

IBM Threat Mitigation Services application security – Express managed Web security

Highlights

- ***Helps protect IT investments and productivity from Web-based threats***
- ***Scans Web traffic for viruses and spyware and helps stop them before they reach the company's network***
- ***Helps enforce Internet usage policies by blocking access to inappropriate Web sites***
- ***Offers a simple to install and use hosted solution designed to provide strong protection at an affordable price***

Increasingly sophisticated business threats

Businesses, organizations and individuals that use the Internet face a significant shift in the nature of security threats. While e-mail is still the most common way attackers attempt to deliver viruses and spyware, it is now generally more secure than in the past. In response to this greater e-mail security, virus and spyware developers are increasingly exploiting Web-browsing applications as a delivery method. Aided by the unrestricted Web surfing of many business and government users and driven by the financial gain that can result from stealing personal information and intellectual property, hackers and virus writers have become motivated, creative and relentless in their pursuit of new vulnerabilities.

Unlike e-mail threats, which typically target an individual machine and require some action by the user, Web security threats can launch sophisticated, coordinated attacks that require little, if any, user action. Spyware, adware and other malicious software often installs itself without the user's knowledge – leaving no trace while it quietly collects information and disrupts system performance. Once it has been installed, malicious software can be difficult to detect and remove, often reinstalling over and over and disabling any security measures. Fighting such an attack can cause a significant drain on an organization's precious IT resources.

Unrestricted Web browsing by employees and staff can make the situation even worse. Today's organizations often have Internet usage policies in place that are meant to curb unproductive surfing. However, they often depend on employees acting in good faith. At the same time, various industry figures indicate that a significant percentage of all business Web activity is not related to official business. Without any technical safeguards in place, even innocuous Web browsing can lead a user to inappropriate content or Web sites that act as launching pads for installing malicious software.

Facing the challenges that these threats impose is difficult for any business to handle, but especially for organizations that rely on limited resources. Because of the sophistication and constant evolution of the threats, as well as the numerous attack methods used, maintaining Web security often requires more resource dedication and focus than in-house IT personnel have available.

Stopping Web security threats before they reach the network

The traditional approaches to Web security have been to install either security software at the desktop or software and hardware appliances at the network edge. The main problem with these approaches is that they allow threats to reach the network – similar to leaving the front door open and hoping that burglars will not walk in.

Most traditional security solutions are also difficult to set up, monitor and maintain. Required updates for virus and spyware definitions can take systems offline, slowing productivity and consuming precious IT support resources. Typically, these solutions provide only limited protection against “zero hour” outbreaks – new and undetected malicious software that can attack an organization's systems before virus definitions are updated. Traditional URL filtering approaches also have their shortcomings, often either overprotecting by blocking access to necessary sites or under-protecting by ignoring suspicious activities from seemingly harmless URLs.

IBM has developed an answer to these issues: Express managed Web security. This powerful solution has been developed to help protect an organization's IT investments and improve productivity by reducing the threat of spyware and viruses delivered via Web-browsing, as well as helping to automatically enforce Internet usage policies by filtering access to inappropriate or potentially dangerous URLs. An integral part of the IBM Threat Mitigation Services, Express managed Web security was created specifically for midsize business and organizations. As a hosted service, Express managed Web security service is simple to install, requires no investments in hardware or software and needs very little client management. The service is priced per user, per month, so the solution can be affordably scaled according to a company's need.

The service is available in three configurations:

- *Anti-virus and anti-spyware*
- *URL filtering*
- *Anti-virus, anti-spyware and URL filtering*

Helping to prevent viruses and spyware from reaching desktops

The Express managed Web security anti-virus and anti-spyware service is designed to offer realtime scanning of an organization's inbound and outbound Web traffic. This service uses virus-scanning engines, as well as spyware, adware and phishing databases that were selected based on their accuracy. Using this service helps provide organizations with a greater level of protection than can be offered by single vendor solutions, which are typically cost-prohibitive to build in house.

