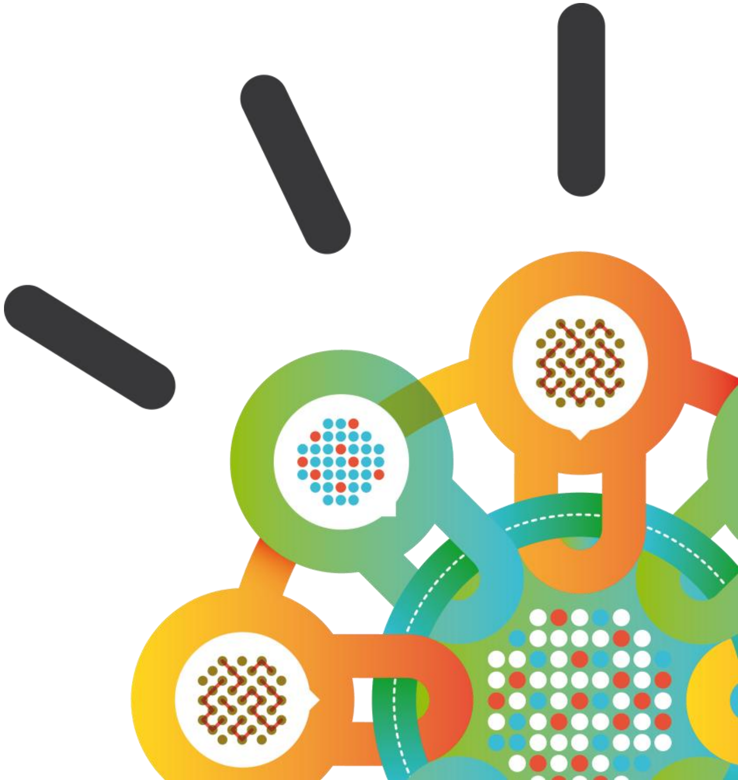
Security Intelligence.
Think Integrated.

IBM Security Systems

Überblick über die neue Brand



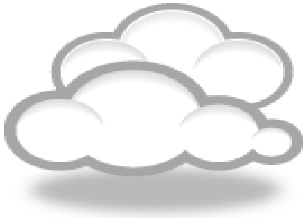
IT-Security ist einfach

- Who?
- What?
- How can I prove it?

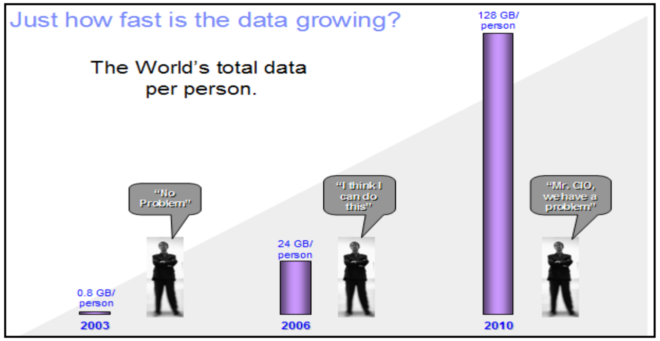
Die Welt wird immer mehr digitalisiert und vernetzt – dies öffnet die Tür für neue Bedrohungen und Schwachstellen…

Mobilität

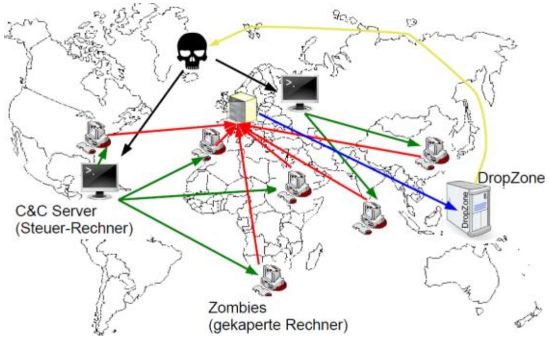
Cloud / Virtualisierung



Daten Explosion

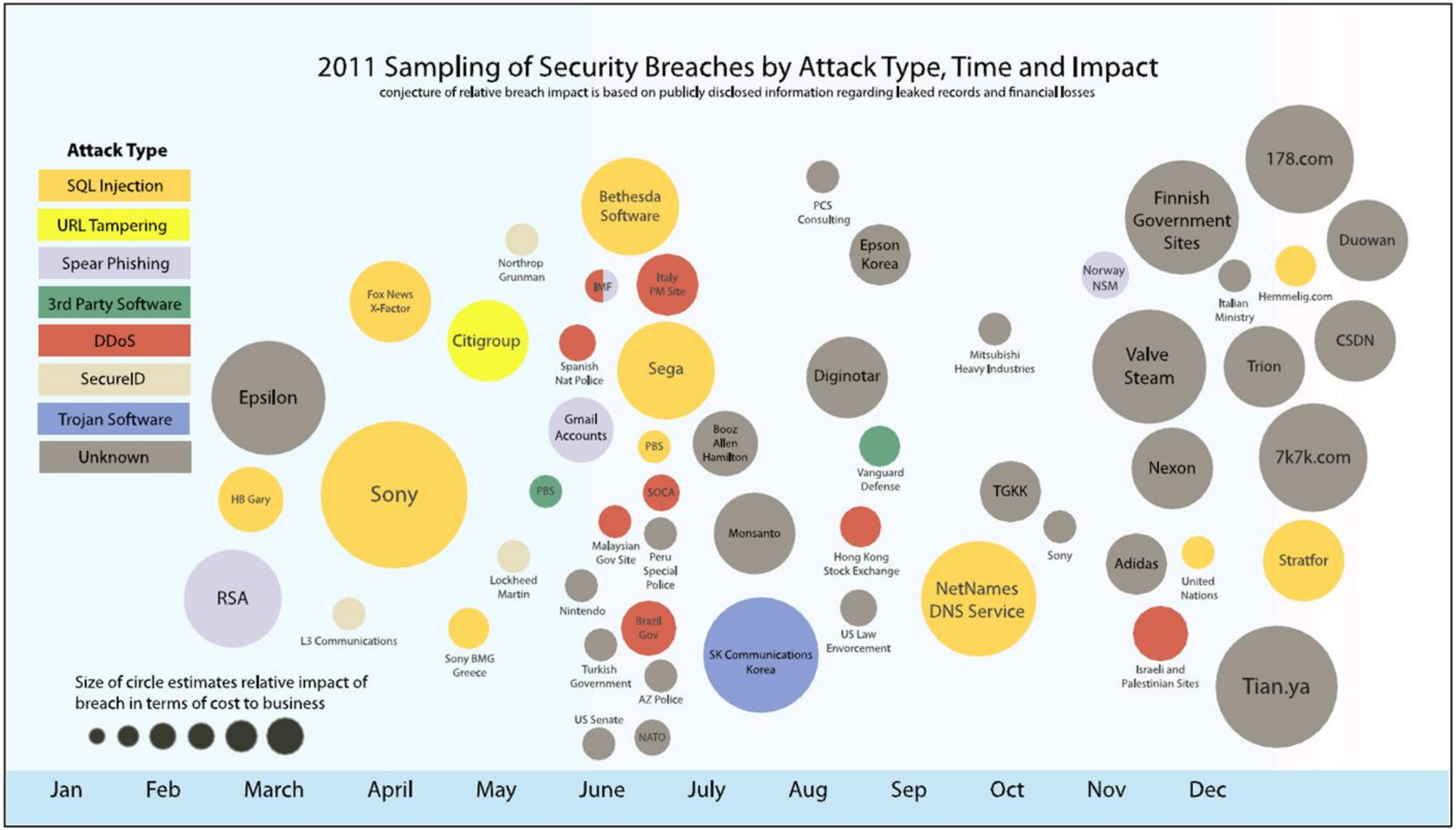


Komplexität der Angriffe



Social Business

Zielgerichtete Angriffe erschüttern Unternehmen und Behörden



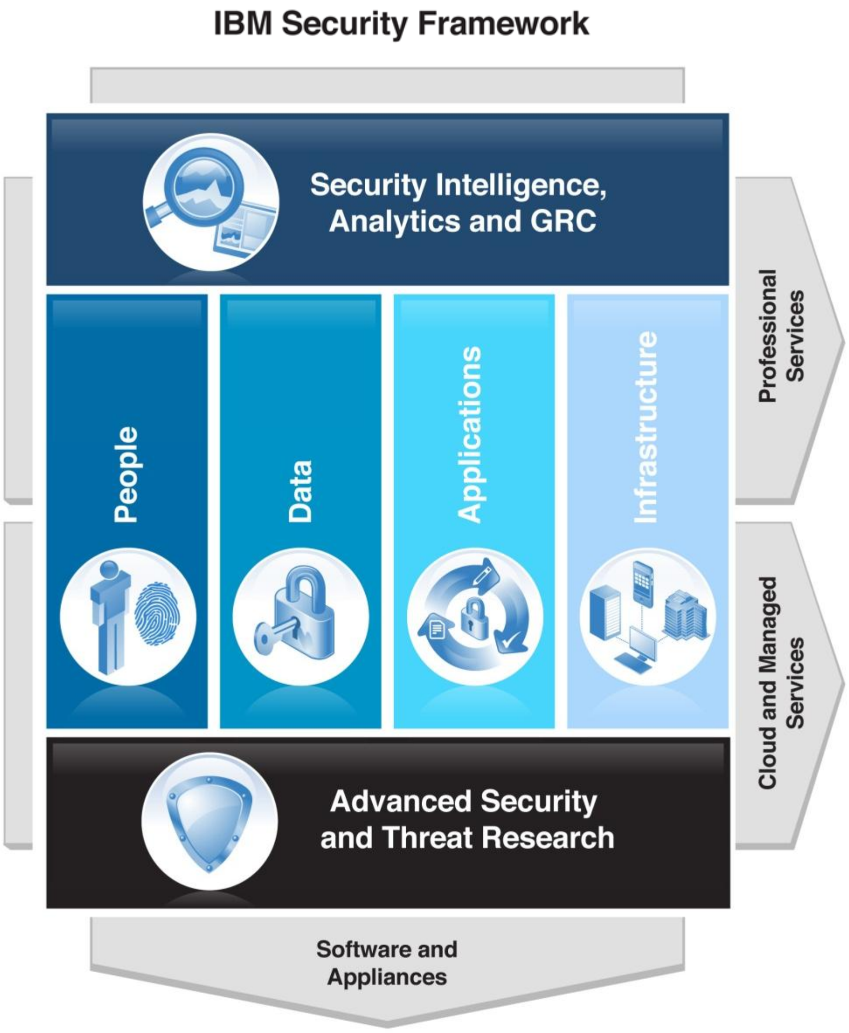
Source: IBM X-Force® 2011 Trend and Risk Report

