IBM

SERVICE & RISK MANAGEMENT FORUM 2011

Securing the Enterprise with IBM Security's Intrusion Protection Solutions

Robert Giberson
Security Architect & X-Force Field Liaison
IBM Security Solutions

Agenda

- X-Force (Brief Recap)
- Drivers of Next Generation Intrusion Prevention
- Emerging Requirements for Intrusion Prevention Systems
- Meeting the Needs of our Clients: Introducing IBM Security's Intrusion Prevention Products
- Questions

SERVICE & RISK MANAGEMENT FORUM 2011

Mission

IBM

To protect our customers from security threats on the Internet by developing a comprehensive knowledge of vulnerabilities and attack methodologies and applying that knowledge through effective protection technologies.

IBM X-Force Research and Development

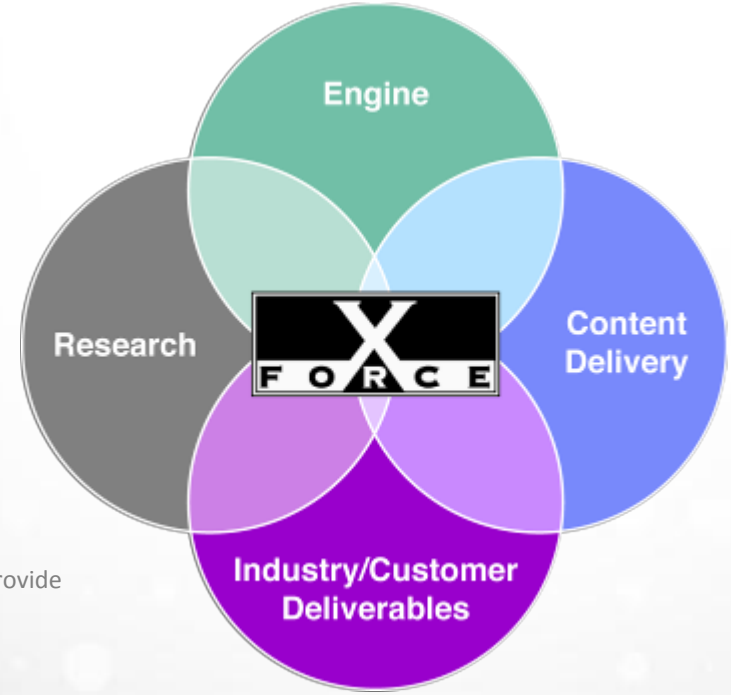
The world's leading enterprise security R&D organization

Engine

- Support content stream needs and capabilities
- Support requirements for engine enhancement
- Maintenance and tool development

Research

- Support content streams
- Expand current capabilities in research to provide industry knowledge to the greater IBM



Global security operations center (infrastructure monitoring)

Content Delivery

- Continue third party testing Dominance
- Execute to deliver new content streams for new engines

Industry/Customer Deliverables

- Blog, Marketing and Industry Speaking Engagements
- X-Force Database Vulnerability Tracking
- Trend Analysis and Security Analytics

The Value of Security Research

Without security researchers we would always be one step *behind* the threat…

Ahead of the Threat – In order to stay one step ahead of the bad guys, you have to understand the vulnerabilities that are being exploited.

Bugs – Security researchers often find bugs before the bad guys do, allowing them to provide protection to customers before vendors have time to deploy a patch.

Understanding the Threat Landscape – By studying the different attack techniques and obfuscation techniques that the bad guys are using – vendors ultimately use this research to create protections that can be less evadable, more apt to detect Botnets and Malware, APT style attack patterns, and new attack techniques.

The Value of Security Research

Research → **Technology** → **Solutions**

- Original Vulnerability Research
- Public Vulnerability Analysis
- Malware Analysis
- Threat Landscape Forecasting
- Protection Technology Research

X-Force Protection Engines

- Extensions to existing engines
- New protection engine creation

X-Force XPU's

- Security Content Update Development
- Security Content Update QA

X-Force Intelligence

- X-Force Database
- Feed Monitoring and Collection
- Intelligence Sharing

Only IBM Security is backed by the IBM X-Force®

Drivers Influencing IPS Evolution

- **IPv6** – Deployments of IPv6 networks (and heterogeneous IPv4+IPv6) are picking up speed.
- **Vulnerabilities and Exploits** – The number of vulnerabilities and public exploits being disclosed is increasing each year.
  - IPS must use more behavioral and anomaly detection and less pattern matching.
- **Obfuscation** – Increases in the obfuscated web pages and files.
  - Obfuscation detection will continue to evolve in IPS.
- **Evasions** – New evasion techniques will continue to be discovered
- **Applications** – The number of web applications will continue to increase
  - Application identification, control (allow/deny), and QoS will be important.
- **Encryption** – Use of SSL and other encryption methods will continue to be used more by both good and bad guys.
  - Inspection of encrypted packets will become standard
- **Compound Documents** and **Container Files** – Increasingly used in attacks.
  - The need to look “inside” of PDF files and Office documents

Critical Factors for IPS

Performance – 20 gigs and beyond.
- As networks grow larger and faster there will be a need for more speed
- As more technologies converge with IPS more bandwidth will be needed

Encryption – The use of SSL and encryption is increasing among both the good guys and the bad guys
- SSL inspection in IPS is going to be standard

Flexibility – A default configuration is rarely useful.
- Every network is different. Flexibility in tuning is critical in making an IPS usable.

Behavioral Inspection – Beyond Pattern Matching.
- Behavioral deep packet inspection protocol decodes will continue to be more important.
- Attackers are hiding their exploit code inside of compound files and container files, making simple pattern matching IPS techniques less useful.

Web Applications – We certainly see the volume of web applications increasing.
- Applications are using HTTP/HTTPS. Being able to identify and allow/deny those applications will is important today, and will be more important in the years to come.

