IBM Security Solutions
Virtual Server Security

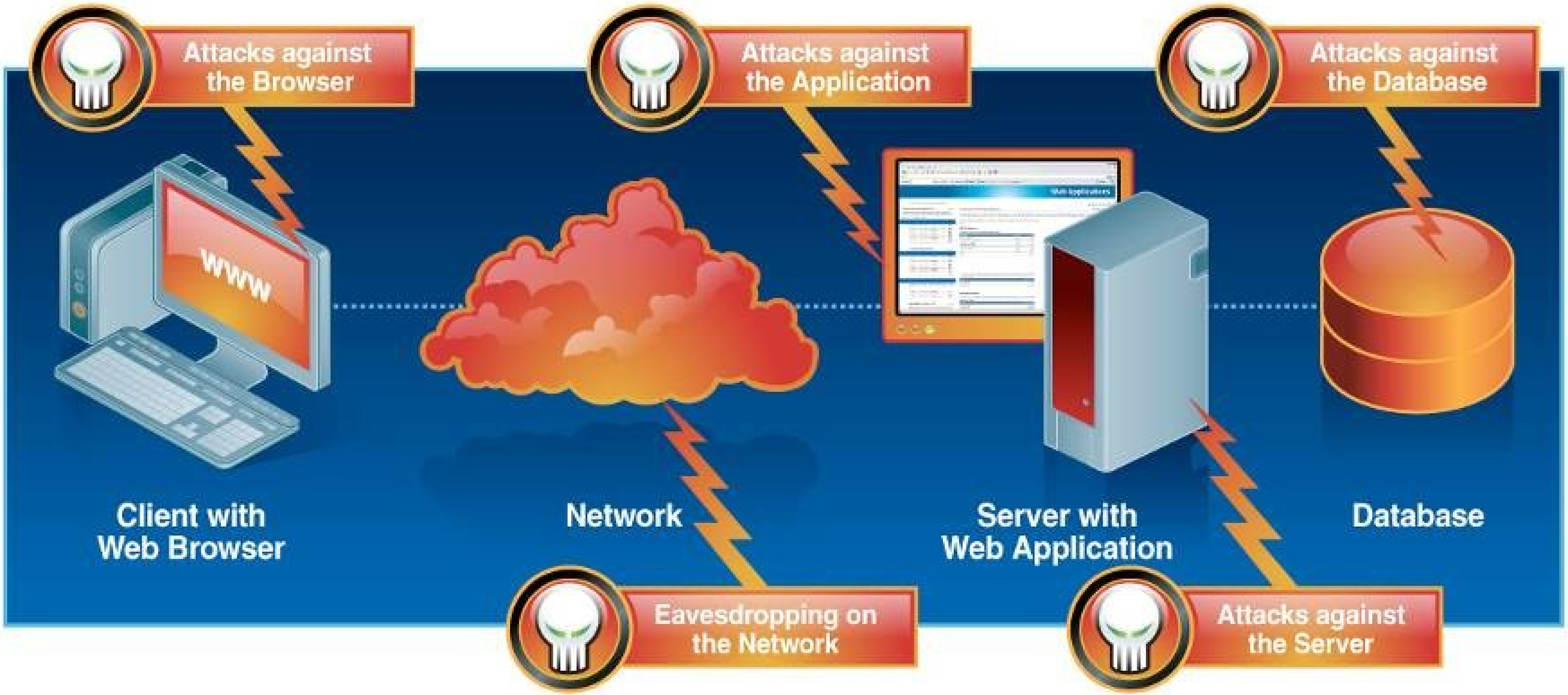
Peter Häufel, IBM Security Solutions

Agenda

- Vorsprung durch Forschung
- Intrusion Prevention Technologie
- Virtual Intrusion Prevention Appliance
- Virtual Server Security
- Beispielprojekte

© IBM Corporation 2009.

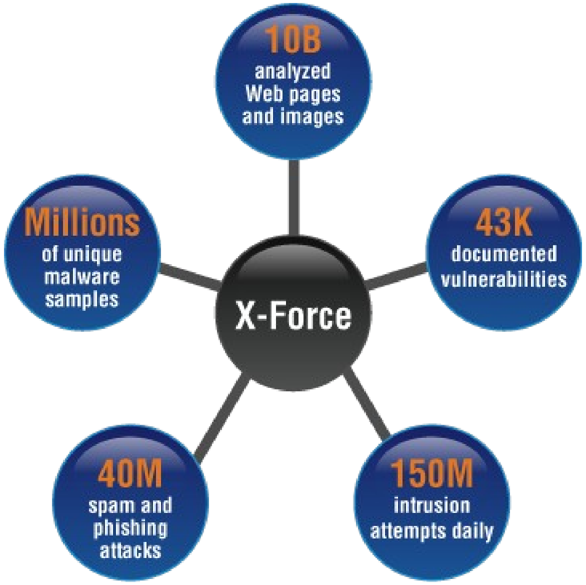
Attack Vectors


Attacks against the Browser
Attacks against the Application
Attacks against the Database
www
Client with Web Browser
Network
Server with Web Application
Database
Eavesdropping on the Network
Attacks against the Server

© IBM Corporation 2009.

Why IBM?
IBM Research, X-Force

IBM Security Research

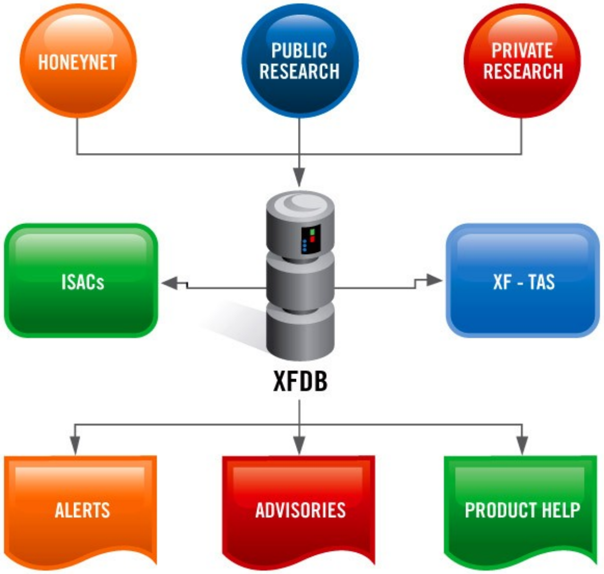


10B analyzed Web pages and images
Millions of unique malware samples
43K documented vulnerabilities
X-Force
40M spam and phishing attacks
150M intrusion attempts daily

Provides Specific Analysis of:

- Vulnerabilities and exploits
- Malicious/Unwanted websites
- Spam and phishing
- Malware
- Other emerging trends

IBM X-Force® Database



Most comprehensive vulnerability database in the world

- Entries date back to the 1990's

Updated daily by a dedicated research team currently tracks over:

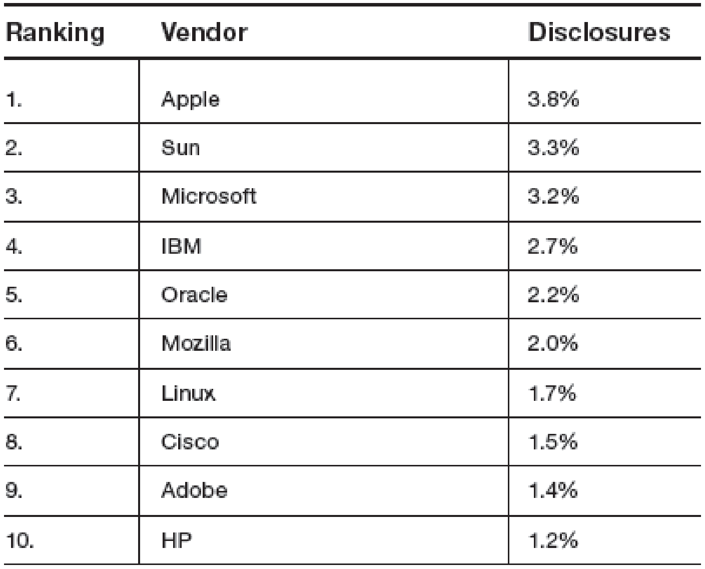
- 7,600 Vendors
- 17,000 Products
- 40,000 Versions

Source: IBM X-Force Database

© IBM Corporation 2009.

Apple, Sun and Microsoft Top Vendor List for Disclosures

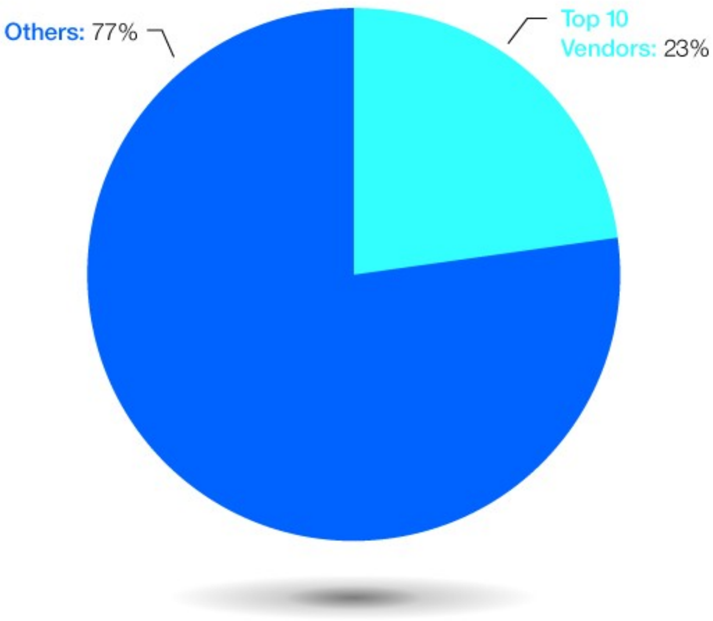
- Top ten vendors account for nearly a quarter (**23%**) of all disclosed vulnerabilities, up from **19%** in 2008.
- Significant changes to the Top Ten List including:
  - Microsoft dropped from #1 to #3 after holding top spot since 2006.
  - Adobe makes it's debut on the top ten list at number nine.



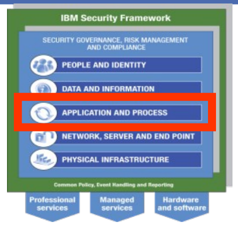
Ranking	Vendor	Disclosures
1.	Apple	3.8%
2.	Sun	3.3%
3.	Microsoft	3.2%
4.	IBM	2.7%
5.	Oracle	2.2%
6.	Mozilla	2.0%
7.	Linux	1.7%
8.	Cisco	1.5%
9.	Adobe	1.4%
10.	HP	1.2%

Table 3: Vendors with the Most Vulnerability Disclosures, 2009

Percentage of Vulnerability Disclosures Attributed to Top 10 Vendors
2009



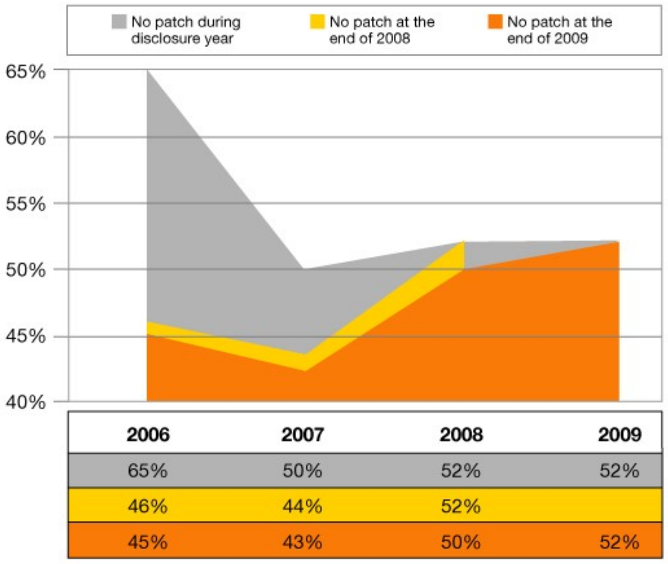
Customers should also be concerned about vendors not on this list. Are those vendors taking security seriously?



