


La protezione preventiva dalle minacce e intrusioni: le soluzioni di IBM Internet Security System

Davide Licciardello, CISSP

Davide.Licciardello@it.ibm.com

Technical Pre-Sales System Engineer



IBM Governance and Risk Management 
Maximize Value, Manage Risk

Agenda

- **Current Threats overview and X-Force value**
- **ISS ESP overview as a Service Oriented Security Architecture (SOSA)**
- **Siteprotector ESP Management solution**
- **Vulnerability Management (Network Scanners)**
- **Network Protection (IPS, IDS, ADS, UTM)**
- **Host and Desktop protection (PFW, AV, Anti-X, HIPS, HIDS)**
- **Content Protection (AS and WF)**
- **Services Overview (MSS, MPS, Compliance Gap-Analysis)**

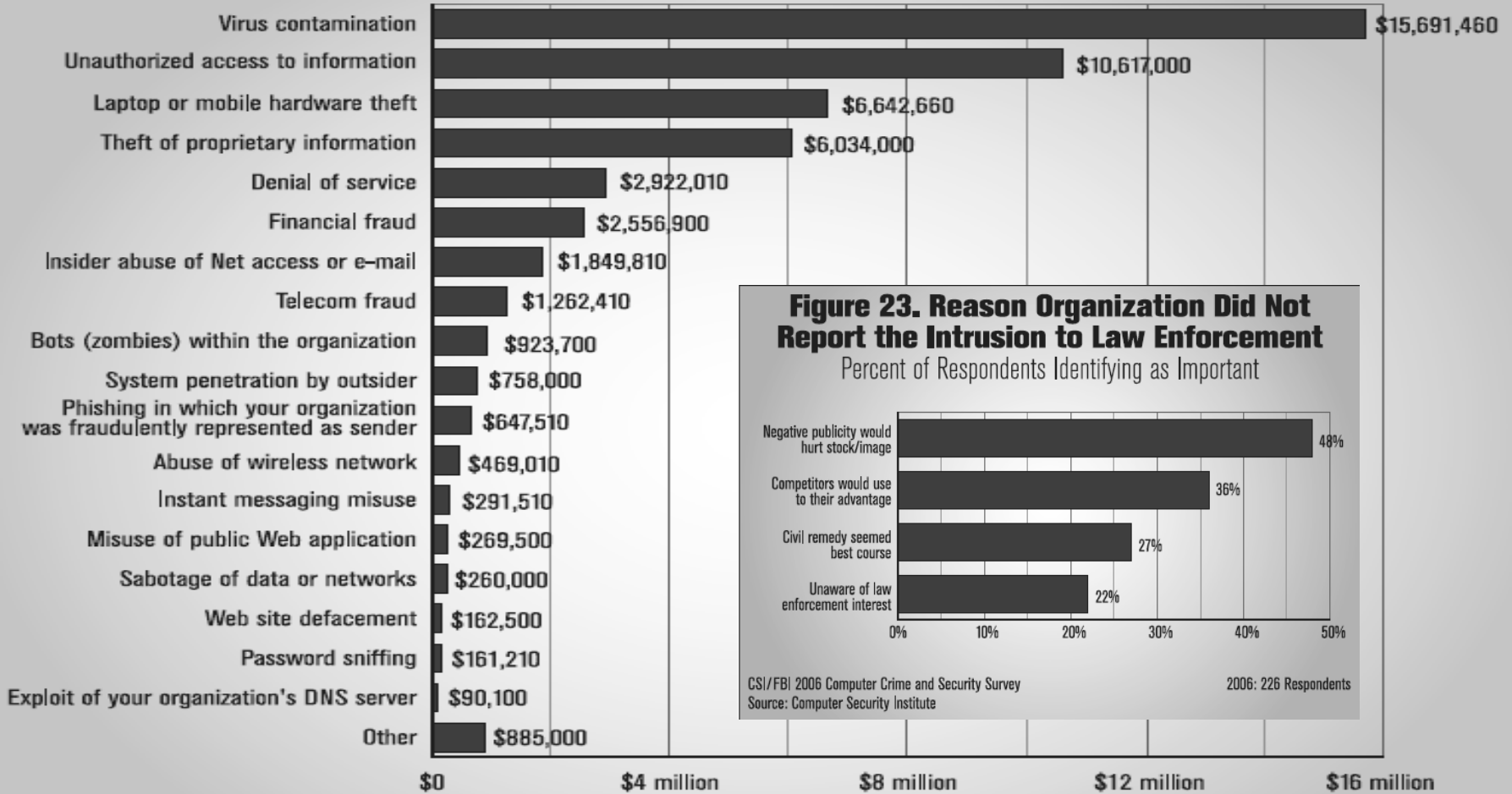
* What makes you special?

Current Threats overview and X-Force value



IBM Governance and Risk Management *
Maximize Value, Manage Risk

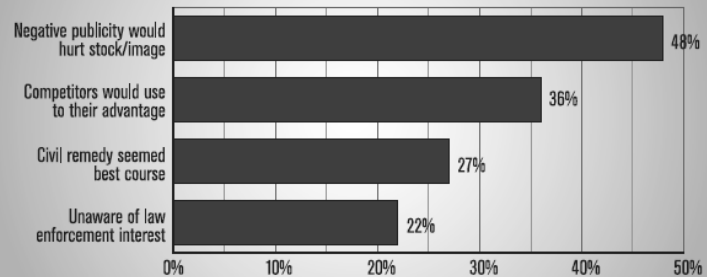
Figure 16. Dollar Amount Losses by Type



Total Losses for 2006 = \$52,494,290

Figure 23. Reason Organization Did Not Report the Intrusion to Law Enforcement

Percent of Respondents Identifying as Important



CSI/FBI 2006 Computer Crime and Security Survey
Source: Computer Security Institute

2006: 226 Respondents

The Changing Threat Landscape



The New Attack Trends...

- Shift from “Glory-Motivated-Vandals” to “Financially-Politically-Motivated-Cyber-Crime”
 - They are more organized and collaborative (They have a **Roadmap**)
- From the “Designer Worm” to the “Designer BOT/Trojan”
 - Patient ZERO *is* the only target, and this implies “Signature engines are no good because of the restricted sample base”
 - Monster.it, Government Web sites, Banks,...
- New emerging Vectors of Penetration and Infection
 - Content Level Vulnerabilities
 - Virtualization
- The BOT-Networks
 - “Computational Currency”
 - SPAM Relays
 - Spyware/Adware subscriptions
 - Distributed Denial of Service Attacks

...REQUIRES New Protection Trends

■ ...Evolving Technologies

- There are too many possible vectors. There is no one miracle technology to protect you from everything. All existing technologies have a space and purpose
 - Protocol Analysis
 - Buffer Overflow Exploitation Prevention
 - Shell Code Heuristic
 - Behavioural Virus Prevention System
 - ...more to come!!!

...REQUIRES New Protection Trends

■ ...Holistic Approach

- There is not one location where all technologies can be deployed in order to protect the entire environment.

Some simple examples:

- **Host Protection**

- Mobile Computers need to be protected locally.
- Javascripts can be analysed and identified once downloaded completely.

- **Server Protection**

- Encrypted traffic to servers can be inspected after decryption.
- Analysis of log files to monitor the activity on the server.

- **Network Protection**

- All clear text traffic inspected in one or more location to protected large IT infrastructures.
- Web Filtering to prevent access to compromised sites.
- Mail Filtering to prevent phishing attacks.
- Anomaly Detection to identify unsuspected traffic.

...REQUIRES Advanced Research

The mission of IBM Internet Security Systems' X-Force is to:

- **A 200 team of professionals focused on security**
- **Research and evaluate threat and protection issues**
- **Develop assessment and countermeasure technology**
- **Educate the media and user communities**



X-Force Advanced Research



* What makes you special?

ISS ESP overview as a Service Oriented Security Architecture (SOSA)



IBM Governance and Risk Management *
Maximize Value, Manage Risk

Preemptive Protection For The Entire Enterprise



proventia[®]management

SiteProtector™

Unified Enterprise Security Console for all products



Enterprise Protection Products
(Appliances and Agents)

proventia[®]network
Enterprise Scanner



All based upon the Proventia
Unified Protection Architecture (UPA)

proventia[®]network

Protection Appliances



Proventia Network MFS
M50, M30, M10

“All-in-One” Protection Appliance

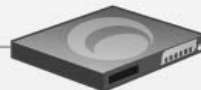
- IDS/IPS
- FW / VPN
- AntiVirus (signature & behavioral)
- AntiSpam
- Web Filter
- Spyware

proventia[®]network

Protection Appliances



Proventia ADS Series –
“Anomaly/Behavioral” Protection and
Network Visibility Appliances



Proventia Network IPS
Preemptive Security for Enterprise Networks
GX4002, GX4004, GX5008, GX5108
G400, G2000

proventia[®]server

Protection Agent



Proventia Server
“Multi-layered” Protection Agent
– Windows
– Linux
RealSecure Server Sensor
– Windows
– Solaris
– AIX
– HP-UX

proventia[®]desktop

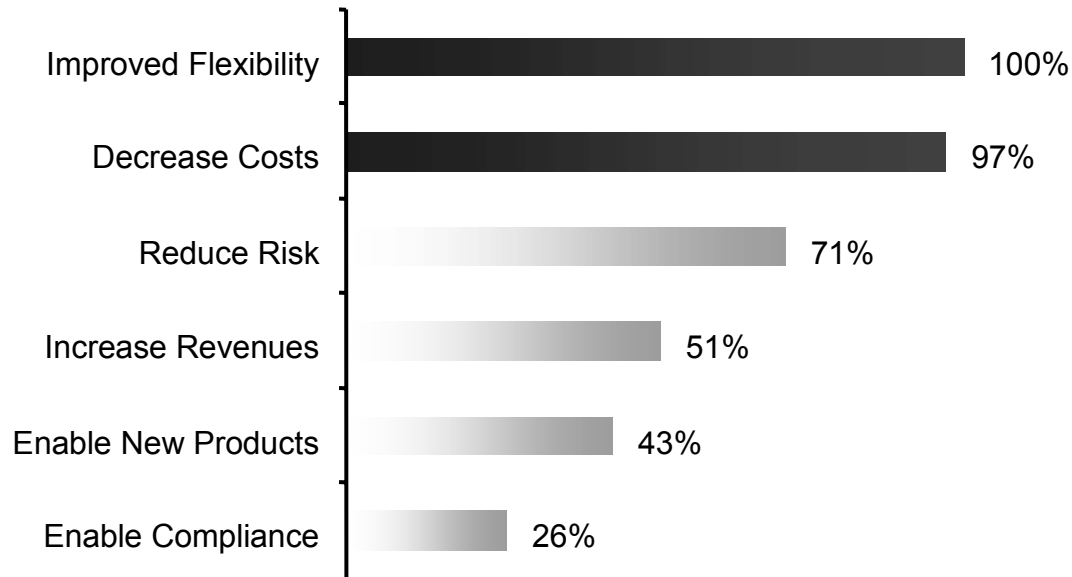
Protection Agent



Proventia Desktop
“All-in-One” Protection Agent
– Firewall
– Virus Prevention System
– Intrusion Protection
– VPN Enforcer
– Buffer Overflow Protection

