



IBM Proventia Network Anomaly Detection System

Enhanced network intelligence and security for enterprise networks

IBM Proventia® Network Anomaly Detection System (Proventia Network ADS) is a network behavior analysis system that enhances network intelligence and security by collecting and auditing network flow data from existing infrastructure devices. Proventia Network ADS complements

and expands upon protection from your existing intrusion prevention system (IPS) to help gain security and compliance advantages, such as:

- Greater network visibility—enhancing compliance and overall security posture using behavior analysis
- Multilayered protection available from IBM Internet Security Systems (ISS)
- Optimized intrusion prevention and the ability to help stop evolving and internal threats

Features and benefits

- **Custom policies**—monitor and enforce network-usage policies for compliance, vulnerability management and abuse of network resources
- **Router and interface visibility**—provides real-time and historic visibility into traffic that traverses routers and interfaces; allows for full visibility into the hosts, services and connections making up the majority of the traffic
- **Risk index**—identifies hosts causing great risk on the network, and analyzes risk by individual users as well by Internet Protocol (IP) addresses
- **Identity-tracking extensions**—view, search and export historical identity mappings to track a user's movement throughout the network
- **Enhanced active threat feeds (ATF)**—keep ATF fingerprints up-to-date and attain new fingerprints without direct Internet connections
- **Platform integration**—works within the IBM Proventia Protection Platform and integrates with IBM Proventia Management SiteProtector to complement intrusion prevention and vulnerability management.

Insider threat detection	
Threat detection	Immediate
Devices tracked	Over 100,000
Groups supported	Hundreds
Network malware detection	Yes
Management software	Use IBM Proventia Management SiteProtector™ centralized management system 2.0, Service Pack 5 or higher
Relational detection	Yes
Statistical detection	Yes
Scan detection	Slow, fast, port, IP sweep, stealth
Stepping-stone detection	Yes
Distributed denial-of-service (DDoS)/ Denial-of-service (DoS) detection	Yes
Protocol blacklist	Yes
Correlate alerts	Yes

Insider threat detection	
Alert management	
Simple Network Management Protocol (SNMP)	Yes (custom management information base [MIB])
Extensible Markup Language (XML)	Yes
Simple Mail Transfer Protocol (SMTP)	Yes
Syslog	Yes
Security Event Management (SEM) support	Yes
Alert feedback	Allow/deny/dismiss
Alert forensics	Searchable flow log

Insider threat detection	
Deployability	
Supports multiple flow types	
NetFlow v5	Yes
NetFlow v7	Optimized for Catalyst 6500
NetFlow v9	Yes
sFlow v2	Yes
sFlow v4	Yes
sFlow v5	Yes
Gigabit packet capture	Yes
Juniper cflowd	Yes
Asymmetric routing	Yes
De-duplicate flows	Yes
Ephemeral ports	Yes
Automatic discovery	Yes
In-house applications	
Domain name system (DNS) support	Yes

Insider threat detection	
Active threat feed	
Behavioral fingerprints	Yes
Delivery	RSS feed
Automatic inclusion	Yes (configurable)
Client required	No
Deployability	Supports multiple flow types

Insider threat detection	
Centralized management via IBM Proventia Management SiteProtector™ system	
Event monitoring	Yes
Device health monitoring	Yes
Centralized updates	Yes
Centralized reporting	Yes

Insider threat detection	
Network worm defense	
Postoutbreak quarantine	On demand
Preoutbreak vaccination	On demand
Preadvisory hardening	On demand
Malware defense safeguard	Automated whitelist generation
Zero-day worm detection	Yes
Infected host discovery	Yes

Insider threat detection	
Interoperability	
Scrub intrusion detection system (IDS) alerts	Yes
Tune IDS	Yes
Suggest firewall rules	Yes
Suggest switch access control lists (ACLs)	Yes
Quarantine using firewall	Yes
Scan for unused services	Yes
SiteProtector	Yes
Device management	
Multiple users	Yes
Web user interface	HTTPS
Command line interface (CLI)	Secure Shell (SSH) v2, Serial
Communication channels	Secure Sockets Layer (SSL)
Operating system (OS)	Hardened Linux®

