


	 IBM Proventia® Network Anomaly Detection System	 IBM Proventia® Network Intrusion Prevention System					 IBM Proventia® Network Multi-Function Security				 IBM Proventia® Network Enterprise Scanner and IBM Internet Scanner Software			 IBM Proventia® Network Mail Security System		 IBM Proventia® Server Intrusion Prevention System IBM RealSecure® Server Sensor IBM Proventia® Desktop Endpoint Security		
IBM ADVANTAGE	Provides a clear view of network behavior while detecting active security threats, risky user behavior, policy violations and performance issues.	Uses IBM Internet Security Systems <i>Ahead of the threat</i> technology to block intrusion attempts, DoS attacks, malicious code transmission, backdoor activity and hybrid network-based threats.					Provides a complete, all-in-one solution for even the most complex networks. Unified on a robust firewall/VPN platform complete with antivirus, antispam, Web filtering and robust intrusion prevention, the appliance stops viruses, worms, hackers, spam and unwanted Web content.				Offers vulnerability protection and helps quantify and reduce overall risk to all network components. Appliance or software solutions identify where risk exists, prioritize and assign protection, and report results.			Preemptive protection and spam control for your messaging infrastructure.		Combines multi-layered technologies to protect desktops and servers from the growing threat spectrum while enabling them to keep data and applications reliable, available and confidential. No single type of protection acting alone is enough to stop today's threats. Multifaceted threats require multiple layers of protection.		
MODEL	Proventia AD5 and AD3	IBM Proventia GX3002	IBM Proventia GX4 series	IBM Proventia GX5 series	IBM Proventia GX6116	IBM Proventia IPS for Crossbeam	IBM Proventia MX1004	IBM Proventia MX3006	IBM Proventia MX5010	IBM Proventia MX5010A (Build to Order Only)	IBM Proventia Network Enterprise Scanner 750	IBM Proventia Network Enterprise Scanner 1500	IBM Internet Scanner	IBM Proventia Network Mail Security System - MS1002-VM	IBM Proventia Network Mail Security System - MS3004	IBM Proventia Desktop	IBM RealSecure Server Sensor	IBM Proventia Server
TYPICAL DEPLOYMENT	Internal Network	Remote Segments	Remote Segments/ Network Perimeter	Network Perimeter/ Network Core	Enterprise Core/High-Speed Perimeter connections Carrier Infrastructure	Carrier Infrastructure Enterprise Core/High-Speed Perimeter connections	SMB/Remote Offices	SMB/Remote Offices/ Medium Gateway	SMB/Large/Medium Gateway	SMB/Large/Medium Gateway	Network core/perimeter scanning; external-to-network scanning	Network core/perimeter scanning; external-to-network scanning	Enterprise/SMB; Auditing environments	Messaging Gateway	Network perimeter	Workstations/Laptops	Servers	Servers