Key Driver: Business Expansion and Security

Benefits resulting from SOSA Solutions



Source: IBM Institute of Business Value Study





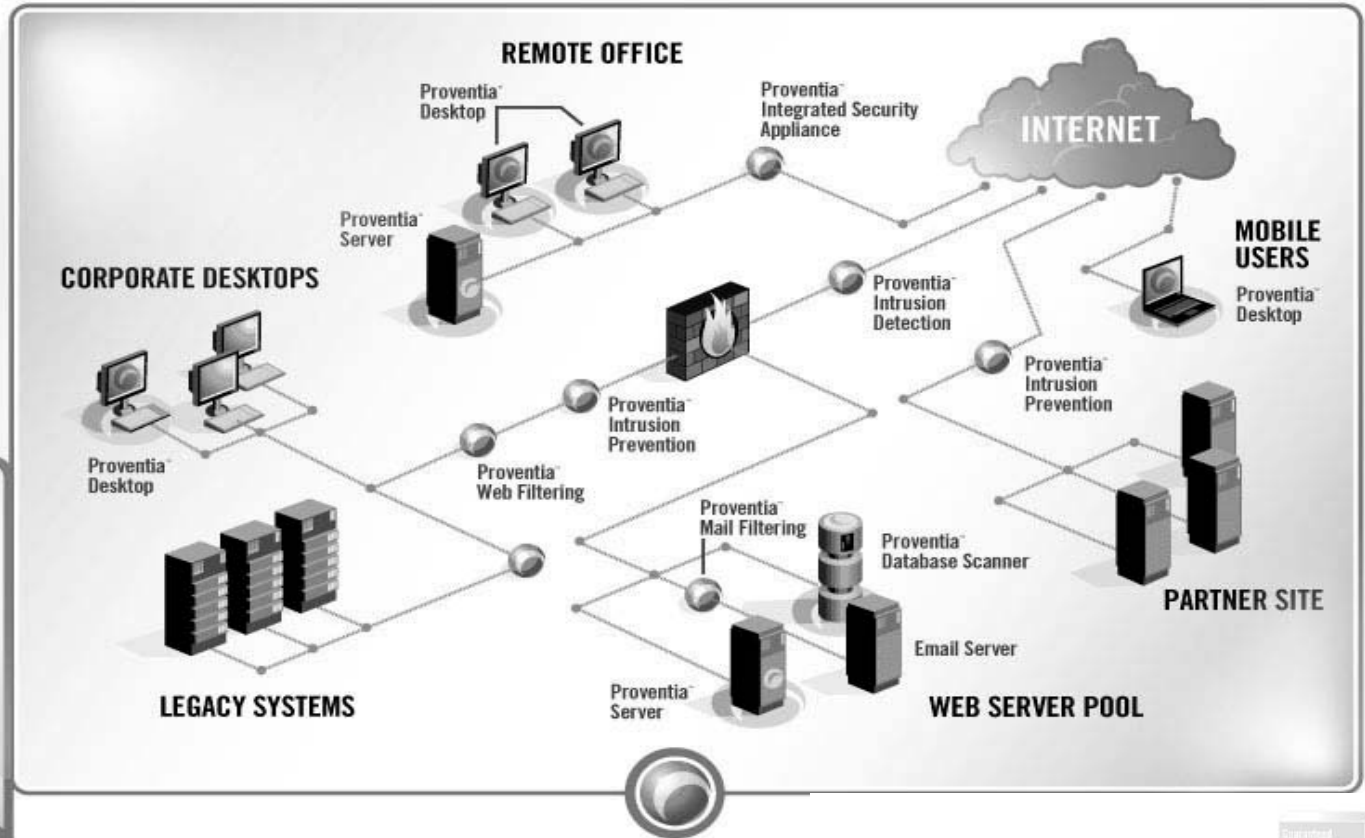
* What makes you special?

ESP Management solution: SiteProtector

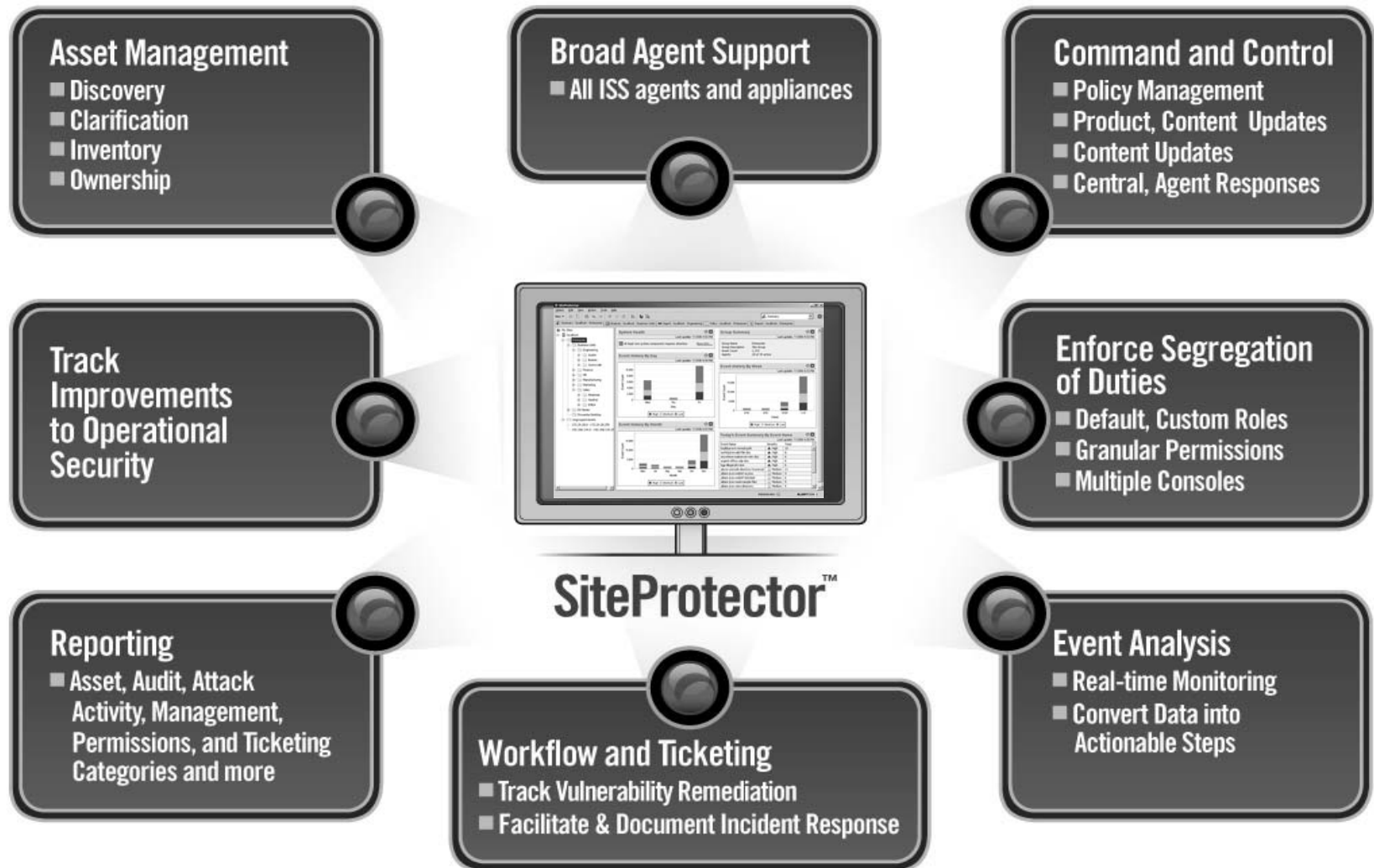


IBM Governance and Risk Management *
Maximize Value, Manage Risk

Siteprotector ESP Management



Families of Functionality



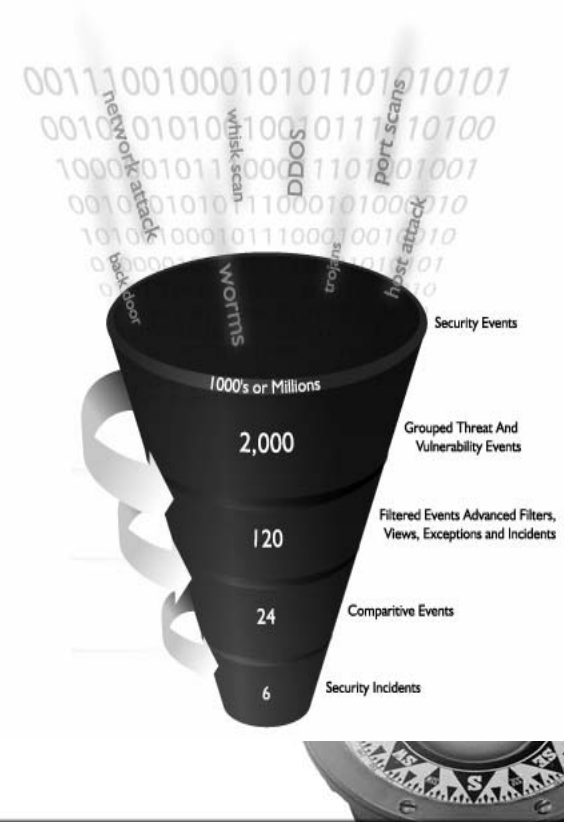
RealSecure Security Fusion 2.0

Impact Analysis

- **Answers the question, “Was the attack successful?”**
- **Correlates stored data about the target instantly**
- **Estimates the impact on the target**
- **Automatically responds**

Attack Pattern Analysis

- **Answers the question, “Are there patterns of attack activity that indicate malicious intent?”**
- **Instantly correlates incoming attacks across multiple security agents**
- **Automatically identifies important security incidents.**



SiteProtector

Object Edit View Action Tools Help

New [Icons]

Analysis

Summary : localhost : Atlantis | Analysis : localhost : Atlantis | Ticket | Reporting : localhost : Assesment | Ticketing : localhost : Atlantis | Policy | Asset : localhost : Business U

My Sites

- localhost
 - Atlantis
 - Business Units
 - Finance
 - Marketing
 - Ungrouped Assets
 - 172.16.0.0 - 172.16.255.255
 - 192.168.1.1 - 192.168.1.254

Time: Start 2005-08-26 00:00:00 EDT, End []

Source IP: Start [], End []

Target IP: Start [], End []

Event Analysis - Detail Time

Incidents/Exceptions

- Show Incidents
- Show Exceptions
- Show Attack Patterns
- Show Uncategorized

Tag Name [] Object Name []

Advanced...

