



Proactively identifying network security vulnerabilities with IBM Internet Scanner software.

The first step to securing your network is knowing your network

IBM Internet Scanner® software provides a solid foundation for network security. It delivers prompt vulnerability assessments for networked systems, including servers, desktops and infrastructure devices. Internet Scanner software improves security and saves time and money by discovering networked assets, identifying security vulnerabilities or weak spots in operating systems and applications, and prioritizing patching and protection activities.

Internet Scanner software probes operating systems, routers/switches, mail servers, Web servers, firewalls and applications—identifying vulnerabilities so that you can address them before hackers access and take control of systems. Scan results are displayed both onscreen and in reports that allow your IT department to respond quickly to critical vulnerabilities.

The Internet Scanner application can also be integrated with the IBM Proventia® Management SiteProtector™ (SiteProtector) system to manage vulnerabilities and other security functions from one console.

Why is vulnerability assessment important?

Because security threats are becoming more numerous and complex—and the costs of information theft are huge.

As business networks become more intricate, their risk of becoming vulnerable to malicious attacks rises. Most companies take “reactive” security measures, such as implementing firewalls and anti-virus programs, which tend to protect against only known threats. If criminals discover and exploit vulnerabilities that your company or your technology vendors are not aware of, serious consequences can result:

- Loss of availability (denial of service)—e.g., your Web or e-mail server becomes inaccessible, or the order-entry system ceases to operate.
- Compromise of integrity—e.g., unauthorized users conduct Web site defacement or e-mail snooping.
- Breaches of confidentiality—e.g., customer records are lost, or confidential information is stolen or made public.

That means downtime, data loss, potential reputation damage and costs to the business. Internet scanning helps to reduce business risk by discovering vulnerabilities throughout your network so you can take measures to protect those entry points before an attack occurs.

How does Internet Scanner software work?

Vulnerability assessment

A sound security-management process starts with asset identification. Internet Scanner software identifies all the devices, services and applications running on your network. The Internet Scanner application has the capability for virtually unlimited asset identification, allowing you to scale with your company's growth.

Internet Scanner software's default policies and common policy-editor features save you out-of-the-box configuration time. Internet Scanner software then efficiently and accurately determines the services, applications or code that may be at risk of attack. It also identifies misconfigurations that could lead to a compromise. Finally, the product performs noninvasive tests to analyze the potential effects of a real attack.

Vulnerability reports

Internet Scanner software generates logical, easy-to-understand reports that include detailed technical, operational and management information. Each report provides instructions for corrective action and vendor sites for security patches with helpful information.

Security research

Clients using Internet Scanner software benefit from the latest IBM vulnerability assessment solutions. Our globally respected IBM Internet Security Systems X-Force® security intelligence team discovers, researches and tests software vulnerabilities. The Internet Scanner application receives prompt electronic updates on the newest threats to ensure that you can identify the latest security holes.

Why choose Internet Scanner software from IBM ISS?

IBM Internet Security Systems (ISS) developed its network scanner more than ten years ago. It is a stable, accurate and time-tested product. Because Internet Scanner software can be centrally managed, your company can maintain tighter control over your network and your security environment. And you will be in compliance with stringent audit requirements for network security. Internet Scanner software is designed to function as a stand-alone product. Yet it seamlessly integrates with the SiteProtector system and other IBM ISS products so that you can manage scanner installations worldwide and optimize your protection.

The IBM protection platform

Internet Scanner software is an integral piece of the IBM protection platform, which delivers preemptive protection as part of a centrally managed security solution. The IBM protection platform enables a four-part process that helps enterprises:

- 1) Assess enterprisewide security risk.
- 2) Prioritize patching and protection activities to accelerate risk reduction.
- 3) Continually protect and secure every layer of the network.
- 4) Demonstrate security risk reduction and compliance.

Discover how the Internet Scanner application can protect your business from Internet threats. Ask us if your company qualifies for a 30-day evaluation. For an onsite demonstration, contact the IBM Internet Security Systems office nearest you. For office locations and to get more product information, visit:

ibm.com/services/us/iss



© Copyright IBM Corporation 2007

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

Produced in the United States of America
04-07
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.

Proventia, SiteProtector and X-Force are trademarks or registered trademarks 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.

All performance data contained in this publication was obtained in the specific operating environment and under the conditions described above and is presented as an illustration. Performance obtained in other operating environments may vary and customers should conduct their own testing.