IBM SolutionsConnect 2013

L'IBM TechSoftware nouvelle génération

28, 29 et 30 août

IBM Client Center Paris

#solconnect13

Transformez vos opportunités en succès

Sec10 – Sécurité des infrastructures
Quand est ce que vous serez attaqué ?

Serge RICHARD - CISSP®
Security Solution Architect – IBM Security Systems

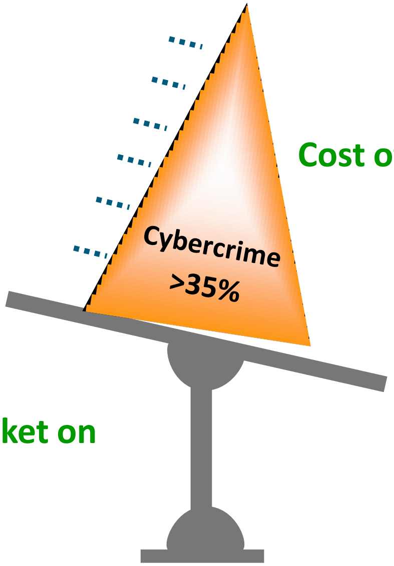
Agenda

- Evolution de l'écosystème des menaces
- L'offre IBM sécurité sur les infrastructures
- Solution globale protection des menaces

Agenda

- Evolution de l'écosystème des menaces
- L'offre IBM sécurité sur les infrastructures
- Solution globale protection des menaces

Bienvenue dans le monde de la Cyber Criminalité…



Cost of Global Cyber Crime

$388B

Global Black Market on Drugs

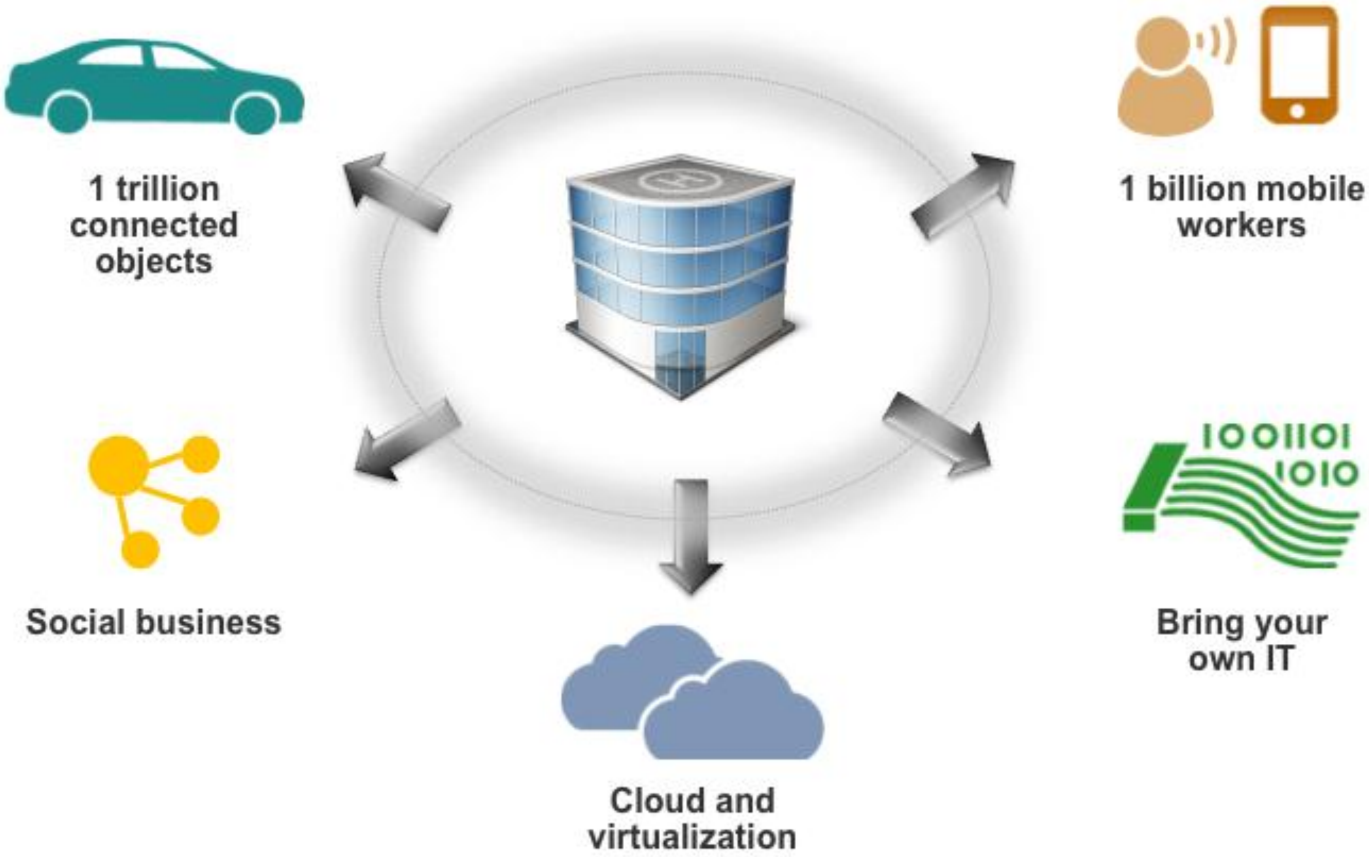
$288B

http://www.symantec.com/about/news/release/article.jsp?prid=20110907_02

“You know you can do this just as easily online.”

L’écosystème change…Si ce n’est déjà fait !!!

Les entreprises sont en perpétuelles mutations



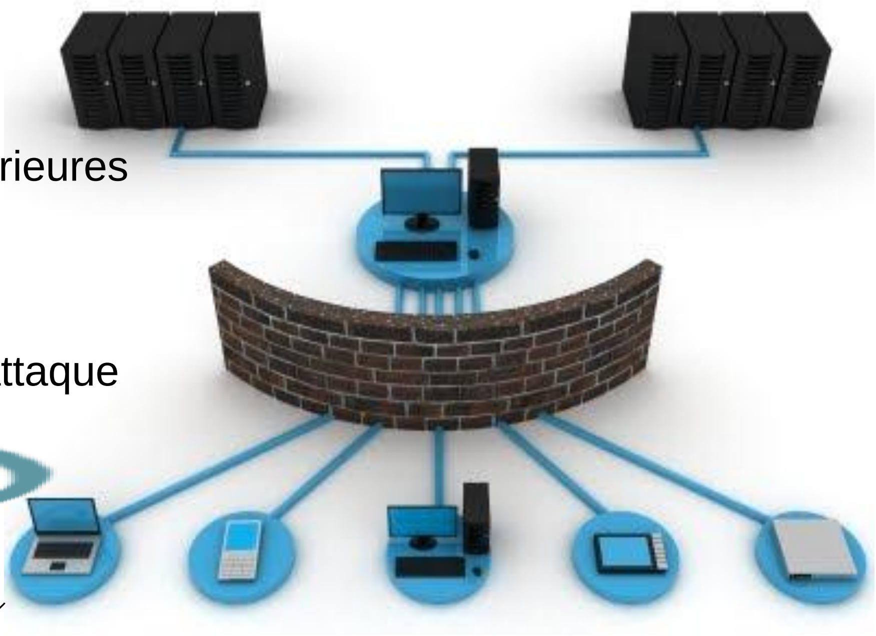
Les limites du périmètre “Cyber” deviennent floues…Comment appréhender cela ?

Jouer la défense…

L’approche traditionnelle de la sécurité repose sur une mentalité défensive

- Suppose un périmètre organisationnel explicite
- Optimisée pour la lutte contre les menaces extérieures
- Une normalisation pour atténuer les risques
- Une prise de conscience des méthodologies d'attaque
- Nécessite une surveillance/un contrôle des flux

Origines de la sécurité Intelligente



Couches de défense essentielles pour une bonne hygiène de sécurité et contre les menaces traditionnelles …***mais les attaquants s’adaptent***

Des attaquants bien organisés et des utilisateurs malveillants sont les clefs pour contourner les défenses de sécurité

Infiltrer un partenaire de confiance et charger un malware sur l’infrastructure cible

Création d’un logiciel malveillant adapté pour infecter une cible particulière et de ce fait ne pouvant pas être détecter les solutions de sécurité du marché

Utilisation des réseau sociaux et de l’ingénierie sociale pour effectuer la reconnaissance des cibles pour hameçonnage dans le but de compromettre les comptes et les serveurs

Exploitation des vulnérabilités zero-day pour permettre un accès aux données, applications, systèmes et terminaux

Communiquer sur les ports autorisés tel que le port 80 pour exfiltrer les données de l’entreprise