IBM Security Systems - Expertise auf Basis eines Security Framework

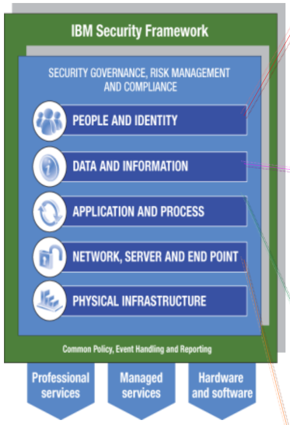
IBM Security Systems

- Einziger Anbieter im Markt mit “end-to-end” Lösungen und Kompetenz
- 6K+ Security Engineers und Consultants
- Einzigartiges research durch X-Force®
- Größte Datenbank über Angriffsvarianten in der Industrie

Intelligence ● Integration ● Expertise

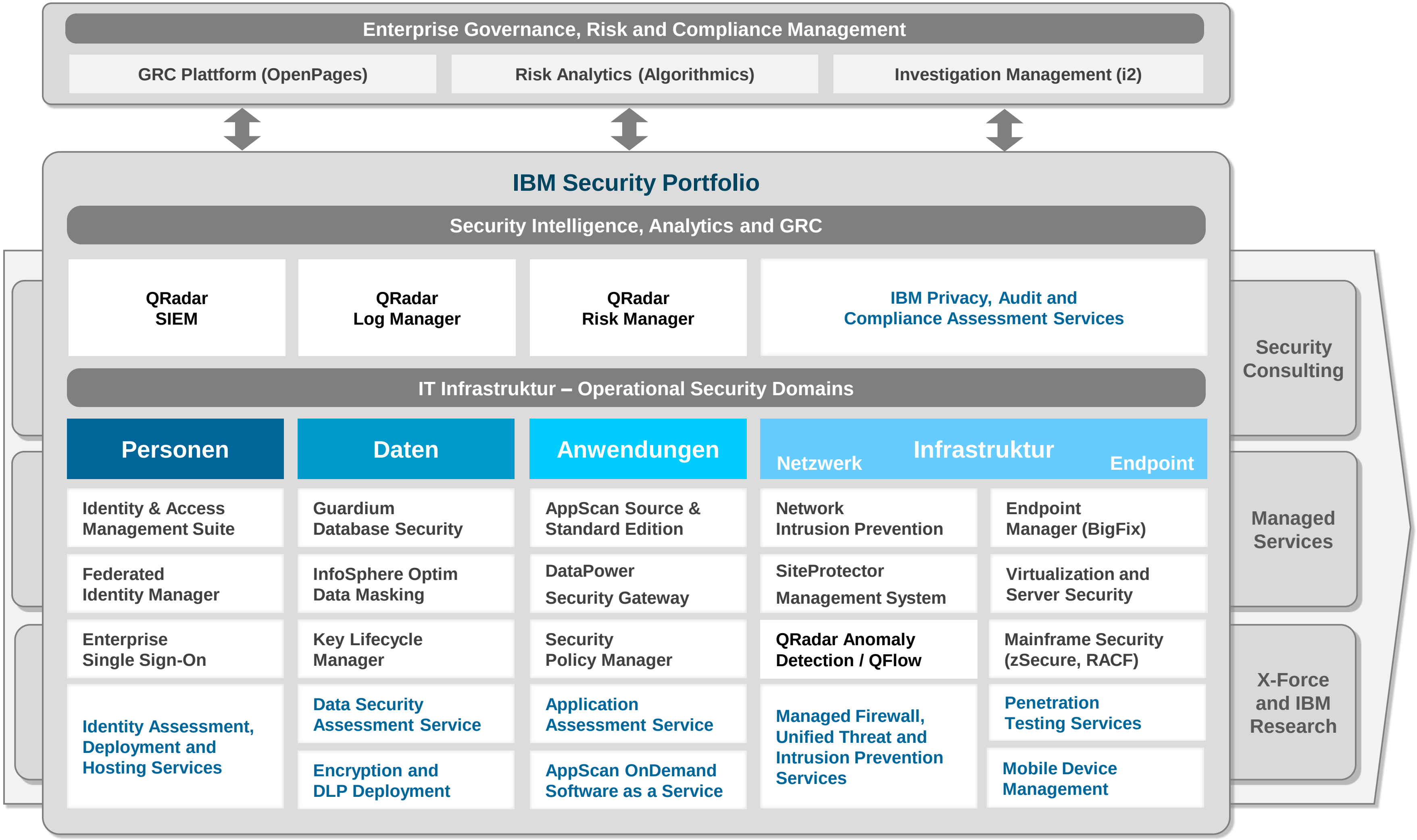

IBM Security Framework
Security Intelligence, Analytics and GRC
People
Data
Applications
Infrastructure
Advanced Security and Threat Research
Professional Services
Cloud and Managed Services
Software and Appliances

IBM Security Systems - Security Intelligence



Basic	Proficient	Optimized
Directory management	User Account & Role management SSO and Strong Authentication Log Management	Role-based analytics Fine-grained entitlements Privileged user management
Encryption	Data Masking Database activity monitoring Data Leakage Protection	Data flow analytics Automated Data Discovery and Classification Encryption Key Management
Dynamic Vulnerability Analysis e-Mail Protection	Static Source Code Analysis Real-time Vulnerability Prevention SOA Message Protection	Application analytics Fraud Detection
Network Host Anti-Virus	Professional Assessments Endpoint Management Virtualized	Advanced Monitoring & Forensics Managed Security Services

IBM Security Systems Portfolio



Enterprise Governance, Risk and Compliance Management

GRC Plattform (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 Infrastruktur – Operational Security Domains

Personen	Daten	Anwendungen	Infrastruktur	
			Netzwerk	Endpoint
Identity & Access Management Suite	Guardium Database Security	AppScan Source & Standard Edition	Network Intrusion Prevention	Endpoint Manager (BigFix)
Federated Identity Manager	InfoSphere Optim Data Masking	DataPower Security Gateway	SiteProtector Management System	Virtualization and Server Security
Enterprise Single Sign-On	Key Lifecycle Manager	Security Policy Manager	QRadar Anomaly Detection / QFlow	Mainframe Security (zSecure, RACF)
Identity Assessment, Deployment and Hosting Services	Data Security Assessment Service	Application Assessment Service	Managed Firewall, Unified Threat and Intrusion Prevention Services	Penetration Testing Services
	Encryption and DLP Deployment	AppScan OnDemand Software as a Service		Mobile Device Management

Security Consulting

Managed Services

X-Force and IBM Research

Products Services

Analysts recognize IBM’s superior products and performance

Domain	Report	Analyst Recognition					
Security Intelligence, Analytics and GRC	Security Information & Event Management (SIEM)	2011	★			2010	★
	Enterprise Governance Risk & Compliance Platforms	2011	★	2011	★		
People	User Provisioning / Administration	2011	★			2010	★
	Role Management & Access Recertification			2011	★		
	Enterprise Single Sign-on (ESSO)	2011*	★				
	Web Access Management (WAM)	2011*	★				
Data	Database Auditing & Real-Time Protection			2011	★		
Applications	Static Application Security Testing (SAST)	2010	★			2010	★
	Dynamic Application Security Testing (DAST)	2011	★				
Infrastructure Network	Network Intrusion Prevention Systems (NIPS)	2010	★			2010	★
Endpoint	EndPoint Protection Platforms (EPP)	2011	★				

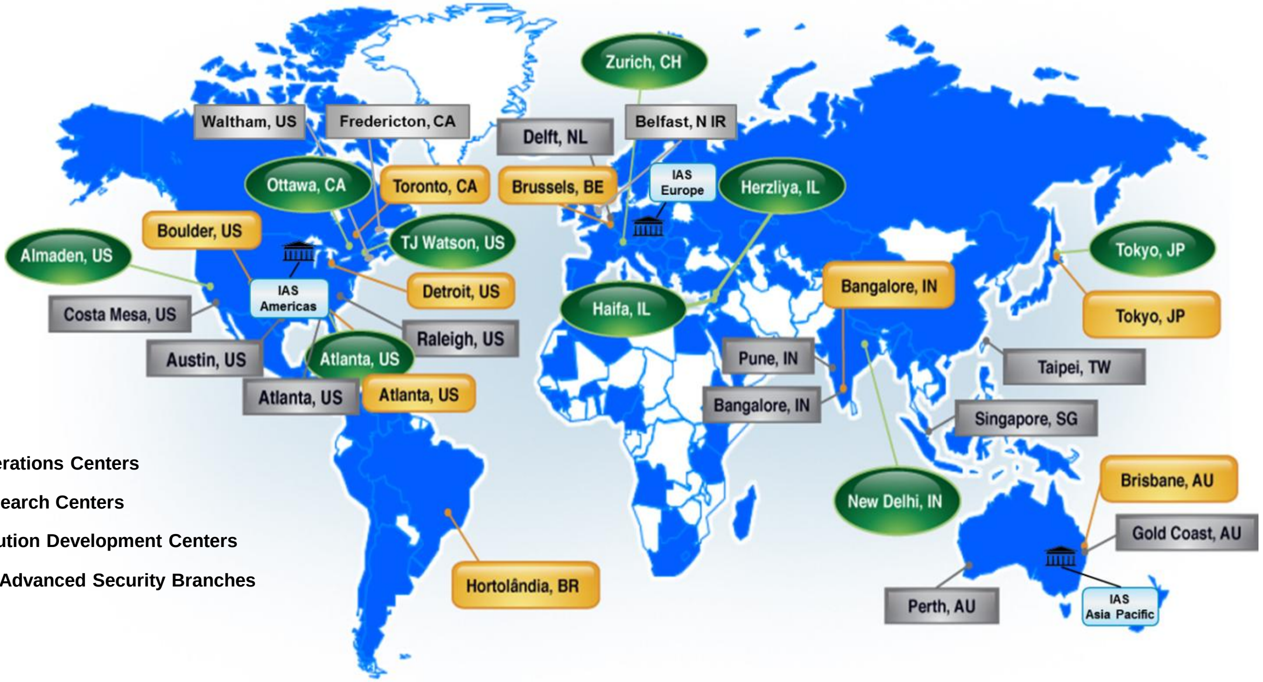
Gartner ★ Challenger ★ Leader ★ Visionary ★ Niche Player