Event Analysis - Detail Time (Agent Analysis)

Time	Tag Name	Status	Severity	Source IP	Target IP	Agent DNS Name
2005-08-26 09:14:27 EDT	decod-webfinger-attempt	Failed attack (blocked at host)	High	172.16.0.15	192.168.1.174	ATLWKS-0173
2005-08-26 09:15:33 EDT	bgp-route-unreachable	Failed attack (blocked at host)	High	172.16.0.8	192.168.2.209	ATLWKS-0464
2005-08-26 09:17:21 EDT	bgp-route-unreachable	Failed attack (blocked at host)	High	172.16.0.14	192.168.2.200	ATLWKS-0455
2005-08-26 09:25:32 EDT	iis-https-reveal-address	Failed attack (blocked at host)	High	172.16.0.10	192.168.3.206	ATLWKS-0717
2005-08-26 09:31:19 EDT	qotd-port-probe	Failed attack (blocked at host)	High	172.16.0.10	192.168.1.198	ATLWKS-0197
2005-08-26 09:41:47 EDT	decod-webfinger-attempt	Failed attack (blocked at host)	High	172.16.0.16	192.168.3.65	ATLWKS-0576
2005-08-26 09:53:21 EDT	qotd-port-probe	Failed attack (blocked at host)	High	172.16.0.6	192.168.3.171	ATLWKS-0682
2005-08-26 10:00:11 EDT	decod-webfinger-attempt	Failed attack (blocked at host)	High	172.16.0.12	192.168.3.90	ATLWKS-0601
2005-08-26 10:06:02 EDT	iis-https-reveal-address	Failed attack (blocked at host)	High	172.16.0.9	192.168.2.192	ATLWKS-0447
2005-08-26 10:06:19 EDT	iis-https-reveal-address	Failed attack (blocked at host)	High	172.16.0.7	192.168.4.144	ATLWKS-0911
2005-08-26 10:10:47 EDT	decod-webfinger	Failed attack (blocked at host)	High	172.16.0.10	192.168.2.53	ATLWKS-0308
2005-08-26 10:17:20 EDT	decod-webfinger	Failed attack (blocked at host)	High	172.16.0.15	192.168.2.200	ATLWKS-0455
2005-08-26 10:26:26 EDT	bgp-route-unre	Failed attack (blocked at host)	High	172.16.0.15	192.168.4.194	ATLWKS-0961
2005-08-26 10:30:19 EDT	decod-webfinger	Failed attack (blocked at host)	High	172.16.0.11	192.168.3.48	ATLWKS-0559
2005-08-26 10:32:18 EDT	bgp-route-unre	Failed attack (blocked at host)	High	172.16.0.1	192.168.1.15	ATLWKS-0014
2005-08-26 10:33:47 EDT	iis-https-reveal	Failed attack (blocked at host)	High	172.16.0.12	192.168.1.36	ATLWKS-0035
2005-08-26 10:35:48 EDT	decod-webfinger	Failed attack (blocked at host)	High	172.16.0.12	192.168.2.9	ATLWKS-0264
2005-08-26 10:36:14 EDT	decod-webfinger	Failed attack (blocked at host)	High	172.16.0.9	192.168.1.23	ATLWKS-0022
2005-08-26 10:39:16 EDT	qotd-port-probe	Failed attack (blocked at host)	High	172.16.0.9	192.168.1.18	ATLWKS-0017
2005-08-26 10:40:22 EDT	bgp-route-unre	Failed attack (blocked at host)	High	172.16.0.1	192.168.3.255	ATLWKS-0766
2005-08-26 10:42:19 EDT	iis-ftp-session-s	Failed attack (blocked at host)	High	172.16.0.4	192.168.1.24	ATLWKS-0023
2005-08-26 10:43:58 EDT	qotd-port-probe	Failed attack (blocked at host)	High	172.16.0.15	192.168.4.38	ATLWKS-0805
2005-08-26 10:46:22 EDT	qotd-port-probe	Failed attack (blocked at host)	High	172.16.0.11	192.168.4.35	ATLWKS-0802
2005-08-26 10:48:21 EDT	iis-https-reveal-address	Failed attack (blocked at host)	High	172.16.0.4	192.168.4.218	ATLWKS-0985
2005-08-26 11:20:30 EDT	iis-https-reveal-address	Failed attack (blocked at host)	High	172.16.0.5	192.168.1.2	ATLWKS-0001
2005-08-26 11:25:18 EDT	iis-ftp-session-status-dos	Failed attack (blocked at host)	High	172.16.0.15	192.168.1.179	ATLWKS-0178

52 rows with 11 selected.

Start | SiteProtector | https://localhost:3994/sit... | Untitled - Notepad | Computer Management | 6:42 PM

Select events or vulnerabilities for ticket creation

Copy

View Security Information...

Create Incident/Exception

Create new response rule...

Clear Events...

Restore Events...

Which agents detected these events?


What events were generated by these attackers?

What attacks came from these targets?

What attacks were against these targets?

New Ticket


Properties...

 What makes you special?

Vulnerability Management products:

**Proventia Enterprise Scanner
&
Internet Scanner**



IBM Governance and Risk Management 
Maximize Value, Manage Risk

2005

FROST & SULLIVAN

Market Leadership Award

Frost and Sullivan
Market Leadership Award



#1 Market Share
6 Consecutive Years

- Workflow and ticket management
- **Fully managed by SiteProtector to deliver an integrated vulnerability management solution**
- **Continuous scanning with scheduled scanning windows**
- **Definable roles and privileges**
- **Scalable Speed**
- **Extensible, scriptable content via EASL, and NASL**
- **Protects your corporate data by identifying where risk exists, prioritizing and assigning protection activities, and reporting on results.**
- Application Fingerprinting
- SSH Support



Proventia ES1500 Appliance



Workflow and Remediation - Prioritization

Vulnerability by Group

Agent : localhost

My Sites

- localhost
 - SP-ES1500
 - Accounting
 - Atlanta
 - Detroit
 - Engineering
 - Great Plains
 - SAP
 - Ungrouped Assets

sqa.qatest.iss.net

Tools Help

Forward Back Refresh Recursion Filters Help Summary

Group Summary

Last update: 10/11/04 5:16pm

Group Name: Atlanta
 Group Description: Atlanta Office
 Host Count: 2500
 Enterprise Scanner: 1 of 1 Active

Asset Watchlist

Last update: 10/08/04 2:16pm

Name	IP Address	Alert Status	Attacks
Drizzle	127.42.19.102		
Snarf	227.0.12.112		
DarkSide	227.0.12.113		
Betty's PC	109.207.14.127		

Site Protector Component Status

MANAGE Last update: 10/10/04 3:30pm

Component	Status	Upgrades	Last Contact
SP Database	Active	--	###:#####
SP Core	Active	--	###:#####
X-Press Updat...	Active	--	###:#####
Deployment M...	Online	Available	###:#####
Event Collecto...	Online	Available	###:#####
Enterprise Sca...	Active	--	###:#####
Enterprise Sca...	Offline	Available	###:#####

Open Tickets

Last update: 01/30/05 05:30

Ticket ID	Category	Owner	Priority	Status
DD596778	Vuln	Crane, Bob	▲ Critical	Open
DR782120	Vuln	Crane, Bob	▲ Critical	Open
PR78515x	Vuln	Sears, Beth	▲ High	Pending
TT389402	Vuln	Rouse, Stu	▲ High	Pending
TR798751	Vuln	Thomas, Raif	▼ Low	Open
TI994Axx	Vuln	Thomas, Raif	■ Med.	--

Available Updates

UPDATES Last update: 10/11/04 5:16pm

XPU 73.12	Enterprise Scanner
SP 4.4.0	SiteProtector
SP 4.4.1	SiteProtector
...	...

Assessment Scans

Last update: 01/30/05 05:30

Atlanta

1051 Hosts scanned

1 of 8 hours remaining

Asset Discovery Status

EDIT POLICY Last update: 01/30/05 05:30

Scan Range: 172.34.213.0 - 172.34.214.0

New IPs identified: 113

45% of range scanned

11% - Est. % of range not scanned

Vulnerability History

Last update: 01/30/05 05:30

High ▲ Med. ■ Low ▼

Month	Count
May	100
Jun	94
Jul	82
Aug	74
Sept	66
Oct	57
Nov	48
Dec	56
Jan	53
Feb	7

Time

Start

End

Source IP

Start

End

Target IP

Start

End

Tag Name

Object Name

Vuln Analysis - Detail (Target)

Tag Name	Severity ▲	Status	Target IP	Agent DNS Name	Object Type
allaire-jrun-view-directory	▲ High	✘ Vulnerable	172.16.34.50	DemoSP2	No Object
amd-pid	▲ High	✘ Vulnerable	172.16.34.50	DemoSP2	No Object
amd-pid	▲ High	✘ Vulnerable	172.16.34.50	DemoSP2	No Object
backdoor-bugs	▲ High	✘ Vulnerable	172.16.34.50	DemoSP2	No Object
badtrans-worm	▲ High	✘ Vulnerable	172.16.34.50	DemoSP2	No Object
biztalk-http-receiver-bo	▲ High	✘ Vulnerable	172.16.34.50	DemoSP2	No Object
cisco-ios-bgp-packetdos	▲ High	✘ Vulnerable	172.16.34.50	DemoSP2	No Object
coldfusion-mx-file-disclosure	▲ High	✘ Vulnerable	172.16.34.50	DemoSP2	No Object
coldfusion-sourcewindow	▲ High	✘ Vulnerable	172.16.34.50	DemoSP2	No Object
cups-udp-dos	▲ High	✘ Vulnerable	172.16.34.50	DemoSP2	No Object
denial-of-service	▲ High	✘ Vulnerable	172.16.34.50	DemoSP2	No Object
denial-of-service	▲ High	✘ Vulnerable	172.16.34.50	DemoSP2	No Object