Nouvelles motivations et sophistication

- Crime organisé
- Espionnage and Activisme
- Nations et Etats

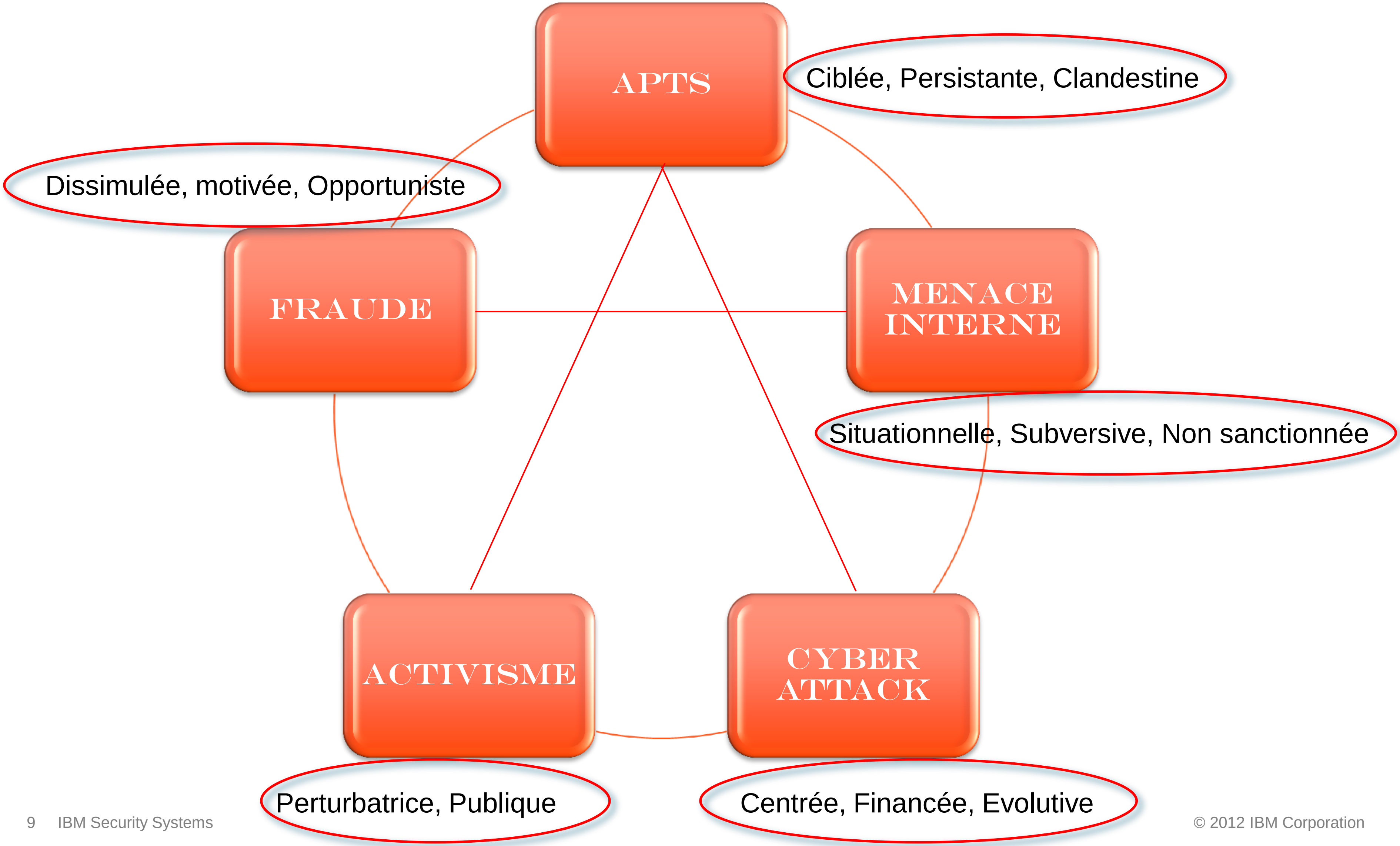
Designer Malware

Backdoors

Spear Phishing

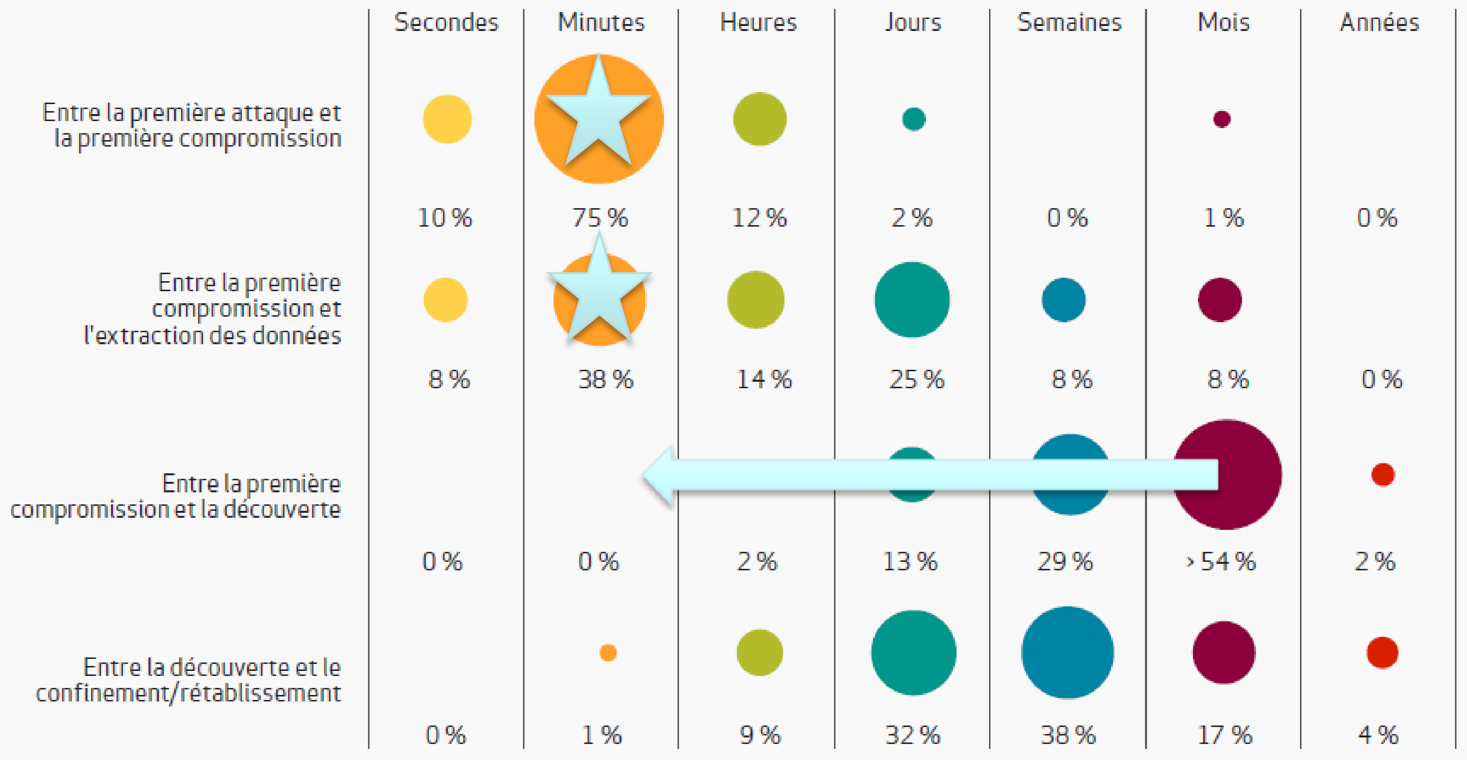
Persistence

Paysage des menaces émergentes


APTS
Ciblée, Persistante, Clandestine
Dissimulée, motivée, Opportuniste
FRAUDE
MENACE INTERNE
Situationnelle, Subversive, Non sanctionnée
ACTIVISME
CYBER ATTACK
Perturbatrice, Publique
Centrée, Financée, Evolutive

Gérer l'attaque au plus vite…

Figure 40. Durée des événements par pourcentage de compromissions



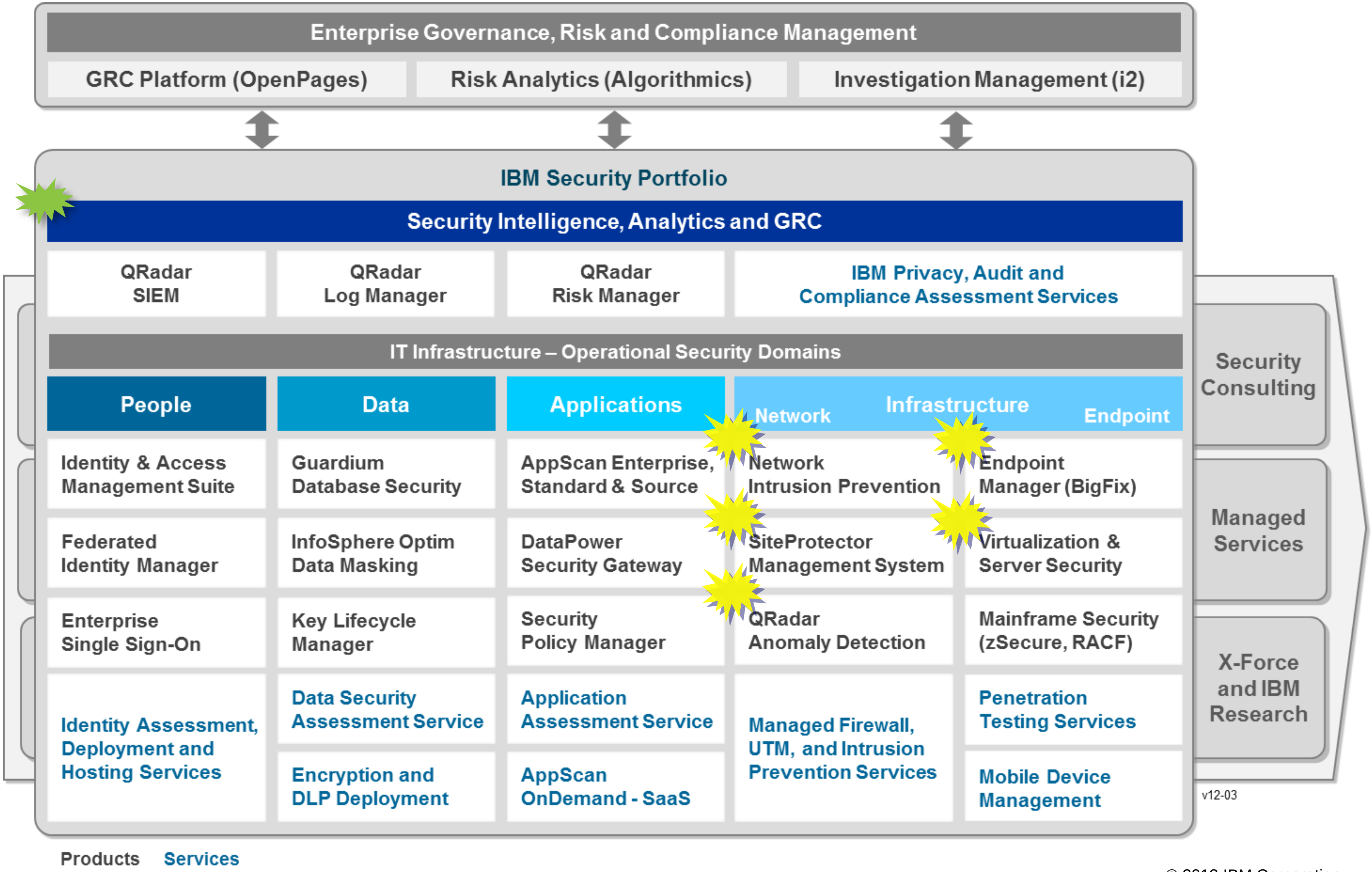
	Secondes	Minutes	Heures	Jours	Semaines	Mois	Années
Entre la première attaque et la première compromission	10 %	75 %	12 %	2 %	0 %	1 %	0 %
Entre la première compromission et l'extraction des données	8 %	38 %	14 %	25 %	8 %	8 %	0 %
Entre la première compromission et la découverte	0 %	0 %	2 %	13 %	29 %	› 54 %	2 %
Entre la découverte et le confinement/rétablissement	0 %	1 %	9 %	32 %	38 %	17 %	4 %

http://www.verizonenterprise.com/resources/reports/rp_Rapport_d_enquete_2012_Sur_Les_Compromissions_De_Donnees_fr_xg.pdf

