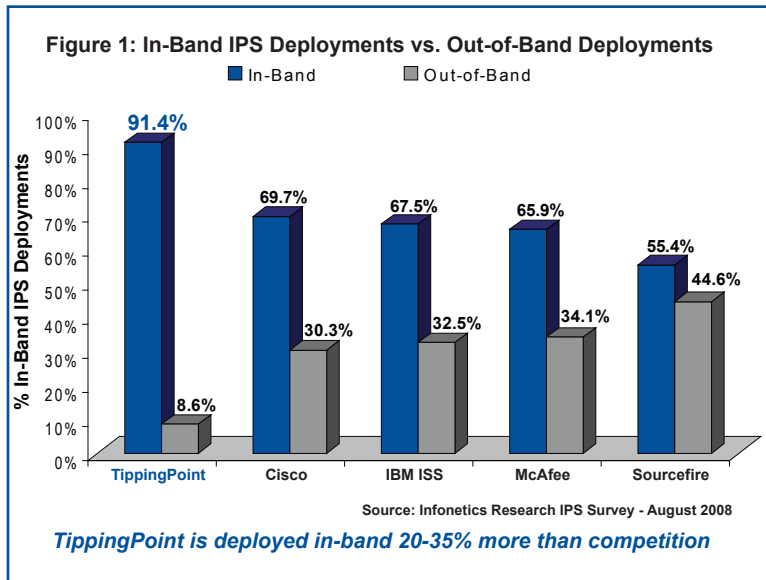
*“This survey shows great variability among IPS vendors with regard to IPS security performance and ease of manageability. TippingPoint outperformed all the vendors in the survey with strong showings across the board, including in-band deployments, effectiveness of security filters, ease of IPS configuration, and repeat IPS purchase intentions.”*

Jeff Wilson  
Principal Network Security Analyst  
Infonetics Research

definitive business assurance payback.

## Where Intrusion Prevention Comes In

This is where intrusion prevention comes in. First, what is an intrusion prevention system (IPS)?



An IPS is an in-band, real-time traffic classification and policy enforcement system – based on deep packet inspection technology – that blocks known and zero-day attacks without human intervention, and with virtually no false positives or application

traffic latency. In order to do this, a very stringent set of product requirements must be met – which is exactly why most intrusion technologies and products remain centered on out-of-band intrusion detection, rather than in-band intrusion prevention. These requirements include:

### 1. In-Line Network Reliability:

To block in real time, a product must be placed in-line, not off a tap or mirror port. This means the IPS must be designed from the ground up to deliver the same reliability and network availability as existing routing and switching infrastructure. And, if there is an issue, the IPS must be able to gracefully and transparently remove itself from the network without disrupting normal business traffic.

### 2. Core Network Performance:

Once an IPS proves that it delivers the reliability to be placed in-band, it must process and inspect traffic at multiple gigabit per second rates of speed. The days of only deploying IPS at the WAN perimeter to block a few exploit-filter matched worms are gone. Now, IPS solutions must be able to protect critical interior network points including the data center, major network segmentation points, and even the network core to provide an effective defense against virtually any attack. To consider IPS deployments at key internal points, not only must organizations be concerned about up-time, they must also ensure critical business application performance is not impeded so that their help desk isn't buried with employee complaints.

**3. Low Latency:** Application performance is not just a function of bandwidth. Low latency must also be ensured. This is a particularly tough challenge for security products. If a security product is going to run with thousands of filters turned on to automatically block malicious traffic, it must perform inspection very rapidly, or packets will be delayed, application response time will be hindered and employees will complain.

**4. Broad Attack Coverage:** The fourth challenge focuses on evolving broad coverage and speed of coverage. To protect networks from the growing number of sophisticated attacks, an IPS must provide broad and deep attack coverage. That means the IPS must be able to stop worms, viruses, Trojans, denial of service attacks, peer to peer bandwidth floods, spyware, phishing, Web

application attacks (such as cross site scripting, SQL injections, PHP file includes), VoIP attacks, and more. In addition, the filters should be designed to cover operating system and application vulnerabilities, not just a few well-known attacks which can easily be fingerprinted with basic exploit signatures. Finally, these IPS filters must be delivered in a timely fashion on a regular basis – which requires world class security intelligence, filter writing, testing, and delivery – a skill set and process not widely available.