IDC Analyze the Future ★ Leader (#1, 2, or 3 in segment)

FORRESTER ★ Leader ★ Strong Performer ★ Contender

* Gartner MarketScope

Expertise: Unmatched global coverage and security awareness



🟨 Security Operations Centers

🟢 Security Research Centers

⬜ Security Solution Development Centers

🏛 Institute for Advanced Security Branches

IBM Research

IBM Institute for Advanced Security

Enabling cybersecurity innovation and collaboration

10B analyzed Web pages & images

150M intrusion attempts daily

40M spam & phishing attacks

46K documented vulnerabilities

Millions of unique malware samples

X FORCE

World Wide Managed Security Services Coverage

- 20,000+ devices under contract
- 3,700+ MSS clients worldwide
- 9B+ events managed per day
- 1,000+ security patents
- 133 monitored countries (MSS)

Ausschnitt aus dem Portfolio:

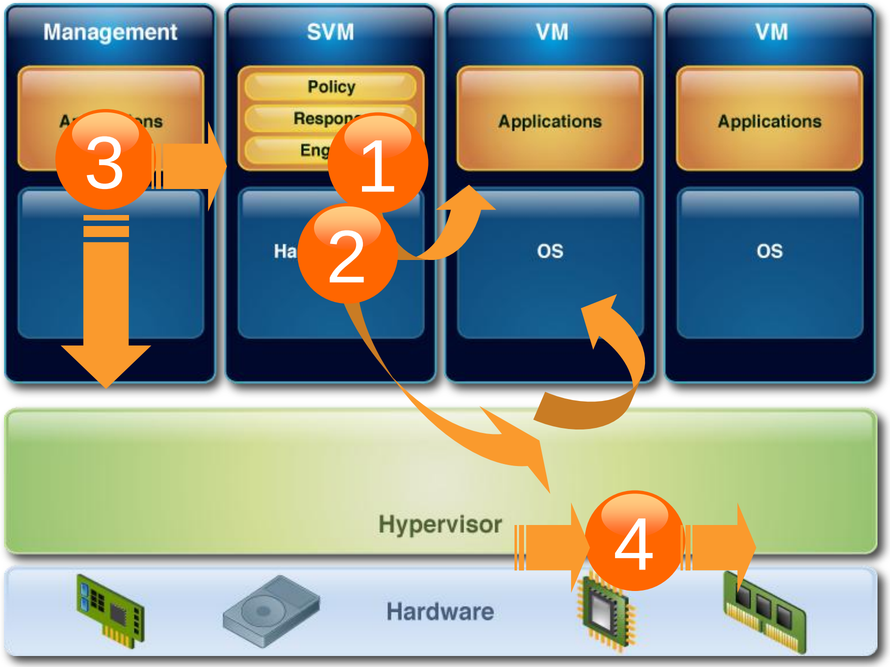
- Virtual Server Protection
- Endpoint Management
- Security Intelligence

Virtual Server Protection

Zugriffsschutz – Was gilt es in virtualisierten Umgebungen besonders zu beachten?

1 **VM-nach-VM Attacken**
Angriffe aus virtuellen Maschinen auf andere Systeme im gleichen Hypervisor

2 **VM-Diebstahl / Kapern von VMs**
Angriffe auf den Hypervisor – über den Hypervisor besteht Zugang zu allen Ressourcen



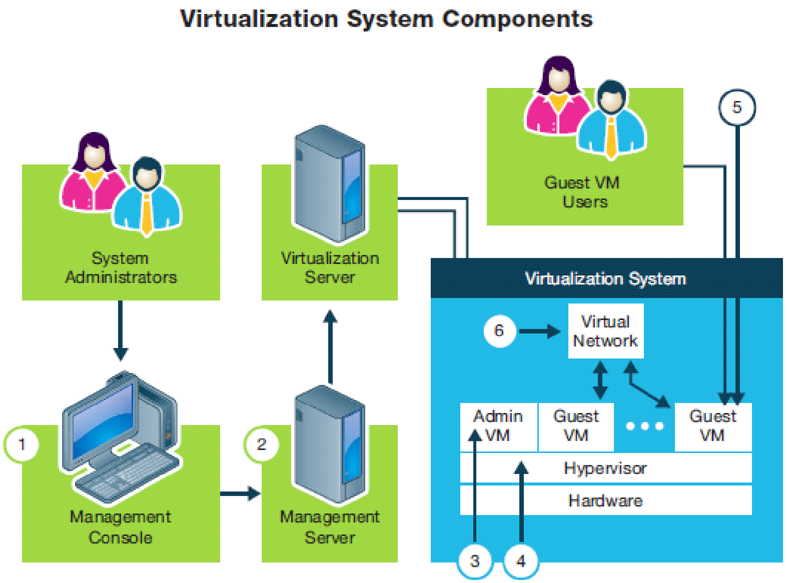
3 **Management Schwachstellen**
Angriffe über die Management Funktion auf die virtuelle Infrastruktur

4 **VM-Sprawl (Wuchern)**
Vortäuschen von Ressourcen um zu transferierende VMs umzuleiten

Neue Sicherheitslücken die mit bestehender Sicherheitsinfrastruktur nicht oder nur sehr aufwändig ermittelt werden können, da sie innerhalb des Hypervisors stattfinden

Schwachstellen in Virtualisierungsplattformen

Analyse von 80 bekannten Schwachstellen



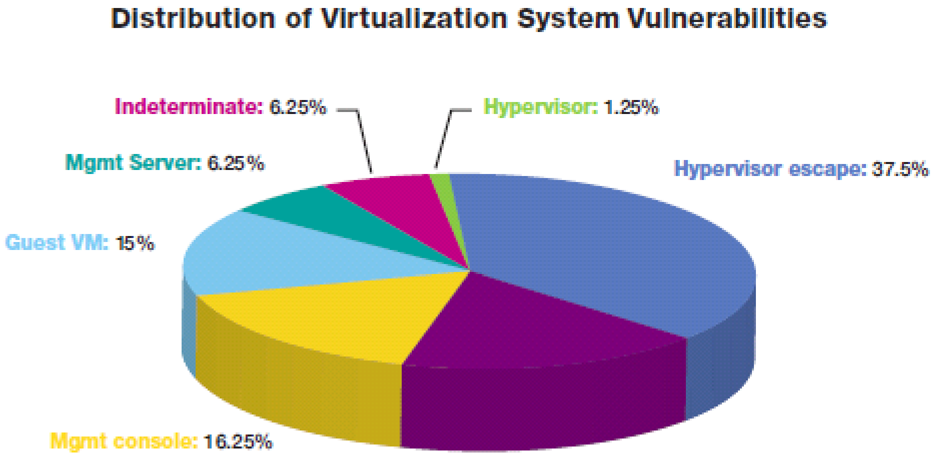


Figure 65: Distribution of Virtualization System Vulnerabilities

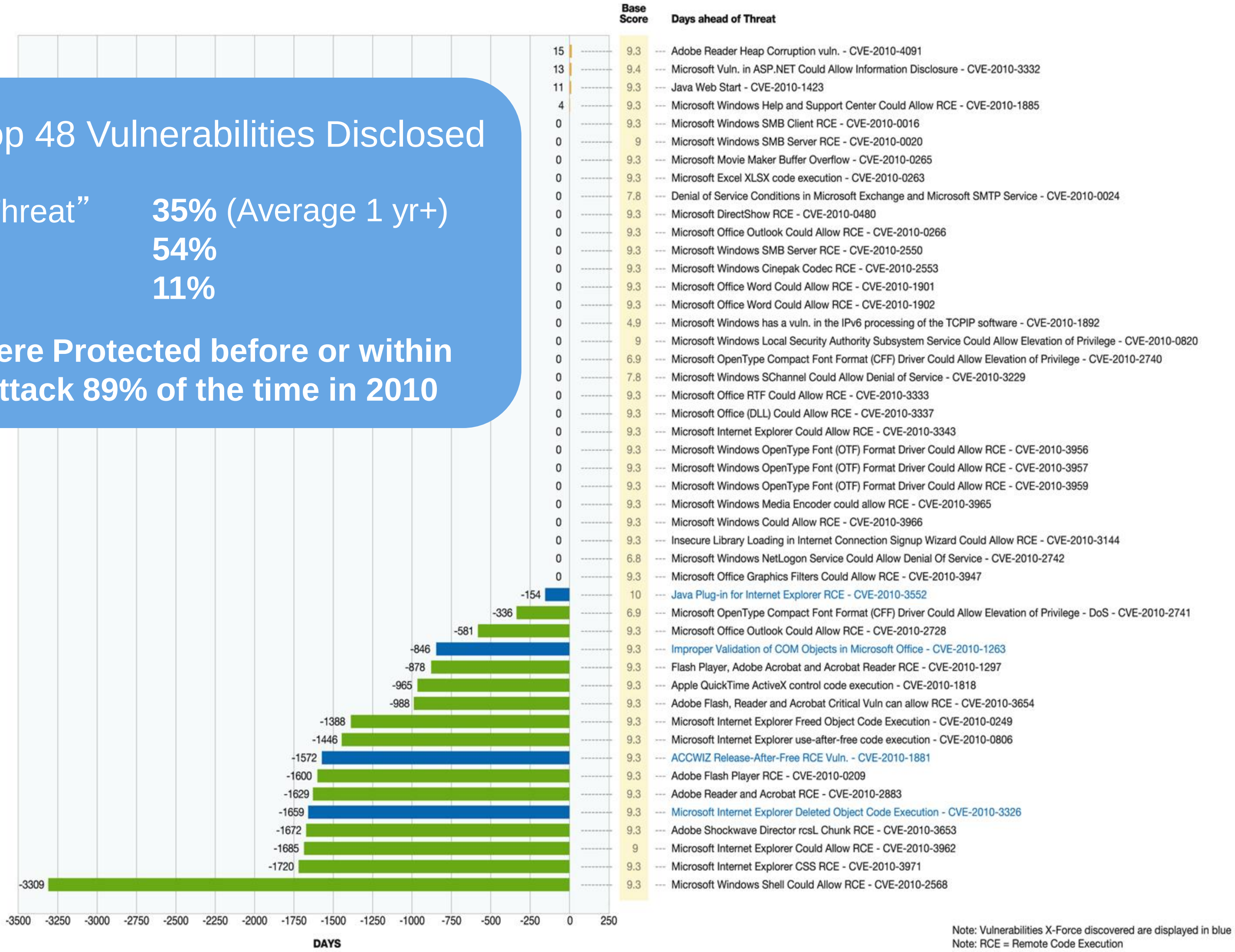
The Result? IBM Delivers Real-World Security Effectiveness

