



The first step in network security is knowing where you are vulnerable. Now IBM provides you with a Free Security Health Scan giving you the insight necessary to remain ahead of threat™.

Why Get A Free Security Health Scan:
<ul style="list-style-type: none"> • Preemptive security from IBM Internet Security Systems (ISS) stops Internet threats before they impact your business.
<ul style="list-style-type: none"> • Identifying and protecting against vulnerabilities limits the business impact of potential security threats.
<ul style="list-style-type: none"> • Delivers up to the minute statistics and detailed actionable information surrounding the current state of your security posture for improved decision making.
<ul style="list-style-type: none"> • Ensures business uptime and improves employee productivity.
<ul style="list-style-type: none"> • Ensures the safeguarding of critical assets and confidential data

What's at Risk?

- Reputation and customer confidence
- Proprietary and confidential data
- Employee productivity
- Business uptime
- Addressing regulatory audits
- Increased costs related to security breaches

Nothing has happened - Why not wait until it does?

Preemptive Security = Productivity Gains

With an effective enterprise security strategy, preemptive protection empowers you to confidently extend networks to improve productivity, reduce costs, and compete effectively in a constantly

changing business environment. Why not spend your time staying ahead of the competition and not letting your security posture cause you hesitation.

The Cost of Reaction

Organizations cannot afford reactive to security. Preemptive security is the only way to keep security- and cost-conscious organizations "ahead of the threat™." It may feel like less money and resources upfront, but the cost of a security breach can be astronomical if placing a value on your brand's reputation. In a recent study it was found that the cost of data breaches cost companies an average of \$182 per compromised record. Is this something you would like to avoid both financially and in loss to your company's reputation?

Protecting Critical Data

Securing your customer data is key in today's business environment. Does your organization have an online presence? Does your organization conduct business online with customers or suppliers? Is your organization looking to grow with online applications and initiatives? Is your organization subject to new regulatory requirements such as Payment Card Industry (PCI), HIPPA or Sarbanes Oxley? While once only a concern for the Fortune 500 these regulations now apply to small and medium size businesses as well.

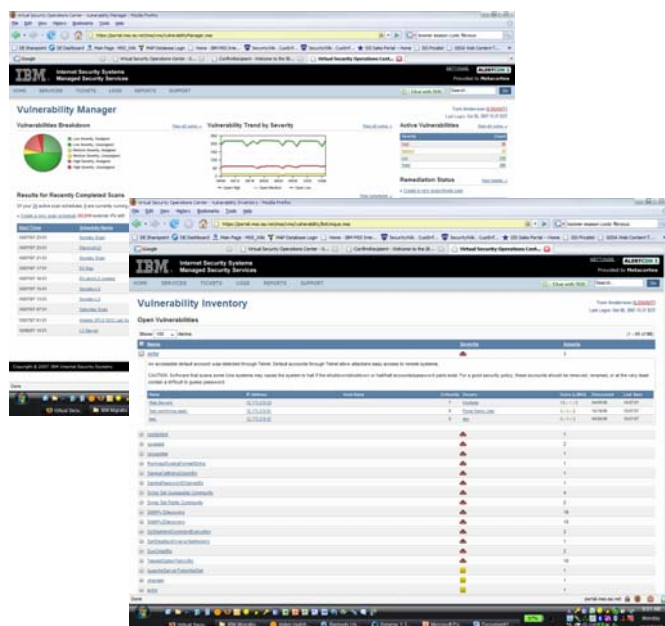
By taking advantage of the Free Security Health Scan from IBM Internet Security Systems you can take the first step in understanding your current security posture. The Free Security Health Scan will then enable you to take the necessary steps to protect your critical data and get focus on your business. With current regulatory mandates, protecting customer data is not an option.

What you get in return

The IBM Free Security Health Scan allows you to experience first hand the benefits of IBM Internet Security Systems' proven protection and remediation capabilities. Trial customers will receive access to the Virtual Security Operations Center (Virtual-SOC) Web portal for up to the minute statistics and detailed actionable information surrounding the current state of your security posture. This limited time offer is for one IP range (up to 25 IP addresses) or up to five individual IP addresses to be scanned one time per week for up to four weeks. Experience why IBM Internet Security Systems is the trusted security advisor to thousands of the world's leading businesses and governments, providing preemptive protection for networks, desktops and servers.

4. Help create justification for security investments
5. Reduce exposures to malicious attacks that could cause potential downtime
6. Considering the benefits of outsourcing? Sample the preemptive technology available to you. Know your options – try out your own Virtual Security Operations Center (SOC)
7. Create awareness of vulnerabilities in the network that would otherwise go undetected until exploited.
8. Identify high risk vulnerabilities minimizing risk of exploitation in the network infrastructure.

