Understanding the Value of Managed Unified Threat Management Solutions

besecure

Managed E-Business Security

Executive Summary

Security threats are becoming increasingly sophisticated and destructive, and continue to disrupt businesses of all sizes and industries (see Exhibit 1). Businesses have to stay on top of the latest network, application and security technology while balancing the needs of the business and customers—a difficult task for most to accomplish alone.

With an abundance of security point solutions required to support a complete corporate security environment, managing, maintaining and integrating these solutions can be too complex for a business to handle internally. Businesses of all sizes and across all vertical markets continue to experience business disruptions as a direct result of security breaches. Whether these incidents affect a single business unit or an entire corporate organization, the damage can still be catastrophic to a company. Lost revenue, a tarnished brand and customer dissatisfaction are a few of the risks businesses can't afford to ignore.

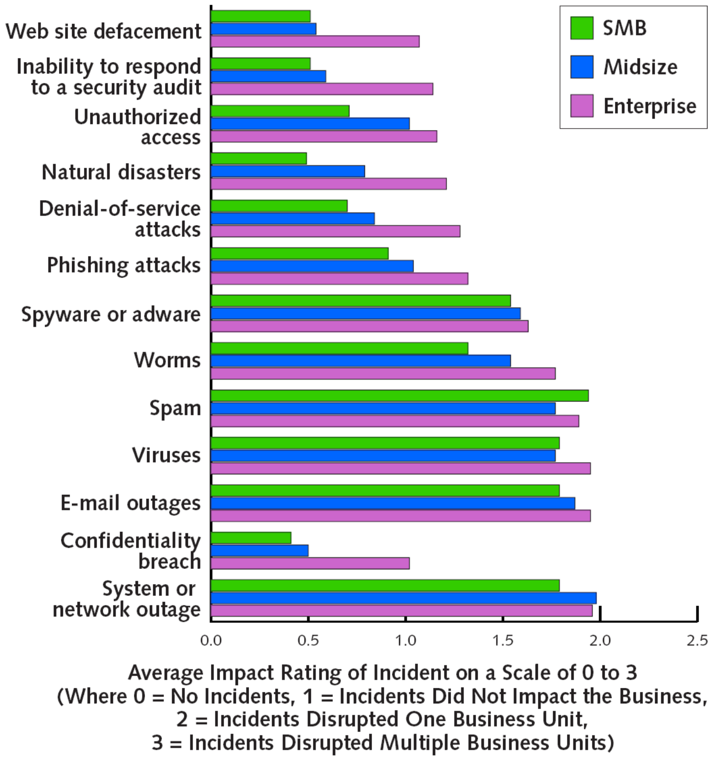
Corporations are aggressively turning to managed security service providers (MSSPs). The challenge is to create the multiple security layers necessary to secure the corporation effectively. To secure the network perimeter and the content coming into and out of the business, many corporations are looking to MSSPs for managed unified threat management solutions as a way to achieve a comprehensive and cost-effective security solution.

Introduction

Securing data, networks and applications is an enormous task for a business, particularly in the rapidly changing world of security threats. Many businesses don't have the expertise, funds or rapid response capabilities necessary to deal effectively with this problem. Not only must the business have the expertise to install its anti-virus, antispyware, firewall, intrusion detection systems (IDSs) and intrusion prevention systems (IPSs), among others, but it must make them interoperate, maintain patches and updates, and monitor these solutions. The costs associated with deploying several point security solutions or managing multiple unified threat management appliances can be overwhelming and unachievable for many businesses. In addition, managing a security environment composed of point solutions can be challenging to manage, maintain and keep up to date. Given the complexities of securing your business, looking to a third-party security service provider for support is a logical and often a prudent decision for many businesses.

