Security Solutions In The Cloud: How IBM Helps You Regain Visibility

Giancarlo V. Marchesi
Manager, Security Worldwide A-Team (SWAT)

Content Provided By: Nicholas Harlow
IBM Security Systems Product Management

Landscape: IT & Security

Current Security Challenges

The world is becoming more digitized and interconnected, opening the door to emerging threats and leaks

Data Explosion

The age of Big Data – the explosion of digital information – has arrived and is facilitated by the pervasiveness of applications accessed from everywhere

Consumerization of IT

With the advent of Enterprise 2.0 and social business, the line between personal and professional hours, devices and data has disappeared

EVERYTHING IS EVERYWHERE

Organizations continue to move to new platforms including cloud, virtualization, mobile, social business and more

Attack Sophistication

The speed and dexterity of attacks has increased coupled with new actors with new motivations from cyber crime to terrorism to state-sponsored intrusions

Fighting To Prevent Access To Corporate Networks

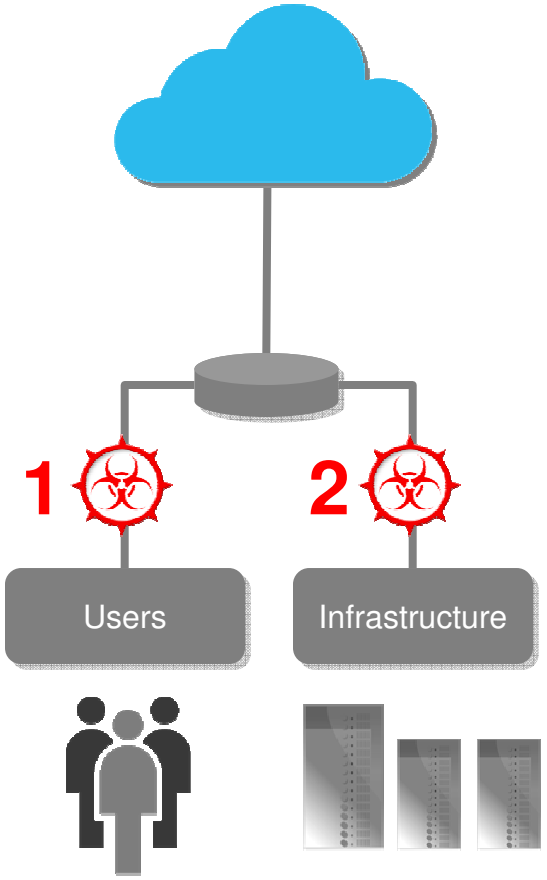
Closer look at the attack vectors of today's threats

1. User Attacks (Client-side)

- **Drive-by Downloads:** User browses to a malicious website and/or downloads an infected file using an unpatched browser or application
- **Targeted Emails:** Email containing an exploit or malicious attachment is sent to an individual with the right level of access at the company

2. Infrastructure Attacks (Server-side)

- **SQL Injection:** Attacker sends a specially crafted message to a web application, allowing them to view, modify, or delete DB table entries
- **General Exploitation:** Attacker identifies and exploits a vulnerability in unpatched or poorly written software to gain privileges on the system



Despite the growing number of techniques used to gain access, one fact remains constant:
a remote attacker must gain access over the corporate network

IBM Security Framework

Delivering intelligence, integration and expertise across a comprehensive framework

