



## Manage, monitor and measure enterprise security with IBM Proventia Management SiteProtector.

### Centralized security management

The IBM Proventia® Management SiteProtector™ system applies policy, product and content updates to a myriad of security agents and appliances through one security management system. SiteProtector unifies the management of IBM protection platform offerings across gateways, networks, servers and desktops, as well as third-party security solutions.

SiteProtector takes on the burden of centrally managing, monitoring and measuring enterprise security—so your overtaxed IT resources can focus on other critical projects. Use it to create help desk tickets and direct IT resources based on the findings of network, gateway and host agents and appliances. Or conduct asset discovery and vulnerability assessment via the same console; command and control mail

security and anomaly detection systems; analyze security events and report on your security processes and posture. By integrating with workflow and ticketing, systems administration, and network and database management tools, SiteProtector can become an integral part of your IT process, rather than a security add-on to contend with.

Proventia Management SiteProtector is available as a self-contained, security management appliance, so you need to purchase only a single device to achieve one of the most robust levels of security management available.

### **Let IBM help you reduce security complexity and optimize value**

#### **Simplify security deployment and management with a single console**

With SiteProtector, IBM Internet Security Systems (ISS) has unified the management of disparate security technologies. This innovative security management system works to eliminate the complexity of piecemeal security management by providing centralized command and control capability for the following types of security devices:

- High-performance network security
- Endpoint or desktop security (including anti-virus)
- Critical server security
- Vulnerability management systems
- Remote office/branch office security
- Internal security
- Mail security

#### **Take advantage of existing infrastructure**

SiteProtector integrates into your existing infrastructure—including Microsoft® Active Directory, Remedy Help Desk and SQL Server 2005—to help make security remediation an easier part of your IT workflow.

#### **Prioritize protection around the highest risks**

The system applies correlation to create prioritized and actionable remediation instructions. By correlating your event data against the vulnerabilities specific to your network, you can focus resources on the greatest risks first. SiteProtector also deemphasizes security events that pose little risk to your organization.

#### **Maintain centralized security policy**

The SiteProtector system's role-based administration is designed to configure and enforce protection policies, monitor security status 24x7, evaluate your policy's status and find your network's weak points from one centralized, enterprise-scalable console. The system produces central responses based on rules or thresholds maintained across all disparate agents and appliances. Its comprehensive reporting options let you measure compliance against your security policies using a single system.

#### **Additional benefits of centralized management**

##### **SiteProtector leaves you with "room to grow"**

A centralized management system must offer the flexibility to deploy more security controls as time goes on. In fact, demonstrating compliance implicitly requires keeping up with the rising standard of due care. What is considered to be adequate protection this year may not be good enough next year. SiteProtector helps to provide for a flexible security deployment roadmap, giving you room to grow your security capabilities over time. Most other vendors do not provide command and control of as many different types of security from a single system as SiteProtector does. Adding to your security infrastructure with SiteProtector lends scalability to enterprise security rollouts.

##### **SiteProtector facilitates compliance**

SiteProtector helps you demonstrate compliance by maintaining a comprehensive asset database, a record of risk reduction and remediation efforts, and centralized security policy. By supplying real-time reports on the security posture of assets, threats and trending, the system delivers business intelligence, allowing you to make cost-conscious decisions

regarding your network. SiteProtector helps organizations such as yours take the following actions toward regulatory compliance:

- Gain visibility into all IT assets
- Build a comprehensive asset database
- Assess risk and assign remediation
- Document blocked security attacks and remediation efforts
- Maintain centralized security policy
- Benchmark against established security policy
- Facilitate policy management, vulnerability management, and incident response policies and procedures
- Track configuration and policy changes

#### **How is Proventia Management SiteProtector different?**

##### **Comprehensive management for all your security technology**

SiteProtector manages the IBM protection platform, including host and network intrusion detection and prevention, anomaly detection, vulnerability management, firewall/virtual private network (VPN), and content security.

##### **Integration with other systems optimizes your investment**

SiteProtector leverages existing infrastructures such as Active Directory for asset identification and classification, and manages access control through existing domain credentials. SiteProtector also integrates with Remedy Help Desk systems and provides a native ticketing functionality as well. It manages security products from Checkpoint, Cisco Pix and others; network management products such as Netcool; and database management using SQL DB clustering.

##### **Scalability facilitates deployment and growth**

Proventia Management SiteProtector can support hundreds of thousands of security devices and networks with more than 1,000,000 nodes. It incorporates “build agent” technology that enables easy deployment for preconfigured product rollouts. This scalability makes this system a preferred solution of government agencies, large-scale commercial enterprises and financial institutions.

##### **Intelligent correlation provides stronger security**

The Proventia Management SiteProtector system’s analytical capabilities range from baseline views to custom-defined asset groupings. With the IBM SecurityFusion™ module, it can also quickly validate or invalidate a security threat by correlating real-time vulnerability and threat information. This allows your staff to concentrate on actual security threats rather than network noise. It can increase the priority level of alerts and reduce console and database clutter by discarding unsuccessful attacks.

##### **Powerful reporting lends to a reduction in risk**

Proventia Management SiteProtector delivers flexible and powerful enterprise-class reporting. Its dozens of predefined reports, as well as customized reporting, allow companies to provide:

- Policy and compliance management reports
- Audit and administration reports
- Vulnerability and configuration-management reports
- Incident and event-management reports
- Reports for business management including overall compliance levels, resolution, current threats and enterprisewide trends
- Granular reports for technical managers detailing compliance at the asset, operating system and line-of-business levels

The SiteProtector system’s reporting capabilities demonstrate compliance as well as dissect the forensics of attacks. It categorizes assets according to regulatory compliance standards. In addition, its reports on vulnerability and threat remediation show how your security posture improves over time. SiteProtector leverages IBM Internet Security Systems’ experience in delivering the most informed security intelligence to provide clients with up-to-the-minute protection.



## **IBM Internet Security Systems delivers comprehensive security management**

IBM Internet Security Systems delivers end-to-end security for the majority of areas of your business. Centrally managed by Proventia Management SiteProtector, our protection platform is an integrated solution combining network, server and desktop protection with vulnerability management and protection.

### **For more information**

Contact the office location nearest you to schedule a consultation. For office locations and more information on Proventia Management SiteProtector, visit:

**[ibm.com/services/us/iss](http://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, SecurityFusion and SiteProtector 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.

Microsoft is a trademark or registered trademark of Microsoft Corporation in the United States, other countries, or both.

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.

Information in this document concerning non-IBM products was obtained from the suppliers of these products, published announcement material or other publicly available sources. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

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.