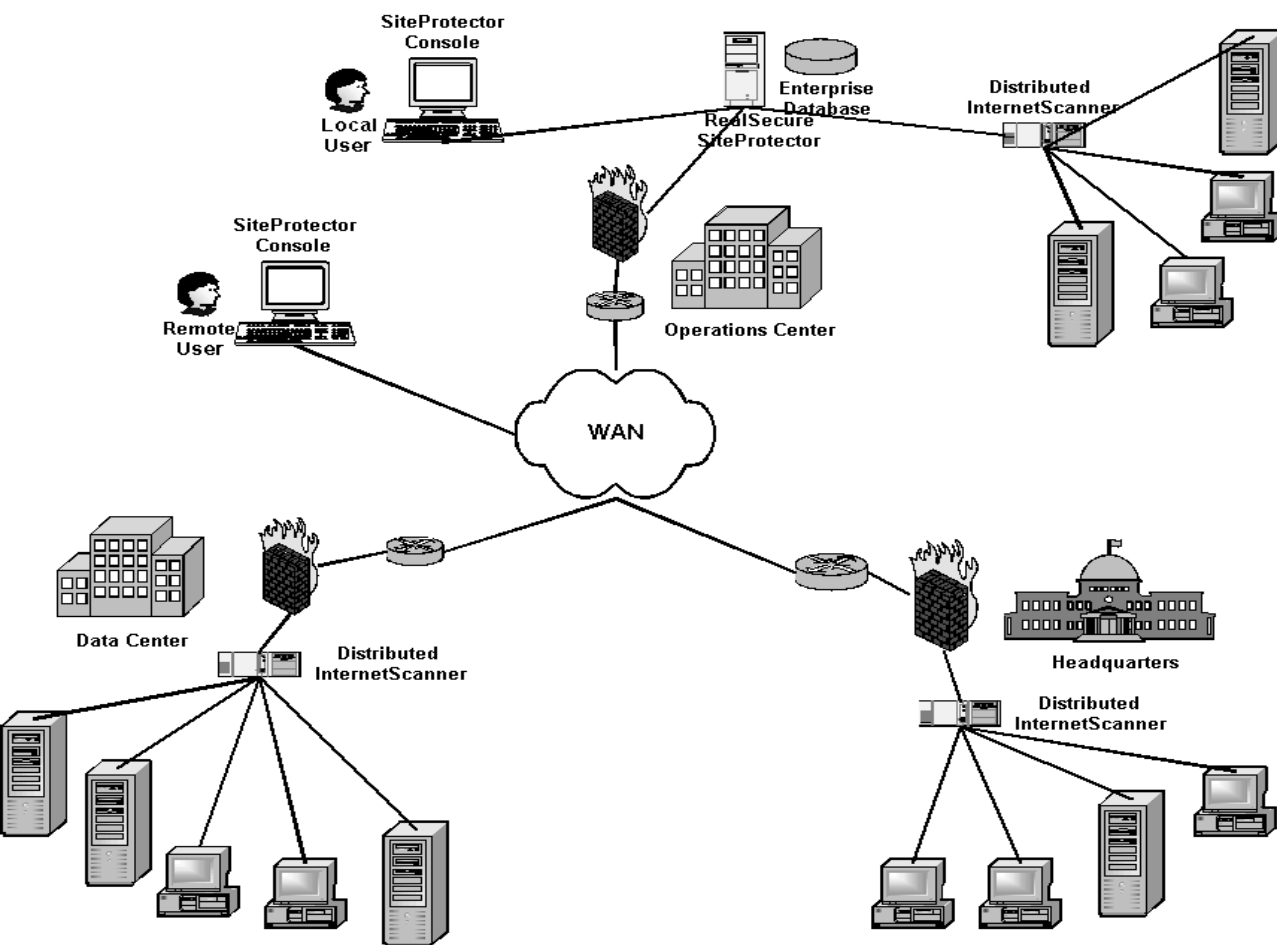
Tag Name

Object Name

Show Uncategorized

Vuln Analysis - Asset (Target)


Target IP	Target DNS Name	Status	# High ▼	# Medium ▼	# Low ▼	Tag Count	Object Count	Latest Event
172.16.34.50	ATL-Kaylor	✘ Vulnerable	1	1	0	1	1	2005-12-21 18:00:00 EST



Run scans and view data from multiple remote scanners, with or without local users.




- Dynamic Check Assignment
- Checks running concurrently
- Ability to not/limit scan on printers or unknowns
- Support for Windows NT 4.0, 2000 Pro, XP Pro SP1a, 2003 Server
- Pause scanning
- User defined nmap database entries

 What makes you special?

Network protection technology and products: Intrusion Prevention/Detection Systems (IPS/IDS)

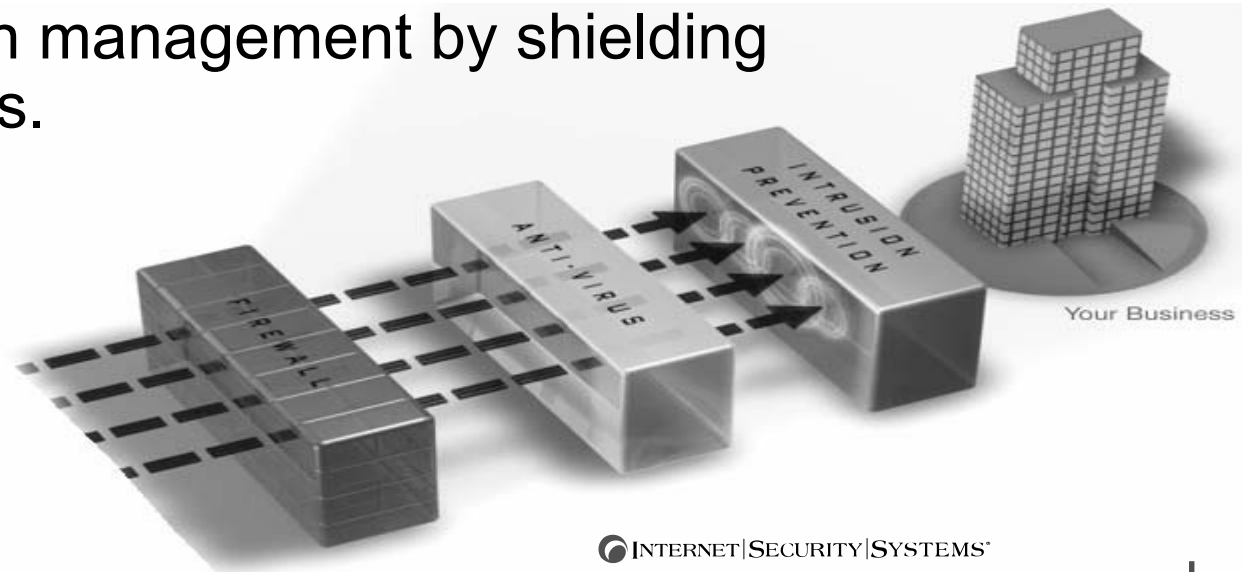


IBM Governance and Risk Management 
Maximize Value, Manage Risk

Network Protection: Proventia® G IPS

Intrusion Prevention Systems

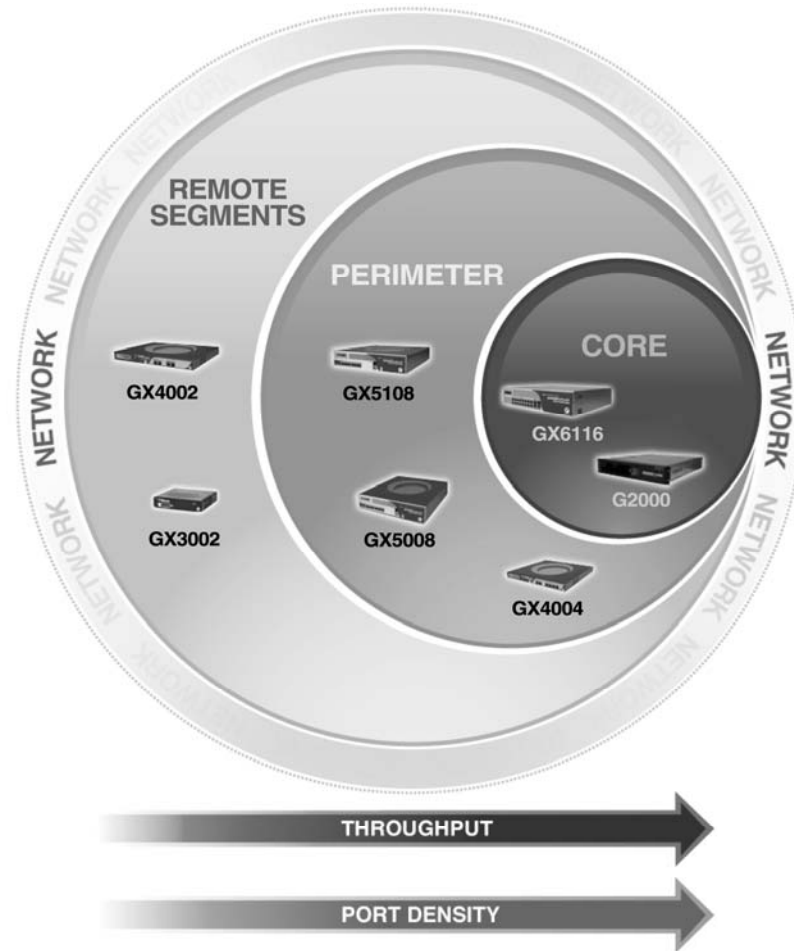
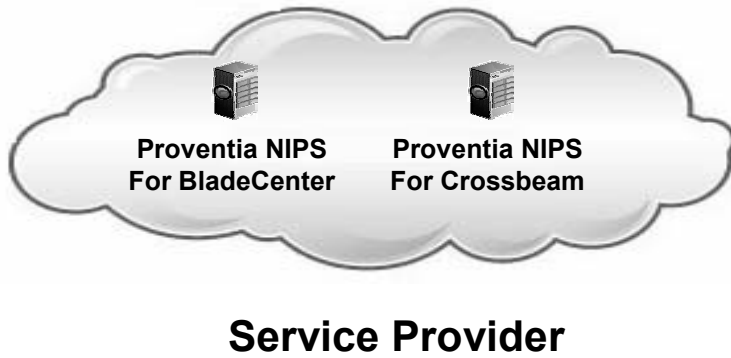
- V-Patch Block malicious and unwanted traffic other technologies cannot recognize.
 - Bots / Trojans / Worms / Spyware / P2P / IM / DoS
- Compliment patch management by shielding new vulnerabilities.