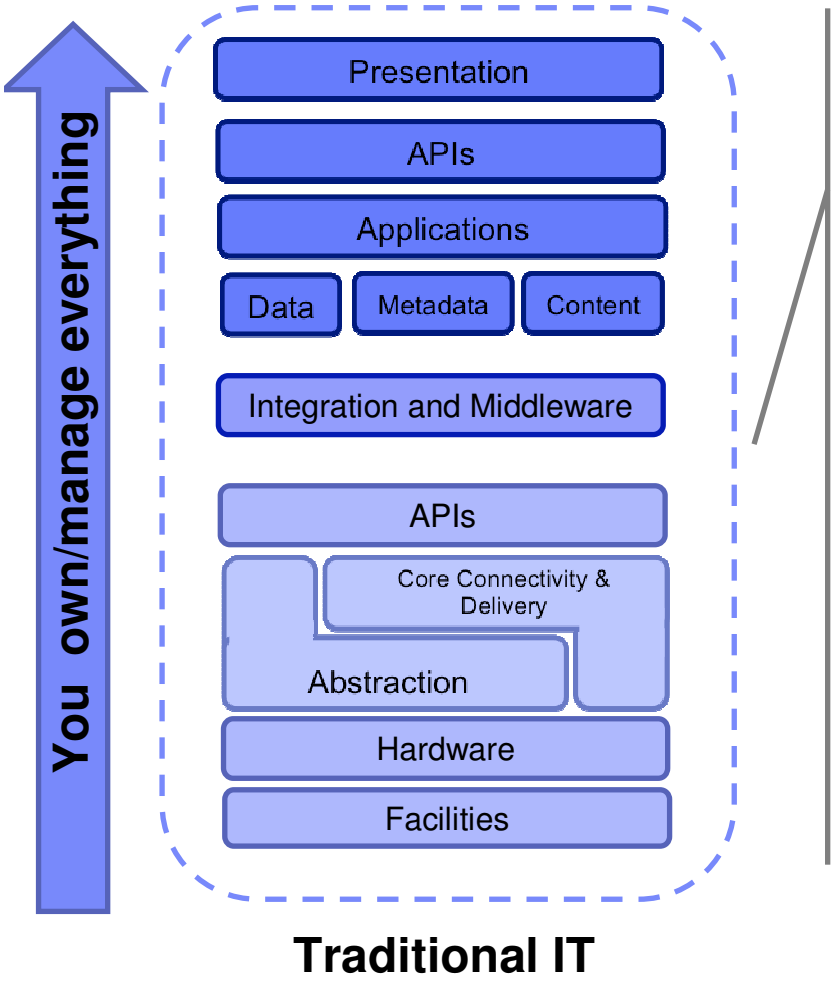
IBM Security

- End-to-end coverage of the security foundation
- 6K+ security engineers and consultants
- Award-winning X-Force® research
- Large vulnerability database