Agenda

- Evolution de l'écosystème des menaces
- L'offre IBM sécurité sur les infrastructures
- Solution globale protection des menaces

What is Threat? (Network, Server and Endpoint)



Enterprise Governance, Risk and Compliance Management

GRC Platform (OpenPages) | Risk Analytics (Algorithmics) | Investigation Management (i2)

IBM Security Portfolio

Security Intelligence, Analytics and GRC

QRadar SIEM | QRadar Log Manager | QRadar Risk Manager | IBM Privacy, Audit and Compliance Assessment Services

IT Infrastructure – Operational Security Domains

People	Data	Applications	Infrastructure	
			Network	Endpoint
Identity & Access Management Suite	Guardium Database Security	AppScan Enterprise, Standard & Source	Network Intrusion Prevention	Endpoint Manager (BigFix)
Federated Identity Manager	InfoSphere Optim Data Masking	DataPower Security Gateway	SiteProtector Management System	Virtualization & Server Security
Enterprise Single Sign-On	Key Lifecycle Manager	Security Policy Manager	QRadar Anomaly Detection	Mainframe Security (zSecure, RACF)
Identity Assessment, Deployment and Hosting Services	Data Security Assessment Service	Application Assessment Service	Managed Firewall, UTM, and Intrusion Prevention Services	Penetration Testing Services
	Encryption and DLP Deployment	AppScan OnDemand - SaaS		Mobile Device Management

Security Consulting

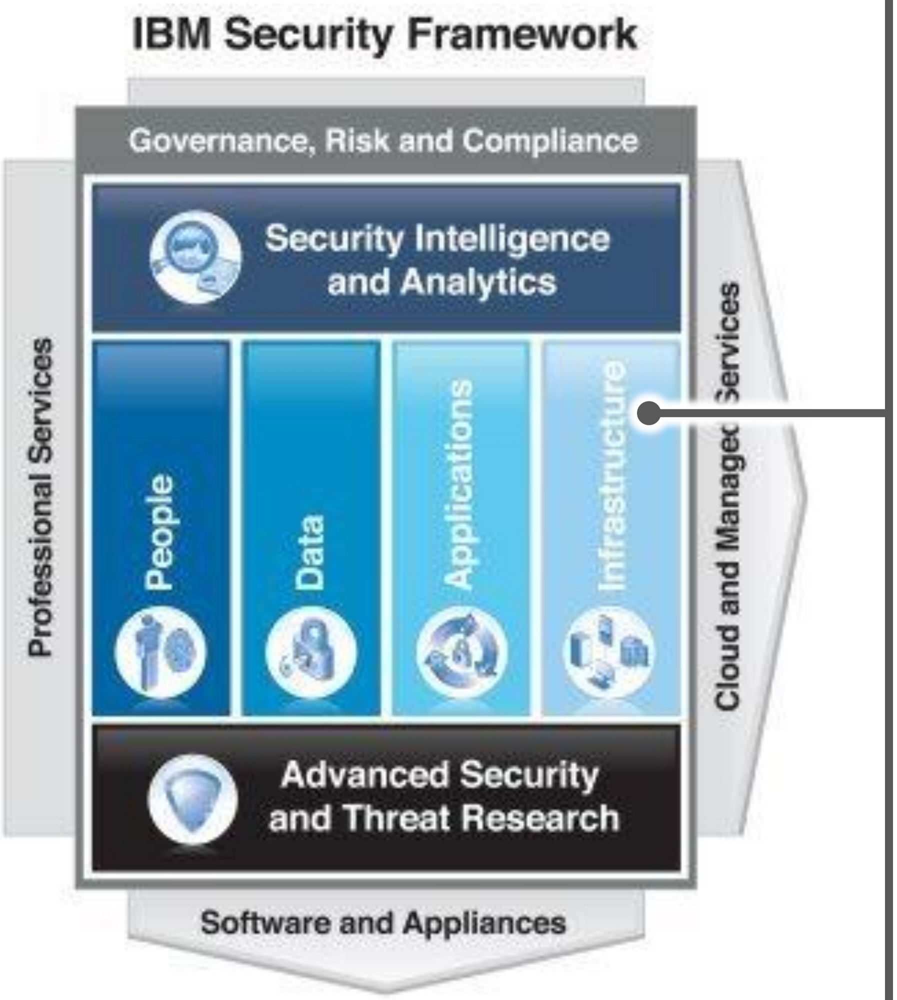
Managed Services

X-Force and IBM Research

v12-03

Products Services

Infrastructure


IBM Security Framework
Governance, Risk and Compliance
Security Intelligence and Analytics
People
Data
Applications
Infrastructure
Advanced Security and Threat Research
Software and Appliances
Professional Services
Cloud and Managed Services

Overview

- **Defense-in-depth** against today's advanced threats
- **Protection for critical IT assets** from the network, to individual hosts, to virtual/cloud-based infrastructure
- **Powered by IBM X-Force** threat intelligence and technology
- **Improved control and responsiveness** to immediate threats through integrated **central management** and **security intelligence**

X-Force Threat Intelligence: The IBM Differentiator

X-Force Threat Intelligence Cloud

X-Force database - extensive catalog of vulnerabilities

Web filter database – malicious or infected websites

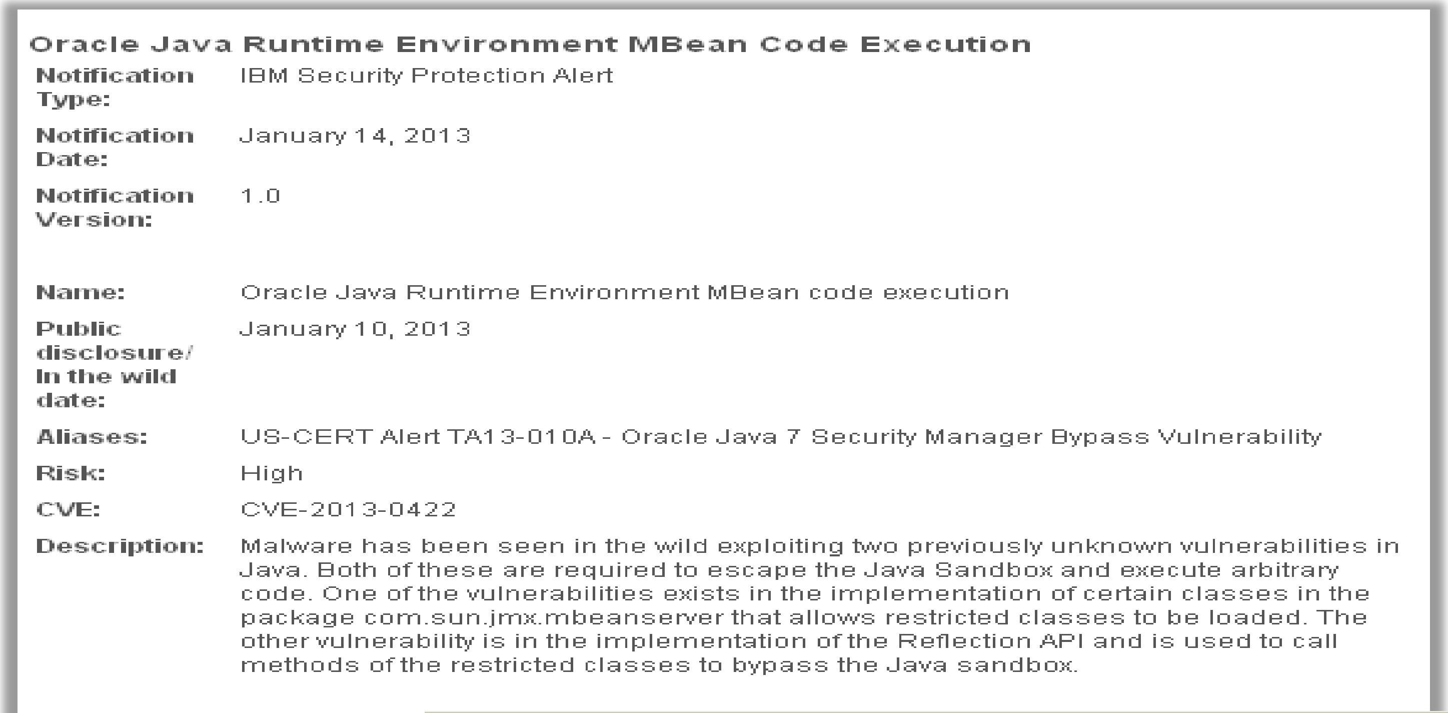
IP Reputation – botnets, anonymous proxies, bad actors

Application Identification – web application information

Vulnerability Research – latest vulnerabilities and protections

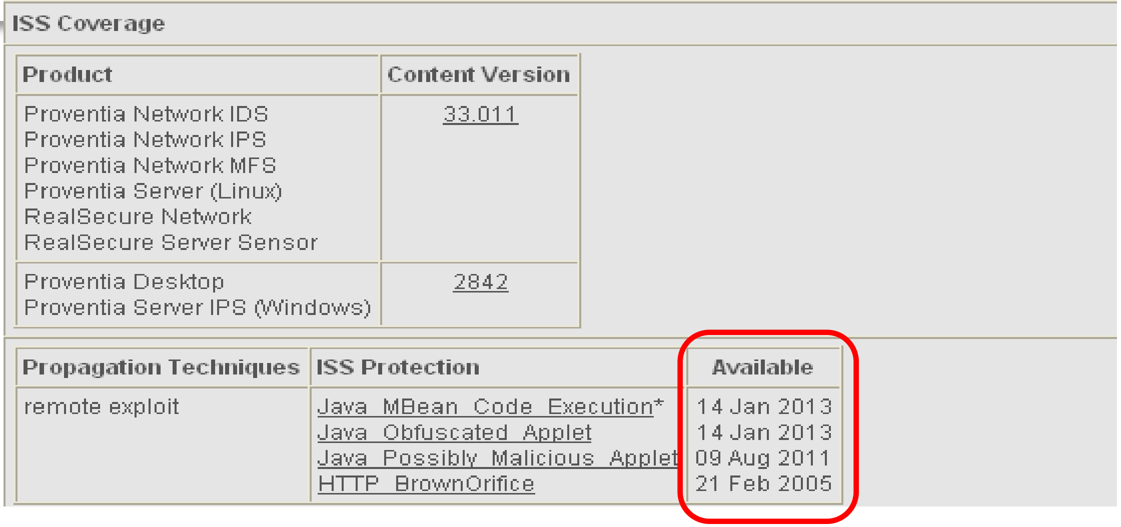
Security Services – manage IPS for 3000+ Customers

Java 0-day exploit example



Oracle Java Runtime Environment MBean Code Execution

Notification Type:	IBM Security Protection Alert
Notification Date:	January 14, 2013
Notification Version:	1.0
Name:	Oracle Java Runtime Environment MBean code execution
Public disclosure/ In the wild date:	January 10, 2013
Aliases:	US-CERT Alert TA13-010A - Oracle Java 7 Security Manager Bypass Vulnerability
Risk:	High
CVE:	CVE-2013-0422
Description:	Malware has been seen in the wild exploiting two previously unknown vulnerabilities in Java. Both of these are required to escape the Java Sandbox and execute arbitrary code. One of the vulnerabilities exists in the implementation of certain classes in the package com.sun.jmx.mbeanserver that allows restricted classes to be loaded. The other vulnerability is in the implementation of the Reflection API and is used to call methods of the restricted classes to bypass the Java sandbox.