INTERNET|SECURITY|SYSTEMS™

proventia® network
Intrusion Prevention System

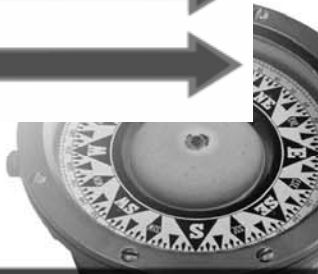
At Every Layer of Your Network



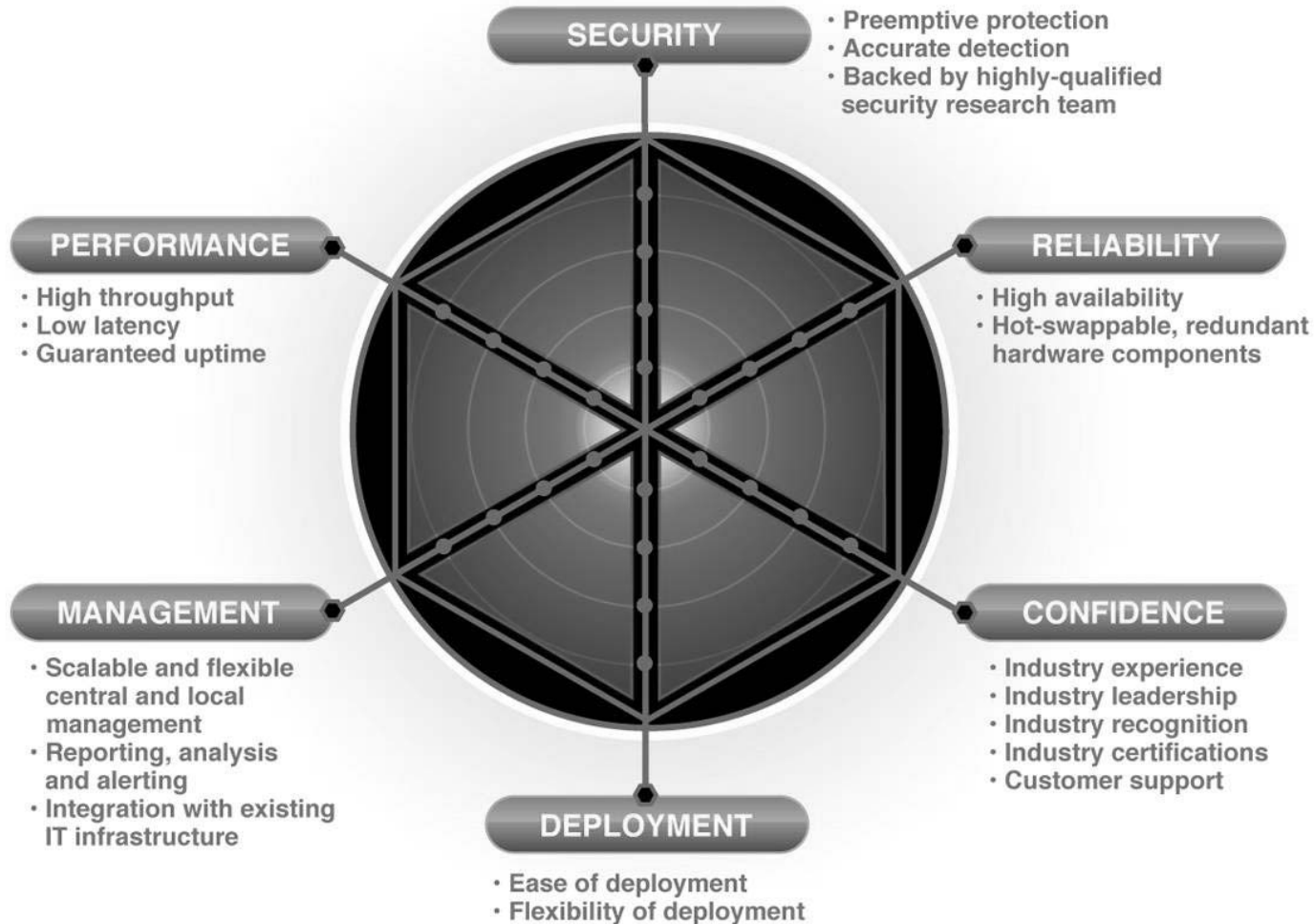
Proventia Network IPS Continuum: The Most Complete Portfolio Available



	Network							
	Remote Segments		Perimeter				Core	
Model	GX3002	GX4002	GX4004	GX5008	GX5108	G2000	GX6116	
Throughput	10 Mbps	200 Mbps	200 Mbps	400 Mbps	1.2 Gbps	2 Gbps	15 Gbps	
Protected Segments	1	1	2	4	4	4	8	

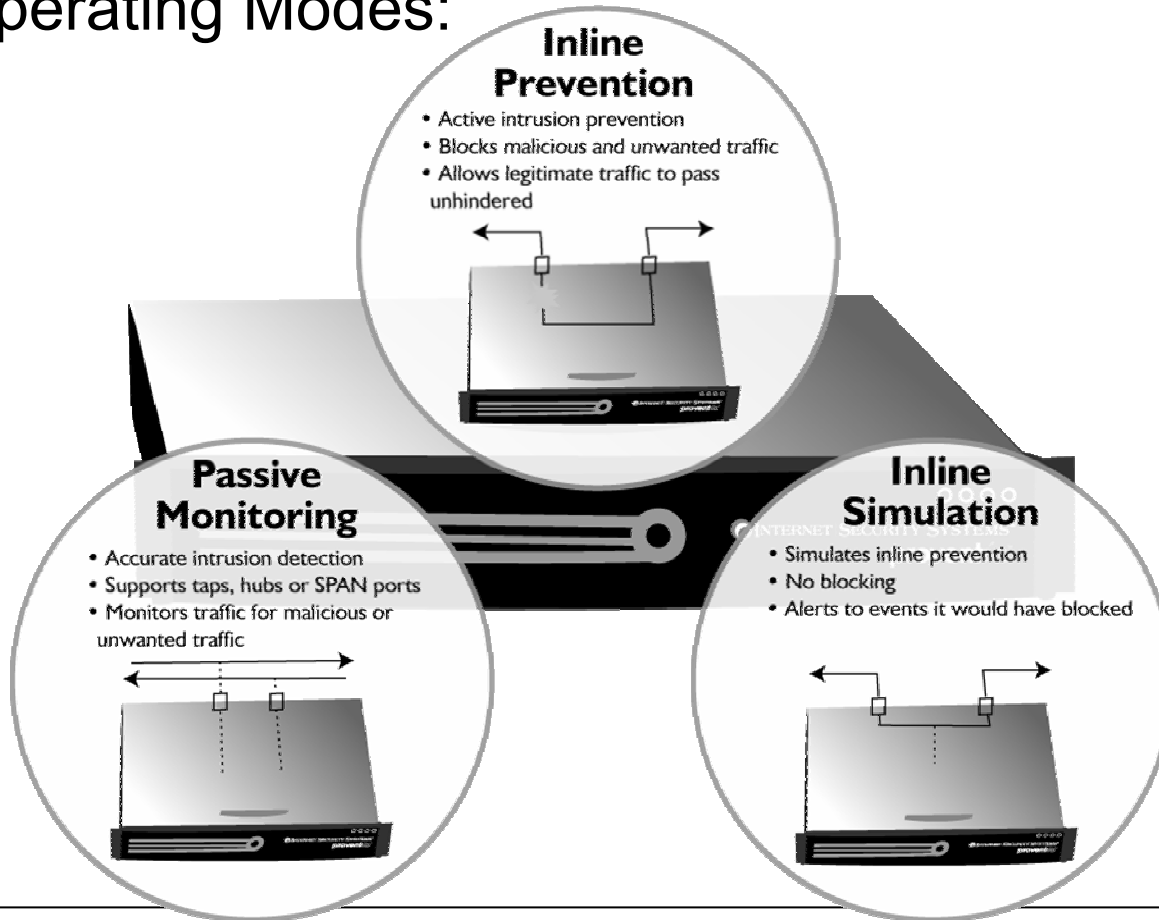



Uncompromising Protection ...



Proventia Network IPS Deployment


Three Operating Modes:



 What makes you special?

Network protection technology and products: Anomaly Detection Systems (ADS)



IBM Governance and Risk Management 
Maximize Value, Manage Risk

CRUMBLING PERIMETER

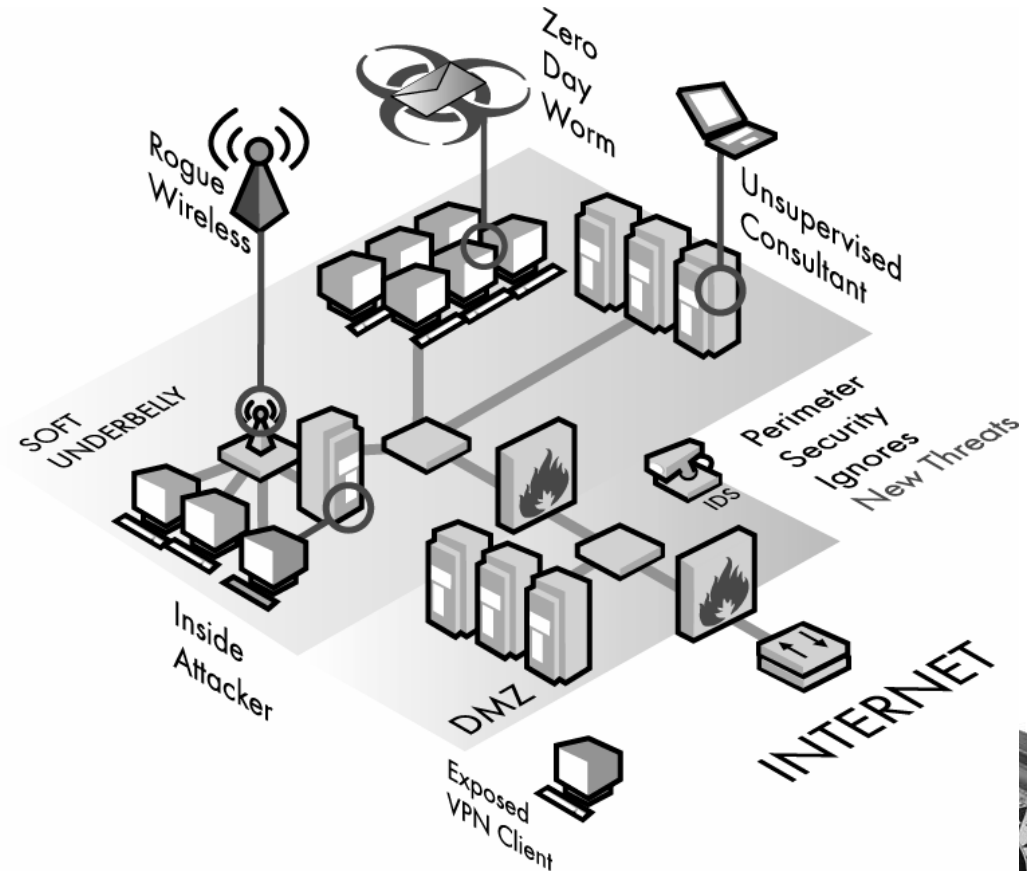
- VPN's, Wireless, Walk-In Vector
- Contractors, partners, customers
- Automated attacks, zero-day worms