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

Note: Vulnerabilities X-Force discovered are displayed in blue
Note: RCE = Remote Code Execution

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

Beispiel:
Intrusion Prevention für Server, Netzwerke, Desktop, VMware

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

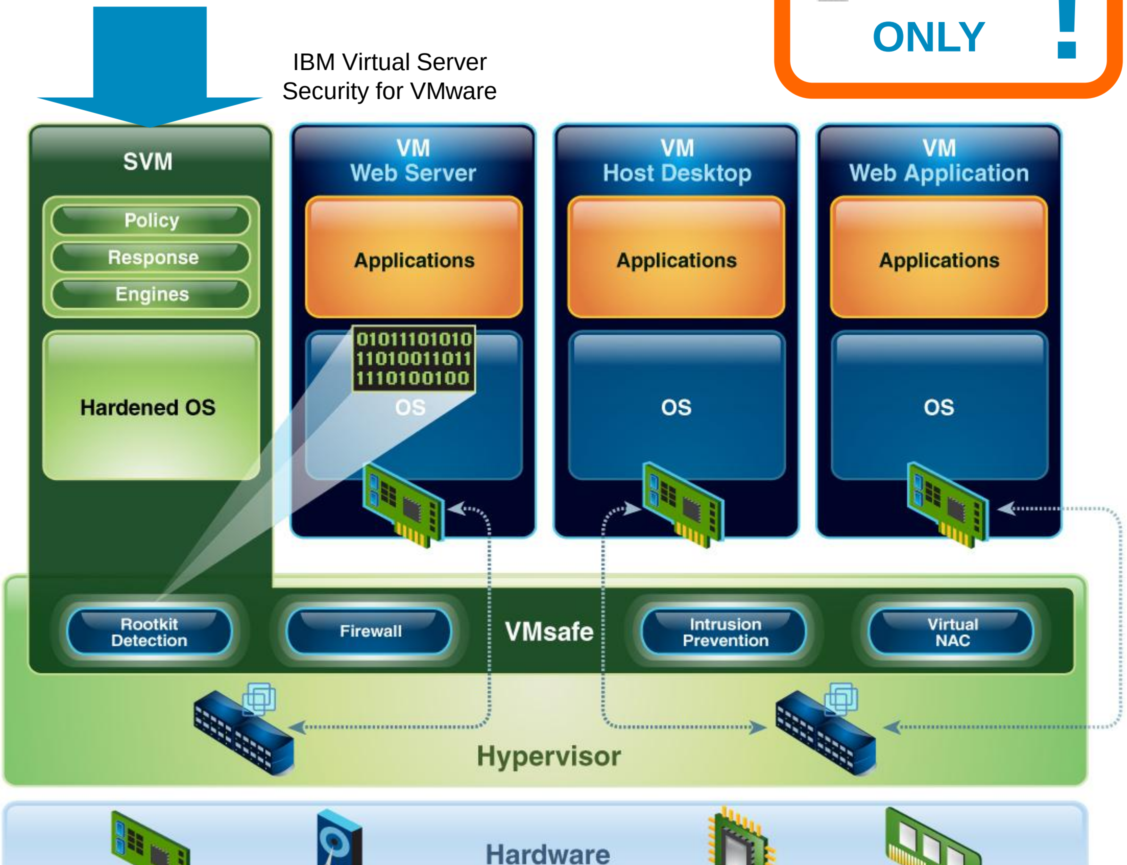
What It Does:
Manages control of unauthorized applications and risks within defined segments of the network, such as ActiveX fingerprinting, Peer To Peer, Instant Messaging, and tunneling.

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

Lösungsansatz:
Die Sicherheitslösung klinkt sich in die Virtualisierungsplattform ein

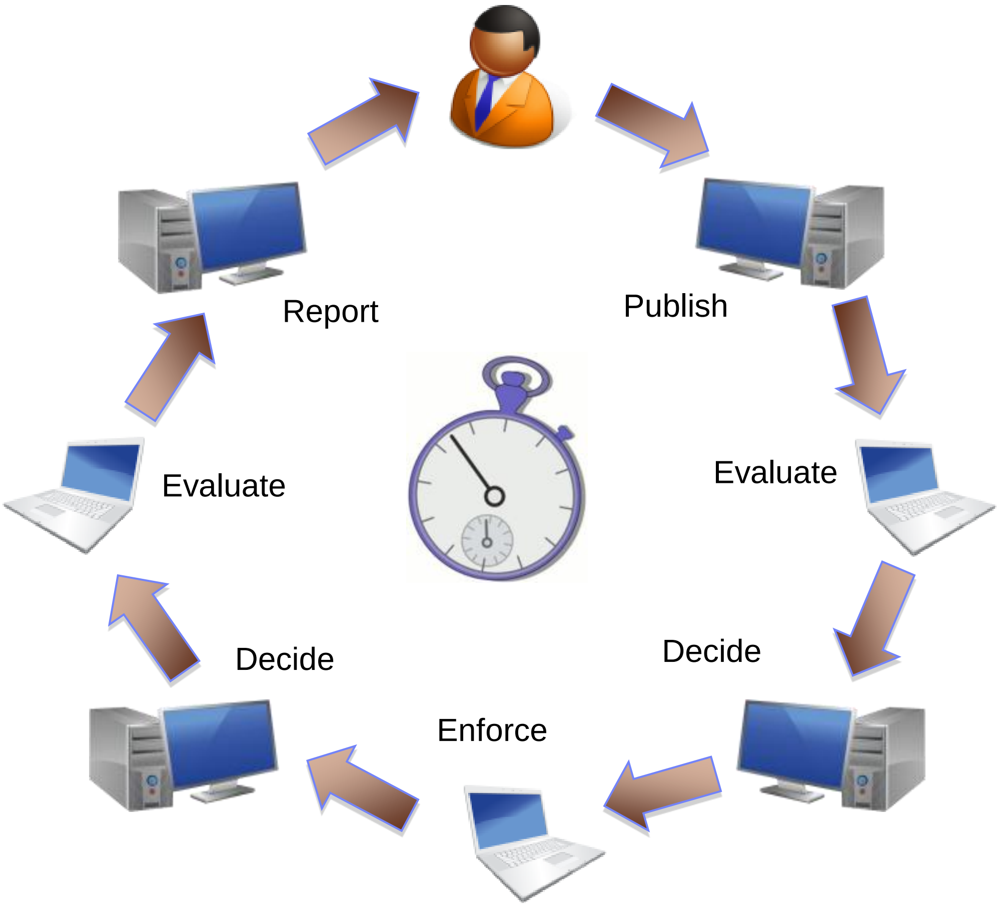
vmware ONLY !

- Unterdrückung der Malware-Verbreitung innerhalb virtueller Server
- Dynamische Erkennung und Absicherung von neuen virtuellen Ressourcen
  - – Auch mobiler VMs (VMotion)
- Eine umfassende Sicherheitslösung für VMWare beinhaltet
  - – Firewall, Intrusion Prevention mit Virtuellem Patch Management
  - – Rootkit Detection
  - – Inter-VM Traffic Analysis
  - – Virtual Network Segment Protection
  - – Virtual Network-Level Protection
  - – Virtual Infrastructure Auditing (Privileged User)
  - – Virtual Network Access Control