MANAGEMENT OPTIONS	SiteProtector, local	SiteProtector, Local, LCD	SiteProtector, Local, LCD	SiteProtector, Local, LCD	SiteProtector, Local, LCD	SiteProtector	SiteProtector, Local	SiteProtector, Local	SiteProtector, Local	SiteProtector, Local	SiteProtector, Local	SiteProtector, Local	SiteProtector, Local	SiteProtector, Local	SiteProtector, Local	SiteProtector	SiteProtector	SiteProtector
MAXIMUM RECOMMENDED NODES/USERS	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	100*	500*	2,500*	2,500*	3,000 per appliance	10,000 per appliance	Unlimited	< 1,000 – Scales to hardware	10,000	Client-based license	Client-based license***	Client-based license
SECURITY CONTENT UPDATES	Active Threat Feed (Powered by X-Force®)	Powered by X-Force	Powered by X-Force	Powered by X-Force	Powered by X-Force	Powered by X-Force	Powered by X-Force; signature antivirus by Sophos	Powered by X-Force; signature antivirus by Sophos	Powered by X-Force; signature antivirus by Sophos	Powered by X-Force; signature antivirus by Sophos	Powered by X-Force	Powered by X-Force	Powered by X-Force	Powered by X-Force; signature antivirus by Sophos	Powered by X-Force; signature antivirus by Sophos	Powered by X-Force; signature antivirus by BitDefender	Powered by X-Force	Powered by X-Force
FORM FACTOR	2U, Collectors -1U	Desktop	1U appliance	2U appliance	2U appliance	Crossbeam X40, X45, X80	Desktop appliance	1U appliance	2U appliance	2U appliance	Desktop	1U appliance	Software	Virtual appliance	2U appliance	Software	Software	Software
CAPABILITIES SUMMARY																		
Intrusion Prevention	Identify zero-day & known worms; block with ACLs	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Scan and block when used with IPS solutions	Scan and block when used with IPS solutions	No	Yes	Yes	Yes	Yes	Yes
Intrusion Detection	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No	Yes	Yes	Yes	Yes	Yes
Antivirus (behavior-based)	Yes	No	No	No	No	No	Yes	Yes	Yes	Yes	No	No	No	Yes	Yes	Yes	Yes	Yes
Antivirus (signature-based)	No	No	No	No	No	No	Yes	Yes	Yes	Yes	No	No	No	Yes	Yes	No	No	No
Content Filtering	No	No	No	No	No	No	Yes	Yes	Yes	Yes	No	No	No	Yes	Yes	No	No	No
Antispam	No	No	No	No	No	No	Yes	Yes	Yes	Yes	No	No	No	Yes	Yes	No	n/a	n/a
VoIP Security	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No	Yes	Yes	Yes
Spyware Prevention	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No	Yes	Yes	Yes	Yes	Yes
VPN	No	No	No	No	No	No	Yes	Yes	Yes	Yes	No	No	No	No	No	No	n/a	n/a
HARDWARE-RELATED SPECIFICATIONS																		
Monitoring or scanning interfaces	n/a	2 x 10/100/1000 Copper	2 or 4 x 10/100/1000 Copper	8 x 10/100/1000 Copper or 4 x 10/100/1000 Copper and 4 x 10/100/1000 SFP (TX/SX/LX) 8 x SFP/mini-GBIC ports (1,000 TX/SX/LX)	16 X 1000 SFP (TX/SX/LX)	8 X 10/100/1000 SFP (TX/SX/LX) per NPM	4 x 10/100/1000 Copper	6 x 10/100/1000 Copper	10 x 10/100/1000 Copper	10 x 10/100/1000 Copper	1	5	Hardware dependent	Two interfaces	4 x 10/100/1000 Copper	n/a	n/a	n/a
Inline protected segments	n/a	1	1 or 2	4	8	4 per NPM	4	6	10	10	n/a	n/a	n/a	Unlimited MX records	Unlimited MX records (10,000 users)	n/a	n/a	n/a