Patches Still Unavailable for Over Half of Vulnerabilities

- Over half (**52%**) of all vulnerabilities disclosed in 2009 had no vendor-supplied patches to remedy the vulnerability.
  - **45%** of vulnerabilities from 2006, **43%** from 2007 and **50%** from 2008 still have no patches available at the end of 2009.

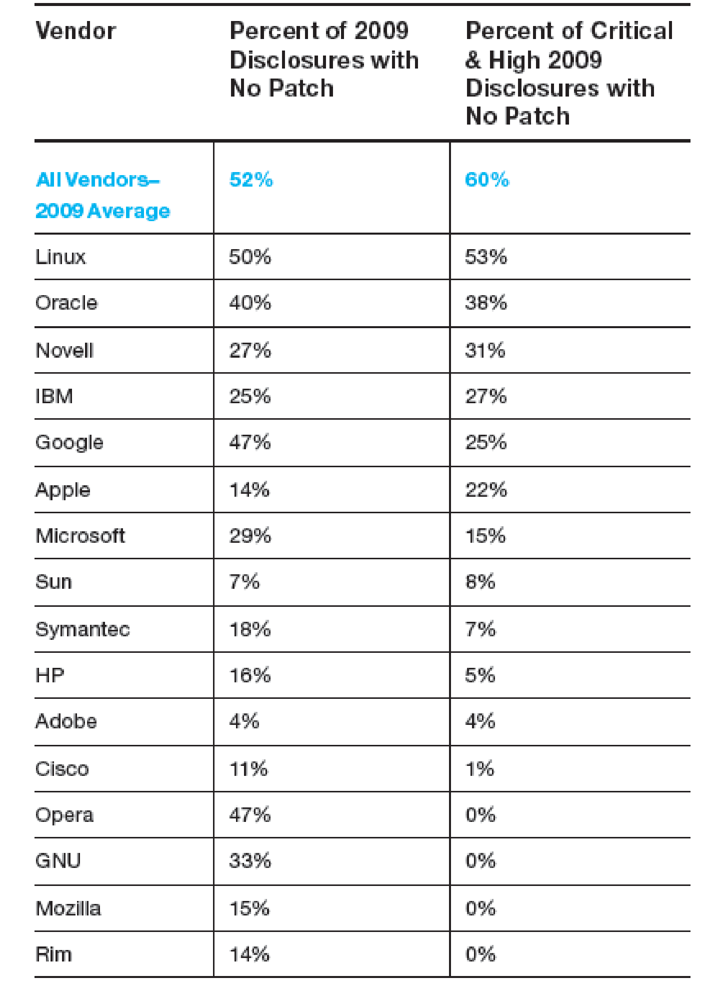
Percentage of Vulnerabilities with Vendor-Supplied Patches by Vulnerability Disclosure Year
2006-2009



	2006	2007	2008	2009
No patch during disclosure year	65%	50%	52%	52%
No patch at the end of 2008	46%	44%	52%	
No patch at the end of 2009	45%	43%	50%	52%

Vulnerability Disclosure Year

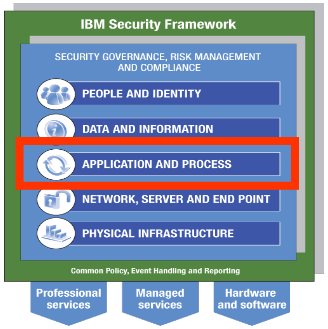
Source: IBM X-Force®



Vendor	Percent of 2009 Disclosures with No Patch	Percent of Critical & High 2009 Disclosures with No Patch
All Vendors– 2009 Average	**52%**	**60%**
Linux	50%	53%
Oracle	40%	38%
Novell	27%	31%
IBM	25%	27%
Google	47%	25%
Apple	14%	22%
Microsoft	29%	15%
Sun	7%	8%
Symantec	18%	7%
HP	16%	5%
Adobe	4%	4%
Cisco	11%	1%
Opera	47%	0%
GNU	33%	0%
Mozilla	15%	0%
Rim	14%	0%

Table 4: Best and Worst Patchers, 2009

Web App Vulnerabilities Continue to Dominate


IBM Security Framework

SECURITY GOVERNANCE, RISK MANAGEMENT AND COMPLIANCE

PEOPLE AND IDENTITY

DATA AND INFORMATION

APPLICATION AND PROCESS

NETWORK, SERVER AND END POINT

PHYSICAL INFRASTRUCTURE

Common Policy, Event Handling and Reporting

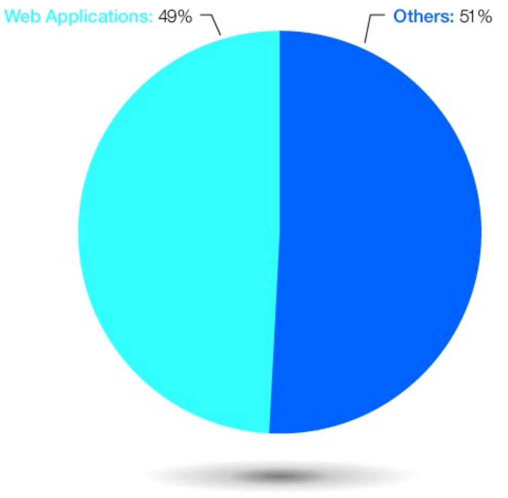
Professional services

Managed services

Hardware and software

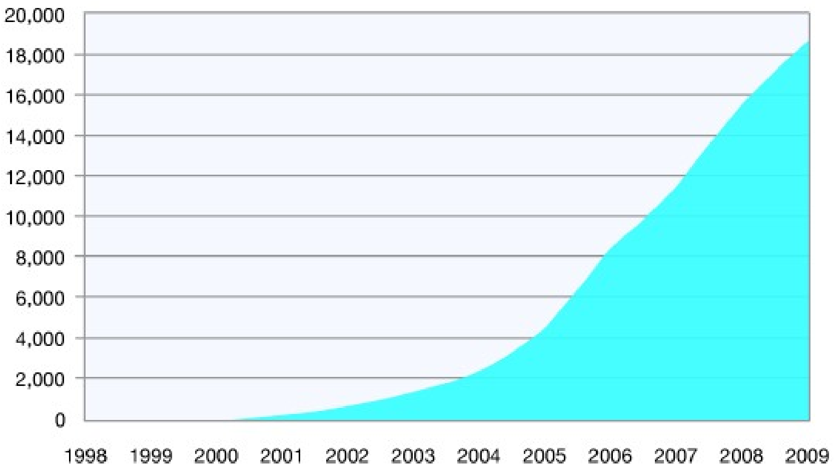
- **49%** of all vulnerabilities are Web application vulnerabilities.
- Cross-Site Scripting disclosures surpassed SQL injection to take the top spot.
- **67%** of web application vulnerabilities had no patch available at the end of 2009.

Percentage of Vulnerability Disclosures that Affect Web Applications
2009



Source: IBM X-Force®

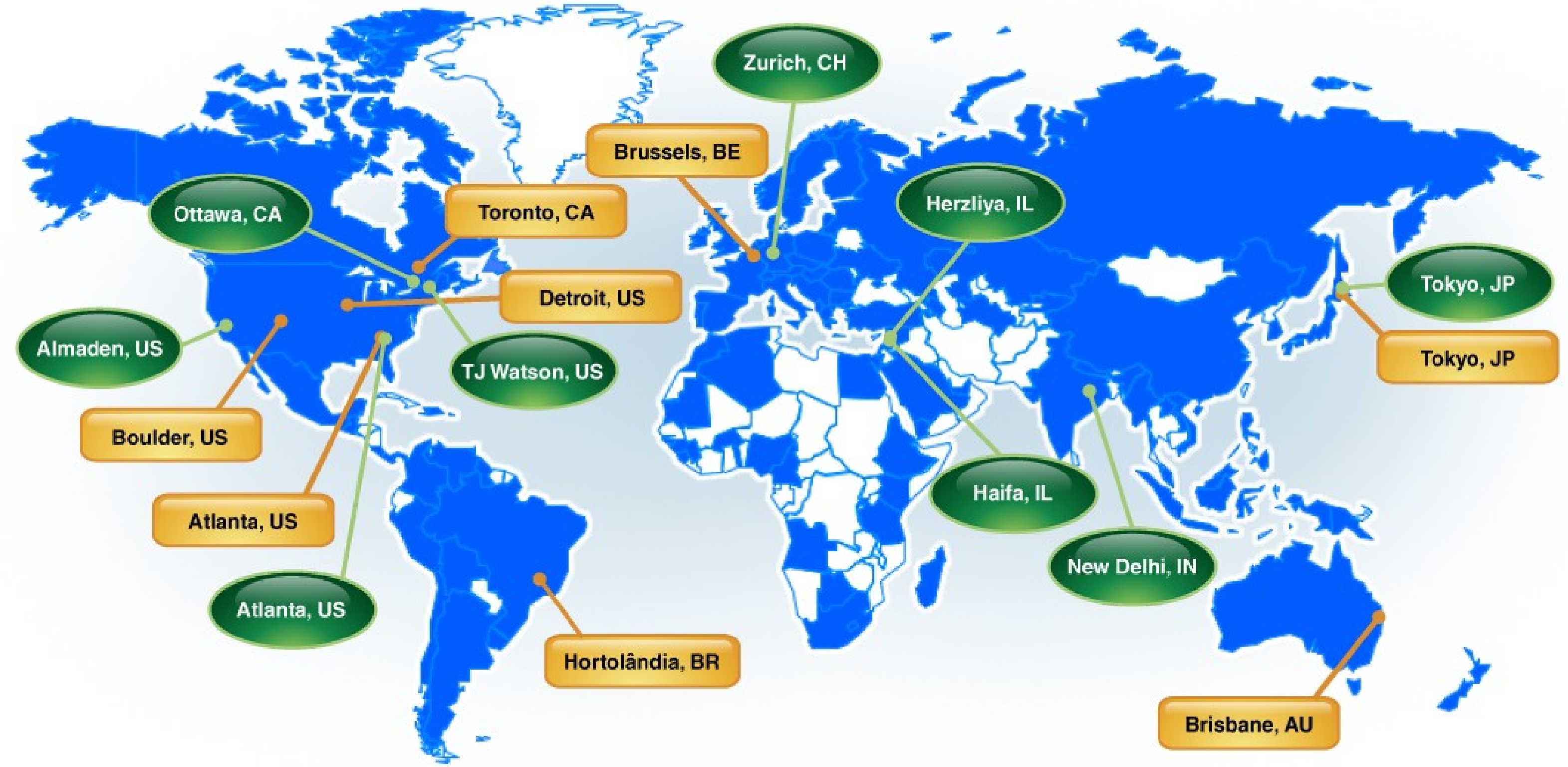
Cumulative Count of Web Application Vulnerability Disclosures
1998-2009