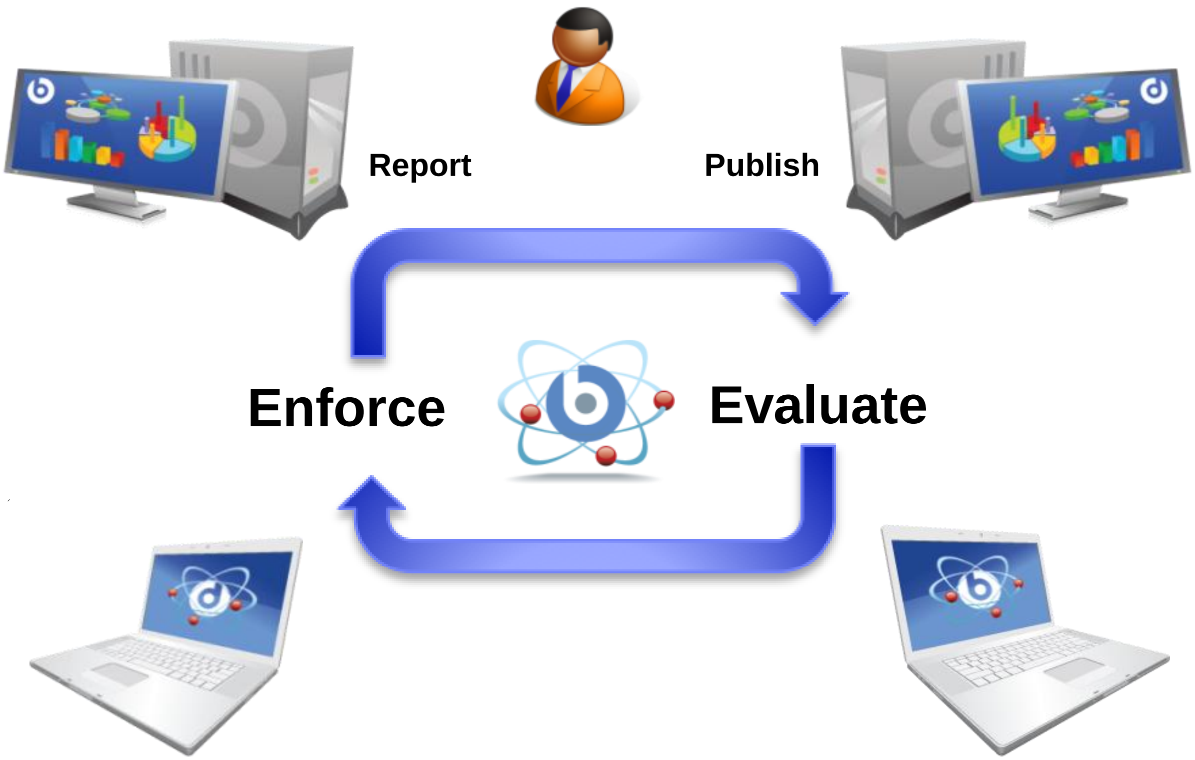


IBM Endpoint Management

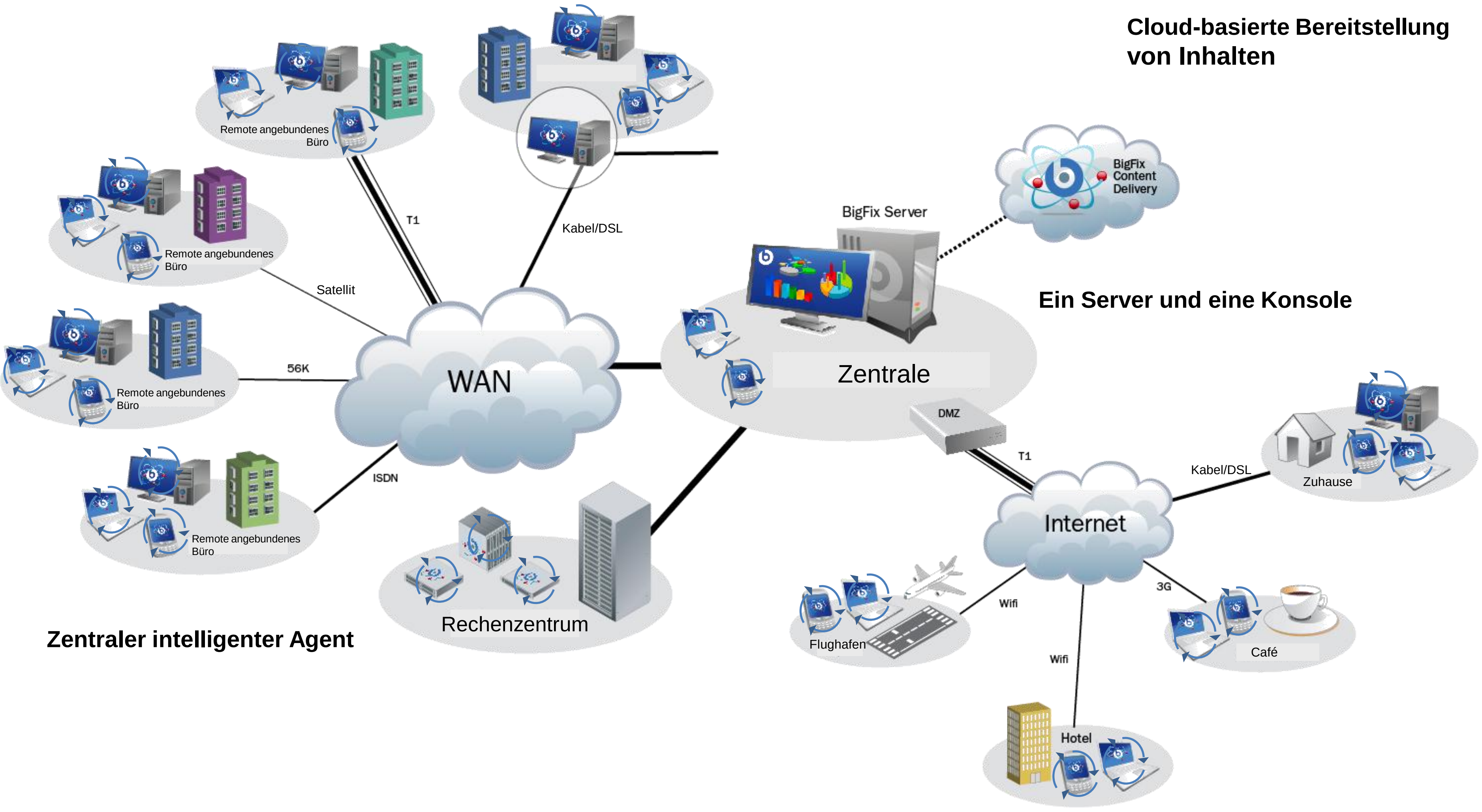
Klassische Softwareverteilung / Provisioning und Patch Mgmt.



Tivoli Endpoint Manager – ein Policy basiertes Modell!



Tivoli Endpoint Manager Architektur



Schlanke, leistungsfähige Infrastruktur

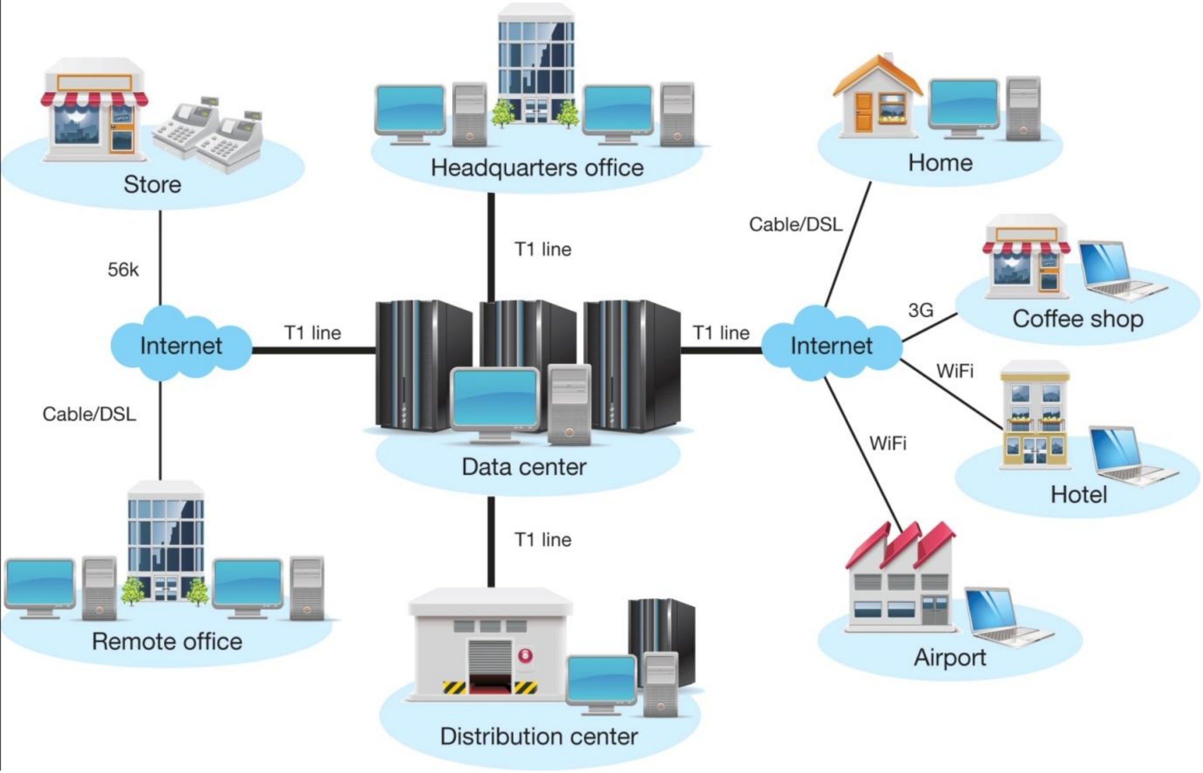
Cloud-basierte Bereitstellung von Inhalten

Ein Server und eine Konsole

Zentraler intelligenter Agent

Tivoli Endpoint Manager: Intelligentes, autonomes und schnelles Endpoint Management

- Network Asset Discovery
- Endpoint HW, SW Inventory
- Patch Management
- Software Distribution
- OS Deployment
- Remote Desktop Control
- Software Use Analysis (add on)
- Power Management (add on)



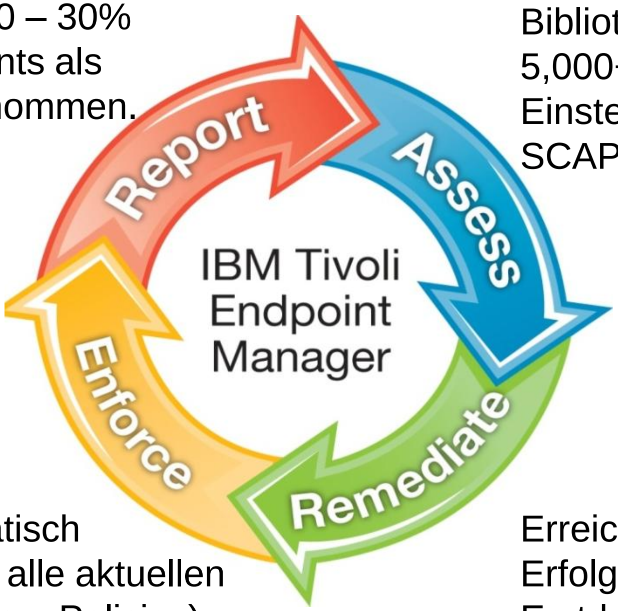
Unabhängig von Standort, Betriebssystem und Uhrzeit – Alle Systeme sind Permanent unter der sicheren Kontrolle des BigFix Agenten.