Throughput available	40,000 netflows per second	10 Mbps	200 Mbps	400 Mbps - 1.2 Gbps	Up to 15 Gbps 6 Gbps inspected	Up to 3 Gbps per NPM	100 Mbps**	200 Mbps**	1600 Mbps**	1600 Mbps**	250 assets/hour	800 assets/hour	Hardware dependent	Scales to hardware	36,000 messages/hr	n/a	n/a	n/a
Concurrent sessions (rated maximum)	n/a	200,000	1,200,000	1,200,000 - 1,450,000	4,600,000	Varies by installation*****	100,000	120,000	150,000	150,000	n/a	n/a	n/a	1024 (default setting)	1024 (default setting)	n/a	n/a	n/a
Maximum connection per second	n/a	3,750	21,000	35,000 - 40,000	160,000	Varies by installation*****	2,125	4,100	12,500	12,500	n/a	n/a	n/a	Scales to hardware	10 messages/sec****	n/a	n/a	n/a
High Availability/Failover	Yes	Not Available	Not Available	Active/Active Active/Passive	Active/Active Active/Passive	Active/Active Active/Passive	Active/Passive	Active/Passive	Active/Passive	Active/Passive	Available	Available	No	Not available	Available	n/a	n/a	n/a
HOST PROTECTION FEATURES																		
Log Auditing	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	No	Yes	No
Application Control	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	Yes	No	Yes
Buffer Overflow Exploit Protection	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	No	n/a	n/a	n/a	n/a	Yes	Yes	Yes
Supported Operating Systems/Platforms	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	Windows	Windows, HP-UX, Solaris, AIX, VMware	Windows, Linux, VMware
VULNERABILITY MANAGEMENT FEATURES																		
Scanning Discovery	Yes	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	Yes	Yes	Yes	n/a	n/a	n/a	n/a	n/a
Asset Classification	Yes	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	Yes	Yes	No	n/a	n/a	n/a	n/a	n/a
Vulnerability Assessment	No	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	Yes	Yes	Yes	n/a	n/a	n/a	n/a	n/a
Scanning Windows Workflow Solution	No	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	Yes	Yes	No	n/a	n/a	n/a	n/a	n/a
Results Reporting	Yes	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	Yes	Yes	Limited	n/a	n/a	n/a	n/a	n/a
MAIL SECURITY FEATURES																		
Spam detection rate	n/a	n/a	n/a	n/a	n/a	n/a	>98%	>98%	>98%	>98%	n/a	n/a	n/a	>98%	>98%	n/a	n/a	n/a
False positive rate	n/a	n/a	n/a	n/a	n/a	n/a	< .01% (1 in 10,000)	< .01% (1 in 10,000)	< .01% (1 in 10,000)	< .01% (1 in 10,000)	n/a	n/a	n/a	< .01% (1 in 10,000)	< .01% (1 in 10,000)	n/a	n/a	n/a
Spam and compliance analysis modules	n/a	n/a	n/a	n/a	n/a	n/a	Yes (20+, customizable)	Yes (20+, customizable)	Yes (20+, customizable)	Yes (20+, customizable)	n/a	n/a	n/a	Yes (20+, customizable)	Yes (20+, customizable)	n/a	n/a	n/a
Anti-phishing/ Image-based Spam	n/a	n/a	n/a	n/a	n/a	n/a	Yes	Yes	Yes	Yes	n/a	n/a	n/a	Yes	Yes	n/a	n/a	n/a
Granular policy control	n/a	n/a	n/a	n/a	n/a	n/a	Yes	Yes	Yes	Yes	n/a	n/a	n/a	Yes	Yes	n/a	n/a	n/a
Global/group/user settings	n/a	n/a	n/a	n/a	n/a	n/a	Yes	Yes	Yes	Yes	n/a	n/a	n/a	Yes	Yes	n/a	n/a	n/a
End user access	n/a	n/a	n/a	n/a	n/a	n/a	Yes	Yes	Yes	Yes	n/a	n/a	n/a	Yes	Yes	n/a	n/a	n/a