IBM Security Protocol Analysis Module
Addressing Today's Evolving Threats

How it Works

- Deep inspection of network traffic
- Identifies & analyzes >250 network and application layer protocols and data file formats

What it Prevents

- Worms
- Spyware
- P2P
- DoS/DDoS
- Cross-site Scripting
- SQL Injection
- Buffer Overflow
- Web Directory Traversal

Protocol Analysis Module (PAM)

Vulnerability Modeling & Algorithms	RFC Compliance
Stateful Packet Inspection	TCP Reassembly & Flow Reassembly
Protocol Anomaly Detection	Statistical Analysis
Port Variability	Host Response Analysis
Port Assignment	IPv6 Native Traffic Analysis
Port Following	IPv6 Tunnel Analysis
Protocol Tunneling	SIT Tunnel Analysis
Application-Layer Pre-Processing	Port Probe Detection
Shellcode Heuristics	Pattern Matching
Context Field Analysis	Custom Signatures
Proventia Content Analyzer	Injection Logic Engine

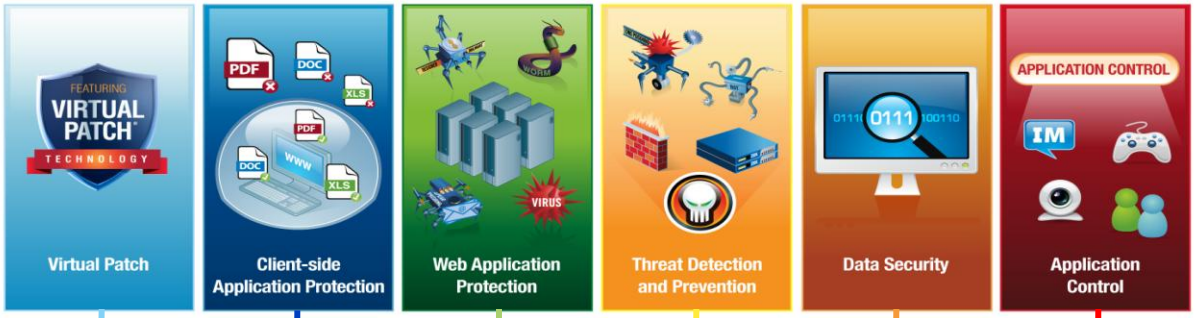
SERVICE & RISK MANAGEMENT FORUM 2011

Protocol Analysis Module

IBM

Intrusion prevention just got smarter with extensible protection backed by the power of X-Force

IBM 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 2009, **52%** of all vulnerabilities disclosed during the year had no vendor-supplied patches available to remedy the vulnerability.

Client-Side Application Protection

What It Does:
Protects end users against attacks targeting applications used everyday such as Microsoft Office, Adobe PDF, Multimedia files and
Web browsers.

Why Important:
At the end of 2009, vulnerabilities, which affect personal computers, represent the second-largest category of vulnerability disclosures and represent about a fifth of all vulnerability disclosures.

Web Application Protection

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.

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.

Data Security

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.

Application Control

What It Does:
Manages control of unauthorized applications 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.

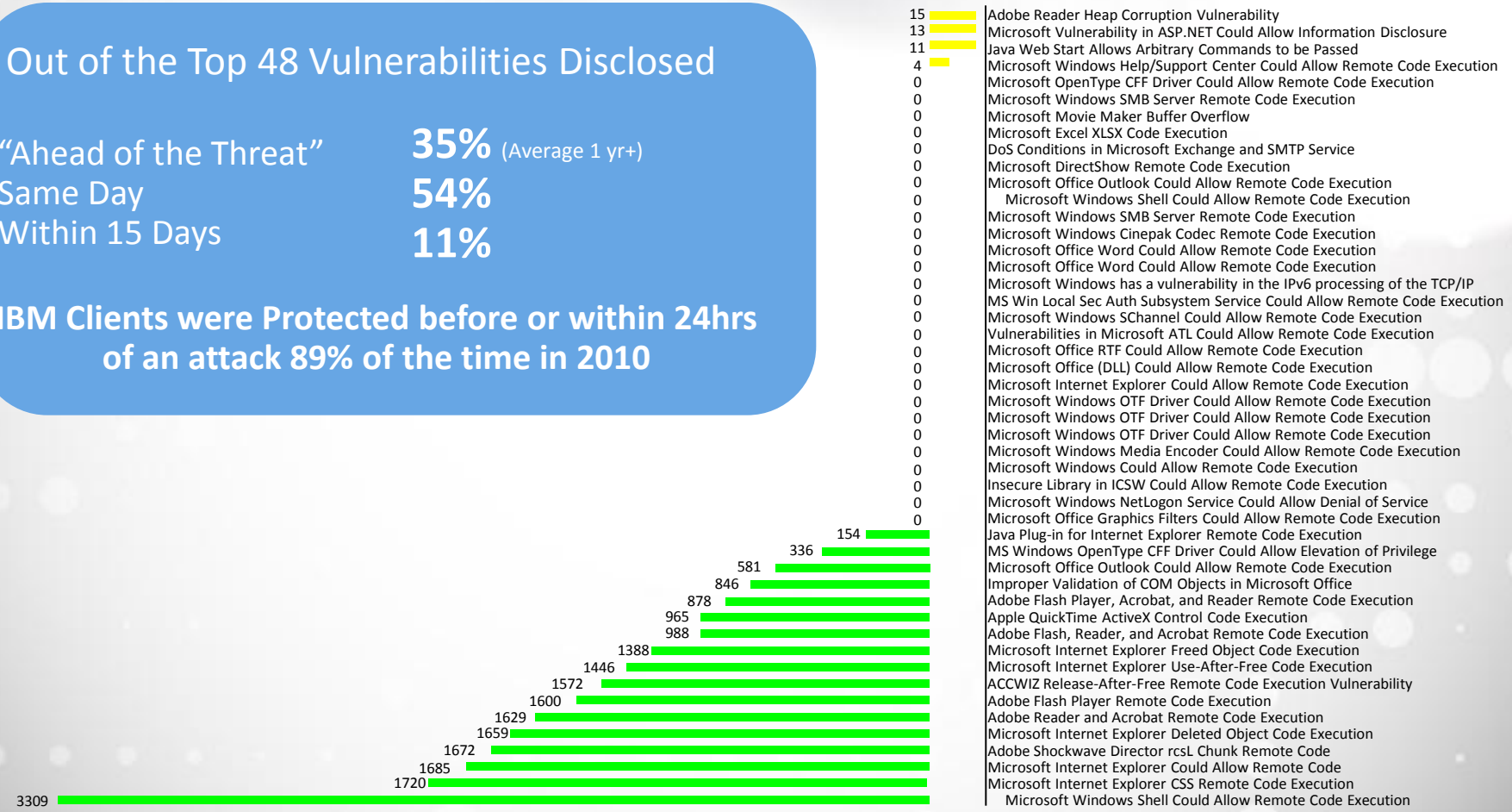
IBM Delivers Real-World Security Effectiveness