CONSTANT TURMOIL

- New business, new applications
- Mergers and acquisitions
- Internal visibility is poor

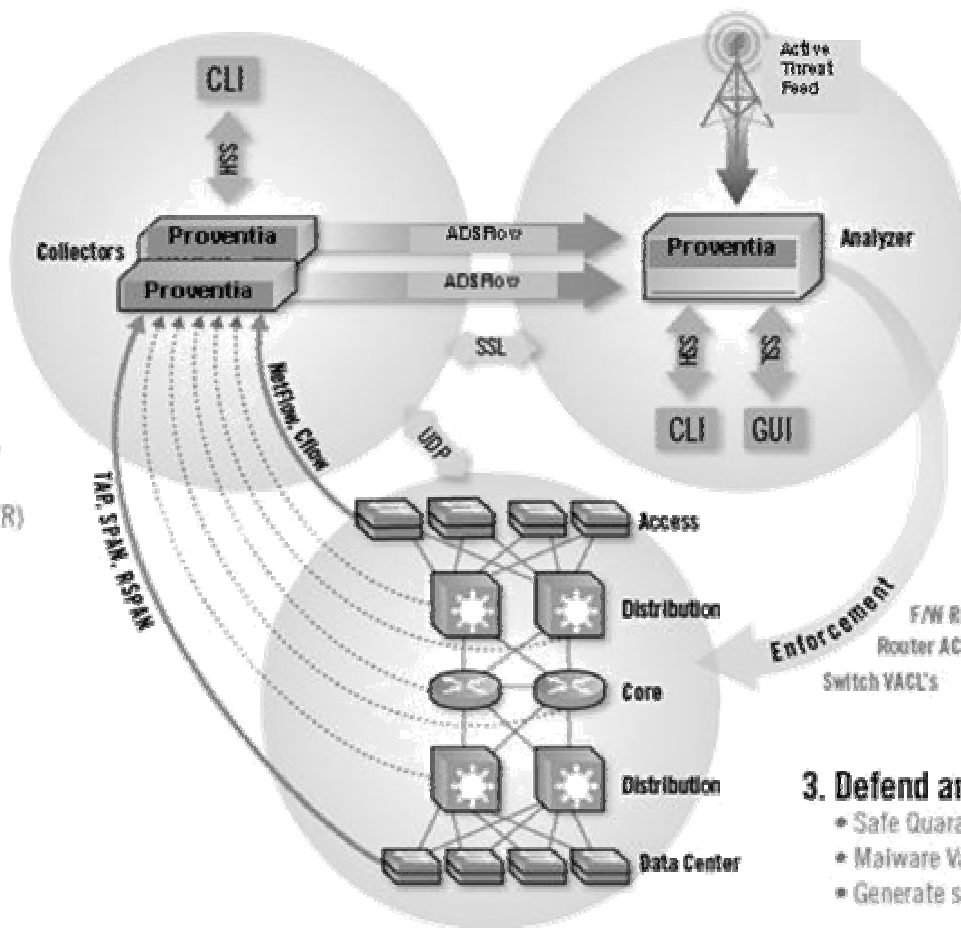
REGULATION

- HIPAA, SOX, GLBA
- Financial Penalties
- Brand Damage, Liability



1. Collect and Model

- Collect flow/packet data
- De-duplicate flows
- Turn unidirectional flows into bidirectional conversations
- Stateful Flow Reassembly (SFR)



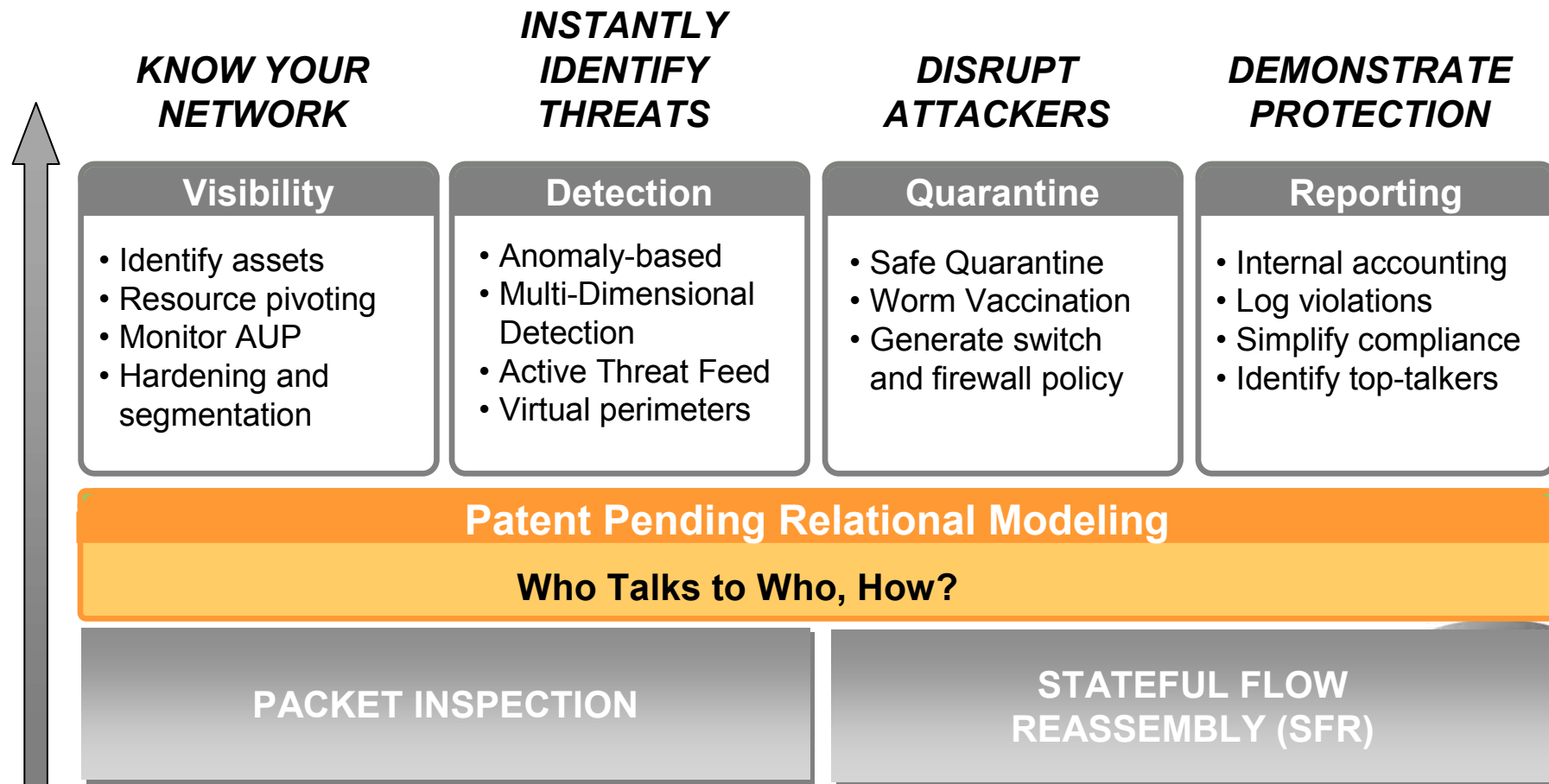
2. Correlate, Analyze & Identify

- Generate ADS relational Models
- Stateful Flow Reassembly (SFR)
- Provide visibility into user, network and application conversations
- Behavioral Analysis
- Multi-Dimensional Detection

3. Defend and Quarantine

- Safe Quarantine
- Malware Vaccination
- Generate switch and firewall policy





Proventia ADS continually develops new algorithms to accurately detect uniquely internal threats:



Worm Detection

Detects propagating patterns of abnormal behavior: the **SQL Slammer worm**.



Active Threat Feed (ATF)

Detects traffic that violates a behavioral fingerprint: **malware, phishing, botnet traffic, etc.**



Rate-Based Anomaly Detection

Detects sudden shifts from baselined traffic levels over time: a **DoS attack on a trading feed**.



Recon Detection

Detects slow scans, fast scans, “stealth” scans, and host sweeps.



Insider Misuse

Detects behavioral violations of specified security policy: **helpdesk worker improperly talking to/accessing payroll database**



Availability Outages

Detects drops in traffic on critical servers and links.



Deployment Guidelines

Model	Description	Flow Sources	Capture Ports	Up to Mbps
AD5003	Analyzer	3	2	200
AD3000	Packet Collector	0	4	1,000
AD3007	Flow/Packet Collector	7	4	1,000
AD3014	Flow/Packet Collector	14	4	1,000
AD3020	Flow/Packet Collector	20	4	1,000
Small Deployment		Medium Deployment		Large Deployment
Analyzer (3 flows, 200 mbs)		Analyzer 12 flow sources, 1gbps		Analyzer 40 flow sources



* What makes you special?

Network protection technology and products: **Unified Threat Modules (UTM)**

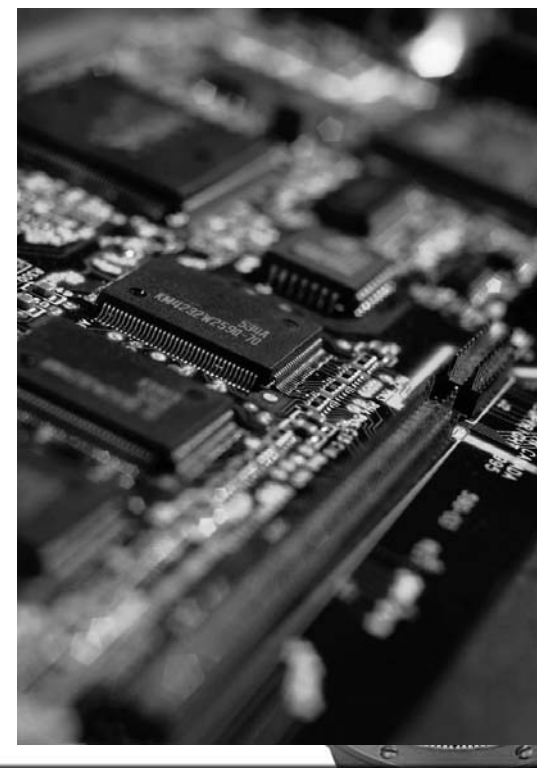


IBM Governance and Risk Management *
Maximize Value, Manage Risk



Network Protection: Proventia® M

- Layer 2/3 Firewall/VPN
 - OSPF Routing
 - Intrusion Prevention
- Antivirus
 - Virus Prevention
 - Web Filter
 - Antispam