Security Incidents Continue to Affect Businesses of All Sizes

Source: Yankee Group, 2006



Managed Security Services

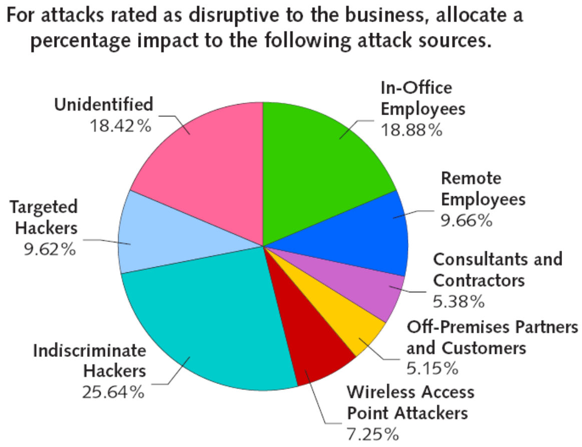
As security threats continue to evolve and become more sophisticated, businesses find themselves in a fierce battle against security breaches. Managed security services provide businesses with an alternative to carrying the security burden themselves. And these services give them the opportunity to leverage the broader knowledge and expertise from the security industry without having to hire many expensive people and install many different point solutions that then need to be managed and maintained. Managed security services provide many businesses with an opportunity to enhance their security strategies and architectures beyond internal capabilities. Businesses considering a managed security service should view the provider as an extension to the organization. All businesses are not alike; they face different priorities, budgets, applications and regulations—each of which influences their decisions on IT, networking and security services. In addition, selecting a managed security services option does not mean that a company has to outsource all security functions. Many businesses outsource just a handful of specific functions or take a co-management approach to security. Regardless of the number of services a business outsources, managed services assist businesses in achieving defense in depth (i.e., core security, edge security and endpoint security are all addressed in the security architecture). Ideally, the architecture includes the integration and linking of these three critical areas of corporate security into one complete solution.

Why Businesses Need Unified Threat Management

Because of the increased sophistication and impact of corporate networks and the security threats the networks face, standalone security products are not effective. To have a complete, end-to-end security solution, multiple security features need to be integrated into a unified security architecture. In this Report, we focus on those security features that make up unified threat management (UTM). UTM is pulling together network security—including firewalls, with anti-virus and antispyware, intrusion prevention and content filtering—into a comprehensive and dynamic threat prevention solution.

In-Office Employees and Indiscriminate Hackers Pose the Biggest Threats

Source: Yankee Group, 2006

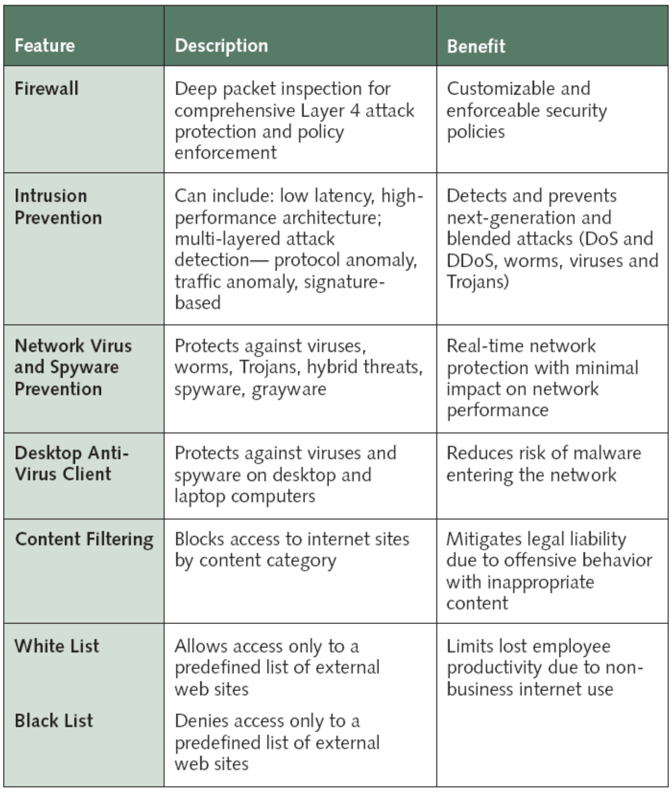


Understanding Managed UTM Offerings

Ease and flexibility are advantages of adopting a managed security services approach to unified threat management. Service providers can deploy a few specific pieces of a threat management solution, such as attack mitigation or anti-virus all the way up to a complete dynamic threat prevention solution based on a business' needs, priorities and budget. UTM solutions offer a comprehensive security solution in that they address both content and network solutions. Corporate security managers don't want to deploy, maintain and pay for separate anti-virus, anti-spyware and firewall solutions to enforce security policies. These separate solutions are an effective threat mitigation approach, but a unified solution will provide an increased level of threat protection to a business, particularly as threats evolve. Businesses need to deploy more multipurpose security solutions and seek a more tightly integrated threat mitigation solution.