## 5. Extreme Filter Accuracy:

Finally, the installation of IPS solutions at critical interior and perimeter network points means filter accuracy is of the utmost importance. If not, security personnel will be buried in piles of alerts, many of which will be false alarms. In that world, automation kills IT productivity because IT staff time is wasted chasing every false alarm, only to miss the real ones.

From worms, spyware and phishing attacks to the latest Web application assaults, IPS vendors promise the kind of comprehensive network security not provided by other solutions. Evaluating IPS products can be extremely confusing, especially given that IPS and IDS vendor and product claims all sound similar.

The value proposition of IPS systems that rely on IDS-centric technology can be misleading until they are deployed and managed in a production network with real-world traffic. Intrusion Prevention Systems (IPS) are supposed to detect and block unwanted network traffic in real time. However, a survey conducted by Infonetics Research

and commissioned by TippingPoint demonstrates that not all IPS vendor solutions deliver the same results in the real world.

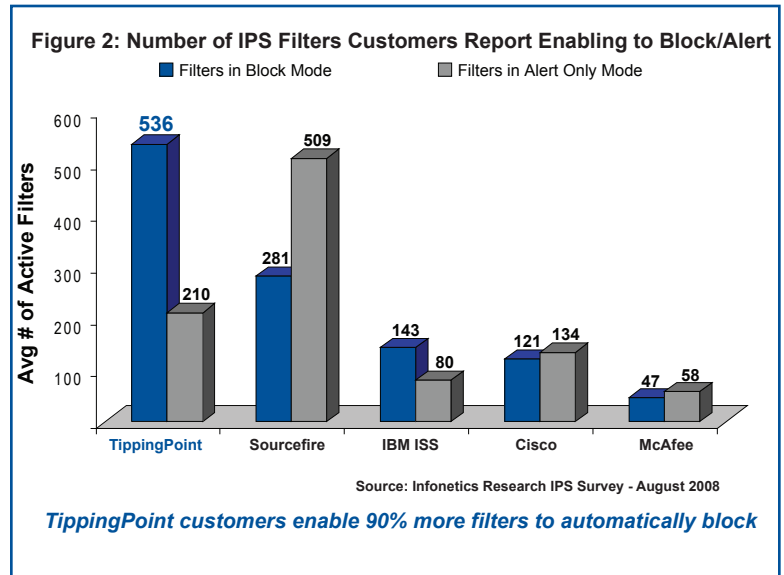
## Real World IPS Insights- Direct from Users

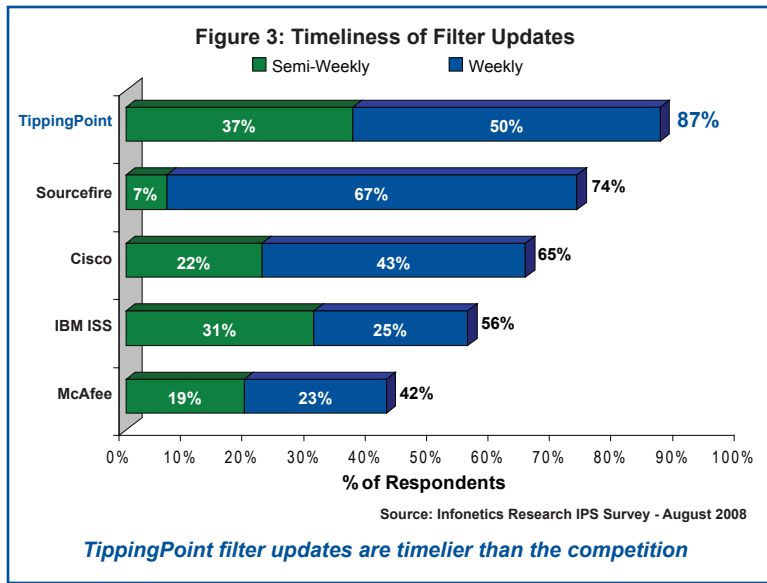
So how do IPS solutions perform in live customer networks?

A recent Infonetics IPS study examines customer experiences with the deployment and management of IPS solutions from a variety of manufacturers. It examines, in particular, how IPS solutions are purchased, deployed and used, including responses from 169 companies that use IPS solutions within their production networks. Respondents in this study were “responsible for managing or planning IPS products and services” for their respective companies. The respondent companies had an average of 9,418 employees each and are customers of one of five IPS vendors: Cisco, IBM-ISS, McAfee, Sourcefire<sup>1</sup> and TippingPoint.