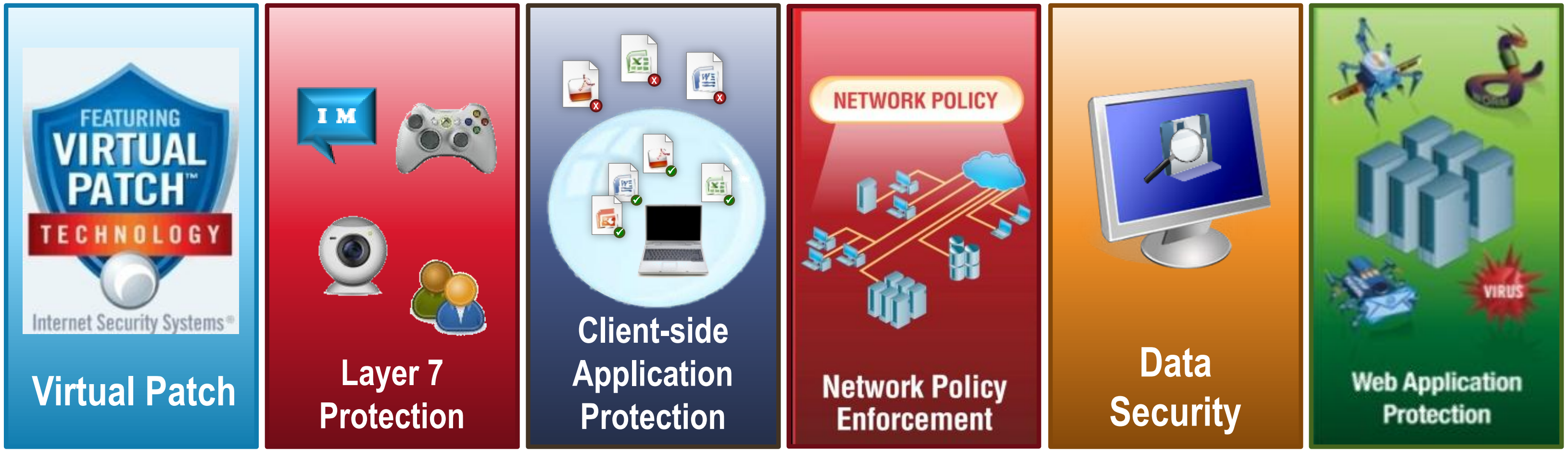
ISS Coverage

Product	Content Version
Proventia Network IDS Proventia Network IPS Proventia Network MFS Proventia Server (Linux) RealSecure Network RealSecure Server Sensor	33.011
Proventia Desktop Proventia Server IPS (Windows)	2842

Propagation Techniques	ISS Protection	Available
remote exploit	Java_MBean_Code_Execution* Java_Obfuscated_Applet Java_Possibly_Malicious_Applet HTTP_BrownOrifice	14 Jan 2013 14 Jan 2013 09 Aug 2011 21 Feb 2005

IBM Advanced Threat Protection Platform

Adaptive Threat Protection – modular core – Protocol Module Analysis



Virtual Patch

Layer 7 Protection

Client-side Application Protection

Network Policy Enforcement

Data Security

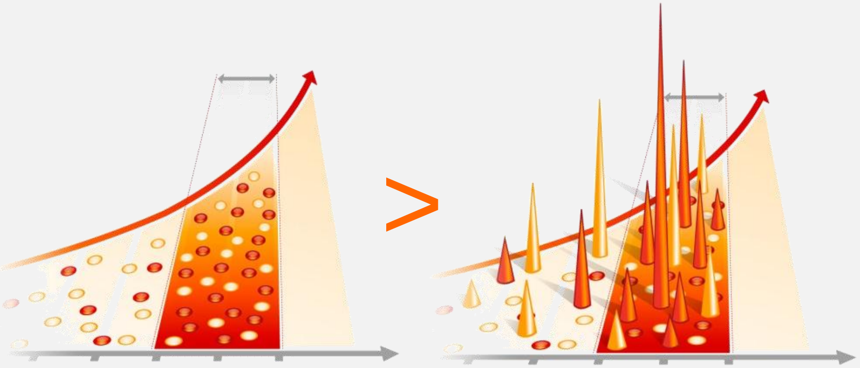
Web Application Protection

Ahead-of-the-threat extensible protection
backed by the power of X-Force®

PAM and XForce: How We Are Better

Pattern Matching

- Protecting from exploits is reactive
  - Too late for many
  - Variants undo previous updates
  - Typical of antivirus and most IDS/IPS vendors
- Signature-based pattern matching engines requires unique signature for each and every exploit vector
  - Signatures do not correlate to vulnerabilities
  - The more signatures loaded the great the impact to performance and inspection capabilities

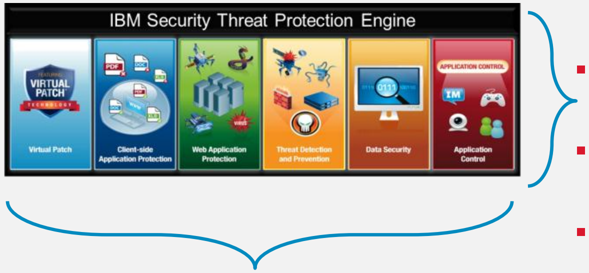


One Vulnerability

Many Signatures

Protocol Awareness

- Protection from Vulnerabilities
  - A protection algorithm shields the vulnerability, provides protection from multiple exploit vectors
  - Protection algorithms provide protection from known and unknown variants of an exploit
  - IBM algorithms do not require a signature update to react to the next variant.
  - The IBM Threat Protection Engine provides protection ahead of the threat


IBM Security Threat Protection Engine
VIRTUAL PATCH
Virtual Patch
Client-side Application Protection
Web Application Protection
Threat Detection and Prevention
Data Security
APPLICATION CONTROL
Application Control

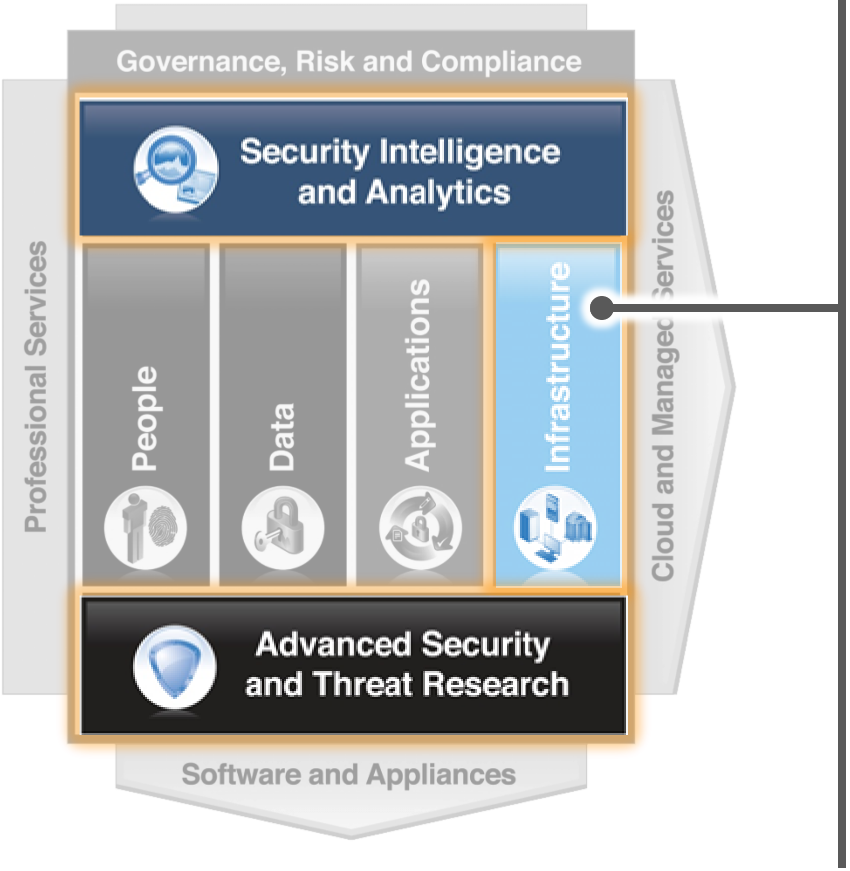
Provides the ability to add new security functionality within the existing solution

- Performs deep packet inspection
- Performs deep protocol and content analysis
- Detects protocol and content anomalies
- Simulates the protocol/content stacks in vulnerable systems
- Provides protection from vulnerabilities not just the current variant of the exploit

Infrastructure (Network)

Area of Focus

Guard against attacks using an Advanced Threat Protection Platform with insight into users, content and applications


Governance, Risk and Compliance
Security Intelligence and Analytics
People
Data
Applications
Infrastructure
Advanced Security and Threat Research
Professional Services
Cloud and Managed Services
Software and Appliances

Portfolio Overview

IBM Security Network Intrusion Prevention (GX IPS)

- Delivers Advanced Threat Detection and Prevention to stop targeted attacks against high value assets
- Proactively protects systems with IBM Virtual Patch® technology
- Protects web applications from threats such as SQL Injection and Cross-site Scripting attacks
- Integrated Data Loss Prevention (DLP) monitors data security risks throughout your network
- Provides Ahead of the Threat® protection backed by world renowned IBM X-Force Research