Source: IBM X-Force®

IBM Global Security Reach

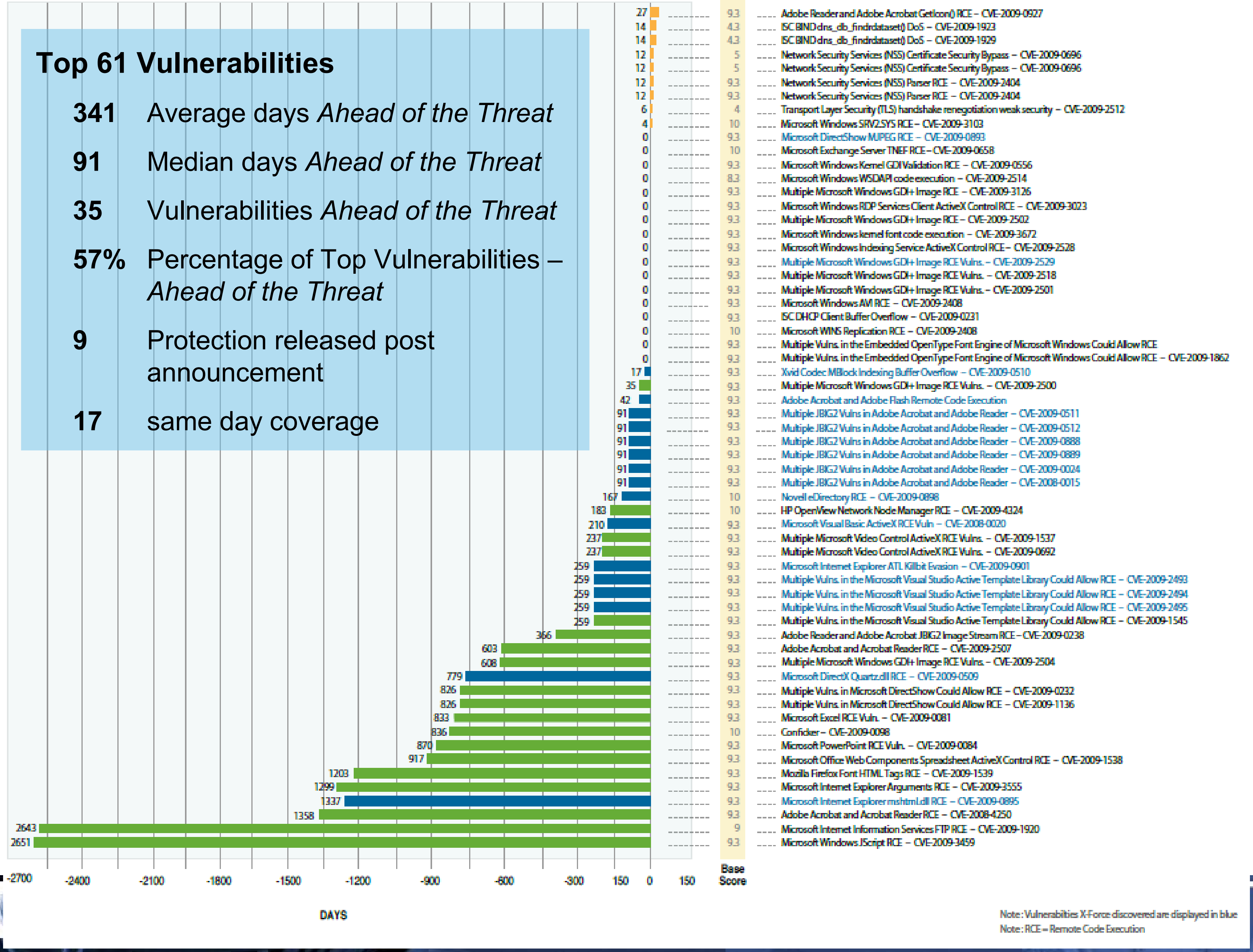
8 Security Operations Centers + 9 Security Research Centers + 133 Monitored Countries + 20,000+ Devices under Contract + 3,700+ MSS Clients Worldwide + 4 Billion+ Events Per Day



IBM has the unmatched global and local expertise to deliver complete solutions – and manage the cost and complexity of security

© IBM Corporation 2009.

Security Effectiveness: Ahead of the Threat – Top Vulnerabilities of 2009



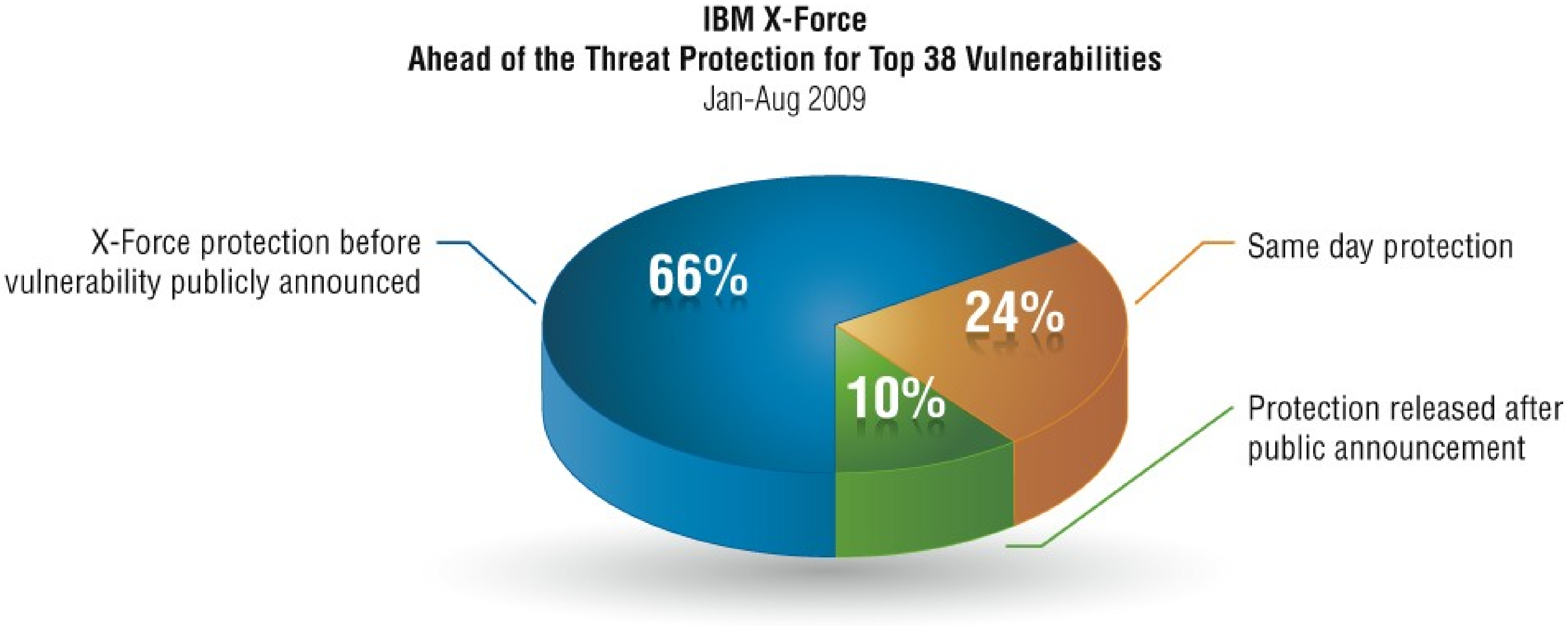
Top 61 Vulnerabilities

341	Average days *Ahead of the Threat*
91	Median days *Ahead of the Threat*
35	Vulnerabilities *Ahead of the Threat*
57%	Percentage of Top Vulnerabilities – *Ahead of the Threat*
9	Protection released post announcement
17	same day coverage

Note: Vulnerabilties X-Force discovered are displayed in blue

Note: RCE = Remote Code Execution

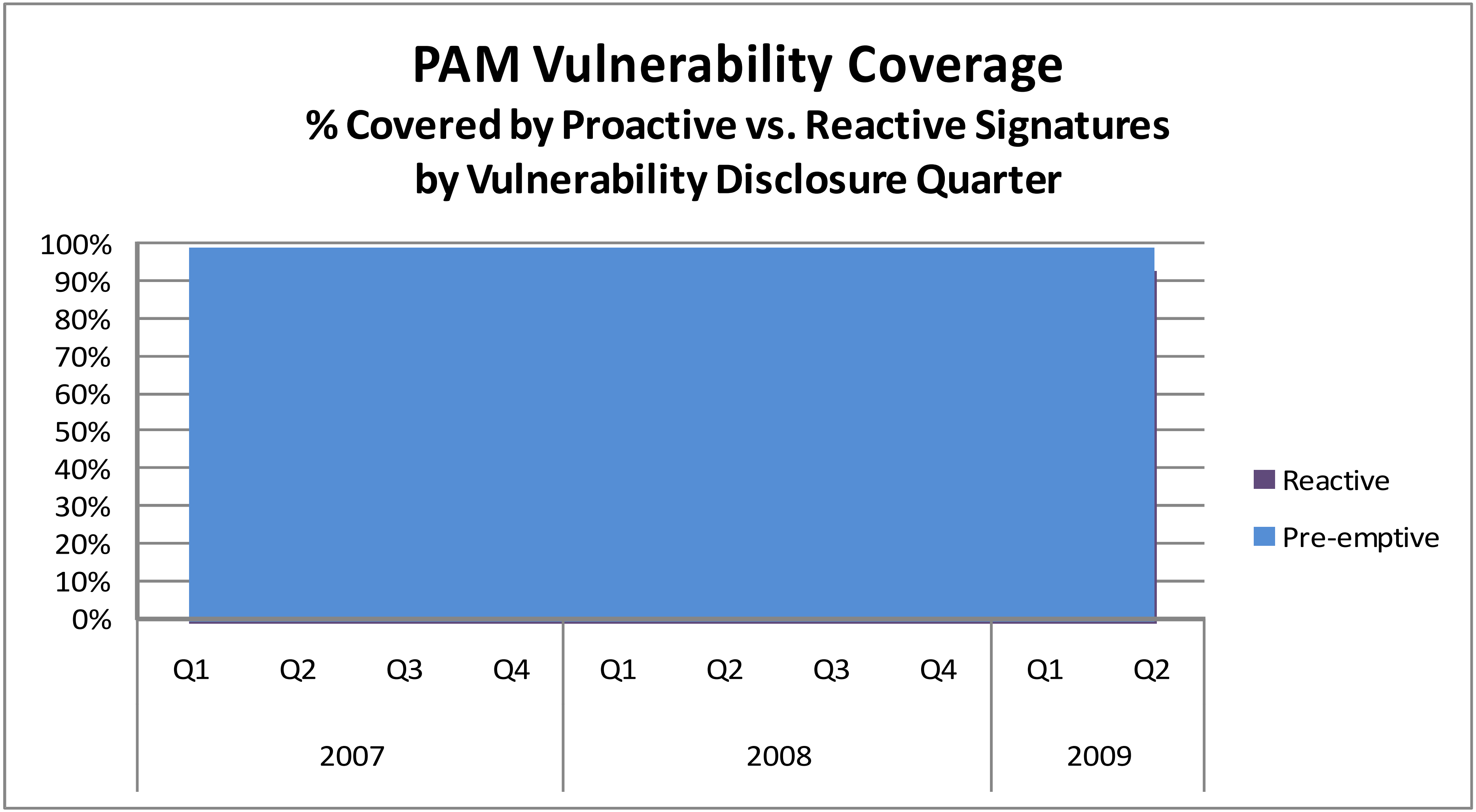
IBM Superior Technology
Keeping Clients "Ahead of the Threat"



IBM X-Force displays "Ahead of the Threat" protection for the Top 38 vulnerabilities from Jan – Aug 2009.

© IBM Corporation 2009.

