

Enhancing the effectiveness of security operations through a central point of management



IBM Proventia Management SiteProtector system



Managing your security operations from a central point

Managing your security infrastructure is never an easy task, but when you're trying to manage multiple devices, security vendors and compliance regulations, it can seem impossible. Over time, the cost and complexity of securing your organization can rise substantially, without a corresponding decrease in your exposure to security risks and noncompliance. Valuable resources are continually diverted from revenue-gathering projects while your IT staff spends hours on day-to-day administration.

Highlights

- ***Reduces the cost and complexity of security management through central control of diverse network and host security devices***
- ***Enhances risk communication through event analytics and flexible, customizable reporting***
- ***Leverages existing investments by integrating with current systems***
- ***Provides flexibility to expand to support additional types and functions of security offerings***

IBM Proventia® Management SiteProtector™ system offers a flexible, one-stop security management system to command and control a broad array of network security agents and devices required to monitor and measure your exposure to vulnerabilities and demonstrate regulatory compliance. It can

reduce the burden of your IT security team by unifying the management of IBM security platform offerings across gateways, networks, servers and desktops, as well as select third-party security solutions. Backed by, and integrated with IBM Internet Security Systems™ (ISS) X-Force® research and development team with its tools, online security information and security updates, the SiteProtector system can help minimize your overall risk and increase efficacy of your security team with maximum cost efficiency.

Easing the cost and complexity of security management

The SiteProtector system helps reduce operational costs by automating and simplifying tasks such as setting policies, applying updates, scanning and enabling protection. From a single interface, you can monitor events and manage all of your IBM ISS technologies, including network and host intrusion prevention, scanning, desktop security and multifunction security. With just one system to deploy, learn and maintain, one vendor to turn to for support and one management console to control your security infrastructure, this innovative solution can help you reduce the

costs and complexity associated with security management and free your IT staff to focus on other critical projects.

You can organize your security devices within the SiteProtector system and create custom-defined groupings for an enterprisewide risk perspective of assets, threats and vulnerabilities. The SiteProtector system includes advanced features to help you correlate and prioritize near real-time vulnerability and threat information to help you quickly assess the information that's most critical or relevant to your environment—enabling IT staff to focus on your greatest risks. You can also use the SiteProtector system to increase the priority level of alerts and reduce console and database clutter by discarding details of unsuccessful attacks. The SiteProtector system facilitates a robust roles and permissions model to help you delegate responsibilities among various team members. Site administrators can use a Web browser from virtually any location to grant selected users the ability to perform certain functions. For example, administrators may allow some users to see and operate security devices located in a certain geography, while limiting others as read-only users without the ability to change security policy.

Evaluating and communicating your risk posture

The SiteProtector system can help you quickly identify and communicate potential threats, and assess your security posture by enabling you to:

- *Identify risk*
- *Perform threat mitigation*
- *Reduce burdensome maintenance*
- *Perform event monitoring and analysis*
- *Set security policy*
- *Discover vulnerabilities*

Easy-to-use, customizable reporting capabilities let you sort information by virtually any parameter and provide auditors and regulators with critical information. The SiteProtector system also allows you to make timely adjustments to policies. Guided analysis capabilities help transform even the new security analyst into a knowledgeable expert, taking the guesswork out of event analysis and aiding your security analyst with logical investigation paths to quickly get to the cause of an issue.

A broad array of reports—both predefined and customized—within the SiteProtector system can allow you to identify and document:

- *Staff who can access the system*
- *Ticketing activities*
- *Policy, audit, assessment, administration and compliance management*
- *Vulnerability and configuration management*
- *Information about overall compliance levels, resolutions, current threats and trends*
- *Detailed information on compliance at the asset, operating system and line-of-business levels*

SiteProtector reporting capabilities not only help ease compliance measures, but they can also provide specific details regarding security breaches. Reports on asset security, vulnerability remediation and trends provide an enterprise view of improvements to your security posture over time and help enable intelligent, cost-effective decisions regarding your network. A forced versioning feature within the SiteProtector policy editor helps enable automated tracking and logging of policy history to further reduce the burden of change-control compliance.

Integrating with existing systems to leverage your investments

The SiteProtector system can provide seamless integration with existing security solutions to leverage your existing investments, including:

- *Microsoft® Windows® Active Directory*
- *Support of Microsoft SQL Server database clusters*
- *VMware ESX 3.5*
- *Remedy ticketing integration*
- *Support of two-factor authentication*

In addition, your own IT department or other vendors can programmatically enable their applications to leverage the SiteProtector data repository.

Expanding to support evolving requirements

The SiteProtector system can scale to meet expanding requirements of today's dynamic enterprise, enabling you to broaden your security by incrementally adding other types of security products, including network and host intrusion prevention systems (IPSs) and multifunction devices. You can also expand in depth by adding more

security devices within a single function. You can scale in both of these dimensions—as well as add policies into your security system—with virtually no increase in operational cost.

Because the SiteProtector system offers a consistent interface that employees can quickly become familiar with, you can nearly eliminate the need for staff to learn new systems when you add new protection—easing the deployment of new protection devices, management of device updates and administration of management policies. The SiteProtector system includes a year of updates, patches and basic technical support.

Why IBM?

IBM Proventia Management SiteProtector system offers a single, easy-to-use central management point to control security policy, analysis, alerting and reporting for your business. With support for a broad array of products, an established track record of protection that is backed by the X-Force team and the ability to expand security coverage, the SiteProtector system can provide a simpler, cost-effective way to manage your security operations.



For more information

To learn more about IBM Proventia Management SiteProtector system, please contact your IBM representative or IBM Business Partner, or visit the following Web site:

ibm.com/services/security

© Copyright IBM Corporation 2009

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

Produced in the United States of America
August 2009
All Rights Reserved

IBM, the IBM logo, ibm.com, Internet Security Systems, Proventia, SiteProtector and X-Force are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at ibm.com/legal/copytrade.shtml.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product or 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.

Disclaimer: The customer is responsible for ensuring compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the reader may have to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law or regulation.



Recyclable, please recycle.