Intelligence • Integration • Expertise

Transition To Cloud IT

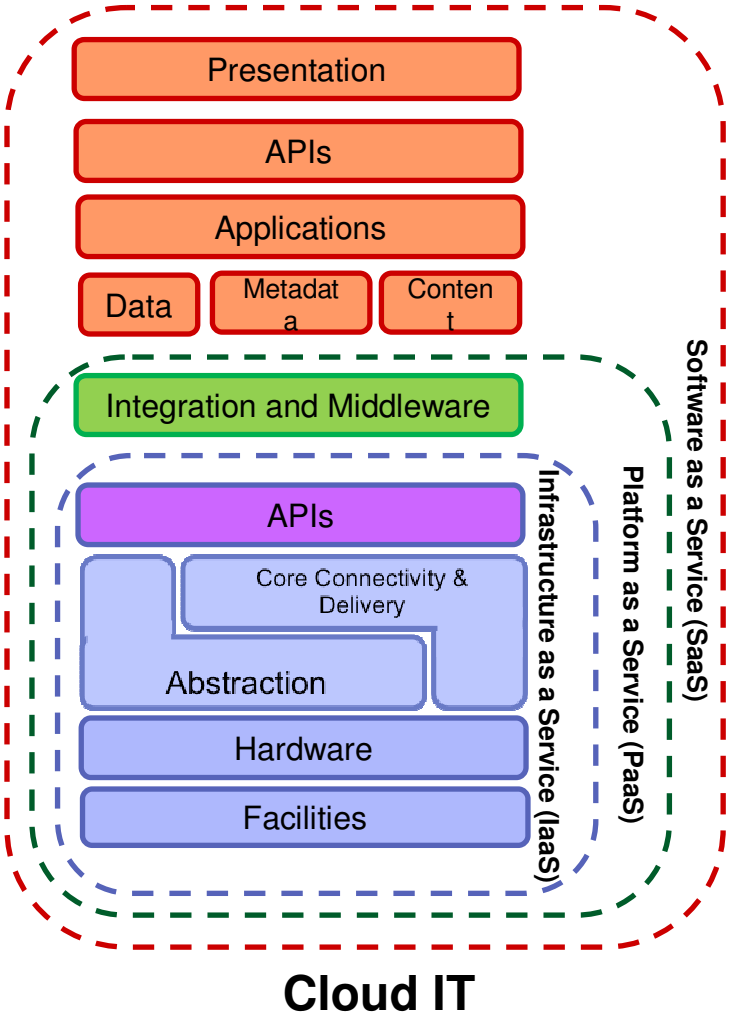
Securing Traditional IT Environments…



Traditional IT

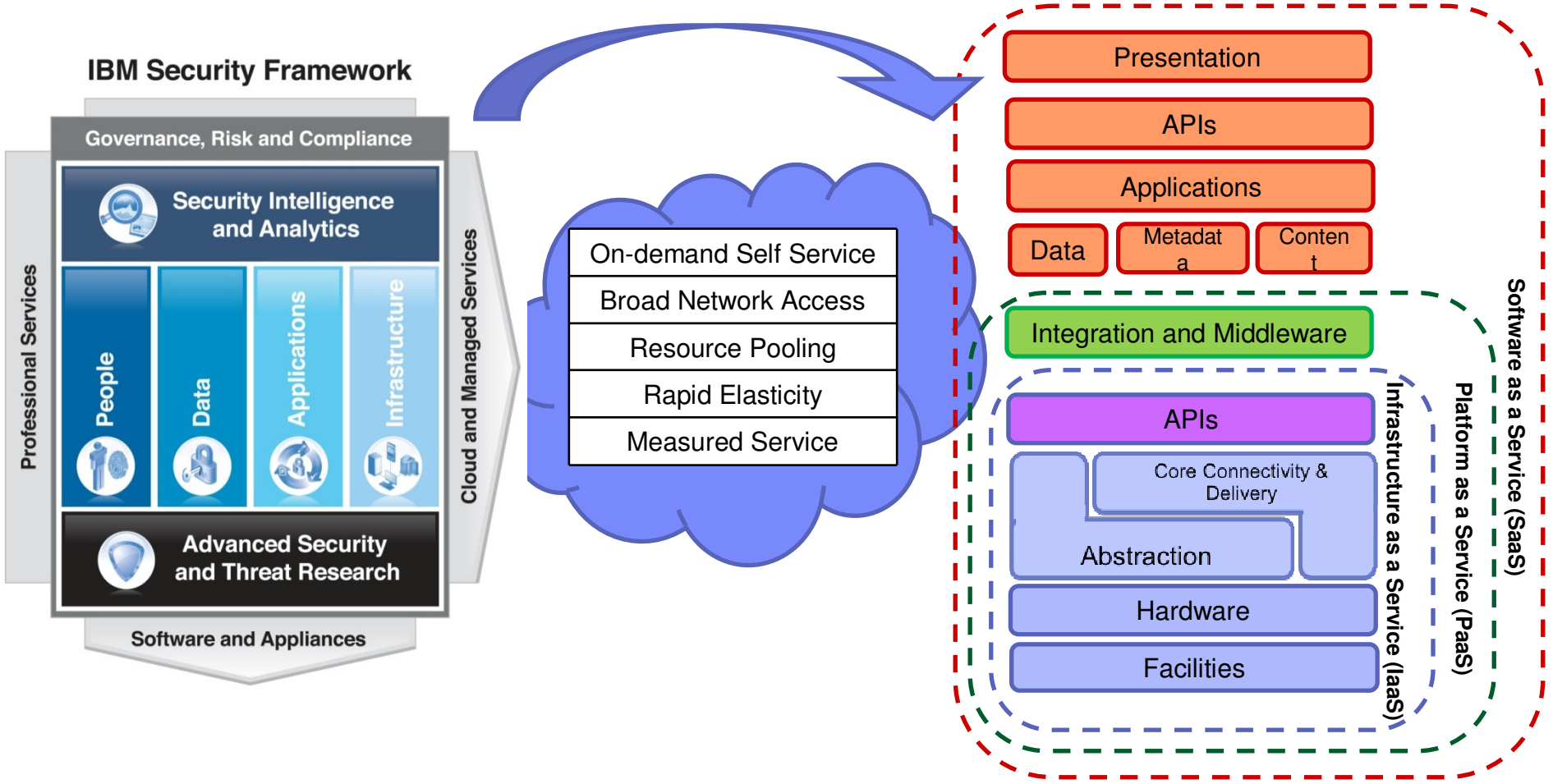
- Entire environment controlled and managed by a single entity
- Security/risk management capabilities typically administered by a single entity (IT/Security administrators)
- Managers can simply add the capability to manage and enforce appropriate security policies, anywhere in the environment
- Audit/compliance: Implement controls, capture necessary data, and report