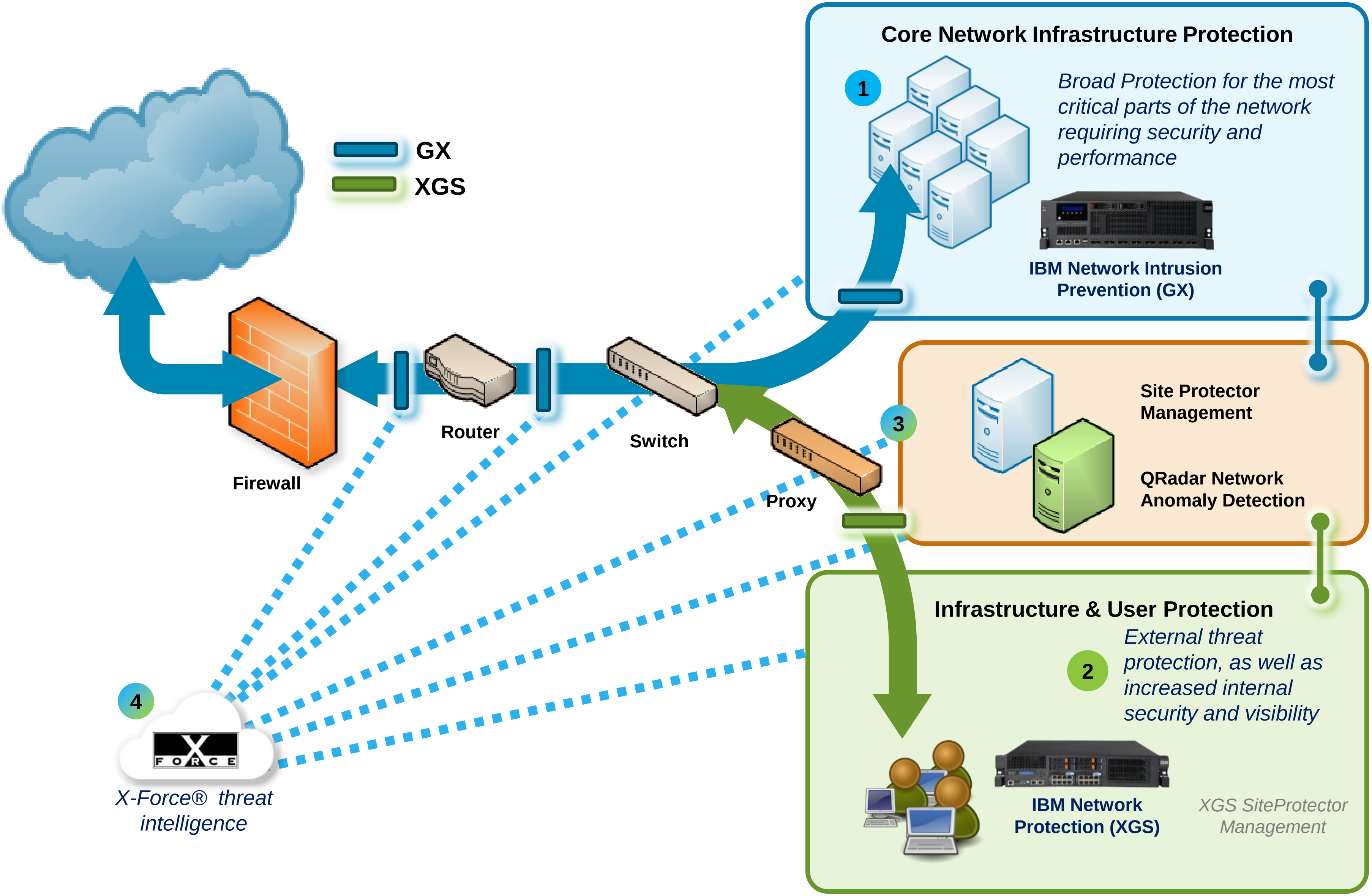
IBM Security Network Protection (XGS)

- Advanced Threat Detection and Prevention to stop targeted attacks against the end user
- Protection users from internet threats such as sources of malware, suspect web applications and compromised web sites

IBM Security SiteProtector

- Provides central management of security devices to control policies, events, analysis and reporting for your business

Protection for Networks, Applications and Endpoints



Core Network Infrastructure Protection

Broad Protection for the most critical parts of the network requiring security and performance

IBM Network Intrusion Prevention (GX)

Site Protector Management

QRadar Network Anomaly Detection

Infrastructure & User Protection

External threat protection, as well as increased internal security and visibility

IBM Network Protection (XGS)

XGS SiteProtector Management

X-Force® threat intelligence

IBM Advanced Threat Protection Platform

GX

Adaptive Threat Protection

FEATURING VIRTUAL PATCH TECHNOLOGY
Internet Security Systems
I M
NETWORK POLICY
VIRUS
SNORT

Virtual Patch

Layer 7 Protection

Client-side Application Protection

Network Policy Enforcement

Data Security

Web Application Protection

Custom Snort Rules

Ahead-of-the-threat extensible protection
backed by the power of X-Force®

Securing Every Layer of your Network

IBM Network Intrusion Prevention

	Remote	Perimeter				Core				
Model	GX4004-200	GV	GX4004	GX5008	GX5108	GX5208	GX7412-5	GX7412-10	GX7412	GX7800
Inspected Throughput	200 Mbps	500Mbps	800 Mbps	1.5 Gbps	2.5 Gbps	4 Gbps	5 Gbps	10 Gbps	15 Gbps	20 Gbps+
Protected Segments	2	2	2	4	4	4	8	8	8	4

Adaptive Threat Protection

- Virtual Patch technology
- Web application protection
- Protection from client-side attacks
- Data and content security
- Application awareness

Protection Modes

- In-line protection
- In-line simulation
- Passive monitoring

Availability

- Active / active high availability
- Redundant hard drives and power supplies

Research / Updates

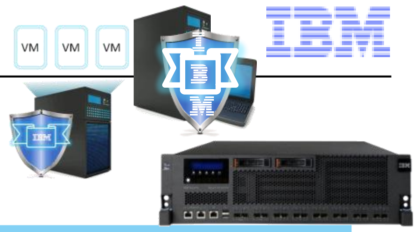
- Updates powered by IBM X-Force® research team
- X-Press Updates – automated updated delivery

Management Options

- Local web-based management
- Centralized management via IBM SiteProtector

Adaptive Threat Protection

	Customer Benefits	Typical Questions
FEATURING VIRTUAL PATCH TECHNOLOGY Internet Security Systems Virtual Patch	Reduce the urgency of installing patches Protect vulnerabilities with no patches	• How much does a patch cycle cost you? • How much could you save by reducing the number of patch cycles? • How do you protect vulnerabilities when you don't have a vendor patch?
	Protect both applications and network with one solution Block disallowed protocols and applications	• How do you protect applications from being exploited? • How do you block 3rd parties (e.g. consultants) from running applications you don't want on your network?
	Improve productivity by protecting the users from being attacked (e.g. through malicious documents) Protect the applications running on the client	• How do you detect 0-day attacks toward the client systems? • How do you detect obfuscated attacks? • Can you protect your clients already at the network level?
	Show compliance to regulations	• How easily can you prove compliance to regulation requirements? • How easily can you enforce your corporate policy? • How easiliy can you enforce your policy agains 3rd parties (e.g. consultants)?



Adaptive Threat Protection

	Customer benefits	Typical questions
	Prevent leakage of sensitive information	• Do you need to monitor the traffic for sensitive information leaving your company? • Do you have DLP requirements?
	Prevent data from being stolen from the DB via web applications Retain brand integrity by protecting your customers' sensitive data	• How do you protect the vulnerabilities of your web-applications? • Do you fix/patch your own web applications? • Do you have PCI compliancy requirements?
	Reduce the complexity of the network security architecture Improved flexibility to implement ad-hoc monitoring**	• Do you have in-house applications/protocols that you want to monitor?

** Custom Snort rules are currently supported on network appliances only, not on host protection or virtualization security offerings

IBM Security Network Protection XGS 5100

The Next Generation of IBM's legendary network security solutions

ADVANCED THREAT PROTECTION	NETWORK VISIBILITY & CONTROL	SEAMLESS INTEGRATION
Protection from sophisticated and constantly evolving threats, powered by X-Force®	Discover and block existing infections, rogue applications, while enforcing access policies	Adaptive deployment and superior integration with the full line of IBM security solutions

Advanced Threat Protection

The XGS protects against a full spectrum of targeted attacks, even over SSL-encrypted traffic

Agile Security Engine protects against Mutating Threats

Infrastructure Threat Protection

System-level Attacks

Service-level Attacks

Web Application Attacks

User Threat Protection

Spear Phishing

Malicious Attachments

Web/Social Media Risks

Ahead-of-the-threat extensible protection backed by the power of X-Force®

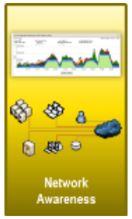
User Protection: IBM Security XGS 5100

Adaptive Network Infrastructure & User Threat Protection

The IBM XGS: Critical Part of Next Gen Network Defense

- Next Generation IPS powered by X-Force® Research protects weeks or even months “ahead of the threat”
- Full protocol, content and application aware protection goes beyond signatures
- Expandable protection modules defend against emerging threats such as malicious file attachments and Web application attacks
- Block evolving, high-risk sites such as Phishing and Malware with comprehensive web site coverage; 17 Billion+ URLs (50-100x the coverage comparatively)
- Control network traffic based upon users, group membership, systems, networks, protocols, applications & application actions - rich support of 1000+ applications and controls for multiple individual actions within each application

Adaptive Client-side Threat Protection

	Customer benefits	Typical questions
	Enhance access control by stopping users from running application without a business need	• Do you know who is running remote management tools? • How do you determine who is allowed to run such applications?
	Prevent attacks from known infected sites (e.g. botnets)	• How do you know that you can trust the traffic from a specific IP? • How much would an infection clean-up cost you?
	Enforce controls on the web usage of the employees	• How do you determine who can post to social media in your company's name? • Would you be interested in stopping your customers from playing on Facebook?
	Identify infections through network behavior Have full visibility of the network usage	• Did you know that "designer malware" usually goes undetected by the average AV? • Do you have visibility of the type of traffic running on your network?

