

Contents

Introduction	1
Where Intrusion Prevention Comes In	1
Where TippingPoint Comes In	3
Summary	4

Introduction

We live in an age where e-commerce and business critical applications are being 'Webified' as fast as possible; security threats are morphing faster than ever; the membership and skill of the global hacking community is rising; and sophisticated scanning, penetrating, and obfuscating tools and techniques are widely available. Worst of all, hackers are now highly motivated to penetrate networks, applications and databases to steal information that can quickly be sold for profit. It's the modern bank robbery and many can easily become successful criminals by stealing and selling information. And, to compound the problem, the risk of being caught is low – how will you trace a botnet attack crafted by a Rumanian teenager using a machine in Bolivia to attack a bank server in the US? Even if you could trace the attack, what law enforcement agency is likely to understand the nature of the crime, let alone help you? In the meantime, you may find yourself on the front page of the Wall Street Journal – for less than positive reasons.

So what should you do? It's a complex problem and you do not have endless staff and budget to protect yourself. In fact, whatever your revenue is, odds are you

spend about 5% of that on IT, and maybe about 8% of that on network and information security. Yet there is an ocean of point products all being positioned as the latest quick fix. So, IT security faces a vexing challenge – how to wisely spend precious few dollars 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 – thus leveraging your precious IT security staff and budget to the fullest extent. That may sound obvious, until you understand that full security automation is much easier said than done – which is why it is valuable for IT security decision makers to have clear requirements guidance that leads to smart security investment and 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*. Here is why:

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.

1. To block in real time, a product must be placed in-line, not off a tap or mirror port. That means the system must be designed from the ground up to not take the network down, or if there is an issue, be able to gracefully and transparently remove itself from the network without disrupting normal business traffic.
2. Once an IPS has proven it can be placed in-band, it must be able to run at multiple gigabit per second rates of speed. The days of just deploying IPS at the WAN perimeter to block a few exploit-filter matched worms are long gone. Now, IPS's must be located at critical interior network points – the data center, major network segmentation points, and even the network core to provide an effective defense against attacks that can come from virtually anywhere, including your mobile employee's laptops which just 24 hours ago might have been connected to a network at Starbucks, an airport, a hotel, or a home network – all of which have far less stringent security protection than your enterprise

environment. But to consider IPS deployments at key internal points, not only must you be concerned about up-time design, you must also ensure critical business application performance is not impeded – lest your help desk be buried with employee complaints.

3. That leads to the third key criteria – 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, it must perform that inspection work extremely rapidly, or packets will be delayed, application response time slowed, and employees will complain.
4. Hence the fourth challenge – evolving broad coverage and speed of coverage. To protect your network from the growing number of sophisticated attacks, the IPS must provide broad and deep attack coverage. That means the product must be able to stop worms, viruses, Trojans, denial of service attacks, peer to peer bandwidth floods, spyware, phishing, cross site scripting, SQL injections, PHP file includes, VoIP attacks, and more. Further, 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*. Lastly, these 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 certification process not widely available in the world.

‘Detect and alert’ is no longer the game – unless you have an enormous security budget to hire expensive staff for the purpose of sifting through mountains of alerts and then hoping that ‘after the fact’ corrective action will somehow appease government compliance agencies and/or personal privacy breach lawyers.

‘Detect and alert’ are no longer the game - unless you have an enormous security budget to hire expensive staff for the purpose of sifting through mountains of alerts and then hoping that ‘after the fact’ corrective action will somehow appease government compliance agencies and/or personal privacy breach lawyers.

5. Finally, broad attack coverage at critical, high bandwidth, interior or perimeter network points means filter accuracy must be treated with an absolute premium. Otherwise, security personnel will be buried in piles of alerts, many of which will be false positives. In that world, automation kills you, because your staff will be run ragged chasing every fire alarm, only to miss the real ones – a complete misuse of their time and a potential disaster for your business.

It is not that IDS is bad – there are legitimate uses of detection and human analysis. But security budgets must be spent with an eye toward ‘biggest bang for the buck’. Given that IDS and IPS are polar opposites; your next security dollar is simply far better spent on network security automation (IPS) rather than informational alerting (IDS). Once you’ve removed the majority of the malicious and unwanted traffic from your 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.

Where TippingPoint Comes In

This is where TippingPoint comes in. TippingPoint was founded specifically to design and build an IPS from inception to address the above requirements. When the company was formed in 2002, intrusion detection systems (IDS) were widely available. The companies that provided those IDS’s are all around today, and continue to sell IDS, and for the most part continue to preach the gospel of how dangerous it is to go in-band and automatically block, simply because their products never were, and are still not, designed to succeed as an IPS. But the market has spoken.

100% of TippingPoint’s installed base is deployed in-band, with over 1,000 filters automatically set to block straight from the factory. Thousands of our IPS’s are today deployed across Fortune 10, Fortune 100, Fortune 1000, Global 3000, small to medium enterprises (SME), and the high end of small to medium business (SMB) – and across every key vertical. We pride ourselves in helping our customers automatically block damaging attacks in a cost effective manner. In the end, our products have been proven time and again to perform

– significantly reducing the cost and complexity of highly effective network security.

An investment in a TippingPoint IPS will be one of the best security expenditures you can make. But, we do not ask prospects to accept our claims on face value. We simply ask that you allow us to provide an IPS evaluation at no charge to you, where your IT executives, network engineers, and security analysts can see first hand why this product lives up to its claims and can provide your company with cost-effective business assurance.

To that end, we would appreciate the opportunity to discuss with you how we are evolving our industry-leading IPS to a broader IPS Secured Network solution that addresses an even richer set of security concerns including network access control and data loss prevention.

An investment in a TippingPoint IPS will be one of the best security expenditures you can make.

Summary

As a final note, an investment in a TippingPoint IPS is an evergreen investment. We intend to remain the world's best IPS to stop malware and other unwanted traffic from harming your network and critical information assets. But, our solution model is expanding.

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:

30, Cecil Street, #18-01
Prudential Tower
Singapore 049712
+65 6213 5999

TippingPoint[®]

www.tippingpoint.com