Security In The Cloud: New Paradigm, New Challenges



- Environment controlled and managed by a multiple, potentially independent entities
- IT resources and security/risk management responsibilities shared across multiple entities (multi-tenancy)
- New deployment model, same security requirements: With less control over the environment, organizations must invest in new ways to manage risk in this environment.
- Audit/compliance: Implement controls, capture necessary data, and report – organizations must coordinate with cloud service providers to ensure compliance and collect and organize required data.

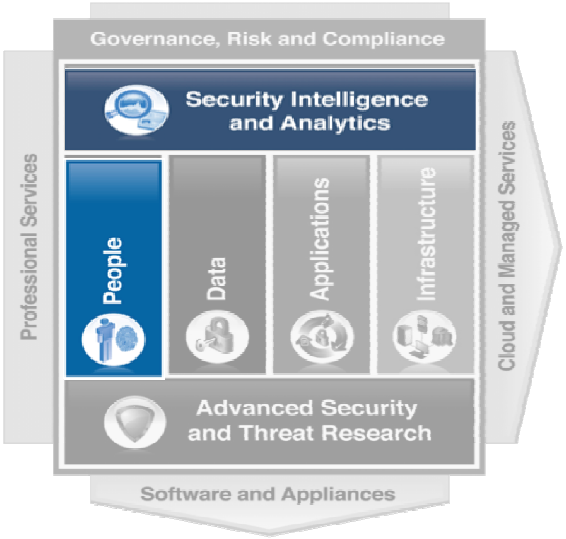
IBM Security: Mapping Security To Cloud Challenges