## In-Band Solutions

Out-of-band devices can detect network attacks, but can't stop them. In-band devices, on the other hand, provide real-time, deep inspection and blocking of data packets at layers 2 through 7. Results from the Infonetics IPS customer survey show distinct differences around in-band





deployments among IPS vendors as shown in Figure 1.

Customers report that over 91 percent of all TippingPoint IPS appliances are deployed in-band, versus Cisco, IBM-ISS and McAfee with less than 70 percent each.

These concerns are valid for any proactive, in-band network security device. If in-band devices happen to fail – and if they’re not engineered to gracefully and transparently remove themselves from the network like the TippingPoint IPS – then network availability can suffer. If in-band devices aren’t specifically designed to deliver the performance necessary to inspect and pass traffic at speeds as fast as the network itself, the impact to throughput and latency can harm application performance. Additionally, if hyper-vigilant IPS systems end up blocking legitimate traffic because of poor filter accuracy; end users will inundate an organization’s IT help desk very quickly.

Well-designed IPS solutions like the TippingPoint IPS can virtually eliminate these customer concerns. It is evident from the number of customers that install the TippingPoint IPS in-line that TippingPoint’s customers are more confident in their IPS solution’s abilities to overcome key concerns than other IPS vendors’ customers.

These results stem from the fact that TippingPoint IPS solutions are custom designed to deliver industry leading reliability, throughput and latency performance. The products range from 200Mbps to 5Gbps throughput performance and the TippingPoint Core Controller IPS solution delivers up to 10Gbps IPS inspection throughput, all while introducing no more than 84 microseconds of network latency.

So what keeps some customers from deploying their IPS appliances in-band? Why are they reluctant to deploy in-band given the benefits that come from proactively blocking malicious attacks? The results of the Infonetics IPS customer survey indicate the primary reasons for out-of-band deployment include:

- Concerns about reliability/availability
- Throughput degradation
- Increased traffic latency
- False positives or blocking of legitimate application traffic

## **Blocking Malicious Traffic: Accuracy Does Matter**

Another critical requirement for in-band intrusion prevention is to enable a large number of filters to block rather than just detect malicious traffic. Filter accuracy – or the ability of the IPS appliance to block malicious traffic without blocking legitimate business applications – gives customers the confidence to enable IPS filters in block mode.

Figure 2 presents the average number of filters that IPS customers enable to block according to the Infonetics data.

The TippingPoint IPS solutions, and more specifically TippingPoint's security research team DV Labs, are well known for delivering IPS vulnerability filters that are extremely accurate and do not block legitimate application traffic. In addition, these vulnerability filters provide complete protection for all current and future exploits targeting the application vulnerability giving customers great zero-day protection. Every TippingPoint IPS is shipped with "Recommended Settings" - filters enabled by default to block malicious traffic.

## Staying Ahead of the Threat

Another critical measure of an IPS solution is the timeliness of filter development and corresponding filter updates to protect against newly discovered or disclosed software vulnerabilities. After all, "better late than never" is not what security administrators want to hear from an IPS vendor. Figure 3 reports the number of customers who responded that their vendor updates IPS filter sets semi-weekly or weekly.

A total of 87 percent of TippingPoint customers report that they receive filter updates twice a week (37 percent) or weekly (50 percent). Cisco customers reported 65 percent had at least weekly updates, and IBM-ISS and McAfee customers reported 56 percent and 42 percent respectively they received at least weekly updates.

These results reflect TippingPoint's significant investments in its DV Labs security research team's IPS filter production and software vulnerability research capabilities. TippingPoint leads the IPS industry

in discovered software application vulnerabilities. These security research and IPS filter production capabilities give TippingPoint the ability to produce IPS filters before vulnerabilities are disclosed by software vendors or very shortly thereafter.

Further, the Infonetics data found that TippingPoint customers are more likely to apply all the IPS filter updates provided compared to customers of other IPS vendors (Figure 4).

Nearly three quarters of all TippingPoint customers surveyed (74 percent) report that they typically apply all of the IPS filter updates delivered by TippingPoint's DV Labs team. This suggests that TippingPoint customers have more confidence in their IPS vendor than competitors' customers.