Protecting our Clients "Ahead of the Threat" in 2010 and Beyond

Out of the Top 48 Vulnerabilities Disclosed

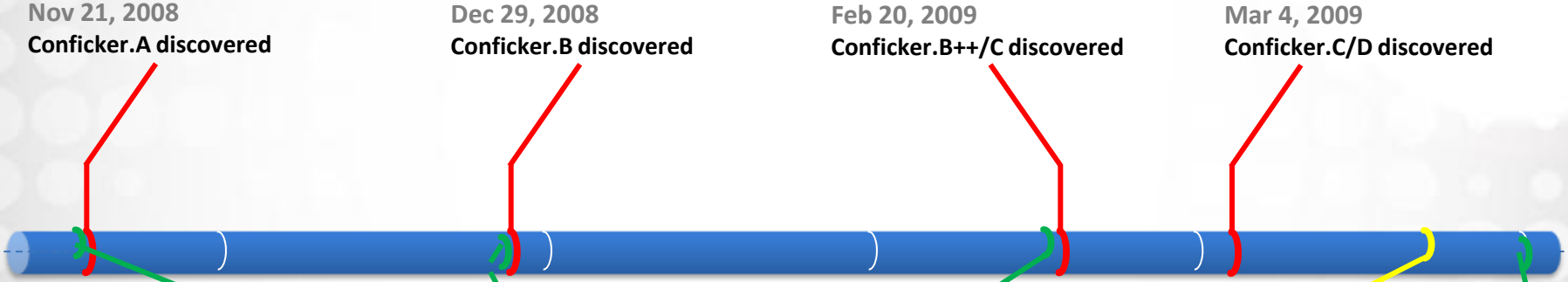
"Ahead of the Threat"	**35%** (Average 1 yr+)
Same Day	**54%**
Within 15 Days	**11%**

IBM Clients were Protected before or within 24hrs of an attack 89% of the time in 2010



Source: IBM X-Force

Ahead of the Threat: Conficker



SERVICE & RISK MANAGEMENT FORUM 2011

Ahead of the Threat: Aurora

IBM

X-FORCE

2006
Pre-emptive "Behavioral" Decodes Developed by X-Force

December, 2009
APT Style Attack
Operation Aurora discovered

Jan 21, 2010
Microsoft Issues Patch

APR-09

Pre-emptive IBM X-Force coverage
Behavioral Decodes
Javascript_Shellcode_Detected
since Mar 28, **2006**
HTML_IE_Script_Error_Code_Execution
since Dec 13, **2006**

Pre-emptive IBM X-Force coverage
Behavioral Decodes
Javascript_Large_Unescape
since Jan 8, 2008
Javascript_Unescape_Obfuscation
since Jan 8, 2008

Pre-emptive IBM ISS coverage
Behavioral Decodes
HTML_Script_Extension_Evasion
since Jul 14, 2009
Javascript_Byte_Splitting
since Sep 8, 2009

IBM IPS Zero Day (Vuln/Exploit) Web App Performance

- IBM IPS Injection Logic Engine has stopped every large scale SQL injection or XSS attack day-zero.
  - Asprox – reported 12/11/2008 – stopped 6/7/2007
  - Lizamoon – reported 3/29/2011 – stopped 6/7/2007
  - SONY (published) – reported May/June/2011 – stopped 6/7/2007
  - Apple Dev Network – reported July/2011 – stopped 6/7/2007

New Vulnerability or Exploit	Reported Date	Ahead of the Threat Since
Nagios expand cross-site scripting	5/1/2011	6/7/2007
Easy Media Script go parameter XSS	5/26/2011	6/7/2007
N-13 News XSS	5/25/2011	6/7/2007
I GiveTest 2.1.0 SQL Injection	6/21/2011	6/7/2007
RG Board SDQL Injection Published:	6/28/2011	6/7/2007
BlogiT PHP Injection	6/28/2011	6/7/2007
IdevSpot SQL Injection (iSupport)	2011-05-23	6/7/2007
2Point Solutions SQL Injection	6/24/2011	6/7/2007
PHPFusion SQL Injection	1/17/2011	6/7/2007
ToursManager PhP Script Blind SQli	2011-07-xx	6/7/2007
Oracle Database SQL Injection	2011-07-xx	6/7/2007
LuxCal Web Calendar	7/7/2011	6/7/2007
Apple Web Developer Website SQL	2011-07-xx	6/7/2007
MySQLDriverCS Cross-Param SQLi	6/27/2011	6/7/2007