* See sizing guide for detailed information regarding # of concurrent users and active device modules
 ** Requires optional external bypass unit for fiber interfaces

*** With option for additional antivirus/anti-spyware subscription
 ***** Based on real world message flow, containing messages of varying sizes including variants with attachments and/or images

***** Determined by the number of blades installed in each implementation

MANAGED SERVICE OFFERINGS

FEATURES	MANAGED PROTECTION SERVICES			MANAGED SECURITY SERVICES					SECURITY ENABLEMENT SERVICES			
	MPS Premium	MPS Select	MPS Standard	MFW Standard	MFW Select	MFW Premium	MIDS/MIPS Standard	MIDS/MIPS Select	Internal VMS	External VMS	SELM Standard	SELM Select
CUSTOMER EXPERIENCE												
Mobile and Web Virtual-SOC Portal Access	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
Comprehensive Online Reporting	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
Customizable Reporting	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
Trending	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
Online SLA Compliance Reporting	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
Full-featured Online Ticketing System	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
Online Workflow and Tools	Incident Tracking, Incident Investigation, Vulnerability Remediation	Incident Tracking, Incident Investigation, Vulnerability Remediation	Incident Tracking, Incident Investigation, Vulnerability Remediation	Incident Tracking, Incident Investigation, Vulnerability Remediation	Incident Tracking, Incident Investigation, Vulnerability Remediation	Incident Tracking, Incident Investigation, Vulnerability Remediation	Incident Tracking, Incident Investigation, Vulnerability Remediation	Incident Tracking, Incident Investigation, Vulnerability Remediation	Vulnerability Remediation	Vulnerability Remediation	Incident Tracking, Incident Investigation, Vulnerability Remediation	Incident Tracking, Incident Investigation, Vulnerability Remediation
XFTAS Security Intelligence	Premium	Premium	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
MPS Workshop	YES	Optional	Optional	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
DEVICE MANAGEMENT												
Health and Availability Monitoring	YES	YES	YES	YES	YES	YES	YES	YES	YES	N/A	Optional, for On-site Aggregator (OA) only	Optional, for On-site Aggregator (OA) only
System Upgrades: OS, Firmware	YES	YES	YES	YES	YES	YES	YES	YES	YES	N/A	Optional, for On-site Aggregator (OA) only	Optional, for On-site Aggregator (OA) only
Security Content Upgrades	YES	YES	YES	YES	YES	YES	YES	YES	YES	N/A	N/A	N/A
Policy and Configuration Changes Through the V-SOC Portal	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
High Availability Add-on	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional	N/A	N/A	N/A	N/A
Log or Data Storage	1 Year	1 Year	1 Year	1 Year	7 Years	7 Years	1 Year	7 Years	1 Year	1 Year	7 Years	7 Years
PROTECTION												
In-line Blocking	YES	YES	YES	N/A	N/A	N/A	Based on platform	Based on platform	N/A	N/A	NO	NO
Guaranteed XF-CAL Protection ¹	YES	YES	YES	N/A	N/A	N/A	NO	NO	N/A	N/A	N/A	N/A
Vulnerability Management Service												
Customer Premise Device Required	NO	NO	NO	NO	NO	NO	NO	NO	YES	NO	N/A	N/A
Complimentary Scans	YES ²	YES ²	YES ²	YES	YES	YES	YES	YES	N/A	N/A	NO	NO
X-Force Protection System (XPS) Automated Analysis	YES	YES	YES	NO	NO	NO	Based on platform	Based on platform	N/A	N/A	NO	YES
Real-time Human Analysis	YES	YES	NO	Optional	Optional	YES	NO	YES	N/A	N/A	NO	NO
Incident Escalation												
E-mail Escalation	Levels 2,3 Incidents	Levels 2,3 Incidents	NO	Optional	Optional	Levels 2,3 Incidents	YES	Levels 2,3 Incidents	N/A	N/A	NO	YES
Telephone Escalation	Level 1 Incidents	Level 1 Incidents	NO	Optional	Optional	Level 1 Incidents	NO	Level 1 Incidents	N/A	N/A	NO	NO
Virtual Private Networks (VPNs)												
Site-to-Site IPSEC Tunnels	N/A	N/A	N/A	YES	YES	YES	N/A	N/A	N/A	N/A	N/A	N/A
Client IPSEC Tunnels	N/A	N/A	N/A	YES	YES	YES	N/A	N/A	N/A	N/A	N/A	N/A
SSL Tunnels	N/A	N/A	N/A	YES	YES	YES	N/A	N/A	N/A	N/A	N/A	N/A
OTHER DETAILS												
Vendor Support	IBM Proventia Network G & M	IBM Proventia Network G, M & Server	IBM Proventia Network G, M, Server & Desktop	IBM ISS, Checkpoint, Cisco, Netscreen	IBM ISS, Checkpoint, Cisco, Netscreen	IBM ISS, Checkpoint, Cisco, Netscreen	IDS - IBM ISS, Cisco; IPS - IBM ISS, McAfee, TippingPoint	IDS - IBM ISS, Cisco; IPS - IBM ISS, McAfee, TippingPoint	IBM ISS	N/A	Any device supporting Syslog, SNMP, or the IBM ISS Universal Logging Agent (ULA)	Leading security products from IBM ISS, Cisco
Available to Partners	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
Pricing Per:	Segment	Device	Device	Device	Device	Device	Device	Device	IP	IP	Device	Device

1) The X-Force™ Certified Attack List is a list of the most serious, high-risk vulnerabilities and attacks, updated quarterly. Currently the list contains around a thousand attacks.
 2) Included with MPS for Networks only.

IBM Internet Security Systems
Ahead of the threat.™