All TippingPoint IPS filter updates from DV Labs include "Recommended Settings" that

Figure 4: Percentage of Customers Typically Applying All Filter Updates

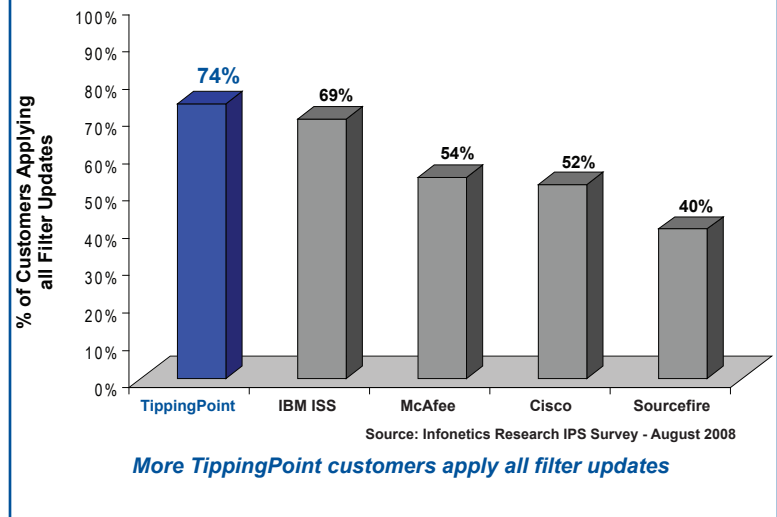
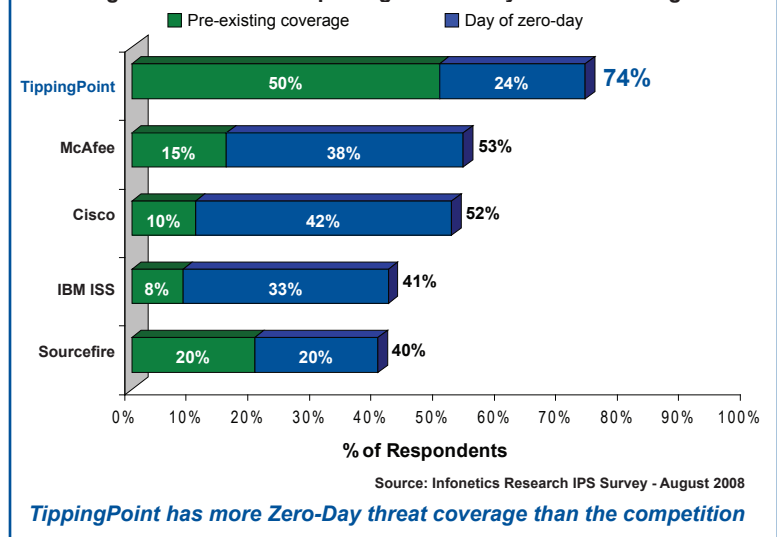
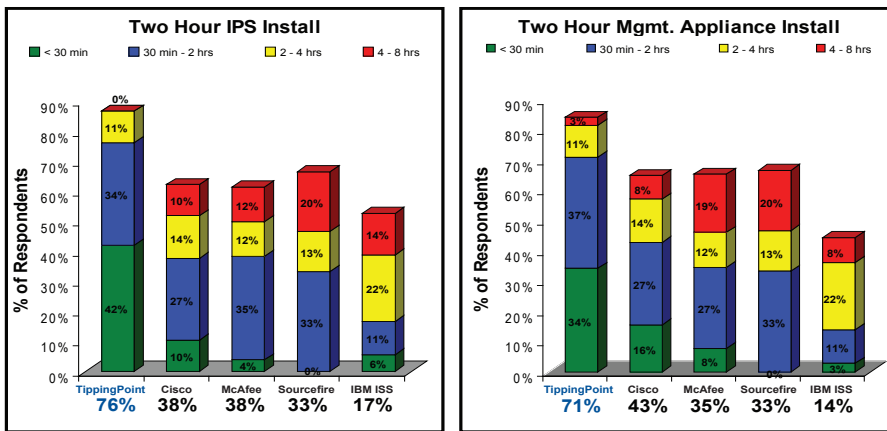


Figure 5: Customer Reporting of Zero-Day Threat Coverage



**Figure 6: Turn-Up Time for IPS and Management Appliances**



Source: Infonetics Research IPS Survey - August 2008

indicate exactly how TippingPoint recommends deploying each new filter by default. It is this filter information that gives customers the confidence to automatically apply TippingPoint’s IPS filter updates.