Introducing
IBM Security Network IPS

Key Pain Points

- Balance security and performance of business critical applications
- Address changing threats with limited expertise, resources, and budget
- Reduce cost and complexity of security infrastructure
- Larger organizations require security at network core

IBM Security Network Intrusion Prevention GX7800 is the newest addition to IBM's market-leading portfolio of Intrusion Prevention security appliances

Core Capabilities

Beyond traditional network IPS
to deliver comprehensive security including:

- Web application protection
- Protection from client-side attacks
- Data Loss Prevention (DLP)
- Application control
- Virtual Patch technology

Unmatched Performance delivering 20Gbps+ of throughput and 10GbE connectivity without compromising breadth and depth of security

Evolving protection powered by world renowned X-Force research to stay "ahead of the threat"

Reduced cost and complexity through consolidation of point solutions and integrations with other security tools

Intrusion Prevention Solutions that Fit your Needs

- Block threats before they impact your organization
- Uncompromising security backed by X-Force®
- Inspected throughput from 200 Mbps to 20Gbps+
- Protection for up to 8 network segments
- Scale from remote offices to the network core

GX7800 and GX7412

IBM Security Network IPS Models

	Remote	Perimeter			Core				
Model	GX4004-200	GX4004	GX5008	GX5108	GX5208	NEW GX7412-5	NEW GX7412-10	NEW GX7412	NEW GX7800
Inspected Throughput	200 Mbps	800 Mbps	1.5 Gbps	2.5 Gbps	4 Gbps	5 Gbps	10 Gbps	15 Gbps	20 Gbps+
Protected Segments	2	2	4	4	4	8	8	8	4

IBM Security Network IPS Deployment Flexibility

INLINE PREVENTION

- Active intrusion prevention
- Blocks malicious and unwanted traffic
- Allows legitimate traffic to pass unhindered

PASSIVE MONITORING

- Accurate intrusion detection
- Supports taps, hubs or SPAN ports
- Monitors traffic for malicious or unwanted traffic

INLINE SIMULATION

- Simulates inline prevention
- No Blocking
- Alerts to events it would have blocked

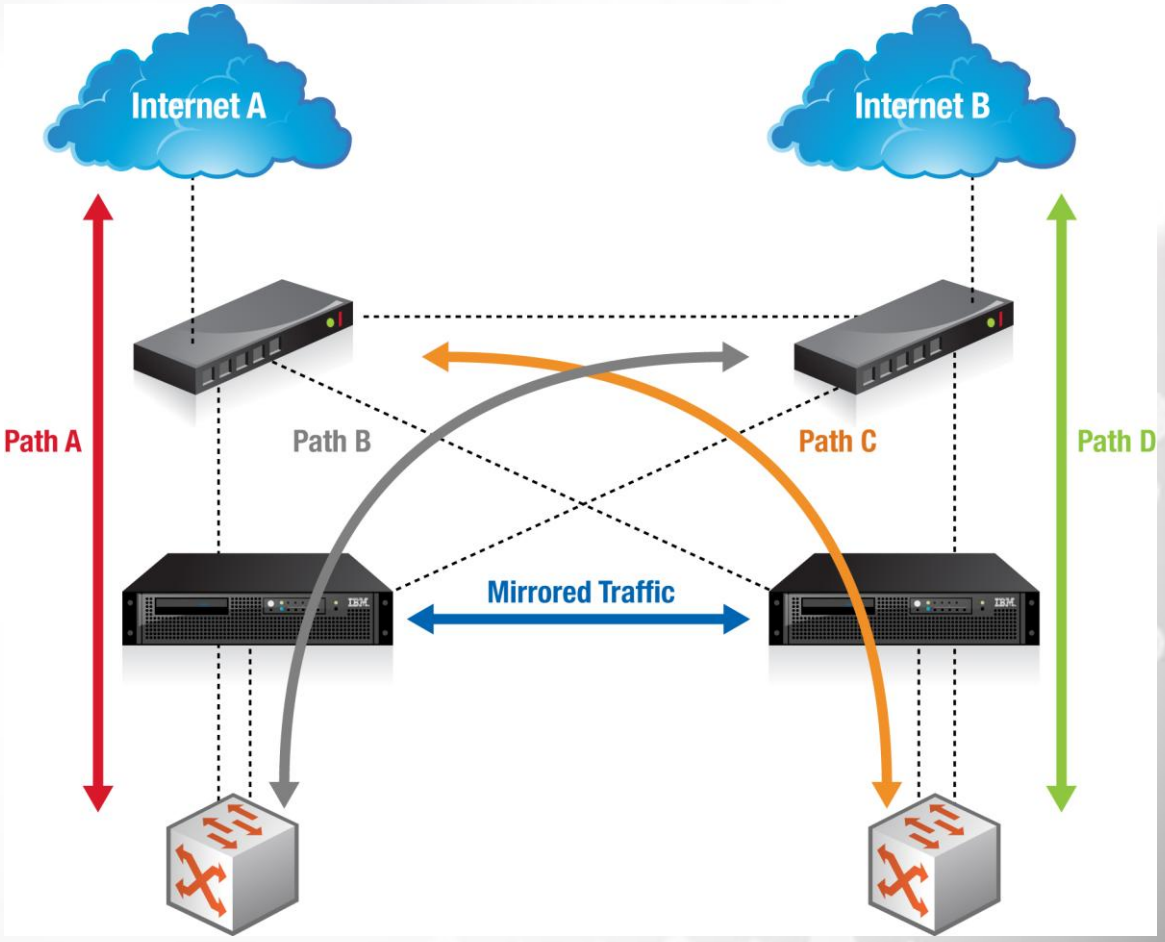
IBM Security Network IPS Availability and Reliability