Proven Security: Extensible, 0-Day Protection Powered by X-Force®

- Next Generation IPS powered by X-Force® Research protects weeks or even months "ahead of the threat"
- Full protocol, content and application aware protection goes beyond signatures
- Expandable protection modules defend against emerging threats such as malicious file attachments and Web application attacks

> *"When we see these attacks coming in, it will shut them down automatically."*
>
> *– Melbourne IT*

> *[The IBM Threat Protection Engine] "defended an attack against a critical government network another protocol aware IPS missed"*
>
> *– Government Agency*

IBM Security Network Protection XGS 5100

IBM Security Threat Protection

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

– Backed by X-Force®

– 15 years+ of vulnerability research and development

– Trusted by the world's largest enterprises and government agencies

– True protocol-aware intrusion prevention, not reliant on signatures

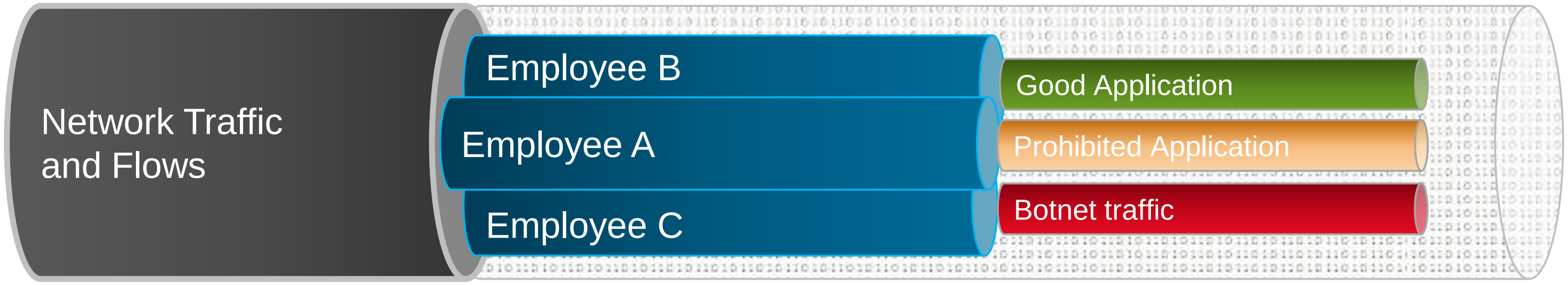
– Specialized engines

- Exploit Payload Detection
- Web Application Protection
- Content and File Inspection

Ability to protect against the threats of today and tomorrow

Network Visibility & Control

The XGS can enforce context-aware access control policies to block pre-existing infections, rogue applications, and corporate policy violations



Deep Packet Inspection fully classifies network traffic, regardless of address, port , protocol, application, application action or security event

Complete Identity Awareness associates valuable users and groups with their network activity, application usage and application actions

Access Control Policies block pre-existing compromises and rogue applications as well as enforce corporate usage policies

375+
Protocols and File Formats Analyzed

1,200+
Applications and Actions Identified

17 Billion+
URLs classified in 70 Categories

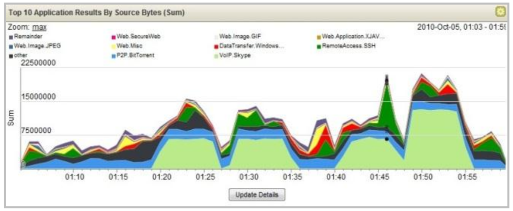
Seamless Integration

The XGS is part of the IBM Security Framework, offering an advanced approach to today's real-world problems

Adaptable Deployment

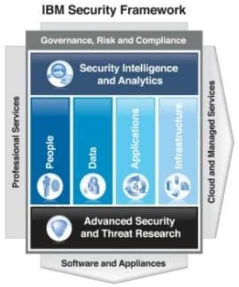
- Unique flexible performance licensing results in lower cost per gigabit protected
- High port density with upgradable network modules to meet present and future connectivity needs
- Built-in bypass and SSL inspection eliminates need for separate hardware, reducing cost and complexity

Advanced QRadar Integration



- Network visibility helps identify sources of high bandwidth consumption
- Helps mitigate known and unknown attacks
- Enhanced analysis and correlation across both IBM and non-IBM products for improved security analyst efficiency

Breadth and Depth of Portfolio

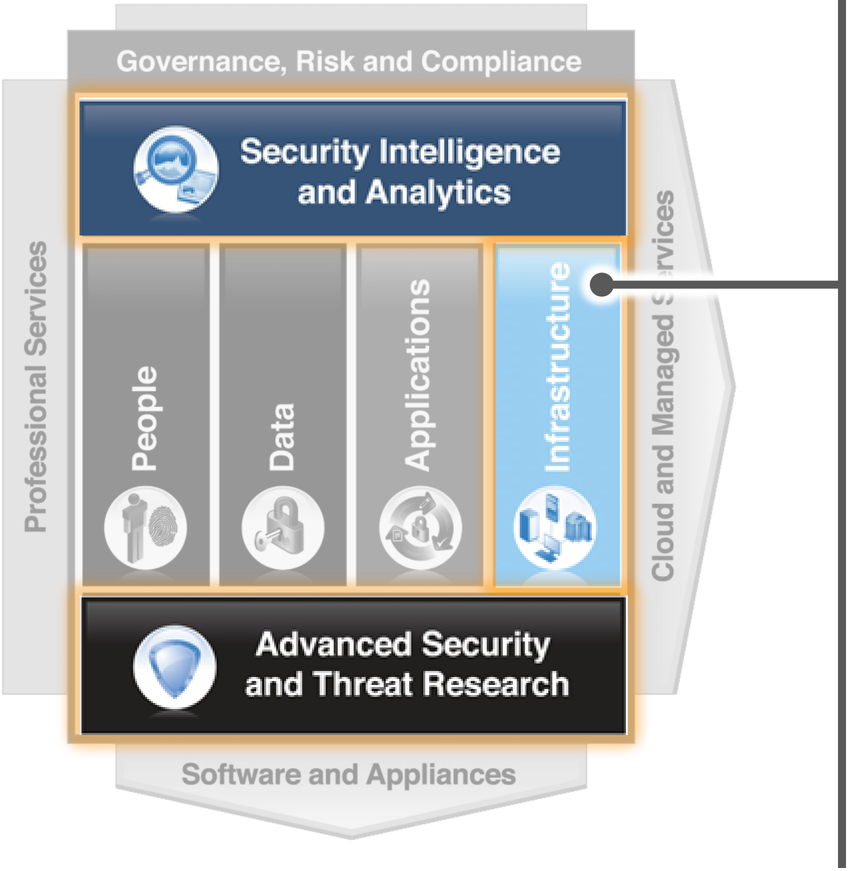

IBM Security Framework
Governance, Risk and Compliance
Security Intelligence and Analytics
Professional Services
People
Data
Applications
Infrastructure
Cloud and Managed Services
Advanced Security and Threat Research
Software and Appliances

- Solutions and services for practically every security need
- Protection of people, data, applications and infrastructure
- Advanced cross-product research & development team

Infrastructure (Host)

Area of Focus

Guard against attacks using an Advanced Threat Protection Platform with insight into users, content and applications


Governance, Risk and Compliance
Security Intelligence and Analytics
People
Data
Applications
Infrastructure
Advanced Security and Threat Research
Professional Services
Cloud and Managed Services
Software and Appliances

Portfolio Overview

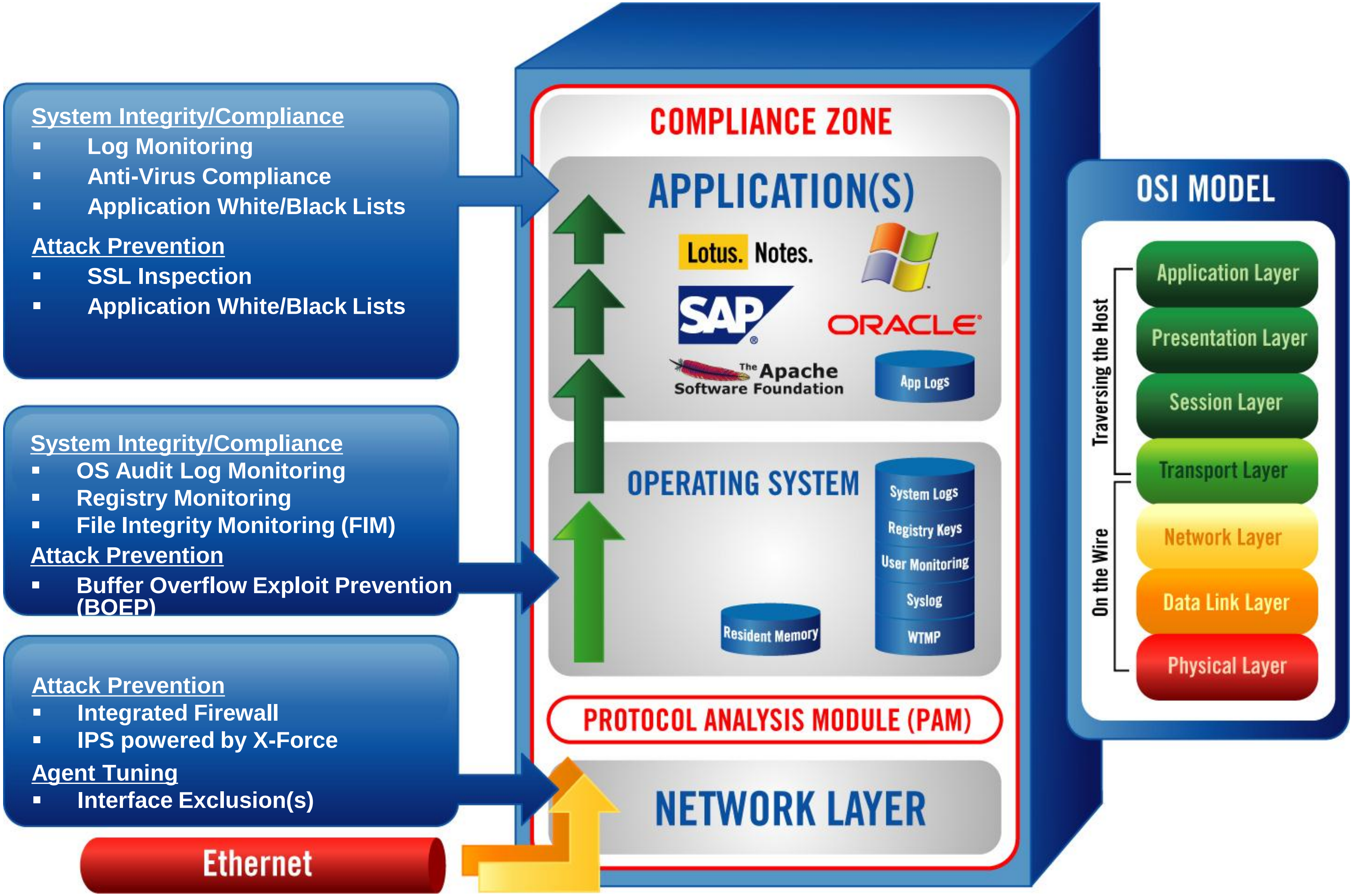
IBM Security Host Protection

- Provides intrusion prevention and firewall to protect the host network, a last line of defense on critical server and client endpoints on a broad array of OS platforms
- Integrates with OS audit capabilities to detect threats at the operating system level
- Monitors 3rd-party text logs for unwanted activity
- Actively monitors critical files for unauthorized changes
- Delivers Advanced Threat Detection and Prevention, IBM Virtual Patch® technology, and web application protection
- Provides Ahead of the Threat® protection backed by world renowned IBM X-Force Research