Managed Unified Threat Management Feature and Benefit Analysis

Source: Yankee Group, 2006



Feature	Description	Benefit
Firewall	Deep packet inspection for comprehensive Layer 4 attack protection and policy enforcement	Customizable and enforceable security policies
Intrusion Prevention	Can include: low latency, high-performance architecture; multi-layered attack detection— protocol anomaly, traffic anomaly, signature-based	Detects and prevents next-generation and blended attacks (DoS and DDoS, worms, viruses and Trojans)
Network Virus and Spyware Prevention	Protects against viruses, worms, Trojans, hybrid threats, spyware, grayware	Real-time network protection with minimal impact on network performance
Desktop Anti-Virus Client	Protects against viruses and spyware on desktop and laptop computers	Reduces risk of malware entering the network
Content Filtering	Blocks access to internet sites by content category	Mitigates legal liability due to offensive behavior with inappropriate content
White List	Allows access only to a predefined list of external web sites	Limits lost employee productivity due to non-business internet use
Black List	Denies access only to a predefined list of external web sites	

In addition to the specific technical features and functionality, a managed unified threat management solution also should provide a business with automatic updates to firmware signatures. Reporting functionality also is a critical piece to a managed solution because it not only enables a business to see exactly what benefits its service provider is providing, but also can be used for internal administration, operations and compliance reporting. Through these additional services, businesses can easily integrate the managed security service as extended member of their IT organization—with clear handoffs and input into other corporate security polices and processes completing a company-wide, in-depth security architecture. Most businesses today can't operate without the internet and corporate network infrastructure. But the more a corporation relies on technology to conduct business, the more it becomes open to various threats against that business. These threats will not go away—if anything, they will get more complex and damaging. Security solutions that are integrated and designed or approached from a comprehensive point of view offer a business a higher level of protection than a series of individual point solutions.

In addition, UTM solutions provide an increased level of protection without a serious impact on network or application performance. This approach enables businesses to maintain a high level of productivity without affecting the security of the business and opening it up to threats or compliance issues.

Conclusions and Recommendations

Traditional perimeter security is not enough to keep out today's hackers because new network and system vulnerabilities are continually identified and targeted. Businesses should realize that they have options when it comes to securing their network and applications environments. By adopting managed security services, including managed unified threat management, businesses can enhance their security capabilities and expertise flexibly and scalably.

Managing security solutions in-house can be expensive, complicated and challenging because of the complexity of business networks and the number of point solutions required to secure the corporate environment. Managed security services provide businesses with a way to extend their IT staff with the expertise and effectiveness they need to secure their business.

Seek tightly integrated threat management solutions.

The multiplicity of point solutions for specific threats (i.e., intrusion prevention systems for worms and denialof- service attacks, web application gateways for application-level attacks, separate software modules for anti-virus, anti-spyware and personal firewalls) presents obvious cost, manageability and scaling issues.

Businesses should deploy a unified threat management solution or a multipurpose solution with tightly integrated threat management capabilities.

View managed security services as an extension of your security strategy, not a replacement.

The fact that you chose an outsourced solution does not mean you can wipe your hands of network and application security entirely. To achieve defense in depth, your business will need to retain certain security aspects and work closely with your provider.

Evaluate the real differences between managed security solutions before selecting an MSSP. Unlike many point solutions, the real differences between managed security services may not be that clear on the surface. Often, the differences are in the service bundles, pricing and portal/reporting functionality. It may not be possible to do an exact comparison of all service providers, but be sure that you know the content of each offer. Ask yourself the following questions: How are equipment costs passed to the end user? What are the differences between levels of services? How customizable are reports, metrics and other portal capabilities?

Know what your managed security service provider is actually doing and achieving for you, and make necessary adjustments.

Just because you've decided to outsource a portion of your security architecture doesn't mean you can ignore it. Utilize the portals, reporting and other functionality that many service providers offer their customers to understand not just how your security solution is performing, but how the provider itself is performing.

About BESECURE

BESECURE is dedicated to the delivery of security services and solutions of exceptional quality, design and value that enable customers to mitigate and manage security risks that threaten their competitive advantage or market position. BESECURE services portfolio includes Security Risk Assessments, IT Security Audits, ISO 27001 consultancy - implementation services, Security Awareness training services and Managed Security services.

BESECURE Managed e-Business Security Services support the monitoring of firewalls, intrusion prevention systems, virtual private networks, content filtering systems, wireless networks and other security related solutions. BESECURE is owned and managed by experienced IT Security professionals that have gained professional experience working in the field for many years for large consulting firms, IT system integrators, service providers and security vendors.

BESECURE security consultants hold certifications from the most well respected vendor neutral institutions such as International Information Systems Security Certification Consortium (ISC)2 and SANS (SysAdmin, Audit, Network, Security) Institute. The delivery of compliance services is provided from qualified ISO27001 auditors. BESECURE Security Engineers are certified from leading information security vendors including Microsoft, Checkpoint, McAfee, Trendmicro.

Resource: Security Analysis Report from Yankee Group, March 2006