High Availability

- Support for multiple configurations (Active/Active or Active/passive)
- Full state maintenance on failover
- Geographic high availability for fail-over to a geographically remote standby IPS device
- Hardware redundancy including power supplies, Hard drives, and cooling fans

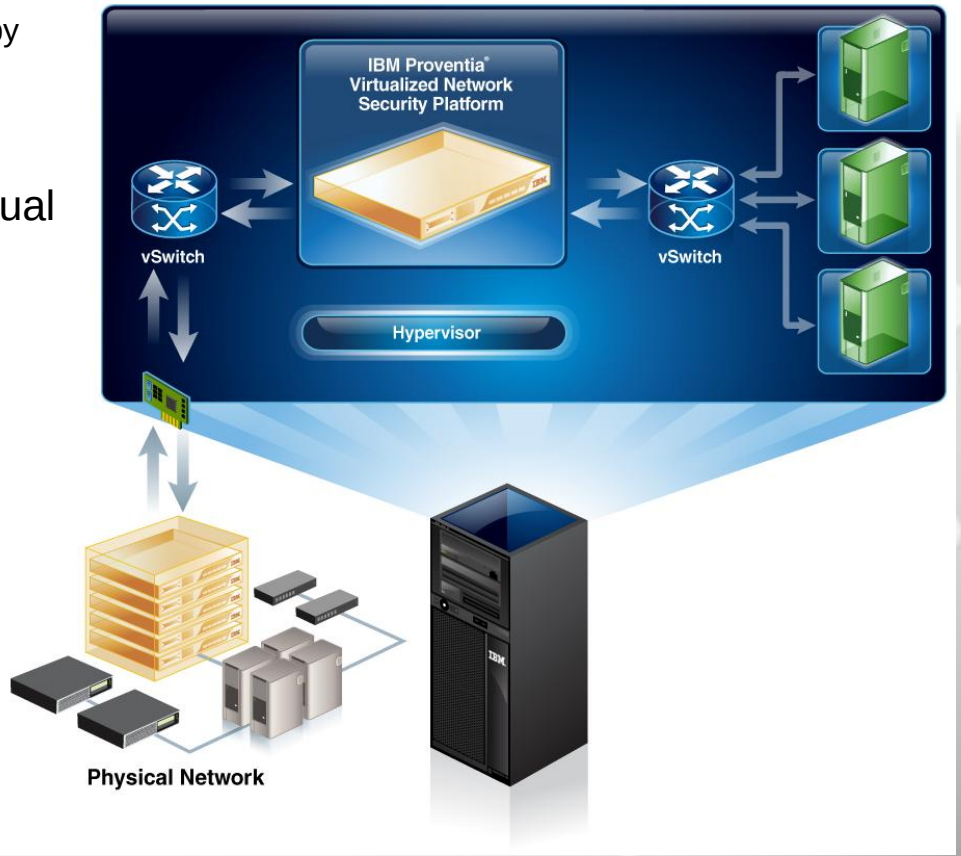
Automatic bypass allows all traffic to pass (fail open)