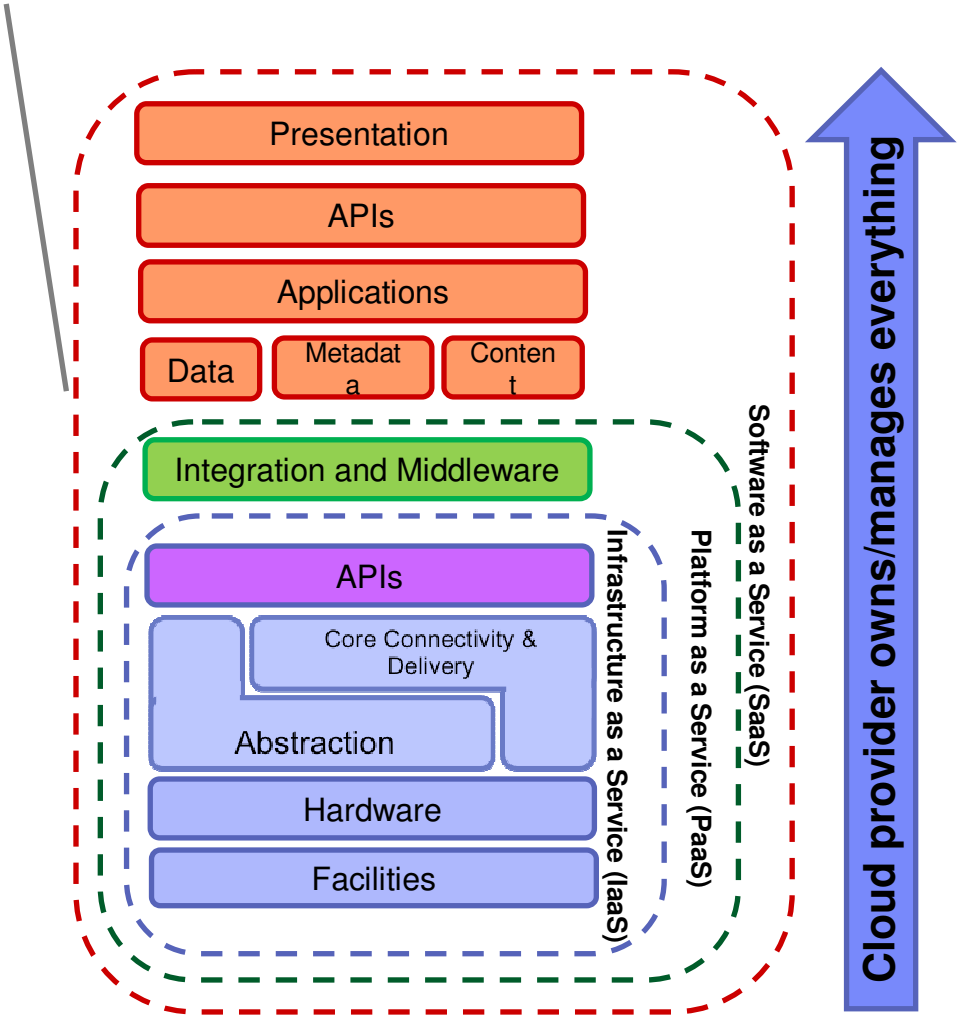


Securing The Cloud

Cloud Security Considerations: Software as a Service (SaaS)

- Cloud provider delivers a complete application
- As a subscriber, you need to manage access entitlements to ensure that your users can use the functions needed for their role
- Security intelligence: Collect, aggregate relevant application logs for audit/compliance