Tivoli Endpoint Manager: Alle Endpoints im sicheren Überblick

- Patch Management
- Security Configuration Management
- Vulnerability Management
- Asset Management
- Network Self Quarantine
- Multi-Vendor Endpoint Protection Management
- Anti-Malware & Web Reputation Service (add on)

TEM findet 10 – 30% mehr Endpoints als vorher angenommen.

Bibliothek mit mehr als 5,000+ Compliance Einstellungen, u.a. für FDCC SCAP, DISA STIG

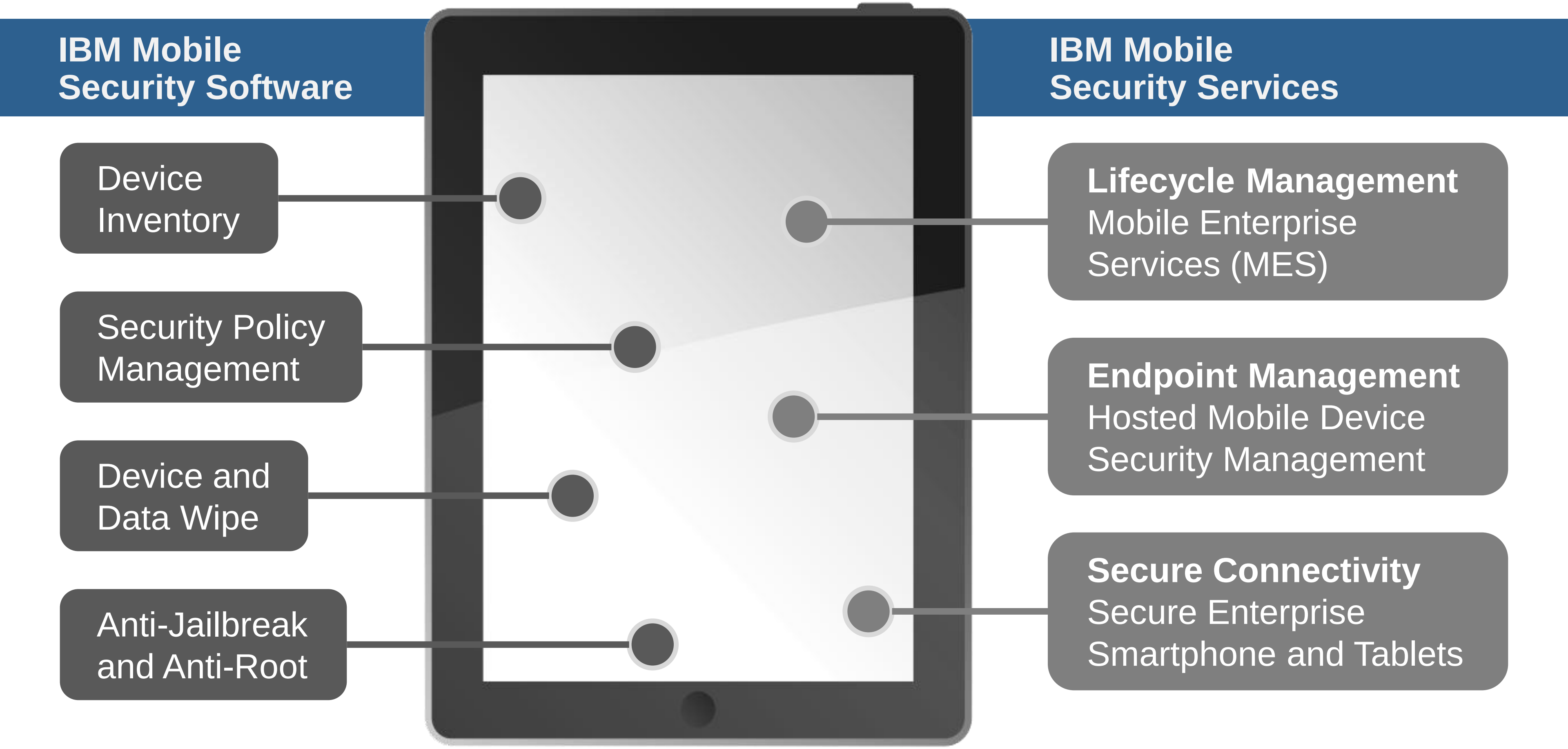


Setzt automatisch und ständige alle aktuellen Richtlinien (sog. Policies) auf allen Systemen durch.

Erreicht bis zu 95%+ Erfolgsquote beim Erstdurchlauf einer Policy oder eines Patch Deployments

Consumerization of IT

IBM is converging traditional endpoint and mobile security management into a single solution with complementary services



IBM Mobile Security Software

- Device Inventory
- Security Policy Management
- Device and Data Wipe
- Anti-Jailbreak and Anti-Root

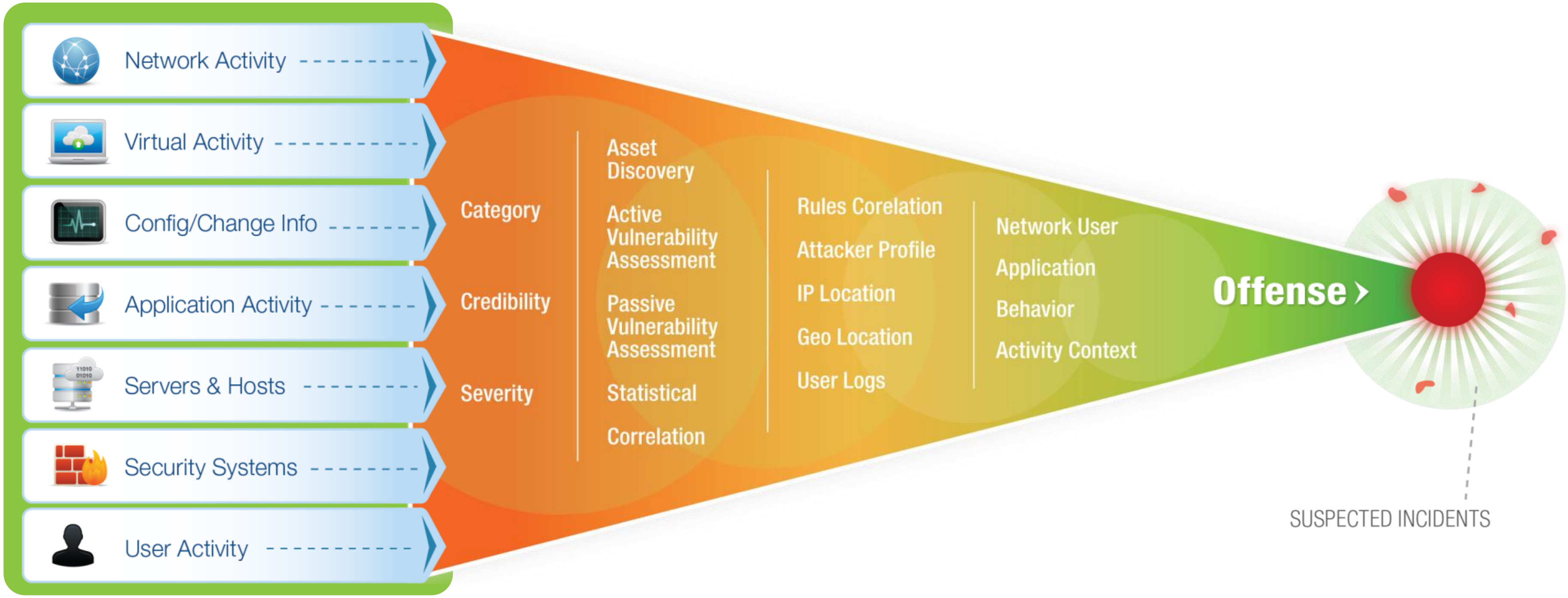
IBM Mobile Security Services

- **Lifecycle Management** Mobile Enterprise Services (MES)
- **Endpoint Management** Hosted Mobile Device Security Management
- **Secure Connectivity** Secure Enterprise Smartphone and Tablets

QRadar

Data Explosion

IBM is integrating across IT silos with Security Intelligence solutions



Sources + Intelligence = Most Accurate & Actionable Insight

Attack Sophistication

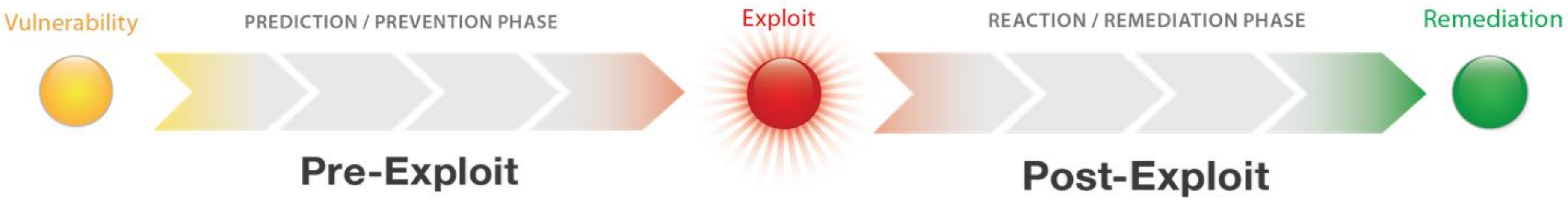
IBM is helping clients combat advanced threats with pre- and post-exploit intelligence and action

What are the external and internal threats?