IBM Endpoint Manager for Core Protection

- Extends the IBM Endpoint Manager platform to protect critical endpoints with an integrated security agent
- Detects and removes malicious software
- Provides a host firewall to block unwanted network traffic
- Integrated web reputation helps to block traffic from suspicious sources
- Helps to protect critical data with integrated data loss prevention

IBM Security Host Protection Overview



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 powered by X-Force

Agent Tuning
- Interface Exclusion(s)

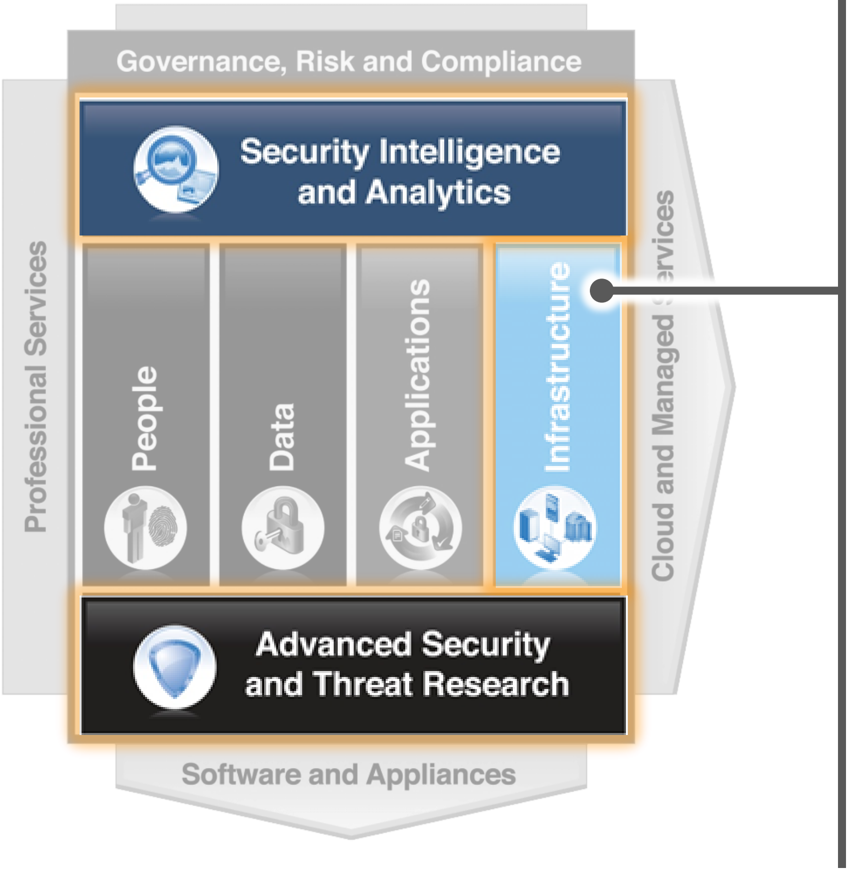
Broad Platform Support

- Windows 2000, 2003, 2003 x64
- Windows Server 2008, 2008 R2 (32-bit and 64-bit)
- Windows XP / Vista / 7
- Red Hat Enterprise Linux 3, 4, 5, 6 (32-bit and 64-bit)
- SuSE Linux Enterprise Server 9, 10, 11 (32-bit and 64-bit)
- AIX 5.1, 5.2, 5.3, 6.1, 7.1
- HP-UX 11.00, 11.11, 11.23 (PA-RISC)
- HP-UX 11.23 (Itanium)
- Solaris 8, 9, 10 (SPARC)
- VMware guest OS, Solaris Containers, AIX WPAR

Infrastructure (Virtualization)

Area of Focus

Guard against attacks using an Advanced Threat Protection Platform with insight into users, content and applications


Governance, Risk and Compliance
Security Intelligence and Analytics
Professional Services
People
Data
Applications
Infrastructure
Cloud and Managed Services
Advanced Security and Threat Research
Software and Appliances

Portfolio Overview

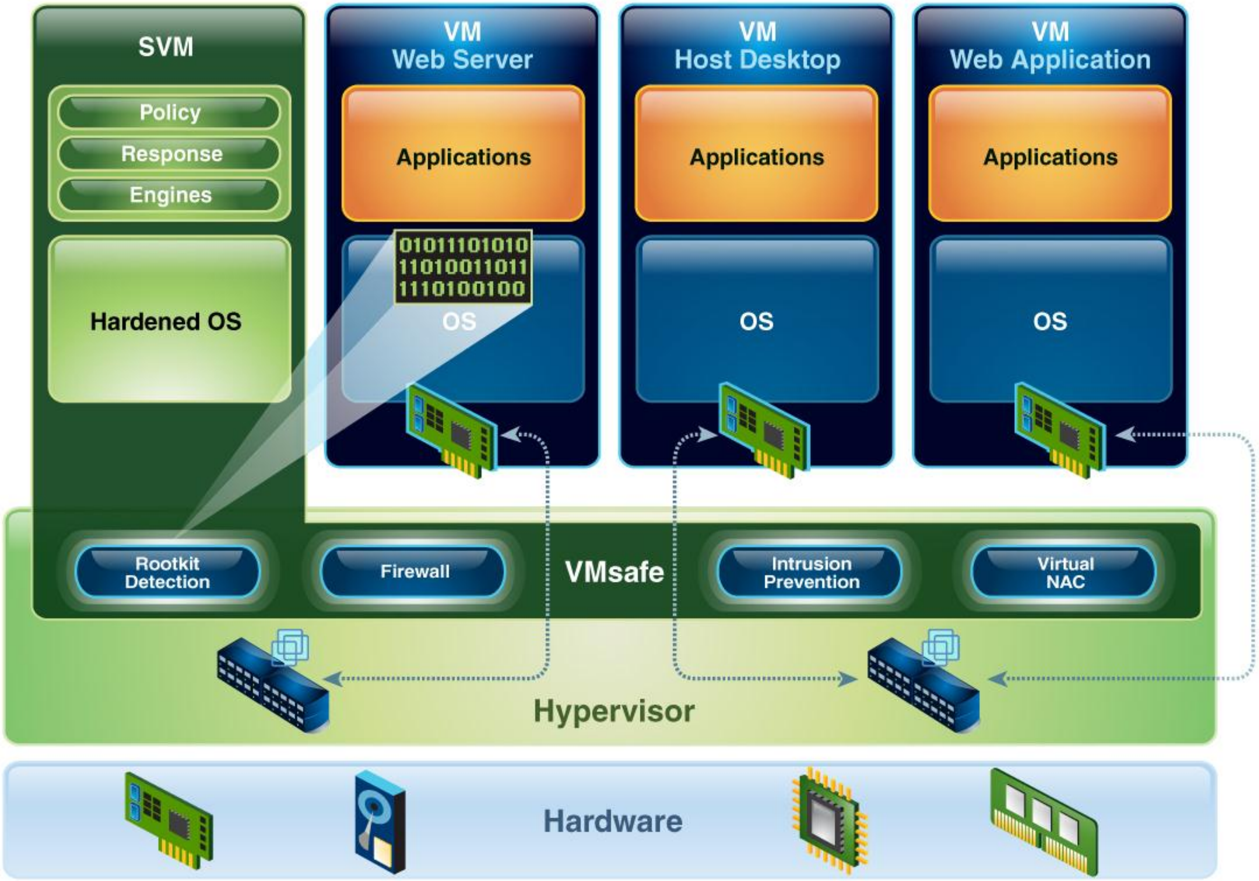
IBM Security Virtual Server Protection for Vmware (VSP)

- Protects against threats not only on the physical network, but also on the virtual network, including intra-VM traffic on a single physical host
- Agentless intrusion protection, firewall, and rootkit detection powered by IBM X-Force and IBM Research
- Virtual infrastructure monitoring can help prevent VM sprawl and automatically quarantine insecure VMs
- Optimizes security footprint for virtualized environments to help lower risk while maximizing VM density

Intrusion Prevention and More

IBM Security Virtual Server Protection for VMware

Integrated threat protection for VMware vSphere

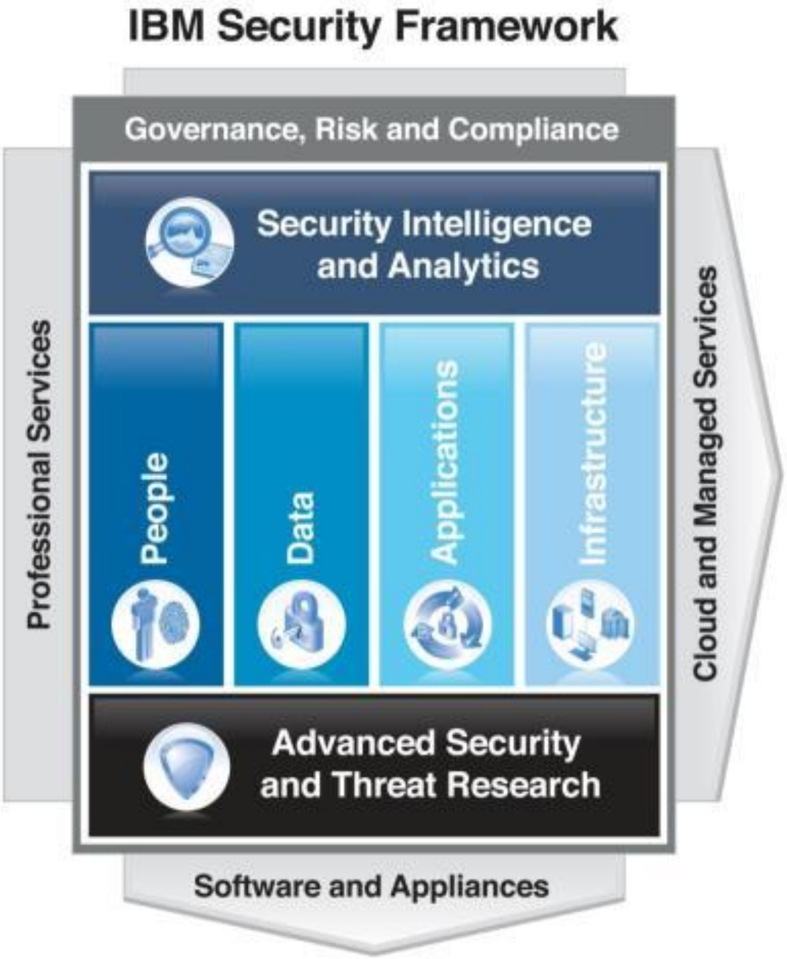


- VMsafe Integration
- Firewall and Intrusion Prevention
- Rootkit Detection/Prevention
- Inter-VM Traffic Analysis
- Automated Protection for Mobile VMs (VMotion)
- Virtual Network Segment Protection
- Virtual Network-Level Protection
- Virtual Infrastructure Auditing (Privileged User)
- Virtual Network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