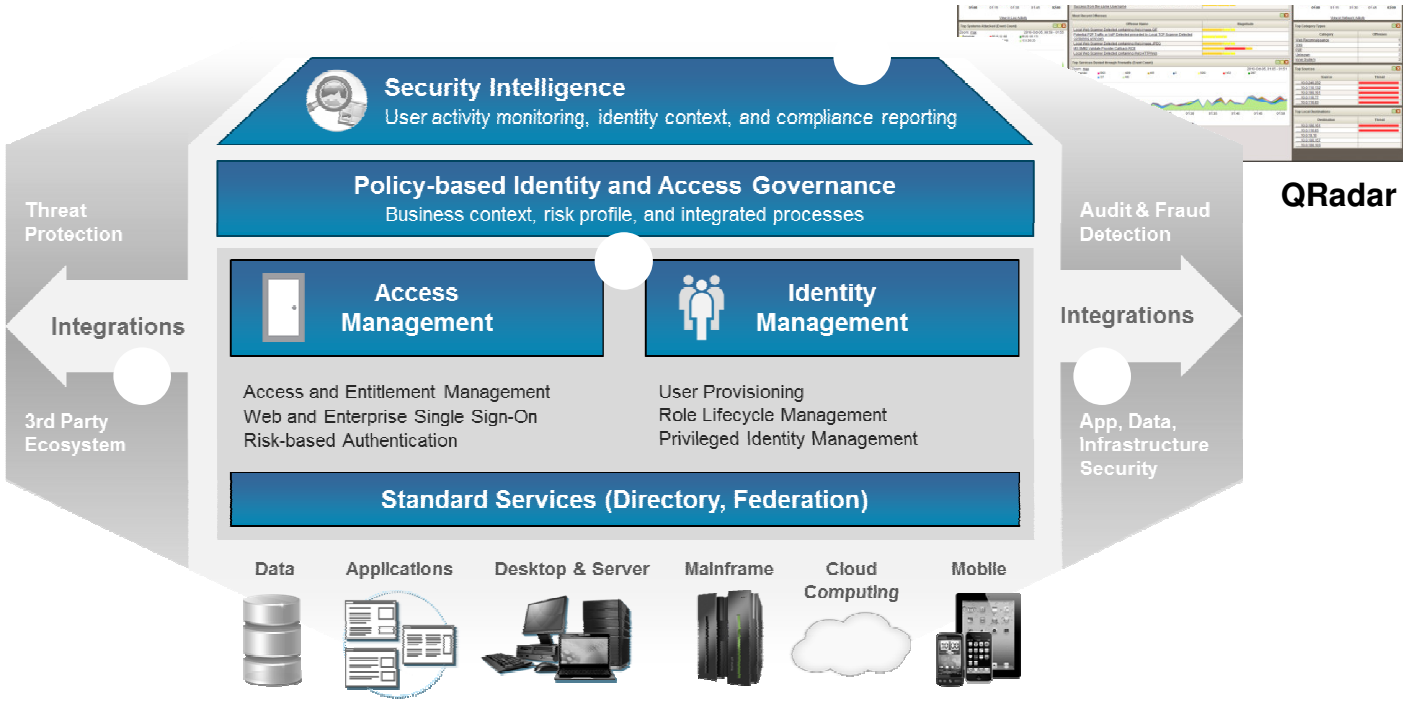


People: Helping take the‘anonymous’ out of digital threats

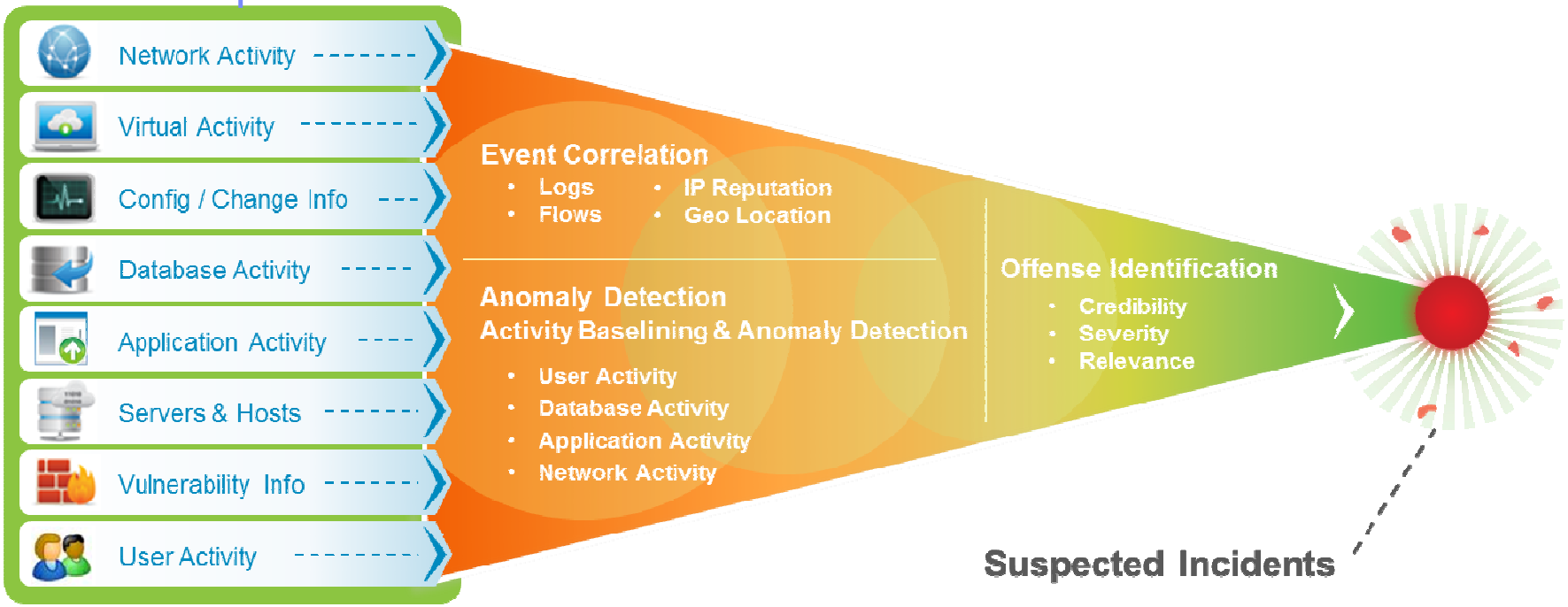
1. Integrated Security Intelligence
Expansion of IAM vertically through governance, analytics and reporting – adding identity context to detected threats

2. IBM Security Identity and Access Assurance Bundle
Management of the entire identity lifecycle: assessing, planning, implementing, auditing, monitoring and maintaining identities and access rights

3. IBM and 3rd Party Ecosystem Integrations



Security Intelligence & Analytics: Stay on top of audit/compliance



Key Themes

Integrated Vulnerability Management

Comprehensive understanding of the configuration and exposure of systems in the environment, enabling contextual analysis to determine vulnerabilities against particular threats