Sometimes, new IPS filters are delivered even before application vulnerabilities are disclosed to the public. When this happens, the IPS vendor is providing “Zero-Day” threat coverage. Hackers can discover application vulnerabilities before software vendors deploy patches to cover them. These Zero-Day threats can leave networks with gaping security holes. To address these threats, IPS vendors need to employ in-house teams of researchers dedicated to conducting ongoing vulnerability research and analysis and to developing Zero-Day filters that plug holes before software patches become available.

How do IPS vendors compare on Zero-Day threat coverage? According to the Infonetics survey data, half of TippingPoint respondents report they receive Zero-Day threat protection – two to three times as many as the closest competitors. Another 24 percent

say they receive protection the day of vulnerability disclosure. Twenty percent of Sourcefire customers report pre-existing Zero-Day coverage, followed by 15 percent of McAfee customers, 10 percent of Cisco customers and 8 percent of IBM-ISS customers (Figure 5).

This is a reflection of TippingPoint’s investments in DV Labs vulnerability research capabilities and the corresponding fact that TippingPoint leads the IPS industry in discovered software application vulnerabilities.

## Ease of Use

Network administrators are less likely to deploy intrusion prevention systems across the expanse of their networks if the solution is difficult to set-up and manage. The Infonetics survey reveals manageability factors for each of the five IPS vendors, including turn-up time and ease of IPS filter configuration.

According to Infonetics’ Jeff Wilson, “*This area is among the most significant findings in the study. Many IPS deployments get completely hung up at the initial configuration stage, or worse, devices are misconfigured and then fail to block attacks.*”

TippingPoint customers reported the fastest turn-up times, with 76 percent stating that TippingPoint IPS appliances can be installed in two hours or less. Thirty-eight percent of Cisco and McAfee customers say they can turn-up their IPS devices in two hours. Only seventeen percent of IBM-ISS customers report two-hour set-up success.

Following deployment, initial and ongoing IPS filter configuration is critical to getting the most out of the IPS solution. It is also important to manage and deploy these filters with minimal investment of IT resources. The Infonetics study categorized IPS filter configuration in three levels:

**Light Effort:** able to navigate the filter inventory, apply filters to segments, and activate policy enforcement in an efficient manner, quickly and independently from vendor assistance in the time-frame expected

**Moderate Effort:** some difficulty in filter inventory navigation, segment application, and/or policy enforcement activation that led to more time consumed than expected for this effort

**Significant Effort:** help required from vendor technical or sales support to accomplish filter inventory navigation, segment application, and/or policy enforcement activation.

As shown in Figure 7, 66 percent of TippingPoint customers reported that a “light effort” was required to configure IPS filters. Comparatively, 22 percent of IBM-ISS customers, 15 percent of McAfee customers and only 14 percent of Cisco customers reported that filter configuration required a “light effort.”

## Real World Wrap Up

The benefits of intrusion prevention have been obvious since a leading industry analyst indicated that “Intrusion Prevention Will Replace Intrusion Detection” in August 2003. However, the Infonetics IPS customer survey

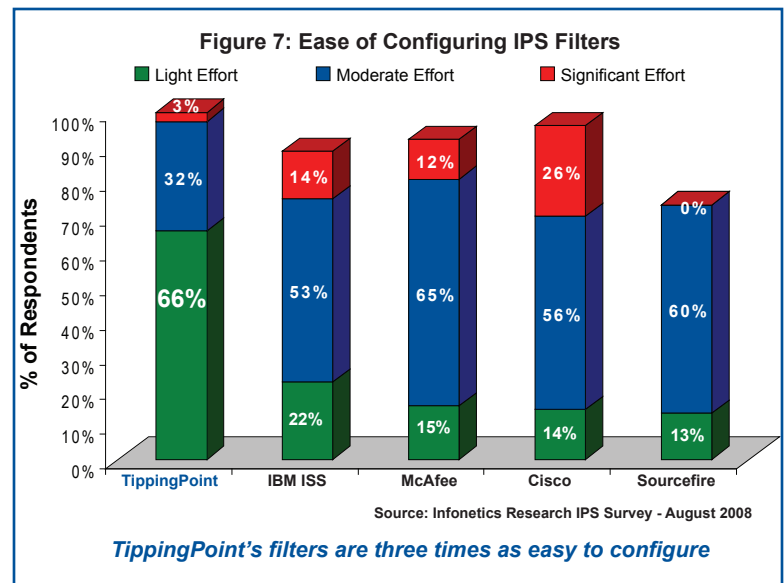
finds that 30-45 percent of customers for some IPS vendors still do not install these products in-band with large numbers of filters enabled to block malicious traffic. They continue to use them out-of-band merely to detect attacks, not to block attacks.