Are we configured to protect against these threats?

What is happening right now?

What was the impact?



Prediction & Prevention

Risk Management. Vulnerability Management.
Configuration and Patch Management.
X-Force Research and Threat Intelligence.
Compliance Management. Reporting and Scorecards.

Reaction & Remediation

Network and Host Intrusion Prevention.
Network Anomaly Detection. Packet Forensics.
Database Activity Monitoring. Data Leak Prevention.
SIEM. Log Management. Incident Response.

IBM Security Intelligence

QRadar SIEM

Product Tour: Intelligent Offense Scoring

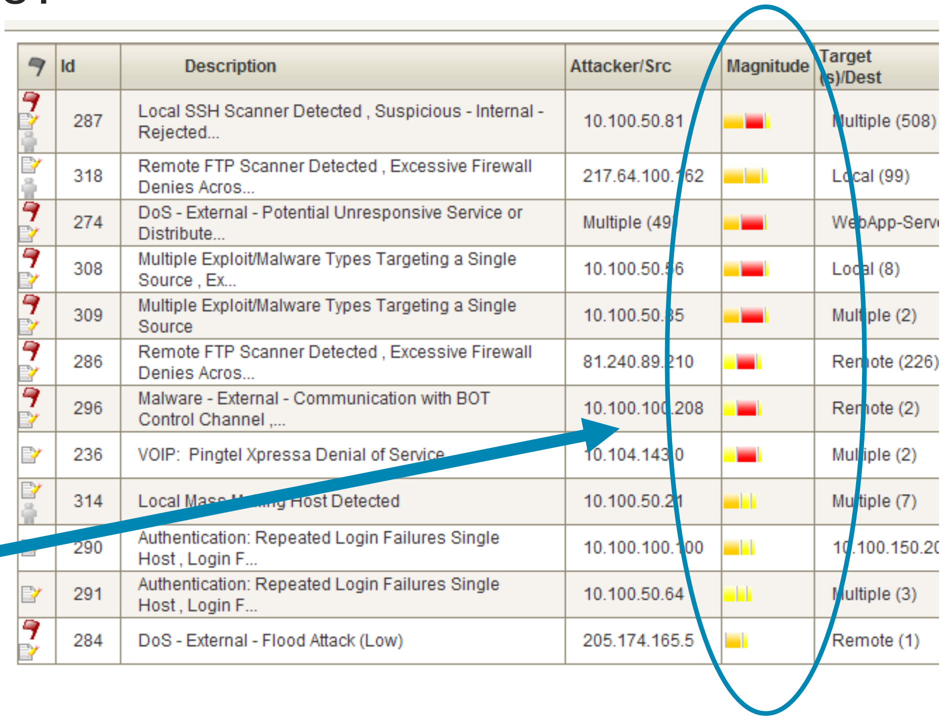
QRadar judges “magnitude” of offenses:

- *Credibility:*
  A false positive or true positive?

- *Severity:*
  Alarm level contrasted with target vulnerability

- *Relevance:*
  Priority according to asset or network value

Priorities can change over time based on situational awareness

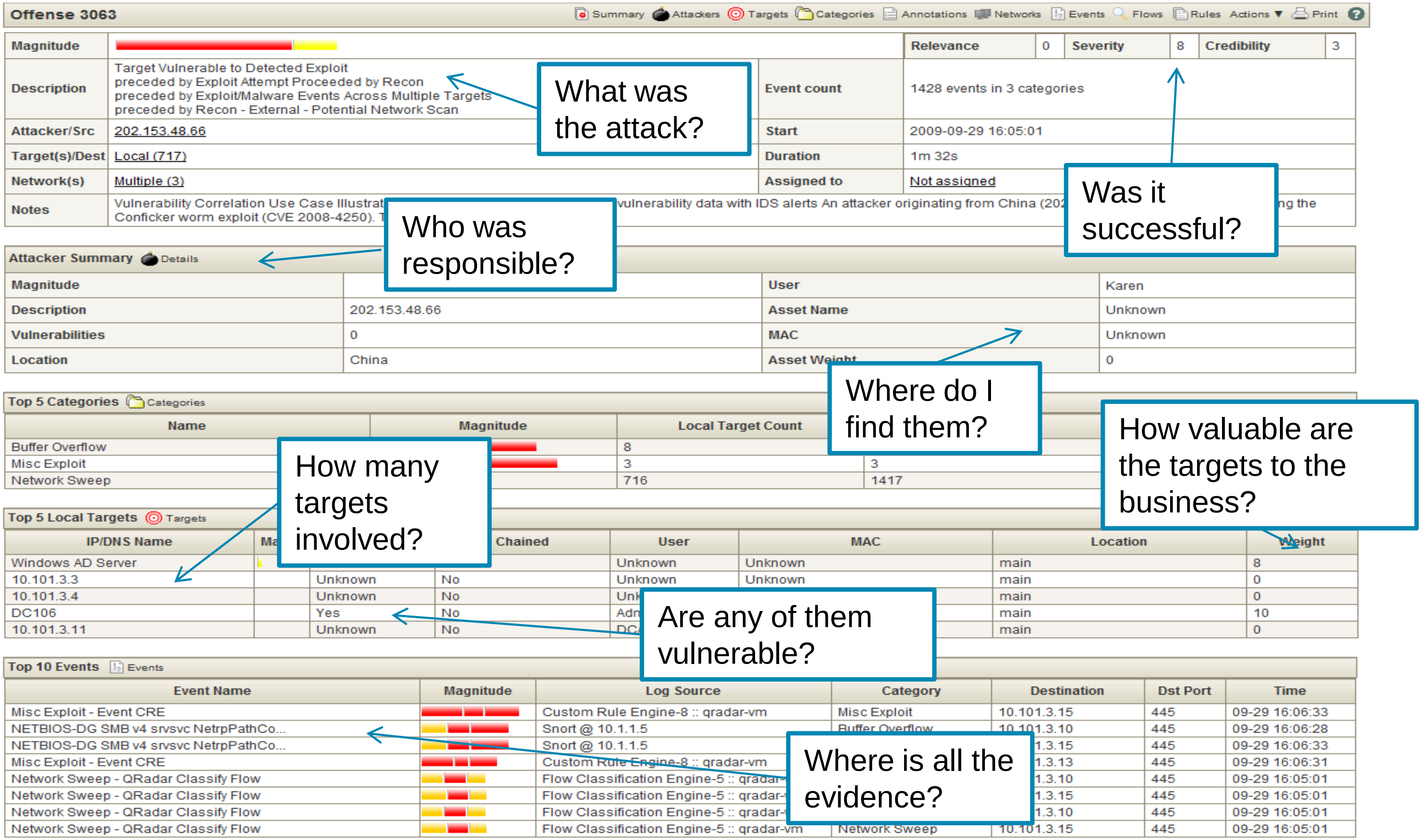


	Id	Description	Attacker/Src	Magnitude	Target(s)/Dest
	287	Local SSH Scanner Detected , Suspicious - Internal - Rejected...	10.100.50.81	🟨🟥	Multiple (508)
	318	Remote FTP Scanner Detected , Excessive Firewall Denies Acros...	217.64.100.162	🟨🟨	Local (99)
	274	DoS - External - Potential Unresponsive Service or Distribute...	Multiple (49)	🟨🟥	WebApp-Serv
	308	Multiple Exploit/Malware Types Targeting a Single Source , Ex...	10.100.50.[illegible]6	🟨🟥	Local (8)
	309	Multiple Exploit/Malware Types Targeting a Single Source	10.100.50.[illegible]5	🟨🟥	Multiple (2)
	286	Remote FTP Scanner Detected , Excessive Firewall Denies Acros...	81.240.89.[illegible]10	🟨🟥	Remote (226)
	296	Malware - External - Communication with BOT Control Channel ,...	10.100.10[illegible].208	🟨🟥	Remote (2)
	236	VOIP: Pingtel Xpressa Denial of Service	10.104.143.[illegible]0	🟨🟥	Multiple (2)
	314	Local Mass Mailing Host Detected	10.100.50.2[illegible]	🟨🟨	Multiple (7)
	290	Authentication: Repeated Login Failures Single Host , Login F...	10.100.100.[illegible]00	🟨🟨	10.100.150.20
	291	Authentication: Repeated Login Failures Single Host , Login F...	10.100.50.64	🟨🟨	Multiple (3)
	284	DoS - External - Flood Attack (Low)	205.174.165.5	🟨	Remote (1)

QRadar SIEM

Product Tour: Offense Management

Clear, concise and comprehensive delivery of relevant information:



Offense 3063 Summary Attackers Targets Categories Annotations Networks Events Flows Rules Actions ▼ Print

Magnitude	🟥🟨		Relevance	0	Severity	8	Credibility 3
Description	Target Vulnerable to Detected Exploit preceded by Exploit Attempt Proceeded by Recon preceded by Exploit/Malware Events Across Multiple Targets preceded by Recon - External - Potential Network Scan	Event count	1428 events in 3 categories				
Attacker/Src	202.153.48.66	Start	2009-09-29 16:05:01				
Target(s)/Dest	Local (717)	Duration	1m 32s				
Network(s)	Multiple (3)	Assigned to	Not assigned				
Notes	Vulnerability Correlation Use Case Illustrat vulnerability data with IDS alerts An attacker originating from China (202 ng the Conficker worm exploit (CVE 2008-4250). T						

Attacker Summary Details

Magnitude		User	Karen
Description	202.153.48.66	Asset Name	Unknown
Vulnerabilities	0	MAC	Unknown
Location	China	Asset Weight	0

Top 5 Categories Categories

Name	Magnitude	Local Target Count	
Buffer Overflow	🟥	8	
Misc Exploit	🟥	3	3
Network Sweep		716	1417