Enhanced Identity Context

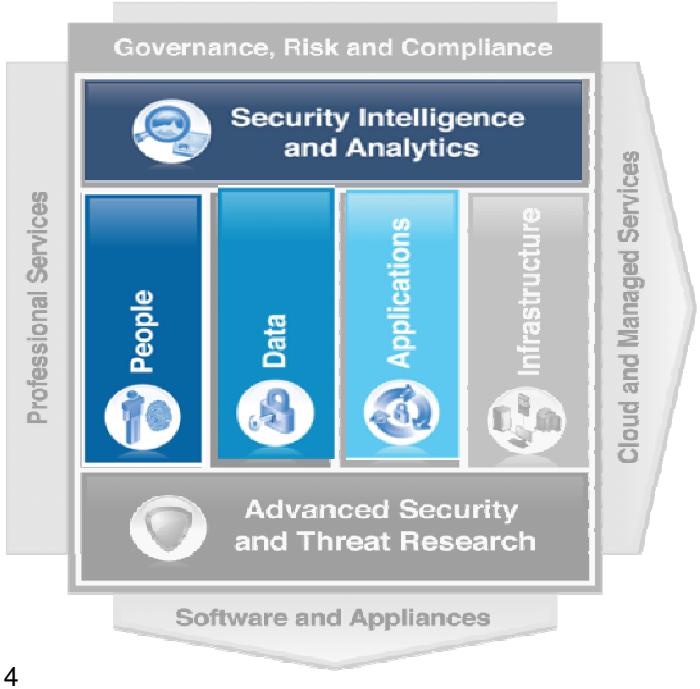
Integrated understanding of users, their roles, level of privilege, geographical location and their typical behaviors to enable enterprises to identify abnormal activity that might indicate insider threat

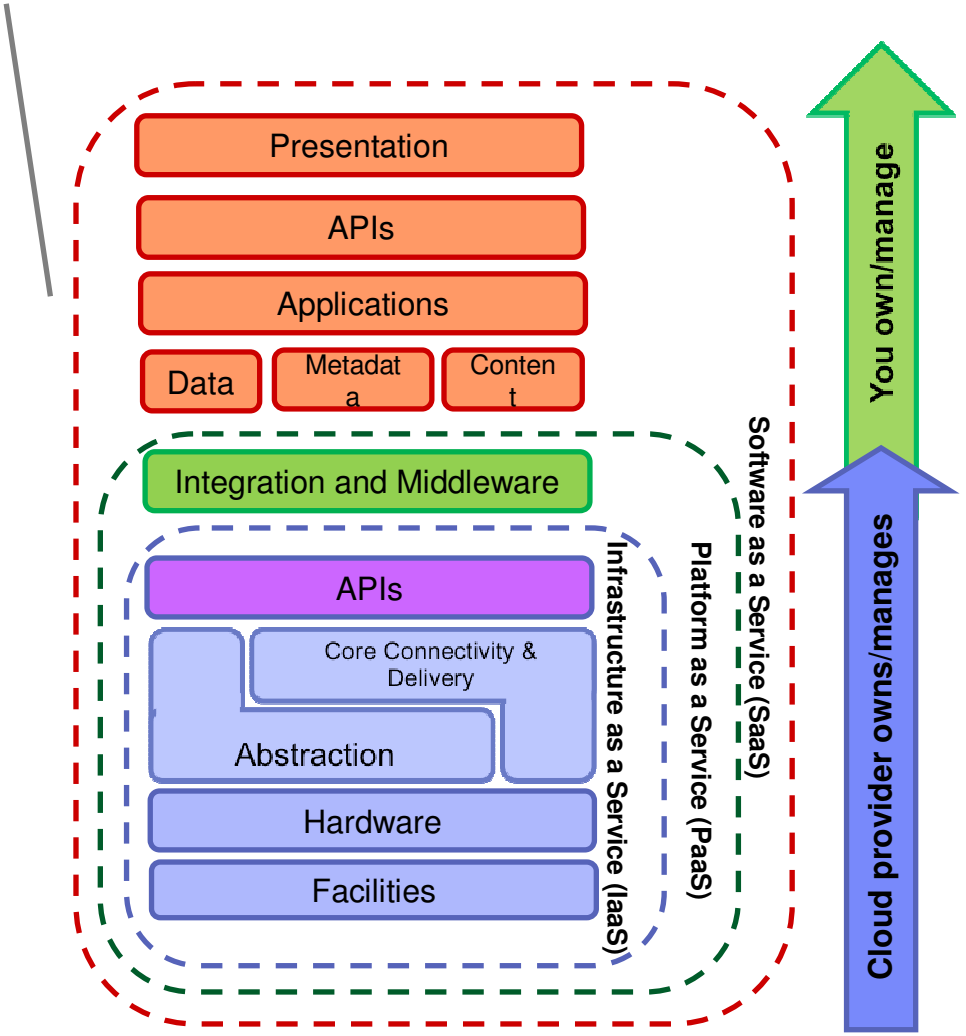
Increased Data Sources for Security Analytics

