The Value of Managed Security Services
Executive Summary

In today’s networked world, being able to connect the right resources to the right opportunities or problems at the right time can give businesses the edge and agility they need to innovate, enter markets, seize share, and grow revenue. But as the business expands across the wide area network (WAN) to meet the needs of today’s global economy, it can introduce risks to the organization that must be mitigated.

The demands placed on the network are increasing from all directions – it’s being challenged to support ever-evolving LAN and WAN landscapes (e.g. the infrastructure is undergoing architectural changes due to consolidation and convergence); it’s being extended outwards to support an increasingly distributed workforce; and it’s being stretched in terms of the bandwidth and capacity required to support all the new media-rich, collaborative (video) applications.

Taking into account the growing complexity of the enterprise networks, the ever-changing application landscape and the rapidly evolving WAN environment, it’s easy to see why many enterprise IT departments struggle to keep their networks secure. The threat vectors are increasing in size and complexity at the same time the threats, themselves, are increasing in number and sophistication. All of this means an organization needs to be more vigilant than ever in their attempts to secure their network and maintain a consistent security stance throughout their operations. It’s why, according to IDC, securing the network is the top concern of WAN Managers.¹

The problem is most organizations are focused on “lights on” activities; just trying to keep their networks up and running takes up most of the IT department’s resources. Many enterprises find themselves lacking the technology and skilled security professionals they need to truly manage and maintain an effective security stance. It’s extremely time-intensive to train staff and ensure they remain up-to-date on all the types of threats facing their organization. As a result, enterprises often struggle to understand the security policies they need, analyze all the traffic on their network to differentiate between benign activity and likely attacks, and quickly respond to reduce the risks facing the organization.

Sometimes enterprises are unable to make the capital investments they need to ensure they have the comprehensive coverage required by today’s dynamic threat landscape. Or, sometimes they simply want or need to focus their attention elsewhere; security is often not a core competency for the organization and, with the finite resources of an IT department, decisions may need to be made about how best to utilize the assets and expertise at hand.

All of these reasons contribute to why many enterprises are turning to managed service providers to help them with their network security needs. Leveraging the staff, resources and expertise of a managed service provider can help organizations ensure they achieve the security stance they need, while reducing costs, relieving the management burden, and ensuring accountability and quick resolution of any issues. The following table shows just what WAN managers feel are the benefits of using a managed service provider:

**Perceived Benefits of Managed Services**

Percentage of respondents ranking each factor #1, #2, or #3

- **Refocus resources on core business**: 72%
- **Reduce network operations costs**: 70%
- **Lack of internal skills/resources**: 55%
- **Improve network/application availability and performance**: 47%
- **Technology/application upgrades/deployments**: 29%
- **Single point of contact/accountability**: 25%

*Source: IDC U.S. WAN Managers Survey, 2007*
This white paper will examine the landscape in which IT departments are operating, the particular security issues they are facing, the potential benefits of turning to a managed service provider and what to expect from a managed security service. It will finish with a quick preview of some of the specific benefits associated with using a managed service that leverages industry-leading Blue Coat technology.

The Affects of the Changing IT Landscape on Security

A recurring theme within IT has always been “do more, with less,” so it’s probably not a surprise that managing and reducing operational expenses is a top priority of most IT departments. More specifically, an IDC survey identified the primary IT directives of executive managers are to improve the efficiency of business operations (58%) and reduce costs (54%). Of course, these objectives are then followed by a seemingly incongruous focus on innovation and increased responsiveness (at 34% and 33%, respectively).

This is the perennial dilemma of IT – how to balance the pressure to reduce the operational costs of the IT infrastructure, while at the same time trying to leverage that infrastructure to do more to drive business growth. The infrastructure is being extended to a wider variety of users, located in increasingly disparate sites, to deliver always-on access to an ever-changing set of business critical services and applications. The reality is to compete, organizations need to be able to quickly connect people and resources to the information and services they need to do business, regardless of where they are located; they need to ensure the business is agile enough to quickly roll out new services and applications to seize rapidly evolving market opportunities.