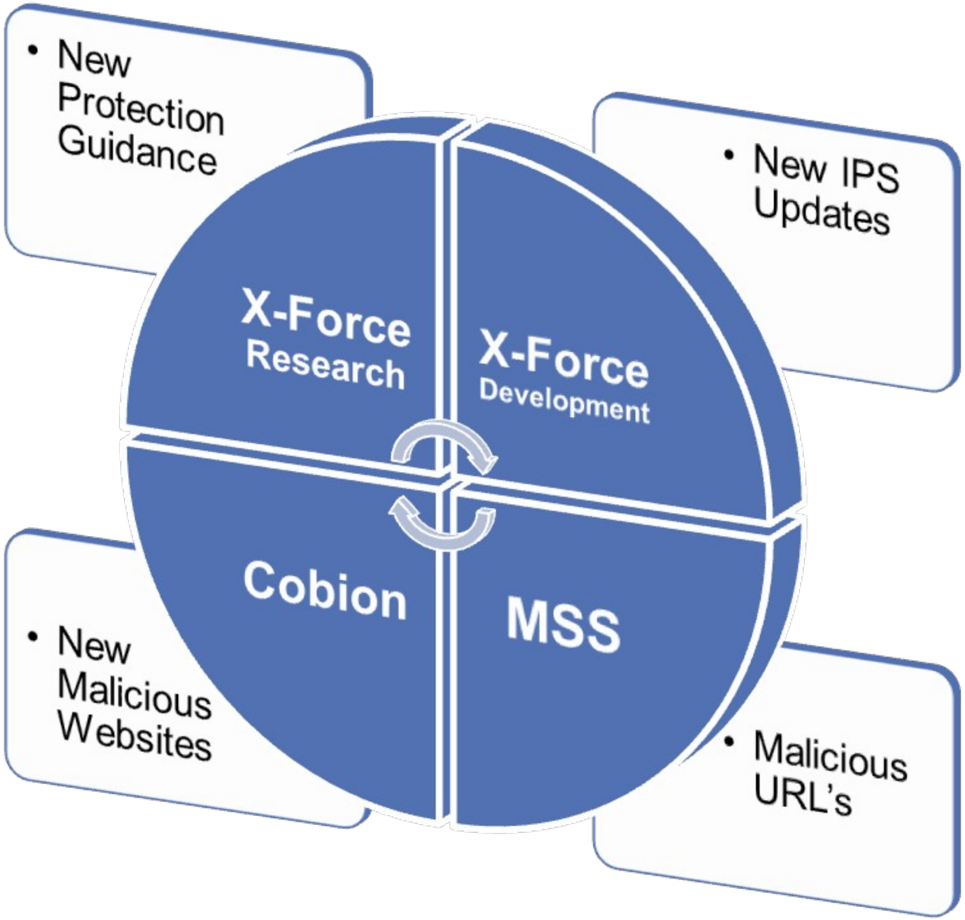
Proactive vs. Reactive Vulnerability Coverage



© IBM Corporation 2009.

IBM X-Force Web Intelligence Lifecycle

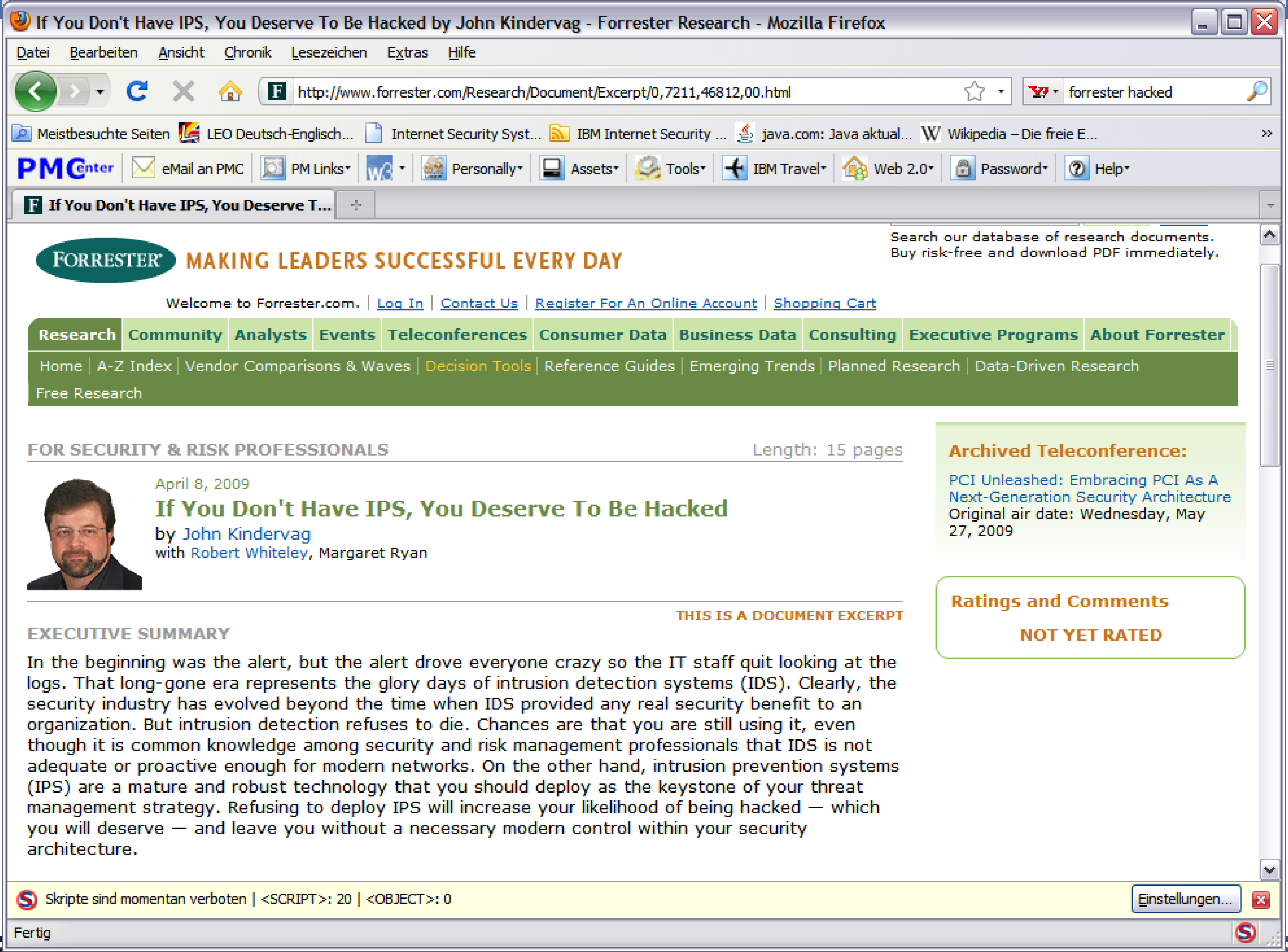
- **Deep Crawl of Known Malicious Websites**
- **Analyze New Exploit Techniques**
- **Provide New Protection Guidance**



- **Develop Protection**
- **Deliver Updates**

- **Classify MSS Links**
- **Find Related Websites (Deep Crawl)**
- **Search for Malware**
- **Find New Malicious Websites**
- **Block All Malicious Domains**

- **Apply Updates**
- **Monitor Browsing of:**
  - **Million of End-users**
  - **Thousands of Customers**
  - **Hundreds of Countries**
- **Block Malicious Links**
- **Send Links to Cobion**


If You Don't Have IPS, You Deserve To Be Hacked by John Kindervag - Forrester Research - Mozilla Firefox
Datei
Bearbeiten
Ansicht
Chronik
Lesezeichen
Extras
Hilfe
http://www.forrester.com/Research/Document/Excerpt/0,7211,46812,00.html
forrester hacked
Meistbesuchte Seiten
LEO Deutsch-Englisch...
Internet Security Syst...
IBM Internet Security ...
java.com: Java aktual...
Wikipedia – Die freie E...
PMCenter
eMail an PMC
PM Links
Personally
Assets
Tools
IBM Travel
Web 2.0
Password
Help
If You Don't Have IPS, You Deserve T...
Skripte sind momentan verboten | <SCRIPT>: 20 | <OBJECT>: 0
Einstellungen...
Fertig

FORRESTER MAKING LEADERS SUCCESSFUL EVERY DAY

Search our database of research documents.
Buy risk-free and download PDF immediately.

Welcome to Forrester.com. | Log In | Contact Us | Register For An Online Account | Shopping Cart

Research | Community | Analysts | Events | Teleconferences | Consumer Data | Business Data | Consulting | Executive Programs | About Forrester

Home | A-Z Index | Vendor Comparisons & Waves | Decision Tools | Reference Guides | Emerging Trends | Planned Research | Data-Driven Research | Free Research

FOR SECURITY & RISK PROFESSIONALS Length: 15 pages

April 8, 2009

If You Don't Have IPS, You Deserve To Be Hacked

by John Kindervag
with Robert Whiteley, Margaret Ryan

THIS IS A DOCUMENT EXCERPT

EXECUTIVE SUMMARY

In the beginning was the alert, but the alert drove everyone crazy so the IT staff quit looking at the logs. That long-gone era represents the glory days of intrusion detection systems (IDS). Clearly, the security industry has evolved beyond the time when IDS provided any real security benefit to an organization. But intrusion detection refuses to die. Chances are that you are still using it, even though it is common knowledge among security and risk management professionals that IDS is not adequate or proactive enough for modern networks. On the other hand, intrusion prevention systems (IPS) are a mature and robust technology that you should deploy as the keystone of your threat management strategy. Refusing to deploy IPS will increase your likelihood of being hacked — which you will deserve — and leave you without a necessary modern control within your security architecture.

Archived Teleconference:

PCI Unleashed: Embracing PCI As A Next-Generation Security Architecture
Original air date: Wednesday, May 27, 2009

Ratings and Comments

NOT YET RATED

© IBM Corporation 2009.

Funktionsweise Intrusion Prevention

Virtual Patch

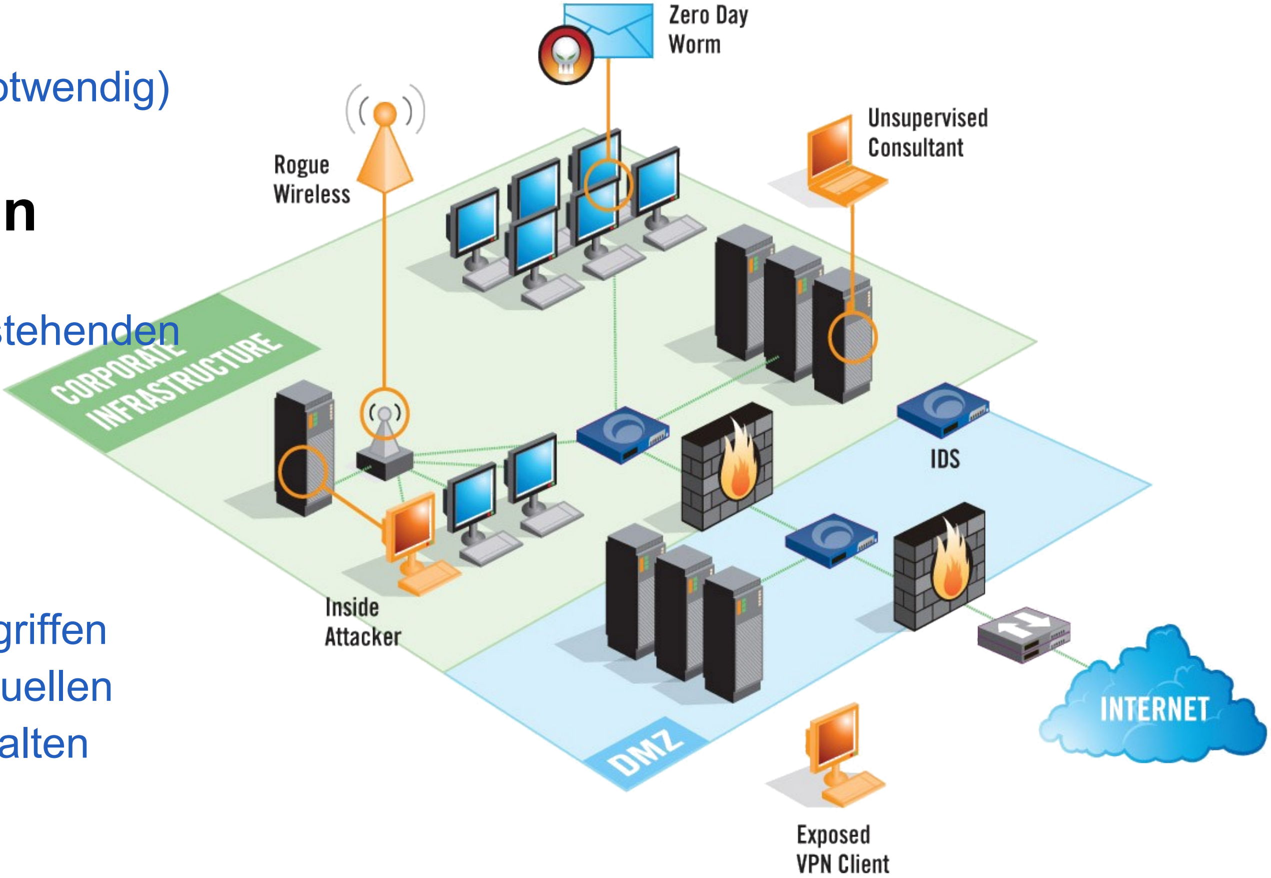
- Reduzierung des Patchaufwandes
- Frühzeitiger Schutz
- Schnelles Roll-Out (falls notwendig)