- Hardware failure
- Power failure
- Software crash



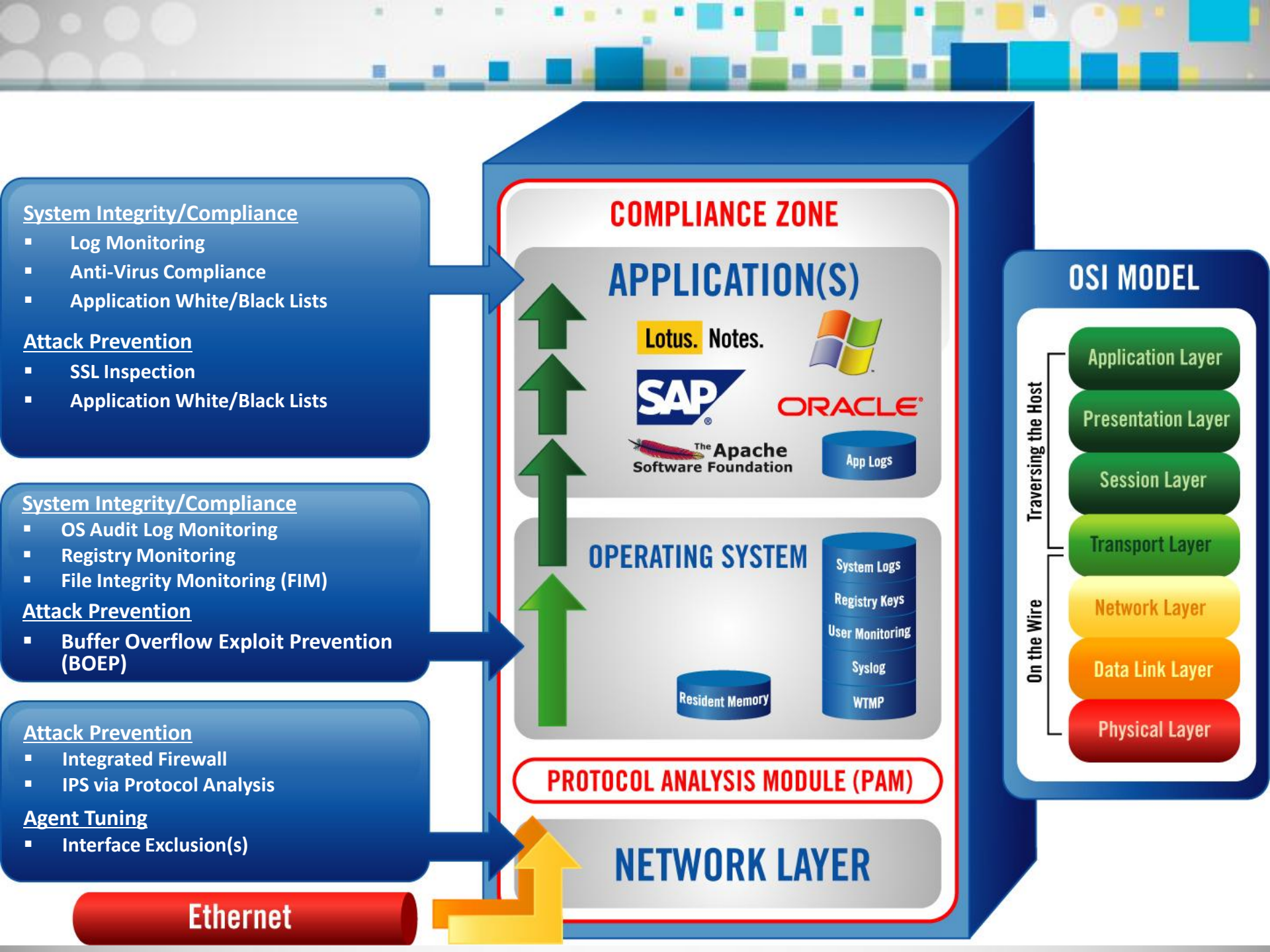
IBM Security Network Virtual IPS

- Market-leading network protection now available on virtual platform
  - World class, vulnerability-based protection powered by X-Force research
  - “Virtual appliance”
- Protection for VMWare ESX & ESXi 4.1 virtual environments
  - Intrusion prevention and network protection for traffic between vSwitches
  - Protect the virtual machines on a server
- Integrate and manage virtual security with traditional network security
  - Single management console
  - Shared security policies



IBM Host Protection

- Prevention Technologies ***(backed by X-Force)***
  - Firewall
  - Intrusion Prevention & Detection
  - Buffer Overflow Protection
  - Application Black & White Listing
  - SSL Inspection
- Compliance Technologies include:
  - Logging the Who, What, When and where of user activity
  - File Integrity Monitoring (FIM)
  - OS Auditing
  - Registry Integrity Monitoring
  - Anti-Virus Compliance
  - Third Party Log Monitoring


System Integrity/Compliance
Log Monitoring
Anti-Virus Compliance
Application White/Black Lists
Attack Prevention
SSL Inspection
Application White/Black Lists
System Integrity/Compliance
OS Audit Log Monitoring
Registry Monitoring
File Integrity Monitoring (FIM)
Attack Prevention
Buffer Overflow Exploit Prevention (BOEP)
Attack Prevention
Integrated Firewall
IPS via Protocol Analysis
Agent Tuning
Interface Exclusion(s)
Ethernet
COMPLIANCE ZONE
APPLICATION(S)
Lotus. Notes.
SAP
ORACLE
The Apache Software Foundation
App Logs
OPERATING SYSTEM
System Logs
Registry Keys
User Monitoring
Syslog
WTMP
Resident Memory
PROTOCOL ANALYSIS MODULE (PAM)
NETWORK LAYER
OSI MODEL
Traversing the Host
On the Wire
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer

Virtual Security Questions

- How many have deployed virtualization?
- Over 50% virtualized?
- Who is responsible for security in organization?
- Developed virtualization security plan before implementation?
- Have means to monitor and control intra-VM traffic?
- Have ability to control new VM deployment? (VM Sprawl)
- Maintain Separation of Duties?
- Quarantine new VM's until patched?

Business Drivers Behind Virtualization

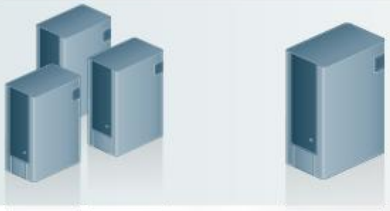
Virtualization drives down total cost of ownership and helps drive efficiency within the IT organization