Agenda

- Evolution de l'écosystème des menaces
- L'offre IBM sécurité des infrastructures
- Solution globale protection des menaces

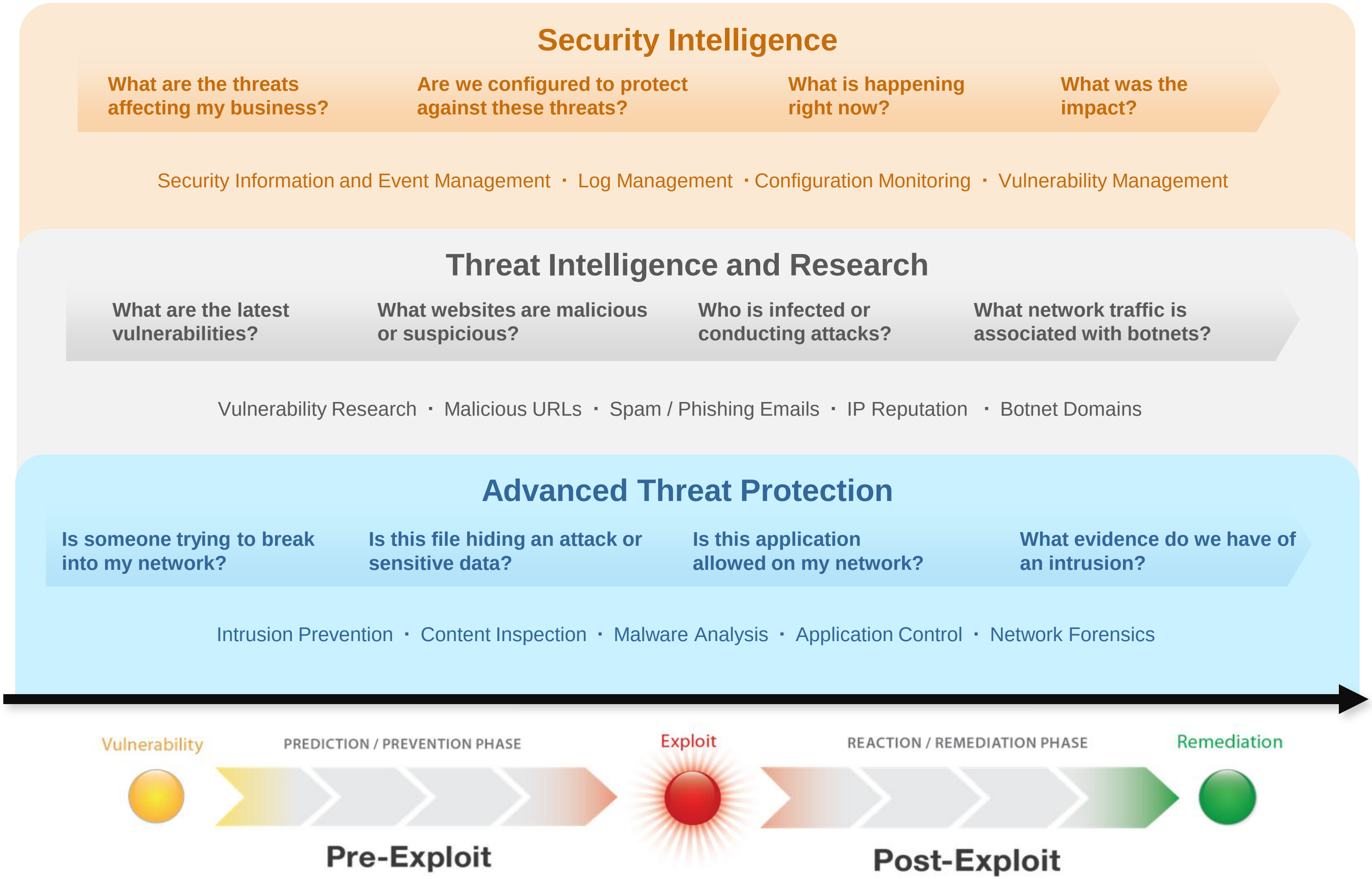
IBM delivers security intelligence in a multi-perimeter world


IBM Security Framework
Governance, Risk and Compliance
Security Intelligence and Analytics
People
Data
Applications
Infrastructure
Advanced Security and Threat Research
Professional Services
Cloud and Managed Services
Software and Appliances

- **Threat Protection**
- IBM Security Network IPS
- IBM Security Intelligence Platform
- **Mobile Security**
- IBM Endpoint Manager
- IBM Security AppScan
- **Cloud Security**
- SmartCloud Security
- Enterprise Key Management Foundation
- **Big Data**
- IBM Security Intelligence with Big Data
- **Foundational Security**
- IBM Security Identity and Access Assurance
- IBM Security Identity and Access Manager
- IBM Security Network IPS
- IBM Security Host Protection
- IBM Payment Card Industry Hardware Option
- **Security Services**
- Incident Response Program Development
- SOC Consulting

Intelligence ● Integration ● Expertise

The Requirements for an Advanced Threat Protection Platform



Security Intelligence

What are the threats affecting my business? · Are we configured to protect against these threats? · What is happening right now? · What was the impact?

Security Information and Event Management · Log Management · Configuration Monitoring · Vulnerability Management

Threat Intelligence and Research

What are the latest vulnerabilities? · What websites are malicious or suspicious? · Who is infected or conducting attacks? · What network traffic is associated with botnets?

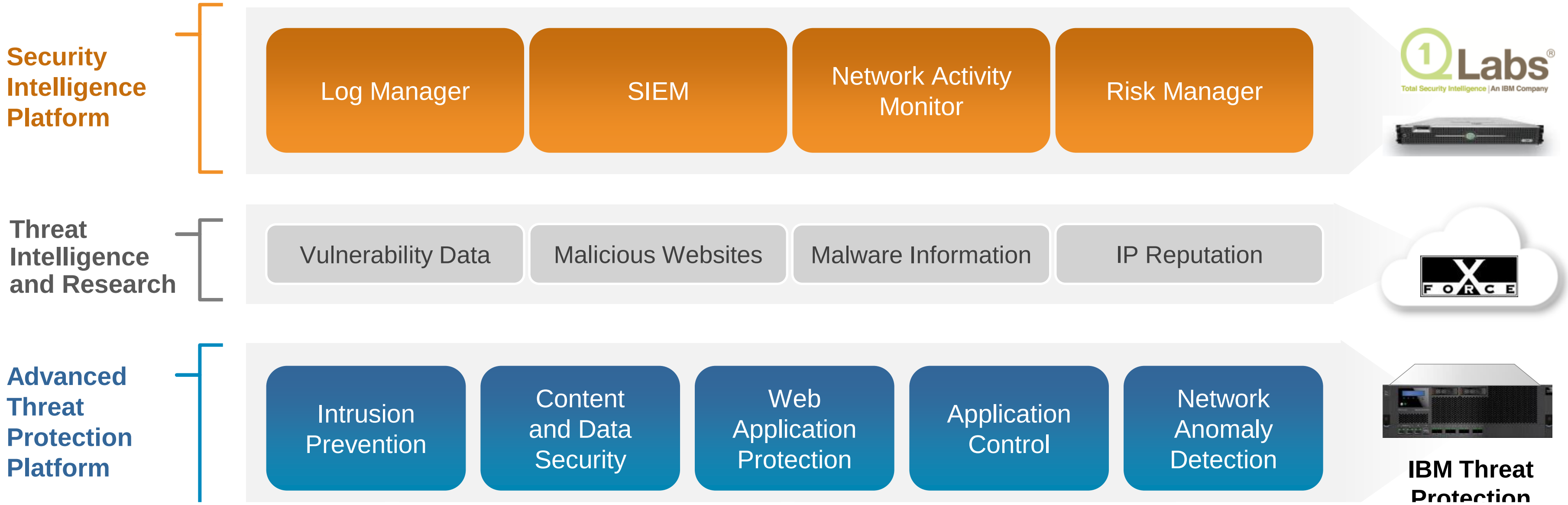
Vulnerability Research · Malicious URLs · Spam / Phishing Emails · IP Reputation · Botnet Domains

Advanced Threat Protection

Is someone trying to break into my network? · Is this file hiding an attack or sensitive data? · Is this application allowed on my network? · What evidence do we have of an intrusion?

Intrusion Prevention · Content Inspection · Malware Analysis · Application Control · Network Forensics

Evolving Threats Require an Advanced Threat Protection Platform: Next Generation Protection, Broad Visibility & Deep Control



Security Intelligence Platform
Log Manager
SIEM
Network Activity Monitor
Risk Manager
Q1 Labs
Total Security Intelligence | An IBM Company
Threat Intelligence and Research
Vulnerability Data
Malicious Websites
Malware Information
IP Reputation
X FORCE
Advanced Threat Protection Platform
Intrusion Prevention
Content and Data Security
Web Application Protection
Application Control
Network Anomaly Detection
IBM Threat Protection

Advanced Threat Protection Platform

Ability to help prevent sophisticated threats and detect abnormal network behavior by leveraging an extensible set of network security capabilities - in conjunction with real-time threat information and Security Intelligence for **comprehensive coverage**

Expanded X-Force Threat Intelligence

Increased coverage of world-wide threat intelligence, including thorough IP reputation investigation, harvested by X-Force, to help make **smarter and more accurate security decisions** across the IBM portfolio

Security Intelligence Integration

Tight coupling between the Advanced Threat Protection Platform and QRadar Security Intelligence platform to provide unique and meaningful ways to help **detect, investigate, and remediate threats**

360-degree Intelligence

Ultimate visibility and sweeping awareness of traffic patterns and network activity, and user behavior to **identify threats**, **respond to anomalies, and prevent attacks**