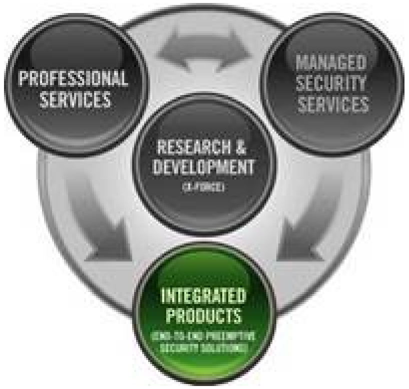
Abwehr von Angriffen

- Blocken von Angriffen
- Keine Ausnutzung von bestehenden Schwachstellen
- Herausfiltern von Malware

Transparenz

- Erkennen von internen Angriffen
- Identifizieren von Angriffsquellen
- Identifizieren von Fehlverhalten





SiteProtector

Unified Enterprise Security Console for all products

Enterprise Protection Products

proventia™ Mail Security

BM Proventia Network Mail Security System and IBM Proventia Network Mail Security System Virtual Appliance provide spam control and preemptive protection for your messaging infrastructure

proventia™ Network Protection

High performance network security with real-time attack, malicious code and hybrid threat blocking.

Allows secure open transactions in a SOA environment which is an effective way to preserve network availability, reduce the burden on your IT resources and prevent security breaches.

Protects Email systems and the data that can leak from these systems

proventia™ Server Protection & Endpoint Security Control

Data Security -- Provides historical data that enables companies to find the origin of a change, breach or string of behavior

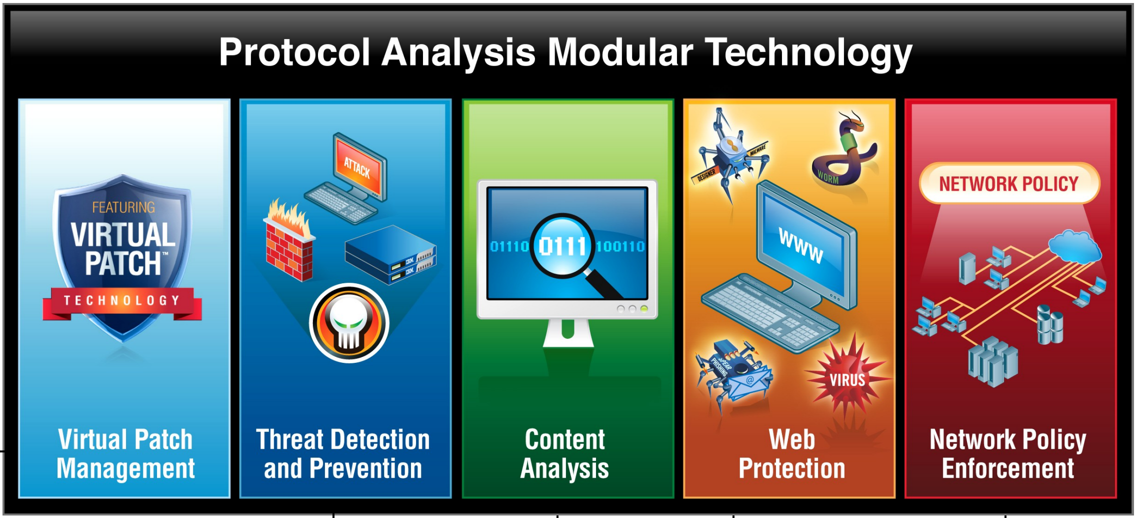
Compliance -- Provides the reporting necessary to prove the security of sensitive information

Future: Data Loss Prevention

IBM X-Force

Extensible Protection Platform

PAM is the engine behind the preemptive protection afforded by many of the solutions of the IBM Proventia product family. PAM is comprised of 5 key technologies.



Protocol Analysis Modular Technology

Virtual Patch

What It Does:
Shields vulnerabilities from exploitation independent of a software patch, and enables a responsible patch management process that can be adhered to without fear of a breach

Why Important:
At the end of 2008, **53%** of all vulnerabilities disclosed during the year had no vendor-supplied patches available to remedy the vulnerability

Threat Detection & Prevention

What It Does:
Detects and prevents entire classes of threats as opposed to a specific exploit or vulnerability.

Why Important:
Eliminates need of constant signature updates. Protection includes the proprietary Shellcode Heuristics (SCH) technology, which has an unbeatable track record of protecting against zero day vulnerabilities.

Content Analysis

What It Does:
Monitors and identifies unencrypted personally identifiable information (PII) and other confidential information for data awareness. Also provides capability to explore data flow through the network to help determine if any potential risks exist.

Why Important:
Flexible and scalable customized data search criteria; serves as a complement to data security strategy

Web Application Security

What It Does:
Protects web applications against sophisticated application-level attacks such as SQL Injection, XSS (Cross-site scripting), PHP file-includes, CSRF (Cross-site request forgery).

Why Important:
Expands security capabilities to meet both compliance requirements and threat evolution.

Network Policy Enforcement

What It Does:
Manages security policy and risks within defined segments of the network, such as ActiveX fingerprinting, Peer To Peer, Instant Messaging, and tunneling.

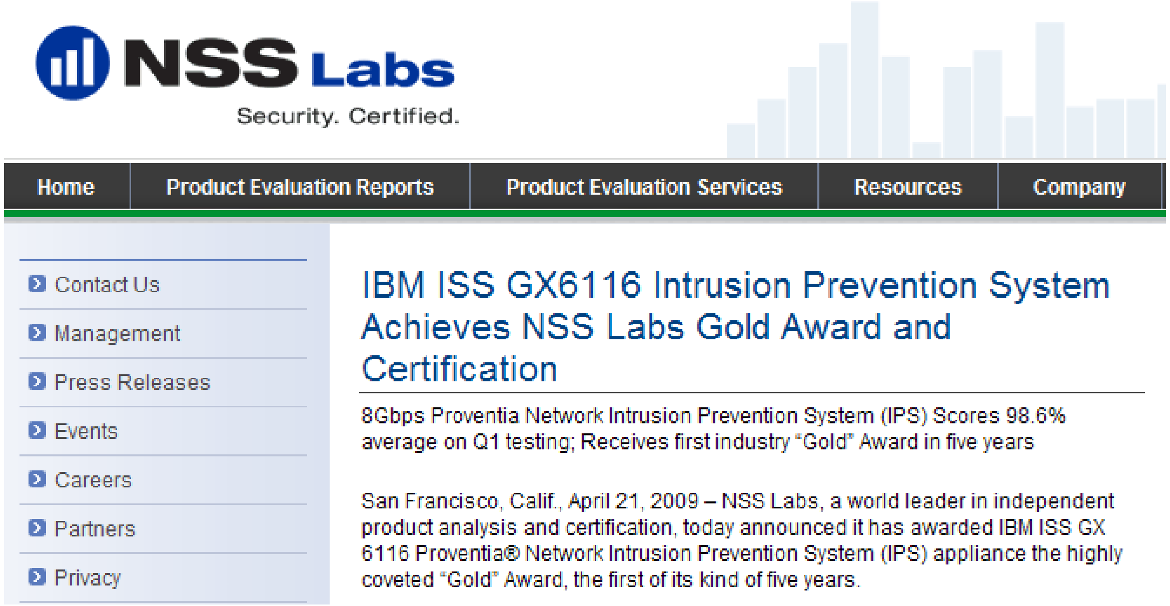
Why Important:
Enforces network application and service access based on corporate policy and governance.

© IBM Corporation 2009.

		Proventia GX				
Perfor-mance	Date of last NSS test	Monthly testing				
	NSS reported performance	8 Gbps				
Security Effectiveness	NSS reported security effectiveness rating	99.75%	99.4%	NA	39,7%	90.7%
	Protocols & data file formats inspected	206	?	?	?	?
	Vulnerability-based Blocking (Virtual Patch)	Since 2003	Limited	NA: reliant upon SNORT signature written to each exploit	Limited	NA
	Shellcode Heuristics	Since 2006	NA	NA	NA	NA
	Injection Logic Engine	Since 2007	NA	NA	NA	NA
	Session-based analysis for asymmetric routing	Since 2003	NA	NA	NA	NA
Extensible Protection	Web application security	Since Q2 2009	NA	NA	Paid service for custom policies	NA
	Data Security	Since Q1 2008	NA	NA	NA	NA
	Web Browser Exploit Prevention	Since 2008	NA	NA	NA	NA

© IBM Corporation 2009.

IBM Security Effectiveness: Validation from NSS



NSS Labs

Security. Certified.

IBM ISS GX6116 Intrusion Prevention System Achieves NSS Labs Gold Award and Certification

8Gbps Proventia Network Intrusion Prevention System (IPS) Scores 98.6% average on Q1 testing; Receives first industry "Gold" Award in five years

San Francisco, Calif., April 21, 2009 – NSS Labs, a world leader in independent product analysis and certification, today announced it has awarded IBM ISS GX 6116 Proventia® Network Intrusion Prevention System (IPS) appliance the highly coveted "Gold" Award, the first of its kind of five years.

http://nsslabs.com/2008/ibm-iss-gx6116-intrusion-prevention-system-achieves-nss-labs-gold-award-and-certification.html

Percentage decreased because IBM requested that the test be made more difficult for vendors.

sting

ly testing

s against

g threat landscape

Aug 2009	95%
Jul 2009	98%
Jun 2009	100%
May 2009	100%
Apr 2009	100%
Mar 2009	99%
Feb 2009	100%
Jan 2009	100%
Dec 2008	100%
Nov 2008	100%

http://nsslabs.com/IBM

NSS Labs GOLD

First IPS to receive NSS Gold Award in 5 years

Only vendor to win a Gold award every quarter in 2009

NSS Labs GOLD NSS Labs GOLD NSS Labs GOLD

© IBM Corporation 2009.