As a result, 90 percent of enterprise respondents to a Nemertes survey say they operate “virtual” organizations, supporting an increasingly geographical dispersed workforce operating out of many remote sites and home offices to be able to address the opportunities of the “modern economy.” However, while users have been moving outward, most enterprise applications and data have been centralized (57% by some accounts). This means that all the services and applications a typical business relies on now have to travel across the WAN to distributed end-users, creating new challenges for the organization.
Enterprises need to ensure their employees, partners and customers can effectively communicate to drive innovation, accelerate problem solving, solicit feedback, and improve responsiveness and business agility. But how does the IT organization keep all these connections secure? Businesses can’t afford to introduce risk to their organizations, but protecting the company’s network from malware, web-based threats and data leakage is increasingly difficult, as the users and the applications they are using to conduct their work, and inevitably their lives, expand further out of the IT organization’s direct control.

Consumer-based services, such as social media apps like YouTube or Facebook, which typical employees use in their personal lives, are increasingly being brought into the corporate environment and applied to solve business problems – many organizations have their own YouTube channel or leverage Facebook (or a similar service) to connect disparate employees to facilitate information sharing and collaboration. While all these can be great technology enablers, they can also introduce risks that can ultimately threaten productivity, corporate compliance objectives and the overall ability to do business if they are not secured.

**The Weak Links**

As globalization accelerates, businesses are racing to compete, while enabling employees, partners, and customers to access the information they need to conduct business at all times, from wherever they are in the world. While this expansion may be a business imperative, from a security standpoint, it’s an IT nightmare. Imagine all the potential entry points created by this expanded network:

- How does an organization keep up with all the latest threats originating from around the world?
- How does an organization remain vigilant about its security posture?
- How does an organization ensure compliance?

Protecting an organization’s intellectual capital and reducing disruptions to business operations is progressively more difficult as the threat vectors constantly change and increase. It becomes a very tall order for most IT organizations, who are already stretched to their limits, from both a budget and manpower perspective, to stay ahead of the ever-increasing threats.
The web gateway, which has traditionally served as a sentry at the point of entry to the network has found its role changing. Now, in addition to filtering Web requests, blocking objectionable content, collecting logs and information to support compliance efforts, and supplying HR with visibility into relevant employee activity (e.g. Joe went to a pornographic site), it is being asked to protect against increasingly sophisticated Web 2.0 threats – such as Web site injections and new search engine bait engines (SEO poisoning). It must also supply visibility to the IT and risk management teams to ensure they understand all the security threats facing the organization.

What used to just be complicated has suddenly become very complex; and every indication is that it will only continue to require more expertise and vigilance as organizations strive to secure their WAN traffic to reduce the overall risks to the organization.

**The Managed Service Advantage**

Enterprises facing the dilemma of how to effectively manage their security and reduce their risks, while still keeping everything else going, are increasingly turning to Managed Service Providers for support. As defined by IDC, a managed service provides enterprises “a ‘help-me-do-it’ or ‘do-it-for-me’ approach to the operation, monitoring and performance optimization of network and/or IT functions.” By contracting a third-party provider to take care of these aspects of an IT’s operations on an on-going basis, an enterprise can:

- **Augment their staff’s expertise** – rely on the managed service provider and their wealth of experience to ensure the network is up-to-date
- **Innovate** – free up staff to focus on other business imperatives, while increasing the overall coverage of the IT infrastructure through global services that can scale to meet the changing needs of the organization
- **Achieve predictability** – a predefined service level agreement (SLA) ensures organizations can expect a predictable level of performance/availability/capacity/etc.; an agreed upon monthly or annual fee means there is visibility into operational costs to ensure the enterprise can confidently plan and manage threat levels
The Value of Managed Security Services

- **Increase responsiveness** – issues are quickly resolved by the managed service provider, reducing overall maintenance and troubleshooting burdens and ensuring IT organizations can stay on top of other IT imperatives.

- **Support compliance and governance requirements** – receive comprehensive records of all activity and actions taken.

**What to Expect From a Managed Security Service**

Enterprises turn to managed service providers for all sorts of reasons, but the ability of a provider to provide broad attack coverage in a 24 x 7 service model creates a cost-effective value proposition that is attractive to many organizations. Some analysts\(^5\) have found managed security services are the fastest growing segment of the information security market.