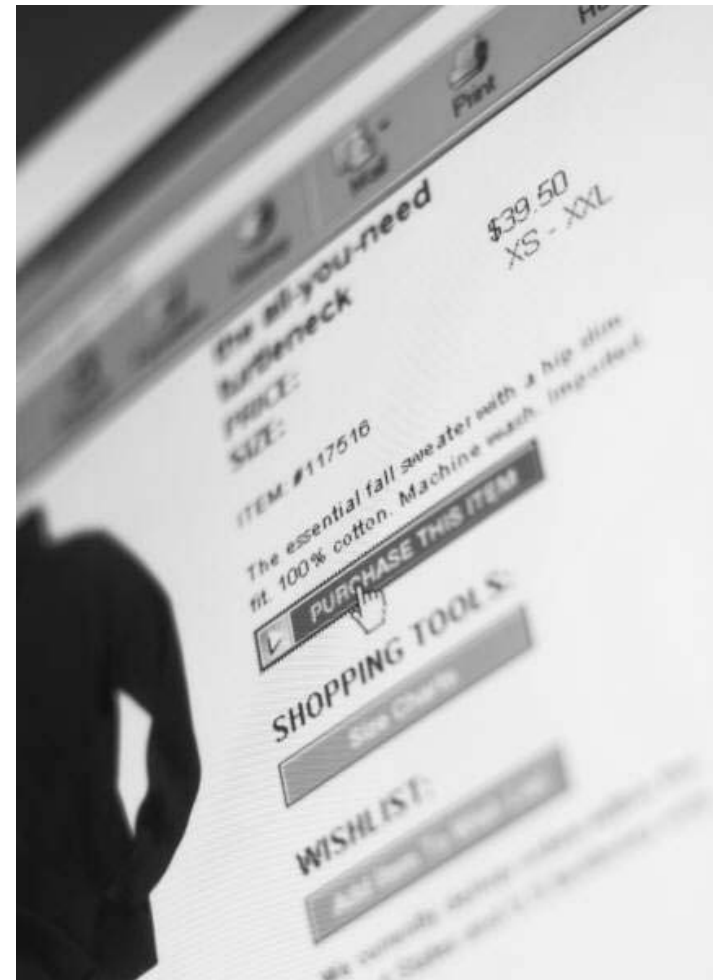
Who is M ideally suited for?

- Franchise Customers and other customers with many remote offices
 - Exclusive Multi-site management features
 - Excellent all-in-one Protection
 - Low price for the performance

- Alternative Corporate Gateways
 - VPN gateways
 - Partner gateways
 - Places where protection valuable, but speed, latency and fail-open are not driving factors

...Ahead of the threats...

- Latest Security Technologies
 - 830 blocks
 - 120k Viruses blocked
 - 60M URL's
 - 2.4 Billion Websites!
 - 1.5 Billion Images!
 - 95% of Spam Filtered
 - 1 in 10,000 false positives
 - Virus Prevention System
 - Spyware Protection
 - Best Performance at lowest cost



Best Protection Without Compromising Performance

Proventia MX1004



Proventia MX3006 and MX5010 Network Multi-Function Security at a Glance



IBM Proventia® MX3006
Multi-Function Security



IBM Proventia® MX5010
Multi-Function Security

Stateful Throughput Speed (Firewall only)

- Protecting 0 vulnerabilities
- Blocking 0 viruses
- Blocking 0 Spam
- Blocking 0 forbidden websites

100 Mbps

200 Mbps

1600 Mbps

Full Inspection Speed

- Protecting over 700 vulnerabilities
- Blocking 0 viruses
- Blocking over 95% of spam
- Blocking available for over 60M URLs by category

100 Mbps

200 Mbps

800 Mbps

Full Inspection Speed

- Protecting over 700 vulnerabilities
- Blocking over 120,000 viruses over SMTP and POP3
- Blocking over 95% of spam
- Blocking available for over 60M URLs by category

43 Mbps

200 Mbps

566 Mbps

Full Inspection Speed

- Protecting over 700 vulnerabilities
- Blocking over 120,000 viruses over SMTP, POP3, HTTP and FTP
- Blocking over 95% of spam
- Blocking available for over 60M URLs by category

34 Mbps

94 Mbps

150 Mbps

Maximum Connections per second

2,125

4,100

4,100

Maximum Concurrent Sessions

101,000

101,000

101,000



* What makes you special?

Host and Desktop protection: Proventia Desktop Endpoint Security



IBM Governance and Risk Management *
Maximize Value, Manage Risk

- **Firewalls and VPNs are *not* enough. Firewalls can't block malicious traffic, and VPNs only encrypt traffic. An attacker can use a VPN as a tunnel right into the corporate network**
- **Users who, unwittingly or intentionally, download potentially dangerous applications or other forms of malicious code**
- **Customers of all shapes and sizes need protection if they are connected to the Internet**
- **Products centered around AV signature antivirus are 100% ineffective against new generations of custom, targeted, and designer attacks. Scan & Remove technologies are less effective with Rootkits and Ransomware, where neither detection nor recovery may not be possible.**
- **Need for a ONE-STOP SHOP SOLUTION for Endpoint Protection.**

Proventia Desktop - Multi-Layered Protection

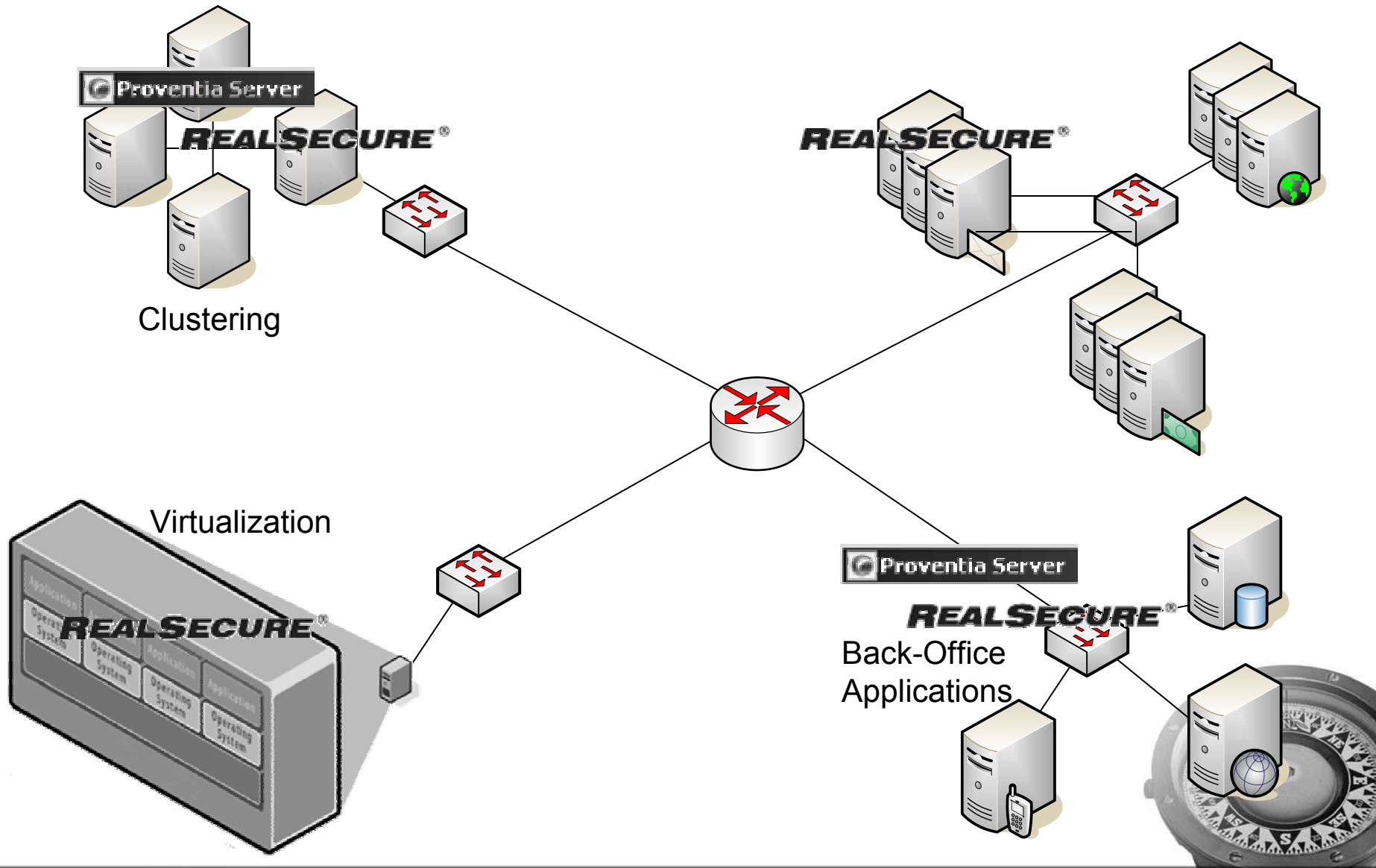


* What makes you special?

Host and Desktop protection: Proventia Server & Server Sensor



IBM Governance and Risk Management *
Maximize Value, Manage Risk



- ISS places a high value on comprehensive OS and new version support
 - Support more heterogeneous environments than any other Server HIPS vendor
 - Windows, Linux (RHEL/SLES), Solaris, HP-UX, AIX, VMWare/Virtualization
 - Early to market on supporting the latest versions and platform evolutions
 - RHEL 4.0 support (and Kernel independent design to assure prompt future support)
 - Solaris 10 (unique and efficient support of the Container architecture)
- Leads the market in Gartner's Nine protection styles coverage
- Defense-in-Depth
 - Seamless integration with network and host security products
- Backed by world-leading X-Force research and development
 - VirtualPatch™ Technology
 - Protocol Analysis Module (PAM)



Server Protection









Proactive Zone **DANGER ZONE** **Compliance Zone** **DANGER ZONE** **Proactive Zone**

File Integrity ■ OS Audit Log ■ Generic Application Text Log ■ Registry Integrity Monitoring

Gartner's Nine Protection Styles of HIPS



	Allow Known Good (Block All Else)	Block Known Bad (Allow All Else)	Unknown
Execution-Level HIPS	7. Application Control 	8. Resource Shielding  BOEP (Windows)	9. Behavioral Containment Upcoming
Application-Level HIPS	4. Application and System Hardening 	5. Antivirus Upcoming	6. Application Inspection
Network-Level HIPS	1. Host Firewall  Firewall	2. Attack-Facing Network Inspection  IPS	3. Vulnerability-Facing Network Inspection  IPS

Source: Gartner, Inc., "Understanding Strengths and Weaknesses of Host-Based Intrusion Prevention Styles," Neil McDonald, 30 January 2006.