IBM Security Virtual Server Protection for VMware

Integrated threat protection and security compliance for VMware vSphere™ 4

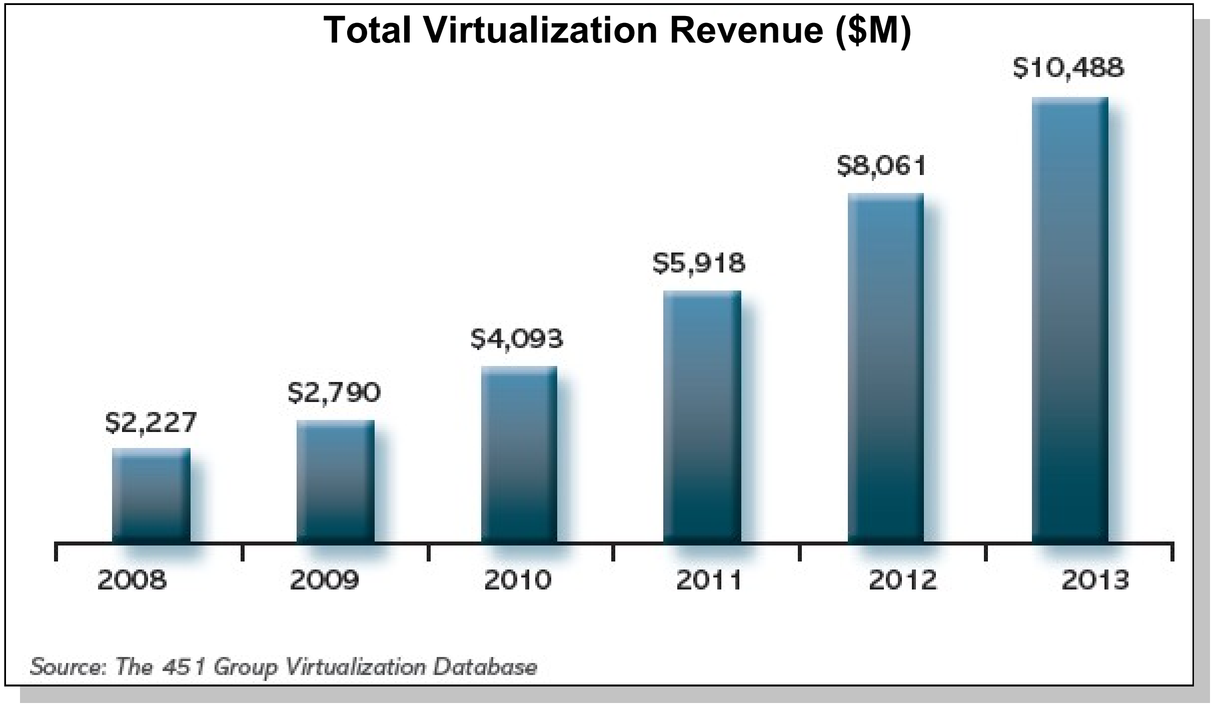
© IBM Corporation 2009.

Virtualization adoption is growing at a tremendous rate

"Virtualization has become a key weapon in CIO arsenals."

- Forrester Research, Inc

"Virtualization will be a cornerstone technology … to support the business needs of the next economic cycle" - IDC



Source: The 451 Group Virtualization Database

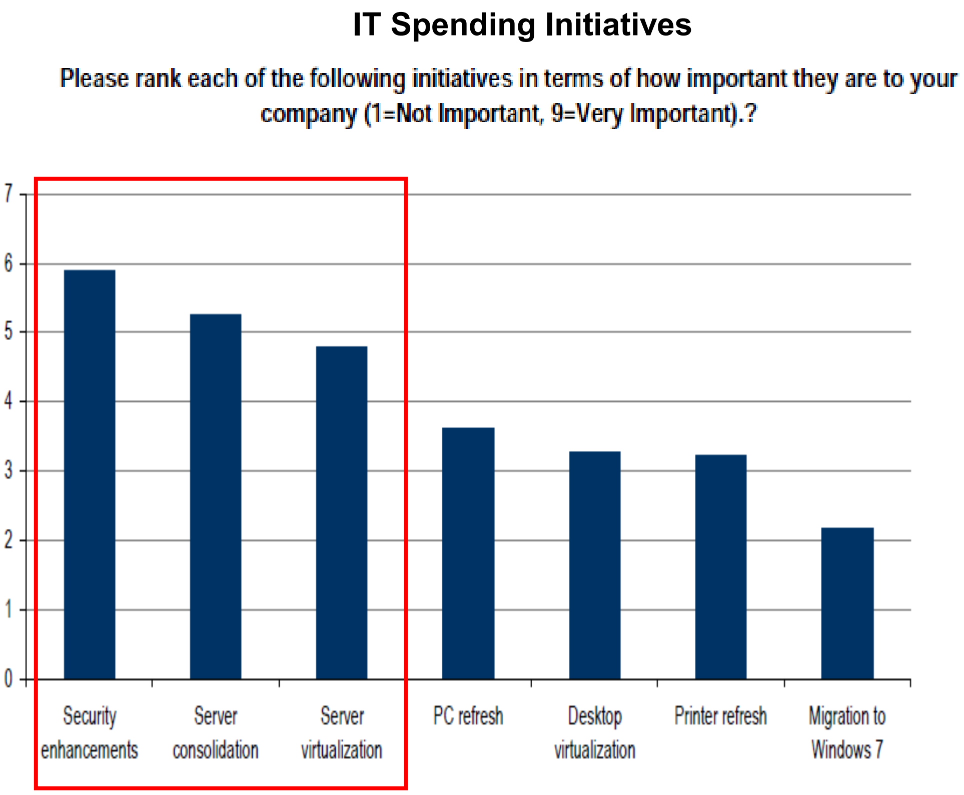
© IBM Corporation 2009.

IT Spending Initiatives Lead to Security

Security enhancements, consolidation and virtualization are ranked high as a key investment priorities

> "To secure virtual infrastructure, the usual security principles must be applied: defense in depth, network design and segmentation, and unified security management."
>
> -451 Group

> "[Virtualization security] will grow at a CAGR of 87% through 2013 – the most aggressive growth forecast for any sector."
>
> -451 Group



IT Spending Initiatives

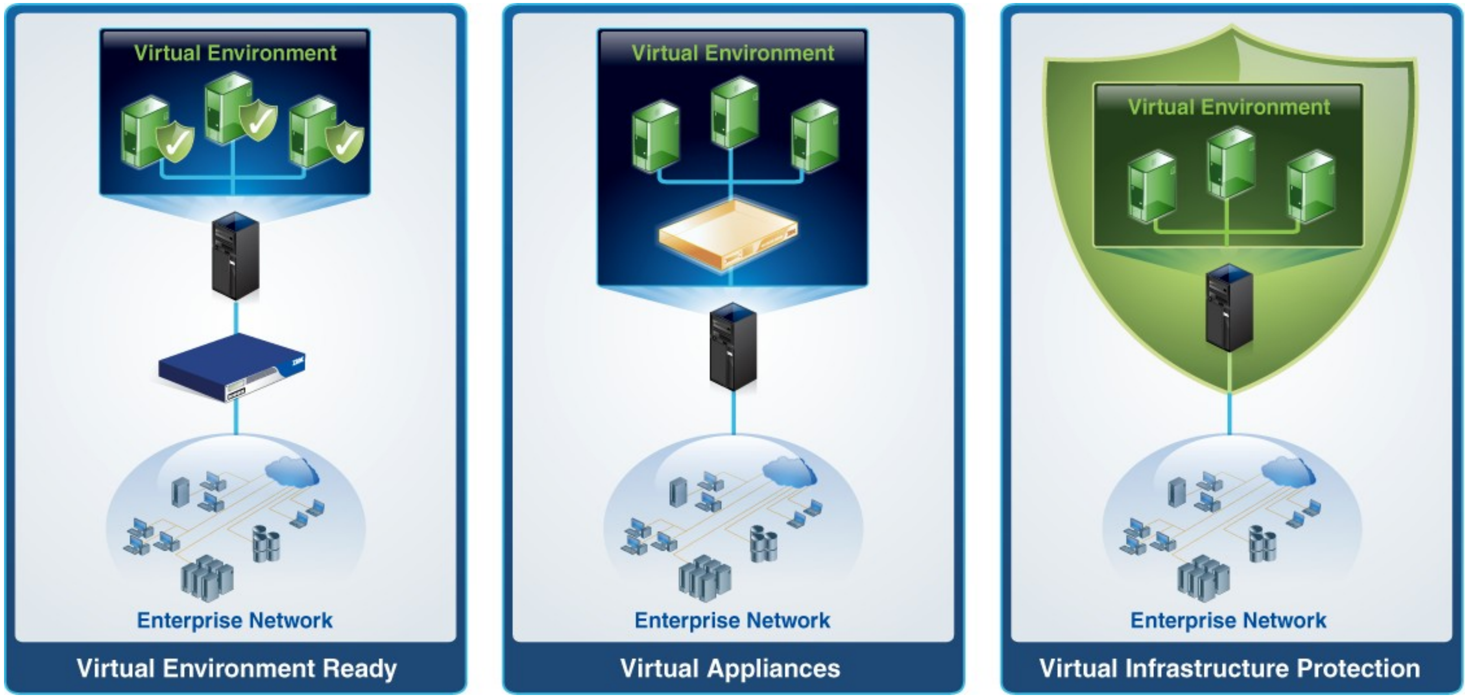
Please rank each of the following initiatives in terms of how important they are to your company (1=Not Important, 9=Very Important).?

Source: IBM GTS Market Insights Analysis based on Goldman Sachs,"IT Spending Survey: Top of mind-Virtualization/PC refresh," September 7, 2009; Bank of America / Merril Lynch, "Spending Intentions Still Muted, Slightly Less Cautious", July 20, 2009

© IBM Corporation 2009.

IBM ISS Virtualization Solutions: Past, Present and Future

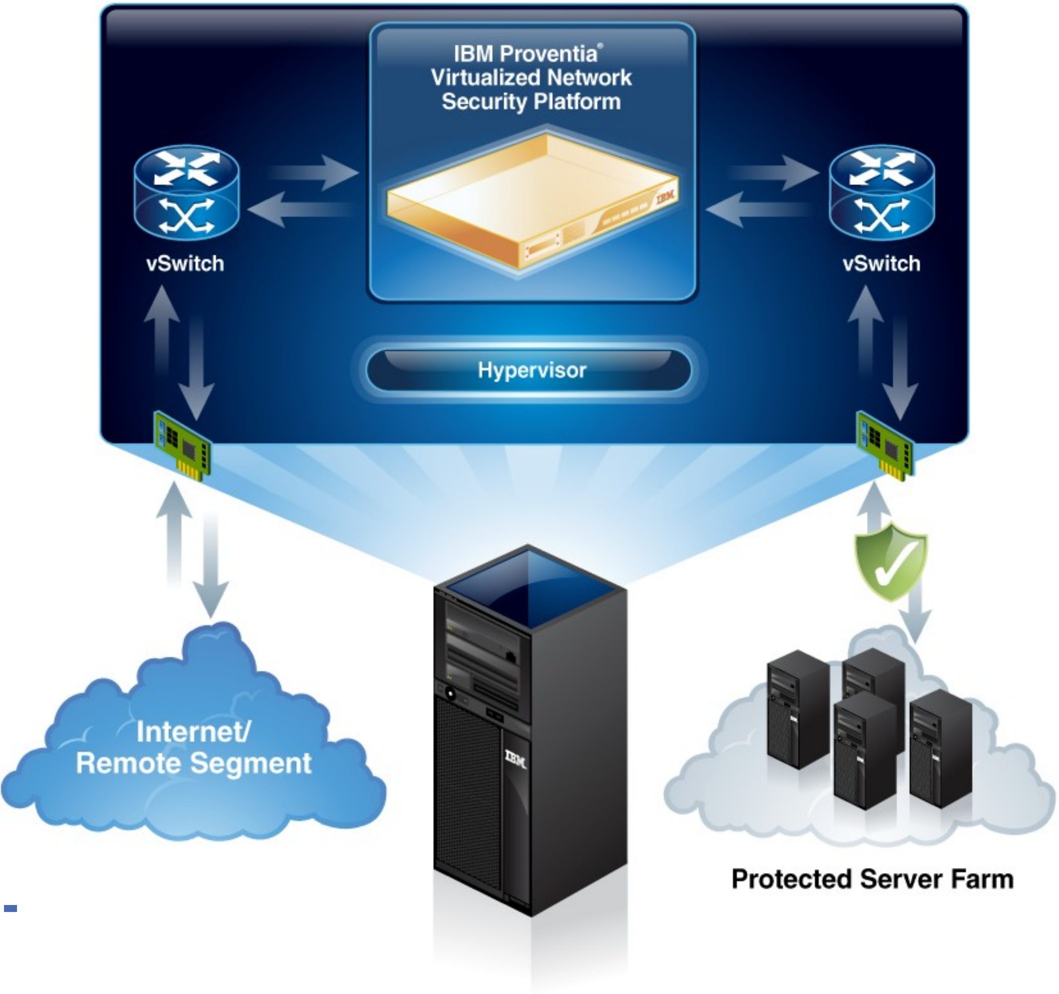
- Current Solution protects the Virtual Systems using our current HIPS portfolio
- The Virtual Proventia NIPS gives you the flexibility to protect traffic inside the virtual environment
- Hypervisor HIPS brings perimeter protection to the virtual environment



© IBM Corporation 2009.

