IBM Proventia Network Anomaly Detection System

Enhancing network intelligence to help improve security posture
While an intrusion prevention system (IPS) can successfully defend a network against most unwanted access and malicious traffic, behavioral detection methods are required to prevent many evolving threats, such as internal misuse or theft, phishing, pharming, botnet armies and propagating worms—all of which inhibit a high-performing network. When anomaly detection is used in conjunction with IPS, businesses can improve network visibility, supporting regulatory compliance and enhancing overall security posture.

IBM Proventia® Network Anomaly Detection System (ADS) is designed to complement firewall and IPS technologies, helping to maximize network intelligence and mitigate evolving threats. By continually examining the behavior of users, networks and applications across the entire enterprise, Proventia Network ADS can expand upon protection from an existing IPS—without causing bottlenecks or requiring network redesign.

Increasing network visibility to help facilitate regulatory compliance
Using Proventia Network ADS with the IBM Proventia Network Intrusion Prevention System can help increase network visibility and leverage the existing central command and control console for enhanced protection. Enhanced visibility makes it easier to meet regulatory requirements. The combination of new ADS functionality with existing IBM protection platform products (e.g., Proventia Management SiteProtector™) can help create acceptable use policies and compliance standards, provide a more complete picture of what is happening on the network and improve visibility into how security affects bandwidth and traffic flow.

Highlights

- **Supports regulatory compliance and enhanced security through improved network visibility**
- **Delivers multilayered protection designed to defend against diverse threats**
- **Helps maximize the value of your existing intrusion prevention system**
To demonstrate full compliance with many security mandates (e.g., the Sarbanes-Oxley Act), your business must not only prevent malicious attacks from outside the organization, but also take necessary and prudent measures to protect against internal risks. Because behavior-based threats are not captured by existing IPS technology, ADS is essential to meeting regulatory requirements. Proventia Network ADS can help your IT organization design custom rules and monitor behavior, measuring what is acceptable and unacceptable against set standards. Based on the rules, Proventia Network ADS generates events to populate data in the central command and control console, creating reports to show compliance with acceptable use policies.

Using IPS or ADS as a stand-alone solution fails to capture the full potential of the multilayered approach IBM Internet Security Systems™ advocates. Through central analysis, risk reports and integrated events, Proventia Network ADS complements IPS by offering a consolidated view of all IPS and ADS events, for a more complete picture of what is happening on the network. Combining ADS events with IPS events takes full advantage of reporting, workflow and analysis features, raising the bar for network security.

Proventia Network ADS also reports abnormal fluctuations in bandwidth or traffic flow to help identify potential risks, providing your security and network teams with valuable insight into network bandwidth and traffic patterns from a security standpoint.

**Combating diverse threats with layers of protection**

When combined with Proventia Network IPS, Proventia Network ADS delivers multilayered protection designed to guard against multiple types of threats. Proventia Network ADS offers the latest in protection technology to help keep your business ahead of the threat. Behavioral fingerprinting, for example, helps enhance protection levels and reduce overall risk.

Proventia Network ADS also augments IPS protection with an Active Threat Feed (ATF) service that provides a constantly updated list of Internet security threats based on behavior and algorithms, not just signatures. Behavioral fingerprint updates are conducted hourly to help keep the ADS system up to date with the latest changes. By combining ATF content with vulnerability updates from the IBM Internet Security Systems X-Force® research and development team, Proventia Network ADS can help Proventia Network IPS discover and block threats regardless of where they originate.

When unknown or unauthorized assets connect to the network, Proventia Network ADS can detect the network flows and immediately alert SiteProtector, which automatically triggers frequent scans of assets as the ADS finds them. Businesses that are also using Proventia Network Enterprise Scanner for vulnerability management can quickly scan the unknown asset and report any vulnerabilities requiring further action.

Proventia Management SiteProtector is designed to streamline management of a multilayered protection platform through centralized command and control. Proventia Network ADS integrates with SiteProtector for analysis and reporting, event management and access to workflow capabilities. As events or risks are detected, your IT team can automate and track the actions taken to protect against threats.

**Getting the most out of your existing IPS solutions**

Proventia Network ADS is designed for quick deployment with virtually no network impact and no need to reconfigure or redesign your network. Once
deployed, the solution can provide additional protection and network traffic data as Proventia Network ADS monitors network flow data, such as that provided by Cisco NetFlow, and network activity. Network intelligence generated by Proventia Network ADS can help maximize the value of existing IPS solutions by helping to improve IPS performance, identify the best position for IPS systems based on traffic flow and verify IPS findings and activity.

Identifying the volume and types of traffic moving across the network can help you tune an IPS for faster performance without increasing risk. Based on network intelligence, you can adjust and tune the number and types of checks performed on specific network segments or assets. Proventia Network ADS can also provide the intelligence needed to help harden the network against unauthorized applications and services, potentially reducing risk even further.

With increased knowledge of network traffic flow, your security teams can better determine how to position IPS systems for the most cost-effective and secure implementation. For areas of the network that may not warrant an IPS, Proventia Network ADS can help track and report unusual network activity and use behavioral risk analysis to help identify potential threats.

Proventia Network ADS provides network intelligence and activity data designed to enhance your security team’s ability to protect against new threats and verify certain IPS findings.

**Why IBM?**
Preemptive security requires industry-leading research, a keen eye for attack trends and techniques, and a streamlined and affordable platform for delivering advanced security solutions that are knowledge based. IBM Internet Security Systems commands the extensive knowledge, innovative research methods and complex technologies required to achieve preemptive security. Our experienced and certified consultants, architects, project managers and subject matter experts are prepared to provide your organization with a comprehensive platform of preemptive security products and services designed to protect your entire IT infrastructure, from the network gateway to the desktop.

**For more information**
To learn more about IBM Proventia Network ADS, contact your IBM representative or IBM Business Partner, or visit:

[ibm.com/services/us/iss](http://ibm.com/services/us/iss)