There are multiple managed security service options offered by providers, ranging from deploying equipment at the organization’s premise (CPE-based) to providing a dedicated hosted service. The goal is to find an MSP that meets the needs of the organization; one that delivers the level of security and reporting needed to maintain a consistent security stance throughout the infrastructure. The service needs to provide real-time protection against:

- **Dubious web sites** – with traditional URL filtering capabilities, providers can reduce risk profiles by ensuring users can’t go to those sites known to be infected with malware or containing objectionable/unauthorized content.

- **The latest malware** – anti-virus and anti-malware capabilities provide protection against viruses and worms that can degrade performance and compromise the integrity of systems and intellectual assets.

- **Web threats** – newer techniques are required to identify and protect against Web 2.0 threats, such as bait-oriented [phishing sites masquerading as a legitimate site to lure users to unwittingly download malware or provide valuable personal information] or web site injection threats [malicious links embedded on otherwise safe and legitimate web sites – e.g. recent attacks on BBC or USA Today].

- **Data leakage protection (DLP)** – robust policy management should allow control, at a granular level, of who is able to do what on the network, to easily identify anomalies [e.g. that application can only be accessed by the Finance department] that could represent a potential threat.

\(^5\) Gartner Dataquest
It should also provide comprehensive logs and customizable reports to ensure all the data required is available to truly understand what’s going on in the network, investigate attacks, and address compliance and regulatory requirements.

The right managed security service will enable organizations to:

- **Set security policies in line with overall business policies** – maintain an acceptable corporate risk level, manage access and protect against threats to support compliance objectives.
- **Stay up-to-date on the latest threats** – keep the network from known and yet to be invented/discovered attacks by leveraging the expertise of the provider’s security professionals.
- **Manage costs** – ideally, sharing the capital infrastructure investments and expertise of many skilled security professionals across multiple organizations should bring the costs down of deploying, managing and maintaining an effective security posture; it should produce savings on in-house training, and reduce the time dedicated to ongoing security management; minimize the potentially devastating affects a successful attack can have on the network; and achieve greater predictability in the security budget with an agreed upon monthly/quarterly/annual service fee.
- **Increase network reliability** – with security professionals dedicated to monitoring and managing the security of the network, 24 x 7, attain quick resolution and appropriate remediation of security incidents to minimize disruptions and the impact of attacks on the network.
- **Maximize staff effectiveness** – ensure they are focused on business critical projects where they can make the biggest impact.

**Powerful Combination of a Managed Services Based on Blue Coat**

Blue Coat has become the platinum standard for security for most managed services, which provides customers with the benefit of relevant security information derived and shared from more than 70 million users. As a result, Blue Coat and the managed service provider can quickly identify localized or worldwide trends and threat levels and ensure organizations are apprised and appropriately protected to reduce risk.

With Blue Coat’s hybrid cloud model, the managed service provider has the unique ability to provide real-time protection against the latest malware and Web threats, including bait-oriented and web site injection attacks. For example, if a user on the corporate network visits a site [www.xxx.com] the
request will be processed by the Blue Coat Secure Web Gateway, which looks up the site on the local database, as well as in the cloud to get real-time information on the threat level posed by that site. If threat-free, the user will be free to go to the site; if, however, a specific link on that site is corrupted, the user will get a message notifying them that it has been identified as malware or violates a corporate acceptable use policy to protect them from infecting their device and the network.

This differs from other solutions that rely on databases that are only updated every few hours, or on a daily/weekly/monthly basis. The Web can change within seconds, so it’s important to have a solution that can keep up with the ever-evolving threat landscape and ensure the organization is effectively protected.

**Conclusion**

The success of almost every organization in today’s networked world relies on the ability to connect people and resources, whenever and wherever they may be. As IT departments work hard to keep up with the ever-increasing demands placed on the network and do more with less, managed security service providers offer a cost-effective solution that alleviates the burden on IT’s resources and staff, freeing them to innovate and focus on other issues core to the business. A managed service that leverages the underlying Blue Coat technology ensures organizations have the resources and expertise at their fingertips to securely roll out all the business-critical applications their increasingly distributed users need to confidently drive the business forward.