

Deriving full value from defence in depth investments

OPINION PAPER

forward »



A decade of joint protection

Deriving full value from defence in depth investments

A Managed Intrusion Prevention Service (IPS) can make all the difference between investment in network security delivering to its full potential or providing basic protection.

Why should network security strategies feature a Managed Intrusion Prevention Service? To answer this we must first consider the business value of effective network security. This is very much a boardroom issue on a number of levels, from its importance in safeguarding corporate information assets (and reputation) to ensuring business continuity and data protection compliance. Poor network security can become a business efficiency issue if a network is infected with viruses, spyware, and worms from peer-to-peer applications that create a bottleneck for network bandwidth.

Typically, investment in network security covers defence in depth products such as firewalls that protect the network from some activity by analysing basic data packet information. However these are generally not robust enough to analyse the contents of those packets in depth and thus require an additional level of protection. Investment in security might also embrace access management technologies such as automated identity management, and data centric solutions such as end-point encryption. Increasingly, these are being tied in to services such as Intrusion Detection Services (IDS), which provides visibility of the network, and IPS, which not only supports real-time visibility but can help mitigate the risk identified.

“ poor network security can become a business efficiency issue ”

IPS versus IDS

Both IDS and IPS contribute a powerful level of network security to information infrastructure in line with defence in depth strategies that aim to enforce the use of multiple security layers. The key difference is clear in the name of each solution.

- **Detect:** IDS is designed as an alert-based tool for detecting a security breach on the network, flagging up suspicious traffic (e.g. unauthorised logins, viruses, Trojans, worms etc) and notifying the network administrator. The IP address from which the threat emanates can then be blocked by the IT team. However, by the time this happens it may be too late and the malicious traffic may already be in an organisation's network.
- **Prevent:** IPS is a more pro-active tool. It prevents malicious traffic from entering the network in real time and can shut down a connection or stop the user session that's originating the attack. An IPS can also interact with the firewall or other parts of the security infrastructure, enabling them to work together in light of a perceived threat. As an inline policy enforcement device, IPS is designed to maximise protection without introducing delays into the network.

“ IPS is a more pro-active tool ”

The ability not just to identify threats but to prevent them, reconfigure itself and make changes to traffic in order to mitigate future threats sets IPS apart from IDS. The vast majority of current leading edge systems are IPS and feature additional functionality such as performing passive OS fingerprinting that can potentially identify the end systems. This function helps validate the false positives that IDS is often criticised for. In effect IPS is the enabling technology for network security policy enforcement.

Adding up the benefits

It's an impressive tool. But all too often investment in IPS is failing to live up to expectations. Organisations are not configuring their systems correctly and thus

“One healthcare organisation achieved a 142% ROI and payback in just 5 months”

simply using their IPS as they would IDS: to detect an intrusion. However, an IPS solution used to full effect will make a significant difference to an organisation's security.

As research by Forrester reveals, payback can be rapid. In its 2009 paper prepared for McAfee, The Total Economic Impact™ Of McAfee's Network Security Platform's Intrusion Prevention System, Forrester found that one healthcare organisation achieved a 142% ROI and payback in just 5 months. The paper identifies quantifiable benefits of the McAfee IPS as follows:

“142% ROI and payback in just 5 months”

- Reduction in help desk calls
- Savings from avoiding manual downloads for cleanups
- Savings from managing signatures, alarms, and policies
- Cost avoidance of security staff.

It points out a number of additional business benefits identified by the organisations interviewed, although generally these were not quantifiable. They included improved network performance and availability, the ability to enforce strict policies and defer bandwidth upgrades, regulatory compliance and more.

What's stopping the payback?

So what's standing in the way of such a powerful network security tool achieving its full potential?

The answer is often a question of time and resource. Exploiting everything IPS has to offer demands input from the internal IT or network security team. All too often those responsible for the new IPS solution simply don't have the time or, indeed, skillset to do more than implement the solution using the in-built default signatures. While these are designed to be powerful enough to block truly malicious attacks, they may not be aligned with an organisation's particular business needs and range of applications.

“threats to an organisation's network won't wait”

It is true that the default values of solutions such as McAfee's IPS can be customised to an organisation's specific application needs, but re-configuring the signatures demands a revision to security policy and this is a traditionally slow process. The problem is that the threats to an organisation's network won't wait. Meanwhile, as powerful as the default signatures are, typically they will not support specific network security policy requirements: that's down to the individual organisation. Importantly, without the time and resource to configure the IPS solution so that it supports the level and speed of response or change to threats that an organisation demands, the IPS solution isn't going to deliver on its true potential.

That's where the joint offering from BT and McAfee comes into play. The BT Managed Intrusion Prevention Service incorporating BT's managed services model and the McAfee Network Security Platform appliance provides a leading edge technology solution that is easier to deploy than other vendors, requires less rack space and provides better port density.

The service draws on BT's world-leading expertise in network engineering across a variety of industries, leading to a higher level of network security, with less complexity, fewer resources deployed in the client organisation and at potentially lower cost than other intrusion services.

Global expertise

Put simply, nobody does it better. BT has extensive experience of monitoring and dynamically managing customers' networks in 170 countries and uses the same Managed IPS service operational teams for its own security needs. McAfee's breadth of coverage, protocols and applications have positioned the company in Gartner's Leader Quadrant for Network Intrusion Prevention Systems. When it comes to security, why work with anyone who isn't the world's best?

A managed service means there is no need to worry about the latest security threats: the worms and viruses, Denial of Service attacks, Spyware, Phishing, VoIP threats and more. BT manages all this and, because it can spread the costs of doing so across a very large customer base, the service will generally be cheaper than an organisation doing it for itself. In partnership with BT the network security policy development can take into account the evolving global threats that only an organisation working with hundreds of multinational companies can stay on top of. A managed service also means that even at weekends and during public holidays the same level of protection will be maintained as if it were a normal working day.

Scalability is another important factor. Buy-in to a new service can be difficult to attain until that service is proven, so organisations demand the flexibility to be able to accommodate new users at a later date. It must also be able to swiftly scale up to meet new business requirements for sharing information across the network, perhaps following a merger or acquisition. The BT Managed Intrusion Prevention Service supports this. It allows an organisation to plan for the long term, to work in partnership with BT on developing and maintaining a secure network environment to meet the evolving business need.

// allows an organisation to plan for the long term //

Furthermore, the potential to meet evolving business needs with in-life hardware refreshes of the McAfee appliance negates the need for regular and expensive updates. Add to this the renowned stability, performance and accuracy of McAfee's Network Security Platform and this is truly a cost-effective solution that provides 24x7x365 real-time protection and support.

Between them BT and McAfee stop millions of network borne attacks every day. It is no wonder that more and more organisations are drawing on this incredible experience to make sure their investment in IPS really works for them.

[To find out more about the BT Managed Intrusion Prevention Service please contact your BT account manager.](#)

BT denies 14 million unauthorised connection attempts each day, quarantines two million viruses per month and blocks million spam messages daily.