What do I do with the scan results?



1. Proof of concept – test drive preemptive protection for a network and Internet perimeter by identifying and remediating security issues found in servers, firewalls, switches and other networked equipment
2. Familiarize yourself with what a preemptive approach to Network security would do for your organization.
3. Create a compelling event to increase internal awareness around security issues

Overall Benefits to a Preemptive Approach

Online risk can be managed with confidence. With preemptive security in place, online risk is no longer a function of doing business.

Preemption lowers security costs by making security less work.

Automatically stopping threats before they impact your business, preemptive security can dramatically reduce workloads and expenses.

Security can be a sure thing. With preemptive security delivered within an integrated platform, organizations can have comprehensive protection that is not only more effective, but can also scale, and be guaranteed* to prevent business losses.

IBM ISS Stays "Ahead of the Threat"

IBM ISS' preemptive security solutions stop Internet threats before they impact your business. From stand-alone solutions, to centrally-managed security systems, to outsourced security management, the IBM ISS protection platform offers complete end-to-end coverage of your enterprise IT infrastructure.

*Money-back guarantee (for Managed Protection Services - Premium Level only): If Internet Security Systems fails to meet the Security Incidents Prevention Guarantee for any given calendar month, Customer's account shall be credited the charges for one full month of the affected Customer's Monthly Monitoring Fee for each instance for which this guarantee has not been met. Please see ISS SLAs for more details.

IBM Internet Security Systems X-Force research and development team

The IBM Internet Security Systems X-Force research and development team is the foundation of IBM Internet Security Systems' preemptive approach to Internet security. The oldest, best-known commercial security research group in the world, this leading group of security experts researches and evaluates vulnerabilities and security issues, develops assessment and countermeasure technology and educates the public about emerging Internet threats. The X-Force team provides IBM Internet Security Systems with the ability to stop more threats because of its knowledge base of information—understanding the tools and techniques used to create attacks and collaborating with government agencies, industry consortia and software developers. X-Force security intelligence, combined with 24x7 threat tracking and analysis through IBM Internet Security Systems security operations centers, enables IBM Internet Security Systems to help organizations stay ahead of the threat.

X-Force research and development team innovation

- The X-Force research and development team leverages its superior understanding of vulnerabilities and exploit methods to develop the engines that make preemptive solutions possible, enabling IBM Internet Security Systems to help protect clients against entire categories of vulnerabilities instead of creating signatures for specific exploits.
- The X-Force team discovers and analyzes previously unknown vulnerabilities in critical software and infrastructure such as e-mail, network infrastructure, Internet applications, security protocols, business applications and Voice over IP (VoIP).
- The X-Force team augments its own findings by collecting data from multiple research sources, researching publicly disclosed vulnerabilities and underground or irresponsibly disclosed 0-day vulnerabilities and analyzing proof-of-concept and exploit code.
- The X-Force team monitors and analyzes global Internet threats 24x7 and updates IBM Internet Security Systems AlertCon in real time, providing the current global Internet threat level.
- The X-Force Vulnerability Database is one of the industry's largest and most authoritative vulnerability database. Containing approximately 30,000 entries, with more than 5,100 added in 2005, it includes detailed analysis of every notable public vulnerability disclosure since 1994.
- The X-Force team discovered 51 percent of the high-risk vulnerabilities found by commercial security research groups from 1998 to 2005, including the vulnerabilities exploited by the Slammer and Zotob worms.
- The X-Force team collaborates with thousands of the world's leading businesses and governments, vertical sector information sharing and analysis centers (ISACs), global coordination centers and other product vendors.

IBM Internet Security Systems Virtual Patch technology

As software vulnerabilities continue to increase, so will the number of patches to install. As a result, many organizations today remain in an ongoing reactive mode, trying to determine which critical patches to apply first. Because IBM Internet Security Systems solutions are powered by proactive research, IBM Internet Security Systems provides a viable alternative to current security patching methodologies. IBM Internet Security Systems Virtual Patch[®] technology has the benefit of proactive security content updates that are focused on vulnerabilities. This systemic approach protects against vulnerabilities during the window of exposure between vulnerability announcement and patch application—thus the term “virtual patch.”

Register for Free Security Health Scan

To register for your free scan, visit

https://www14.software.ibm.com/webapp/iwm/web/signup.do?lang=en_US&source=healthscan&S_TACT=6N7AJ79W