Facilitate Physical Consolidation

Reduce the number of sites

Enable Cloud Computing

Reduce the number of servers

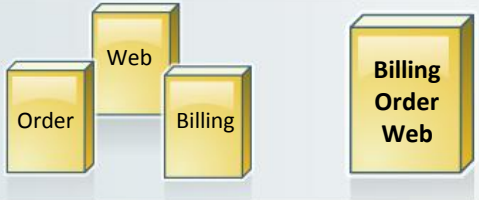


Achieve High Performance

Centralize data from different sources

Improve Service Levels

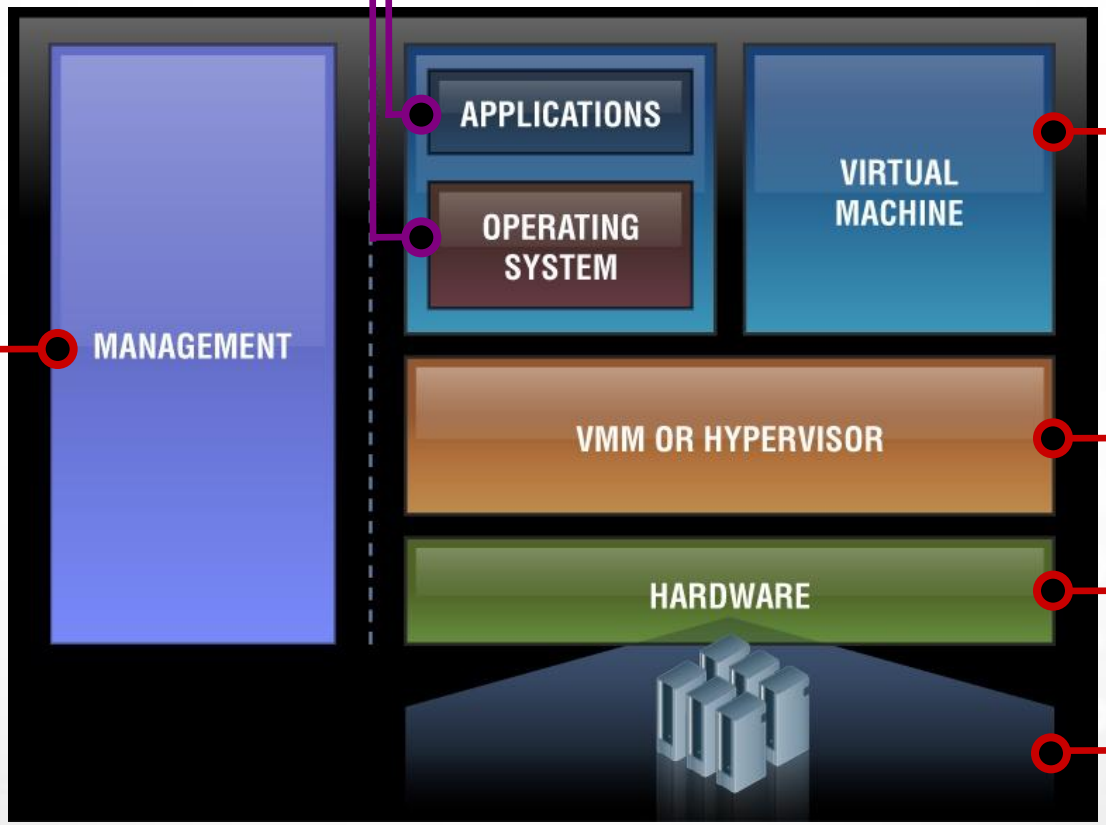
Increase application efficiency



Security Challenges with Virtualization

- Traditional Threats
- New threats to VM environments

Traditional threats can attack VMs just like real systems



Management Vulnerabilities
———————————
Secure storage of VMs and the management data
———————————
Requires new skill sets
———————————
Insider threat

Virtual server sprawl
———————————
Dynamic state/relocation
———————————
VM theft

Resource sharing
———————————
Single point of failure
———————————
Loss of visibility

Stealth rootkits

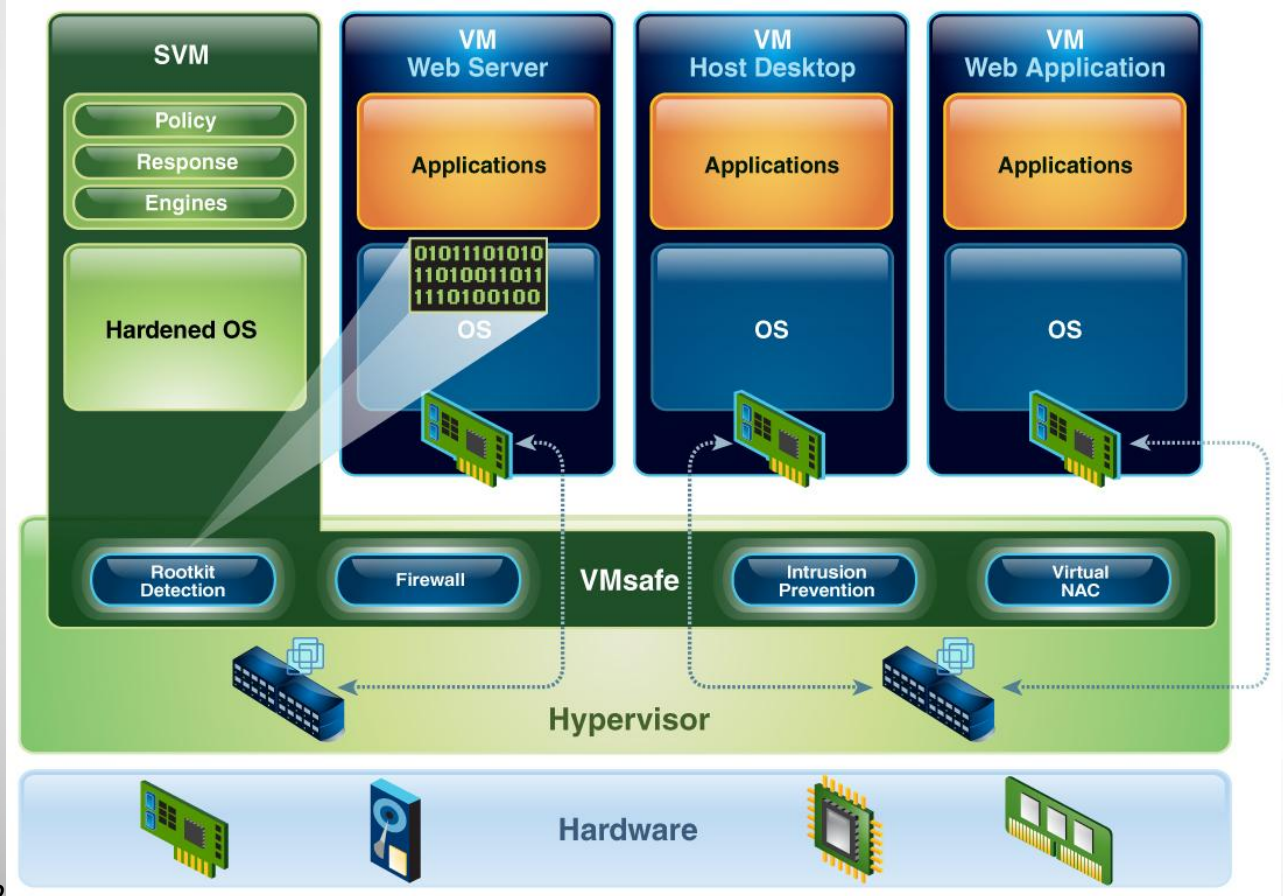
Virtual NIC's and switches are targets

MORE COMPONENTS = MORE EXPOSURE

IBM Security Virtual Server Protection for VMware

Integrated threat protection for VMware vSphere 4.x

Helps customers to be more secure, compliant and cost-effective by delivering integrated and optimized security for virtual data centers.