The anti-virus and anti-spyware service is designed to quickly analyze the content of a Web page or a file-type request and determine if it is safe to pass on to the end user's browser. Unacceptable requests are quarantined and deleted.

However, the anti-virus and anti-spyware service does more than help protect a company's IT infrastructure against known threats; it also helps safeguard against unidentified malicious activities. Using an advanced heuristic analysis, the service is designed to improve its capabilities the more it works. It identifies patterns of activity associated with threats, which helps it to prevent the "zero-hour" attacks that have become increasingly prevalent. Since the service analyzes Web threats outside of the network, the risk of those threats infecting an organization's systems can be vastly minimized.

Because the service monitors outbound traffic as well, it can detect and prevent attempts to launch spyware and virus attacks from within the network, thereby helping to protect company and brand reputation. This comprehensive service is fully hosted and designed to operate with little oversight by IT personnel. At the same time, organizations can retain control over their service, using a Web-based administrative interface to set preferences – permitting non-invasive adware, for example – as well as to establish alerts and reporting features.

Allowing safeguarded, controlled Internet access

The Express managed Web security URL filtering service assists organizations in enforcing Internet usage policies and helps ensure relevant regulatory and legislative compliance by monitoring and

controlling the content that enters the network. It also helps to prevent accidental visits by business users to inappropriate sites. Moreover, it can help defeat phishing and spoofing techniques that may lead users to inadvertently reveal confidential information or install spyware.

The service is highly configurable and allows for various URL category – and content-based policies, providing businesses with greater control while helping to protect employees and brand reputation. URL filtering is designed to:

- *Enforce policies based on file types, in order to restrict broad content types, such as audio and video*
- *Control access to more than 60 URL categories and block anonymous proxy services that reroute traffic to inappropriate destinations*
- *Block access to Web-based e-mail, which is usually not work related and can circumvent desktop antivirus and anti-spyware software*
- *Restrict access to some sites during business hours and allow fewer restrictions after hours*
- *Configure user- and group-level settings using existing directory information*

Unlike e-mail, for which a certain amount of delay is tolerable, efficient Web browsing for business purposes requires speed. The anti-virus, anti-spyware and URL filtering services are designed to monitor Web traffic and redirect threats to IBM's security-rich infrastructure with no noticeable delay to the end user.

All of the Express managed Web security modules are accessible to administrators via a Web-based interface that is easy to use and enables organizations to modify services as needs change. The services are also designed to complement the Express managed e-mail security solution.

Helping to lower the cost of securing Web access

Express managed Web security offers compelling potential business benefits. By identifying and removing threats before they reach the network, this enhanced level of protection helps organizations achieve business-critical goals such as:

- *Enhancing business continuity*
- *Improving employee productivity*
- *Protecting company information*

Because they are hosted solutions, IBM's anti-virus, anti-spyware and URL filtering services help companies to avoid additional investments in hardware and software, while improving the protection of the business, infrastructure and productivity. Express managed Web security modules include IBM Help Desk services, in conjunction with access to the IBM Incident Response Team, which is ready to assist organizations in the unlikely event of a Web security breach.

About IBM Internet Security Systems

IBM Internet Security Systems™ (ISS) is the trusted security expert to global enterprises and world governments, providing products and services that protect against Internet threats. An established world leader in security since 1994, IBM ISS delivers proven cost efficiencies and reduces regulatory and business risk across the enterprise. IBM ISS products and services are based on the proactive security intelligence conducted by the IBM ISS X-Force® research and development team – a world authority in vulnerability and threat research.

For more information

To learn about Express managed protection services for server, please contact your IBM Business Partner, IBM sales representative or visit:

ibm.com/businesscenter/smb/us/en/security



© Copyright IBM Corporation 2008

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America

03-08

All Rights Reserved

IBM and the IBM logo are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

X-Force is a trademark or registered trademark of Internet Security Systems, Inc., in the United States, other countries, or both. Internet Security Systems, Inc., is a wholly-owned subsidiary of International Business Machines Corporation.

Other company, product and service names may be trademarks or service marks of others.

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.