Top 5 Local Targets Targets

IP/DNS Name	Ma		Chained	User	MAC	Location	Weight
Windows AD Server	🟨			Unknown	Unknown	main	8
10.101.3.3		Unknown	No	Unknown	Unknown	main	0
10.101.3.4		Unknown	No	Unk		main	0
DC106		Yes	No	Adm		main	10
10.101.3.11		Unknown	No	DC		main	0

Top 10 Events Events

Event Name	Magnitude	Log Source	Category	Destination	Dst Port	Time
Misc Exploit - Event CRE	🟥🟥🟥	Custom Rule Engine-8 :: qradar-vm	Misc Exploit	10.101.3.15	445	09-29 16:06:33
NETBIOS-DG SMB v4 srvsvc NetrPathCo...	🟨🟥🟥	Snort @ 10.1.1.5	Buffer Overflow	10.101.3.10	445	09-29 16:06:28
NETBIOS-DG SMB v4 srvsvc NetrPathCo...	🟨🟥🟥	Snort @ 10.1.1.5		1.3.15	445	09-29 16:06:33
Misc Exploit - Event CRE	🟥🟥🟥	Custom Rule Engine-8 :: qradar-vm		1.3.13	445	09-29 16:06:31
Network Sweep - QRadar Classify Flow	🟨🟥🟨	Flow Classification Engine-5 :: qradar-		1.3.10	445	09-29 16:05:01
Network Sweep - QRadar Classify Flow	🟨🟥🟨	Flow Classification Engine-5 :: qradar-		1.3.15	445	09-29 16:05:01
Network Sweep - QRadar Classify Flow	🟨🟥🟨	Flow Classification Engine-5 :: qradar-		1.3.10	445	09-29 16:05:01
Network Sweep - QRadar Classify Flow	🟨🟥🟨	Flow Classification Engine-5 :: qradar-vm	Network Sweep	10.101.3.15	445	09-29 16:05:01

What was the attack?

Was it successful?

Who was responsible?

Where do I find them?

How many targets involved?

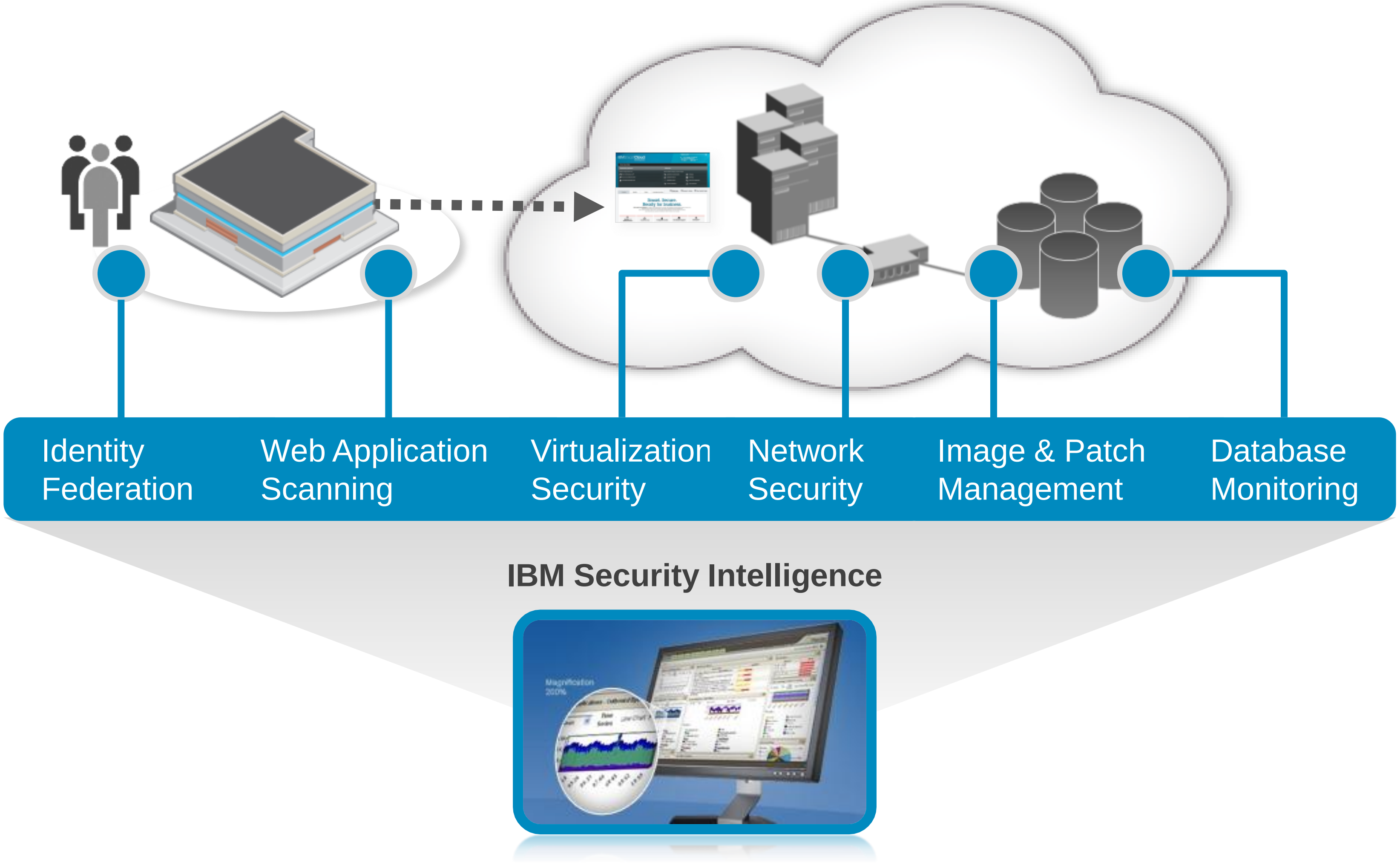
How valuable are the targets to the business?

Are any of them vulnerable?

Where is all the evidence?

Everything is Everywhere

IBM is helping clients adopt cloud with flexible, layered security solutions



Identity Federation

Web Application Scanning

Virtualization Security

Network Security

Image & Patch Management

Database Monitoring

IBM Security Intelligence

Intelligent solutions provide the DNA to secure a Smarter Planet

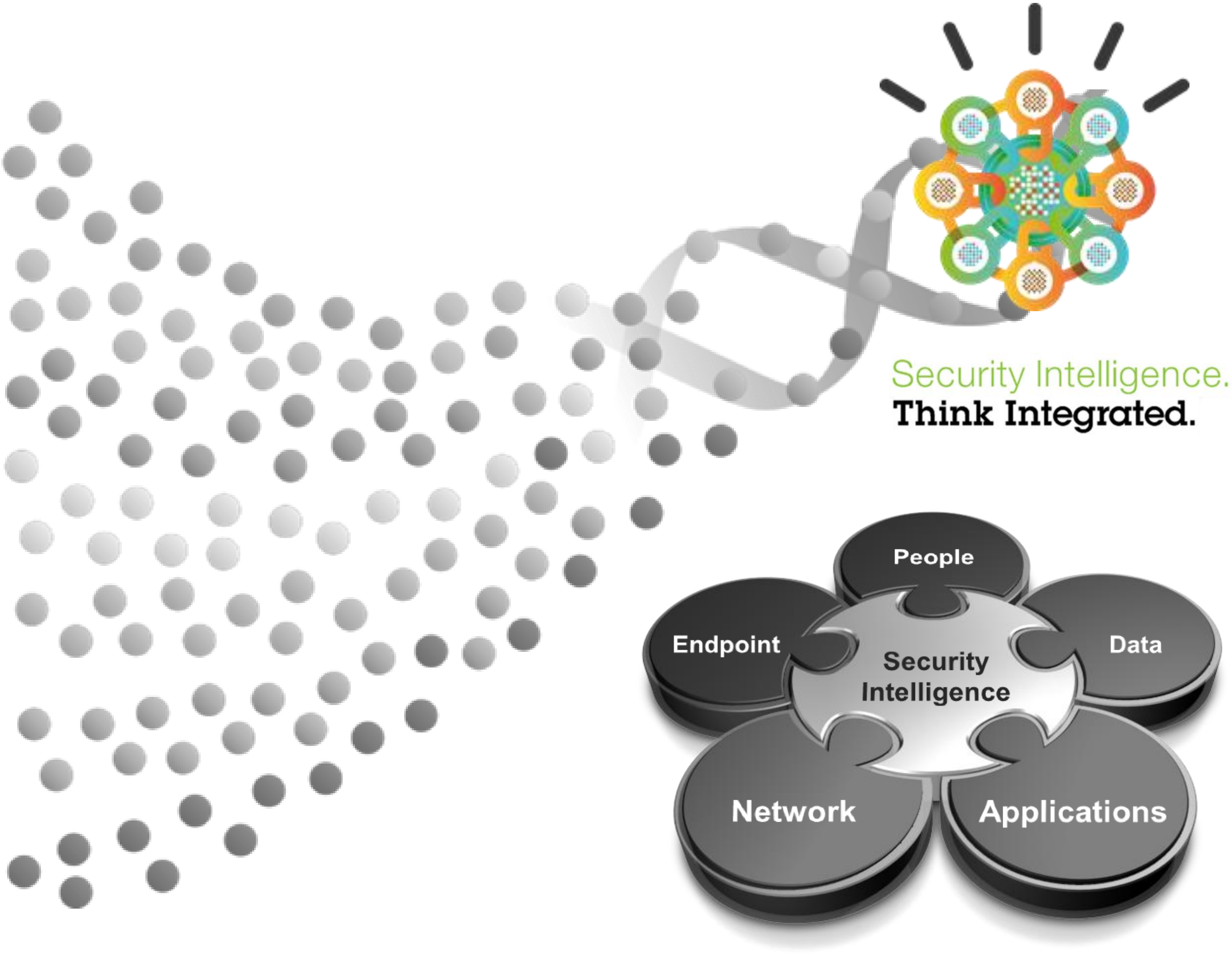
Security Intelligence, Analytics & GRC

People

Data

Applications

Infrastructure



Security Intelligence.
Think Integrated.

ibm.com/security