IBM Virtual Server Security for VMware

- VMsafe Integration
- Automatic Discovery
- Firewall and Intrusion Prevention
- Rootkit Detection/Prevention
- Inter-VM Traffic Analysis
- Automated Protection for Mobile VMs (VMotion)
- Virtual Network Segment Protection
- Virtual Network-Level Protection
- Virtual Infrastructure Auditing (Privileged User)
- VM discovery
- Virtual Network Access Control
- Accelerator w/MIA (Optional)

SERVICE & RISK MANAGEMENT FORUM 2011

IBM

SERVICE & RISK MANAGEMENT FORUM 2011

Not a technical problem, but a business challenge

IBM

IF IBM X-FORCE® WAS RUNNING IT

Many readers have asked, if IBM X-Force were running the IT department and saw what happened this year, what would you do? Well, here are ten actions beyond the basics that X-Force would do if we ran the IT department.

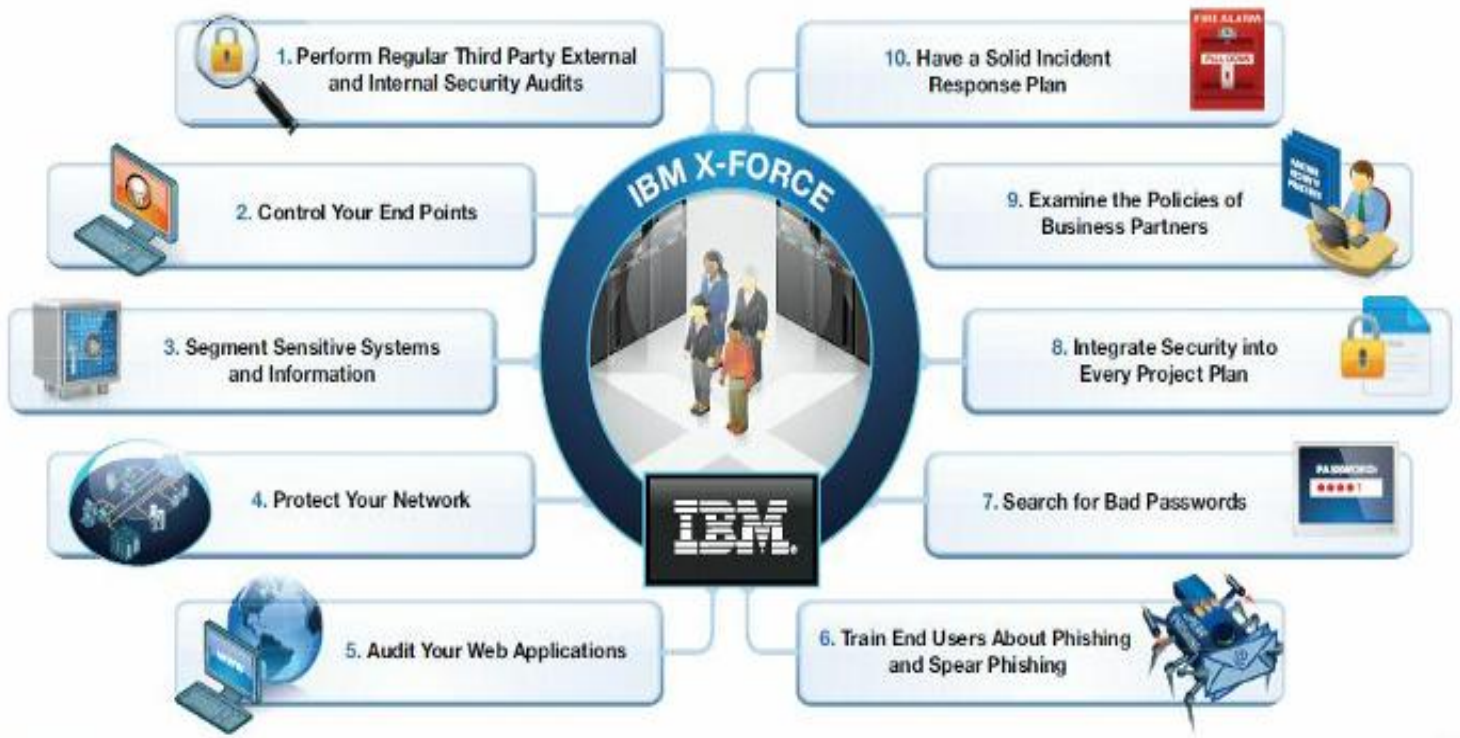


Figure 3: If IBM X-Force Was Running IT

SERVICE & RISK MANAGEMENT FORUM 2011

IBM

For More IBM X-Force Security Leadership

X-Force Trend Reports

The IBM X-Force Trend & Risk Reports provide statistical information about all aspects of threats that affect Internet security,. Find out more at http://www-935.ibm.com/services/us/iss/xforce/trendreports/

X-Force Security Alerts and Advisories

Only IBM X-Force can deliver preemptive security due to our unwavering commitment to research and development and 24/7 global attack monitoring. Find out more at http://xforce.iss.net/

X-Force Blogs and Feeds

For a real-time update of Alerts, Advisories, and other security issues, subscribe to the X-Force RSS feeds. You can subscribe to the X-Force alerts and advisories feed at http://iss.net/rss.php or the Frequency X Blog at http://blogs.iss.net/rss.php