Virtual appliance protects physical network segments

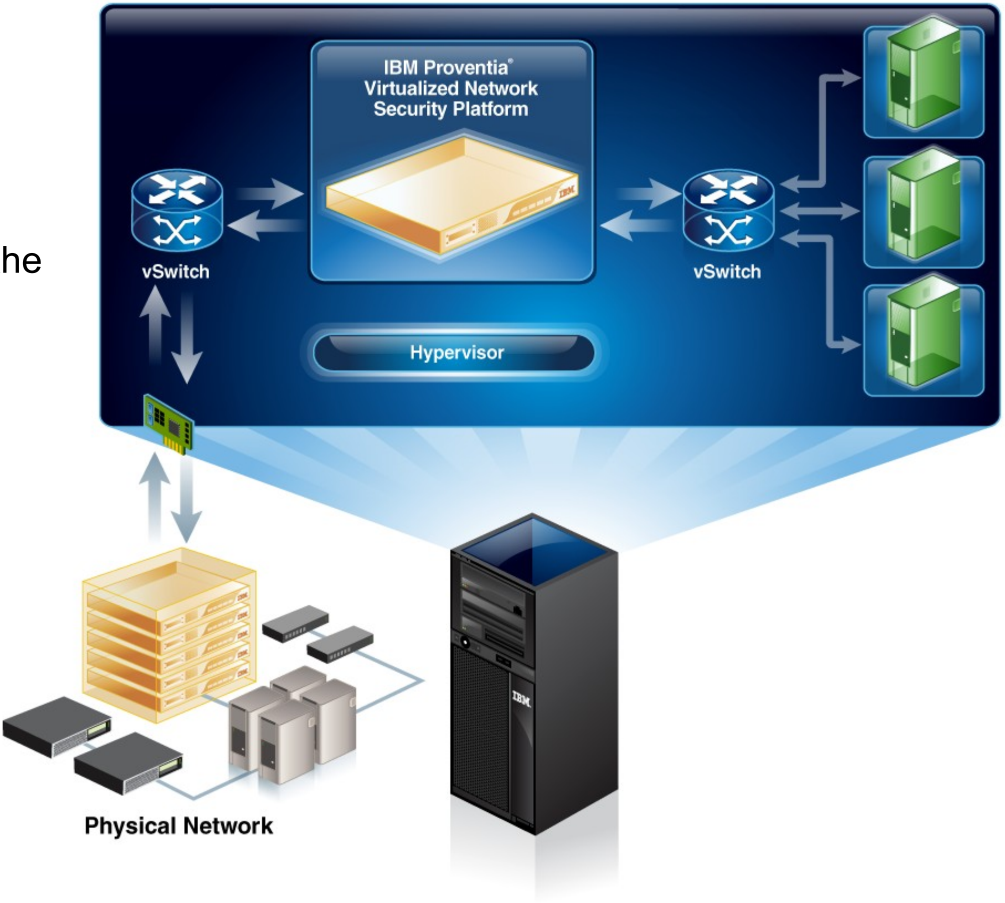
- **Use virtualization to deliver X-Force powered protection**
  - Preinstalled and preconfigured network protection packaged as a VM
- **Best of breed security & the benefits of virtualization**
  - Scalable and consume less power than physical appliances (GREEN)
  - Leverage existing virtualized infrastructure to deploy security solutions
- **Lowered complexity with centralized operations**
  - Managed the same as all Proventia products
  - Manage virtual security with same platform
- **Upgrade from previous software-based IDS solutions**



© IBM Corporation 2009.

Virtual appliance protects virtual network segments

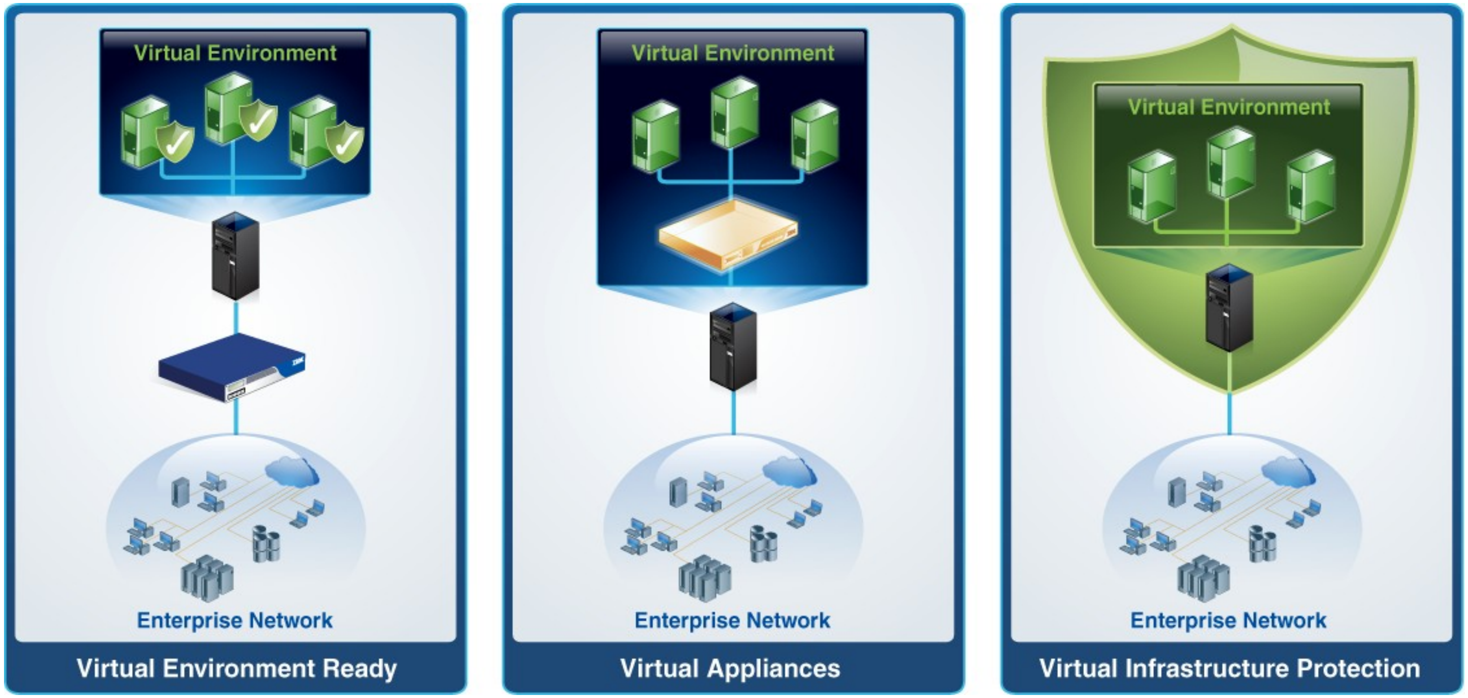
- **Protection for virtual network segments**
  - Intrusion prevention and network protection for traffic between vSwitches
  - X-Force powered protection for all traffic to the virtual machines
- **Self contained solution**
  - Protection without any alteration to server images, virtual servers or applications
  - Security delivered without integrating with the virtual infrastructure
- **With security in place, accelerate virtualization adoption for critical applications**
  - X-Force dedicated research
  - Apply and enforce a consistent security of VMs in your dynamic environment
- **Integrate and manage virtual security with traditional network security**
  - Single management console
  - Shared security policies across virtual and physical appliances



© IBM Corporation 2009.

IBM ISS Virtualization Solutions: Past, Present and Future

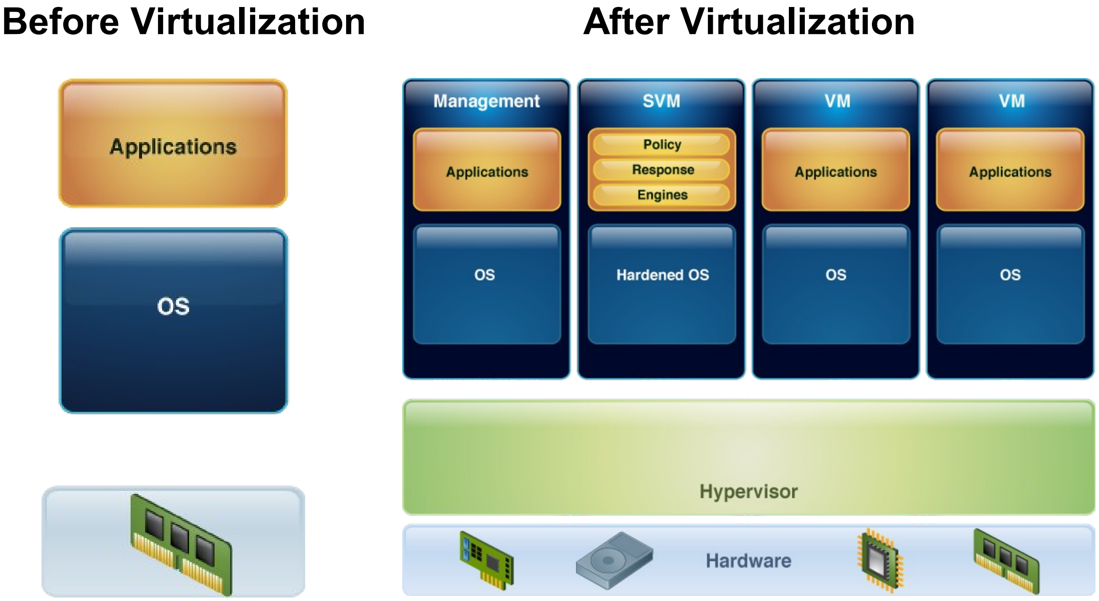
- Current Solution protects the Virtual Systems using our current HIPS portfolio
- The Virtual Proventia NIPS gives you the flexibility to protect traffic inside the virtual environment
- Hypervisor HIPS brings perimeter protection to the virtual environment