World-class support	
Technical support	
Hours available – standard	24x7x365
Hours available – premium	24x7x365
Number of support incidents	Unlimited
Number of designated callers	From two to five
Additional designated callers	Optional
Additional languages	Optional
Customer portal	Yes
Customer knowledgebase	Yes
Warranty	One year + contract
Advanced hardware replacement	Yes
Correlate alerts	Yes

World-class support	
Ports	
Collector (AD3000, AD3007, AD3014, AD3020):	
• Copper Gigabit Ethernet	
• Fast Ethernet management port	
• Serial console port	
Analyzer (AD5003):	
• Copper Gigabit Ethernet	
• Fast Ethernet management port	
• Serial console port	

World-class support	
Device security	
Hardened OS and network stack, fully encrypted communications channels	
Built-in firewalling support, rejecting packets by default (transparent to pings and port scans)	

System specifications					
Model	AD5003	AD300	AD3007	AD3014	AD3020
Purpose	Analyzer	Packet collector	Flow/packet collector	Flow/packet collector	Flow/packet collector
Performance characteristics					
Flow sources	3/7*	0	7	14	20+
Maximum packet capture throughput	200 Mbps	1,000 Mbps	1,000 Mbps	1,000 Mbps	1,000 Mbps
Packet capture interfaces	1	4	4	2**	4
Management/flow interfaces	1	2**	2**		2**
Form factor	2-RU	1-RU	1-RU	1-RU	1-RU
Dimensions					
Height (in/cm)	3.45/8.75	1.7/4.3	1.7/4.3	1.7/4.3	1.7/4.3
Width (in/cm)	16.93/43.0	16.93/43.0	16.93/43.0	16.93/43.0	16.93/43.0
Depth (in/cm)	26.46/67.2	26.46/67.2	26.46/67.2	26.46/67.2	26.46/67.2
Weight (lb/kg)	70/31.8	37/16.8	37/16.8	37/16.8	37/16.8
Lockable front bezel	Yes	Yes	Yes	Yes	Yes
Redundant power supplies	Yes	No	No	No	No
Redundant storage	Yes (onboard RAID)	No	No	No	No
Power dissipation					
Units	AC	AC	AC	AC	AC
Amps	8.9/5.4	6.5/3.2	6.5/3.2	6.5/3.2	6.5/3.2
Hertz (H)	50/60	50/60	50/60	50/60	50/60
Input range (V)	100–127/200–240	100–127/200–240	100–127/200–240	100–127/200–240	100–127/200–240
Operating temperature	+50°F–+95°F (+10°C–+35°C)	+50°F–+95°F (+10°C–+35°C)	+50°F–+95°F (+10°C–+35°C)	+50°F–+95°F (+10°C–+35°C)	+50°F– +95°F (+10°C–+35°C)
Non-operating temperature	-40°F–158°F (-40°C–+70°C)	(-40°C–+70°C) -40°F–158°F	-40°F–158°F (-40°C–+70°C)	(-40°C–+70°C) -40°F–158°F	-40°F–158°F (-40°C–+70°C)
Relative humidity (non-operating)	95 percent @ 30°C (90°F)	95 percent @ 30°C (90°F)	95 percent @ 30°C (90°F)	95 percent @ 30°C (90°F)	95 percent @ 30°C (90°F)
Emissions	FCC Class A	FCC Class A	FCC Class A	FCC Class A	FCC Class A

* In a stand-alone deployment, the AD5003 accepts network flows from up to three flow sources and raw packet data. In a deployment that includes an analyzer and one or more collector appliances, the AD5003 accepts consolidated flow feeds from up to seven collector appliances.

** Supports an interface for flow collection separate from the management interface.

Proventia Network Anomaly Detection System model numbers

- Proventia AD5003 AD5003-1-P
- Proventia AD3000 AD3000-1-P
- Proventia AD3007 AD3007-1-P
- Proventia AD3014 AD3014-1-P
- Proventia AD3020 AD3020-1-P

For more information

Learn how the IBM Proventia Network Anomaly Detection System can protect your business ahead of the threat and help to simplify your security management. To evaluate the Proventia Network Anomaly Detection System today, call 1 800 776-2362, e-mail sales@iss.net, or 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 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.

Linux is a registered trademark of Linus Torvalds 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.

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.

* U.S. Patent No. 7,093,239