TippingPoint’s customers were more confident in their IPS purchase and they consistently ranked TippingPoint at the top – often by large margins – on each and every key IPS performance and manageability measure. Figure 8 summarizes these results.

TippingPoint’s customers display more loyalty for repeat IPS purchases than other competitor’s customers. In fact, the Infonetics IPS customer survey shows that 62 percent of TippingPoint’s IPS customers with intentions to purchase additional IPS products will “definitely stay with their existing IPS vendor” without even reviewing competitive offerings.

## Summary

TippingPoint was founded specifically to design and build an IPS from inception to address the requirements outlined in this paper. When TippingPoint was formed in 2001, intrusion detection systems (IDS) were widely available. The companies that provided those IDS solutions



**Figure 8: IPS Survey Summary**

| In Band Blocking                      | TippingPoint | Cisco | IBM ISS | McAfee | Sourcefire |
|---------------------------------------|--------------|-------|---------|--------|------------|
| 1. In-Band IPS Deployments            | 1            | 2     | 3       | 4      | 5          |
| 2. Reasons Preventing IPS Deployments | 1            | 2     | 3       | 4      | 5          |
| 3. Filters in Block Mode              | 1            | 4     | 3       | 5      | 2          |
| Filter Effectiveness                  |              |       |         |        |            |
| 1. Number of Attacks Blocked          | 1            | 5     | 4       | 3      | 2          |
| 2. Timeliness of Filter Updates       | 1            | 3     | 4       | 5      | 2          |
| 3. Zero-Day Threat Coverage           | 1            | 3     | 4       | 2      | 5          |
| Ease of Use                           |              |       |         |        |            |
| 1. IPS Turn-Up Time                   | 1            | 2     | 5       | 3      | 4          |
| 2. Ease of IPS Configuration          | 1            | 4     | 2       | 3      | 5          |

Source: Infonetics Research IPS Survey - August 2008

**Customers rank TippingPoint highest in every main category**

are still around today, continuing to sell IDS. These vendors continue to preach how dangerous it is to go in-band and automatically block malicious traffic simply because their products are not – and never were – designed to be implemented as an IPS. But the market has spoken. ‘Detect and alert’ is no longer the game – unless there is an enormous security budget to hire expensive staff to sift through mountains of alerts and hope that ‘after the fact’ corrective action will somehow appease government compliance agencies and/or personal privacy breach lawyers.

It is not that IDS is inherently bad – there are legitimate uses of detection and human analysis. But security budgets must be spent with an eye toward getting the ‘biggest bang for the buck’. Security dollars are far better spent first on network security automation (IPS) rather than

informational alerting (IDS). Once the majority of the malicious and unwanted traffic has been removed from the network through IPS automation, highly valued security personnel become far more productive – as they can focus their energy and effort on unusual network and application activity.

TippingPoint IPS’s are built to be deployed in-band, and customer feedback shows that TippingPoint products are trusted in-band, with large numbers of filters automatically set to block straight from the factory. Tens of thousands of TippingPoint IPS’s are currently deployed across Fortune 1000, Global 3000, small to medium enterprises (SME), and even some small to medium businesses (SMB) – and across every key industry vertical. TippingPoint automatically blocks damaging attacks in a cost effective manner, significantly reducing the cost and complexity of highly effective network security.

An investment in a TippingPoint IPS is one of the best security expenditures an organization can make. TippingPoint’s product evaluation program provides a TippingPoint IPS for evaluation. IT executives, network engineers, and security analysts can see first-hand why TippingPoint can provide your company with cost-effective business assurance.

<sup>1</sup> While Sourcefire customers were included in the Infonetics survey, only a small number of Sourcefire customers responded to the survey. Therefore, the Sourcefire results are based on a small number (< 30) of customer responses.

**Corporate Headquarters:**  
7501B North Capital of Texas Hwy.  
Austin, Texas 78731 USA  
+1 512 681 8000  
+1 888 TRUE IPS

**European Headquarters:**  
Herengracht 466, 2nd Floor  
1017 CA Amsterdam  
The Netherlands  
+31 20 521 0450

**Asia Pacific Headquarters:**  
47 Scotts Road  
#11-03 Goldbell Towers  
Singapore 228233  
+65 6213 5999

**TippingPoint®**

[www.tippingpoint.com](http://www.tippingpoint.com)