Security Challenges with Virtualization: New Complexities

New complexities

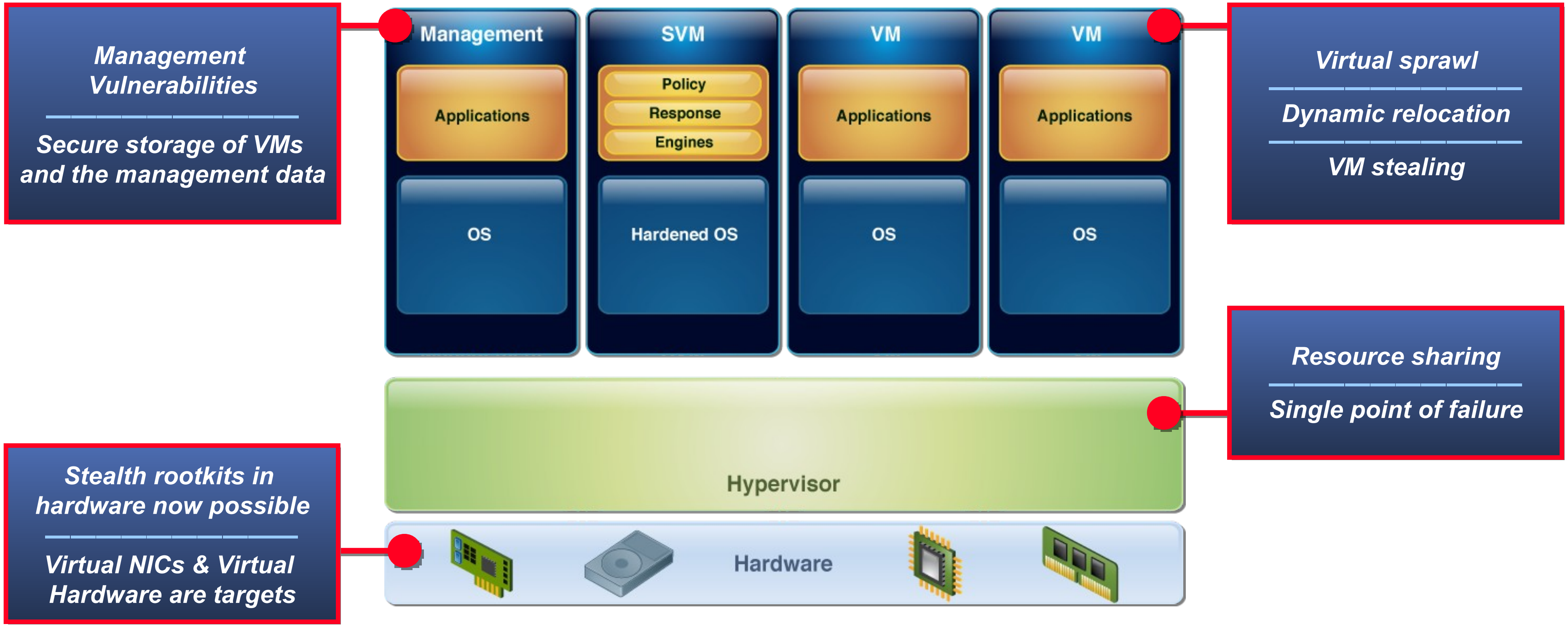
- Dynamic relocation of VMs
- Increased infrastructure layers to manage and protect
- Multiple operating systems and applications per server
- Elimination of physical boundaries between systems
- Manually tracking software and configurations of VMs



- 1:1 ratio of OSs and applications per server

- 1:Many ratio of OSs and applications per server
- Additional layer to manage and secure

Security Challenges with Virtualization: New Risks



Management Vulnerabilities

Secure storage of VMs and the management data

Virtual sprawl

Dynamic relocation

VM stealing

Resource sharing

Single point of failure

Stealth rootkits in hardware now possible

Virtual NICs & Virtual Hardware are targets

© IBM Corporation 2009.

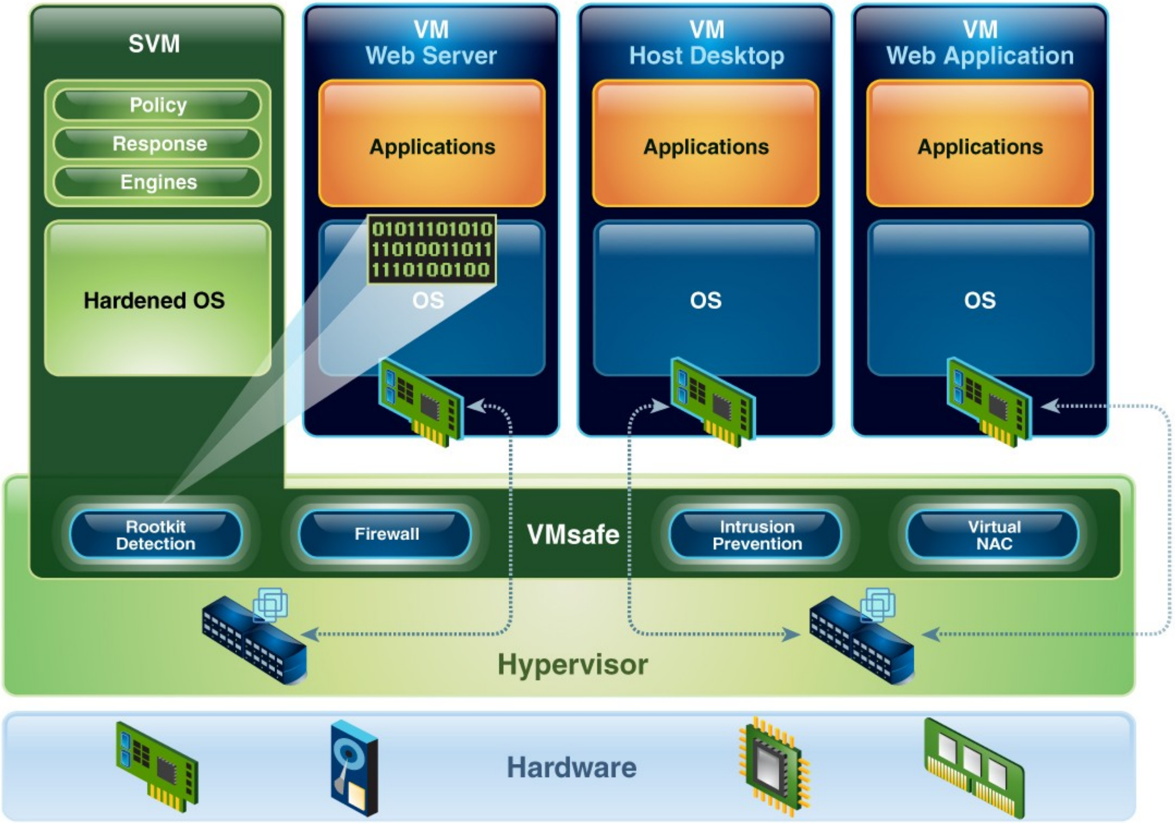
Security Challenges with Virtualization: Using traditional security for a virtual data center may add cost and complexity

Legacy Security in Virtual Environment

	Seems Secure …	… Not Secure Enough
Network IPS	Only blocks threats and attacks at the perimeter	Should protect against threats at perimeter <u>and</u> between VMs
Server Protection	Secures each physical server with protection and reporting for a single agent	Securing each VM as if it were a physical server adds time and cost
System Patching	Patches critical vulnerabilities on individual servers and networks	Needs to track, patch and control VM sprawl
Security Policies	Policies are specific to critical applications in each network segment and server	Policies must be more encompassing (Web, data, OS coverage, databases) and be able to move with the VMs

Virtual Server Security for VMware enables customers to realize the benefits of virtualization without reducing their security posture

- Provides dynamic protection for every layer of the virtual infrastructure
  - Hypervisor
  - Operating System
  - Network
  - Applications
  - Virtual machine (VM)
  - Inter-VM traffic



© IBM Corporation 2009.

IBM offers the broadest, most integrated, defense-in-depth virtualization security with *one product*

Feature	VSS	Altor	Reflex	Trend	McAfee
Firewall	✓	✓	✓	✓	✓
Rootkit Detection					
Hypervisor-Level (VMsafe) Integration	✓		✓		
Intrusion Prevention	✓			✓	
Intrusion Detection	✓	✓	✓	✓	
Virtual Patch	✓				
Visibility into Virtual Network Activity	✓	✓	✓		
Virtual Network Segment Protection	✓				
VM Sprawl Management	✓	✓	✓		
Central Management	✓	✓	✓		✓
Web Application Protection	✓			✓	
Inter-VM Traffic Analysis	✓	✓	✓		

Business Partner Benefits & Pricing

- Pricing
  - –Product
    - €4,040.20 EUR - SVPV-BASE-1-P (SVPV-BASE-1-P) License for 2 Processors
    - €1,613.70 EUR - SVPV-ADD-1-P (SVPV-ADD-1-P) License for Addl 2 Processors
  - –Maintenance
    - €808.04 EUR - SVPV-BASE-1-P-M (SVPV-BASE-1-P-M) for 2 Processors
    - €322.74 EUR - SVPV-ADD-1-P-M (SVPV-ADD-1-P-M) for Addl 2 Processors

- Benefits
  - –Partners can mine leads from install base of VMware sales
  - –Selling a data center solution will ***drive more revenue for you!!***
    - Virtual Server Security for VMware provides sellers with the opportunity to generate ***recurring revenue with each software agent license*** sold with yearly maintenance contracts
      - –Creates additional opportunities to visit with customer
      - –Creates up-sell/cross-sell opportunities
      - –Improves customer satisfaction
  - –Business Partners must be ISS authorized

Kundenprofil Zielkunden

- Kunden mit bestehender oder geplanter VMware Umgebung
- 5+ VMware Hosts
- Grundverständnis für IT-Security muss vorhanden sein
- Gute Chancen bei Neuprojekten / Erweiterungen

© IBM Corporation 2009.

Fragen

- Wie haben sie Ihre IT-Security in der VMware Umgebung realisiert?
- Nutzen sie das volle Einsparungspotential von Virtualisierung?
- Haben sie Teile Ihrer Infrastruktur aus Sicherheitsgründen noch nicht virtualisiert?
- Haben sie den Heise-Ticker (o.ä.) bezüglich Sicherheitsbedenken in virtualisierten Umgebungen verfolgt?
- Wie schätzen sie das Risiko von Virtualisierung ein?
- Haben sie versucht Ihre traditionelle IT-Security in virtuellen Umgebungen nachzubilden?
- Wie haben sie die Security Herausforderungen in virtuellen Umgebungen gelöst?

Beispielprojekt 1:

- Kunde: Gehobener Mittelstand Automotive
- Anforderung: Keine Kommunikation zwischen virtuellen Servern
- Volumen:
  - 4 Server mit je 4 Quad Prozessoren
  - 17K Softwareumsatz
  - Plus Beratungsleistung, Installation und Dokumentation
- Vorteil für Kunde:
  - Geringere Hardwarekosten
  - Anforderung erfüllt
  - Bessere Transparenz
  - Reduzierung des unternehmerischen Risikos
  - BP bleibt Ansprechpartner auch für IT-Security

Beispielprojekt 2

- Kunde: Großkunde
- Anforderung: Compliance Issue lösen
- Volumen:
  - 170 Server mit je 4 Quad Prozessoren
  - 400K Softwareumsatz
  - Plus Beratungsleistung, Installation und Dokumentation
- Vorteil für Kunde:
  - Patchkosten reduziert
  - Anforderung erfüllt
  - Bessere Transparenz
  - Frühzeitige Erkennung von Fehlfunktionen
  - Reduzierung des unternehmerischen Risikos

© IBM Corporation 2009.

Peter Häufel – *Partner Account Manager*
IBM Security Solutions
haeufel@de.ibm.com
Tel: +49.175.7252260

Questions?