RealSecure Server Sensor



Proventia Server



Features

- New OS event signatures for Windows Server 2003 and Active Directory
- Web Application Protection Module for IIS 6 (SSL inspection)
- Driver-level packet trusting (inspection bypass)
- Interface exclusions (Unix only)
- Usability
 - Installation logic for Windows Server Sensor
 - Silent installation for AIX
 - Custom installation path for AIX and HP-UX
- TCP Resegmentation support for AIX customers
- Platform Support
 - Solaris 10 (and Containers)
 - HP-UX 11.23
 - Windows Server 2003 SP2
 - ISA Server 2006
 - AIX 5.4

* What makes you special?

Content protection technology and products: Proventia Network Mail Security

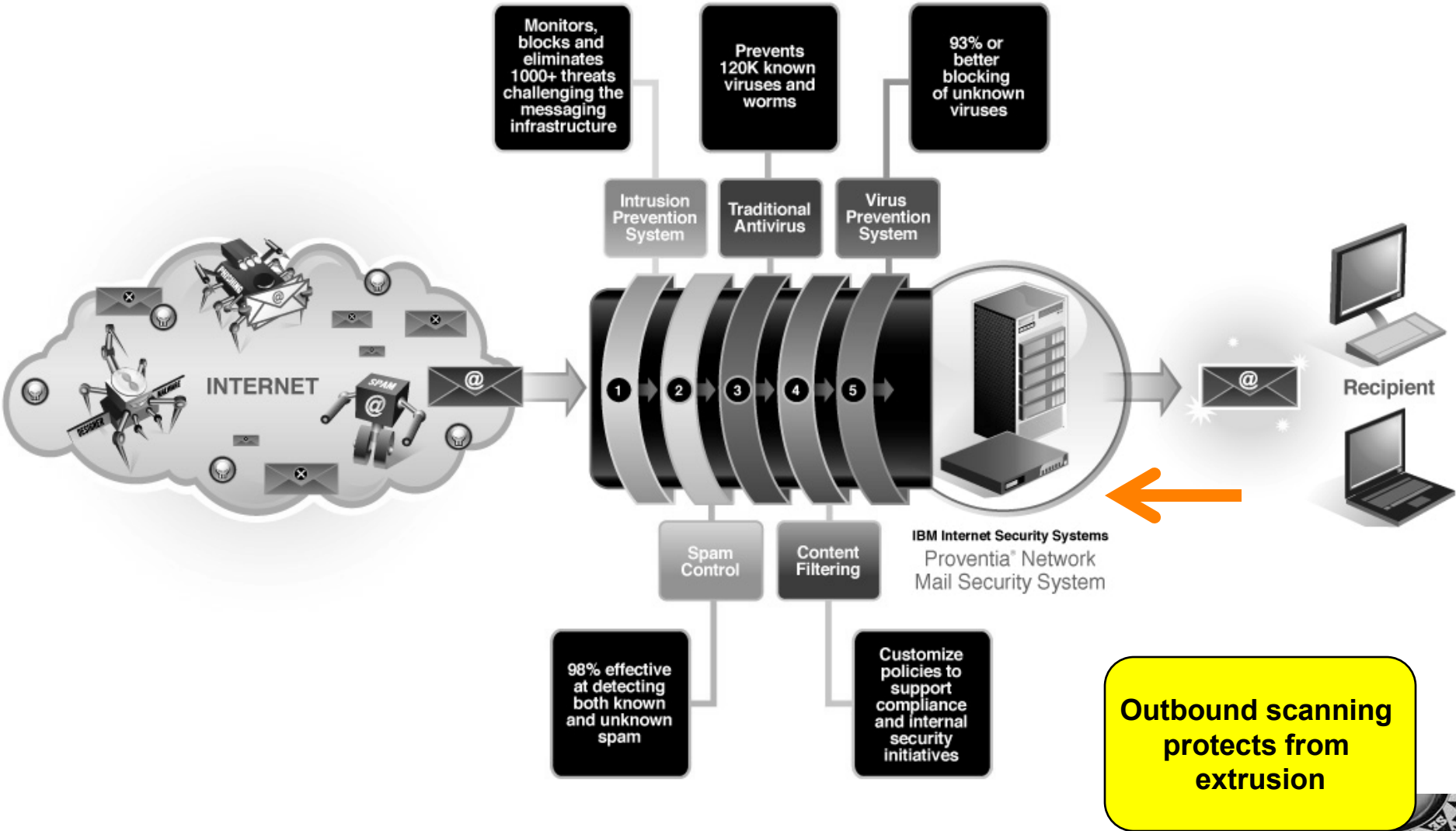


IBM Governance and Risk Management *
Maximize Value, Manage Risk



- Proventia Mail Security
 - Scalable enterprise-class solution
 - Best-in-breed anti-spam and anti-virus, including VPS
 - Clustering support for failover and large-scale deployments
 - Highly flexible and scalable rules-based policy management
 - Easy to deploy, easy to manage
 - Stand-alone or managed thru SiteProtector

Proventia Network Mail: Multi-layered Email Protection



Welcome to Proventia Network Mail

- First and only mail security vendor with **Virus Prevention System**
- First and only mail security vendor with **integrated IPS technology**
- Our **Proventia Filter Database** utilizes more than 500 web crawlers and 800 spam collectors, analyzing more than 5.9 billion web pages and images to date – second in size only to Google!
- Backed by X-Force and C-Force research and development





* What makes you special?

Content protection technology and products: **Proventia Web Filter**

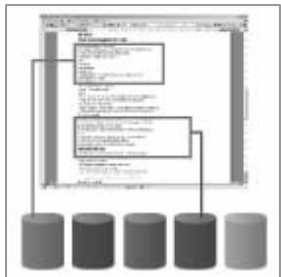


IBM Governance and Risk Management *
Maximize Value, Manage Risk

Core technologies



Text recognition (OCR)



Text classification



Object recognition



Face recognition



Pornography & nudity detection



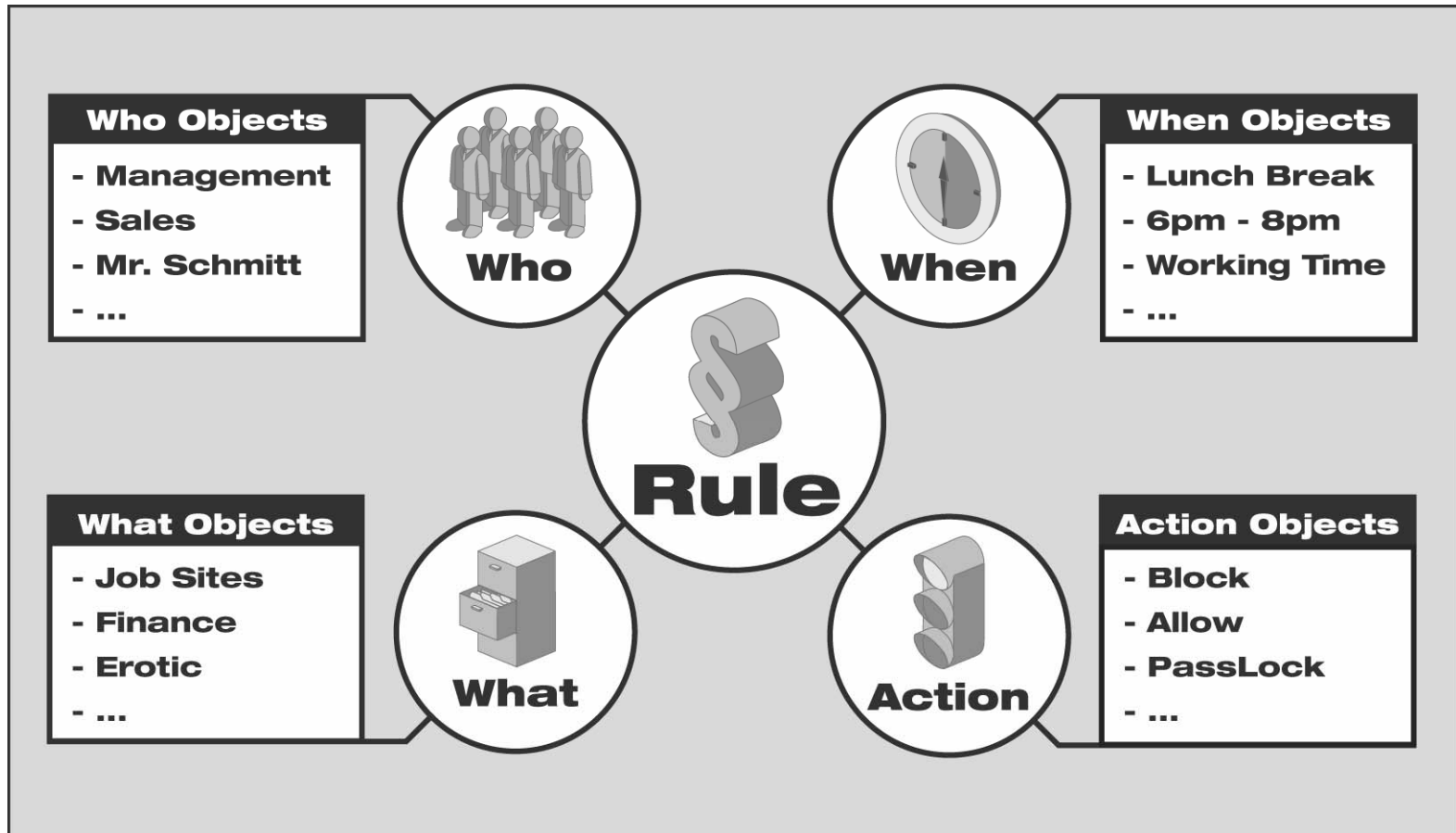
Digital fingerprint



Comparison of similarity and identity



ISS Web Filter – Policy Workflow





Proventia Web Filter – world's largest URL filter list

- **Topicality**

- Crawlers collect image and text data from the Internet 24 hours a day on 365 days, which adds up to **120 million pages each month**
- Every day, customers receive updates, equaling some **100,000 new categorized sites**

- **Quality**

- Largest URL database meets practically every filtering requirement by means of indexed URLs in **60 categories**

- **Quantity**

- World's largest URL filter list contains **60 million URLs**
- World's largest database with **2.6 billion** evaluated web pages and images
- In-house Computer Center with more than 1000 servers.



* What makes you special?

Advisory Services and MSS overview



IBM Governance and Risk Management *
Maximize Value, Manage Risk

X-Force Threat Analysis Service



Multiple Platforms & Products

La protezione preventiva dalle minacce e intrusioni: le soluzioni di IBM Internet Security System


Davide Licciardello, CISSP

Davide.Licciardello@it.ibm.com

Technical Pre-Sales System Engineer

Questions ?



IBM Governance and Risk Management 
Maximize Value, Manage Risk