Integration with X-Force intelligence and other external feeds to use in analysis for determining relevant vulnerabilities and potential threats

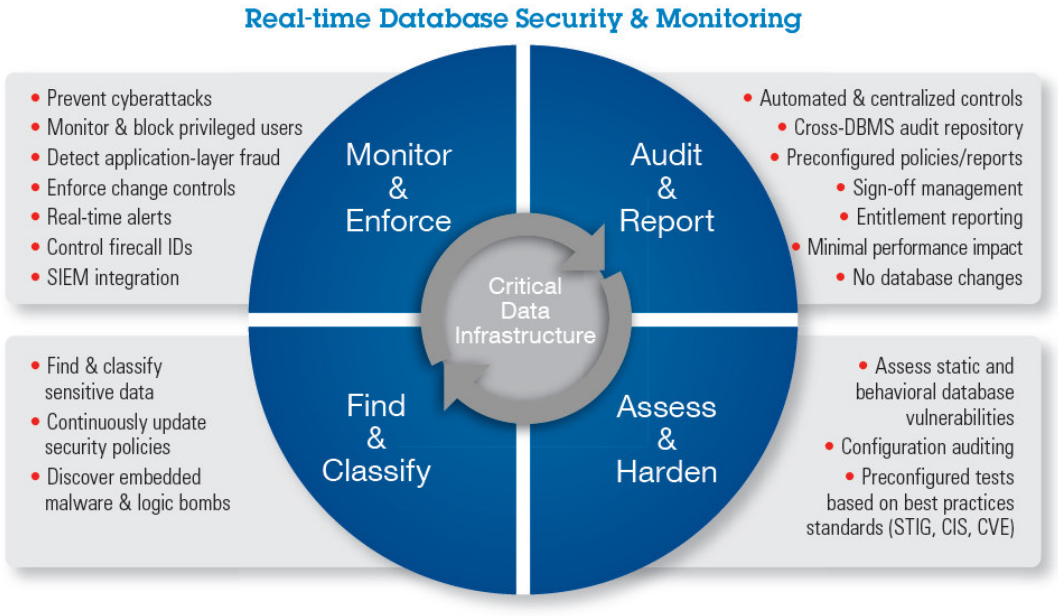
Cloud Security Considerations: Platform as a Service (PaaS)

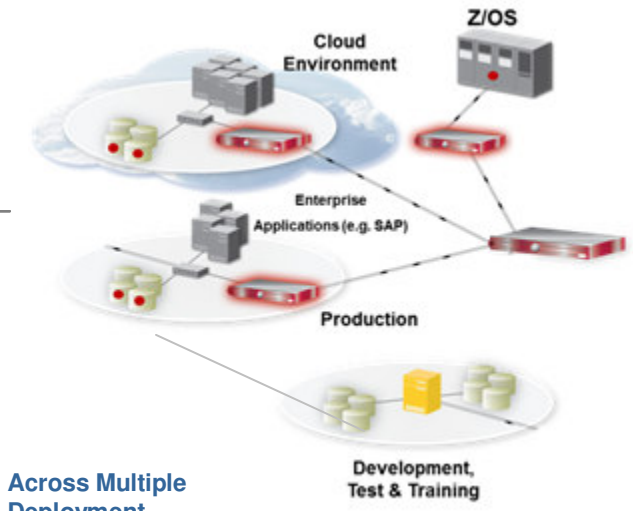
- Cloud provider delivers a complete platform
- You provide the application
- Same access entitlements management and security intelligence requirements as SaaS case
- Now, you are also responsible for data and application security, as well





Data Security: Ensure your customer's information is safe





Across Multiple Deployment Models

Key Themes

Reduced Total Cost of Ownership

Expanded support for databases and unstructured data, automation, handling and analysis of large volumes of audit records, and new preventive capabilities

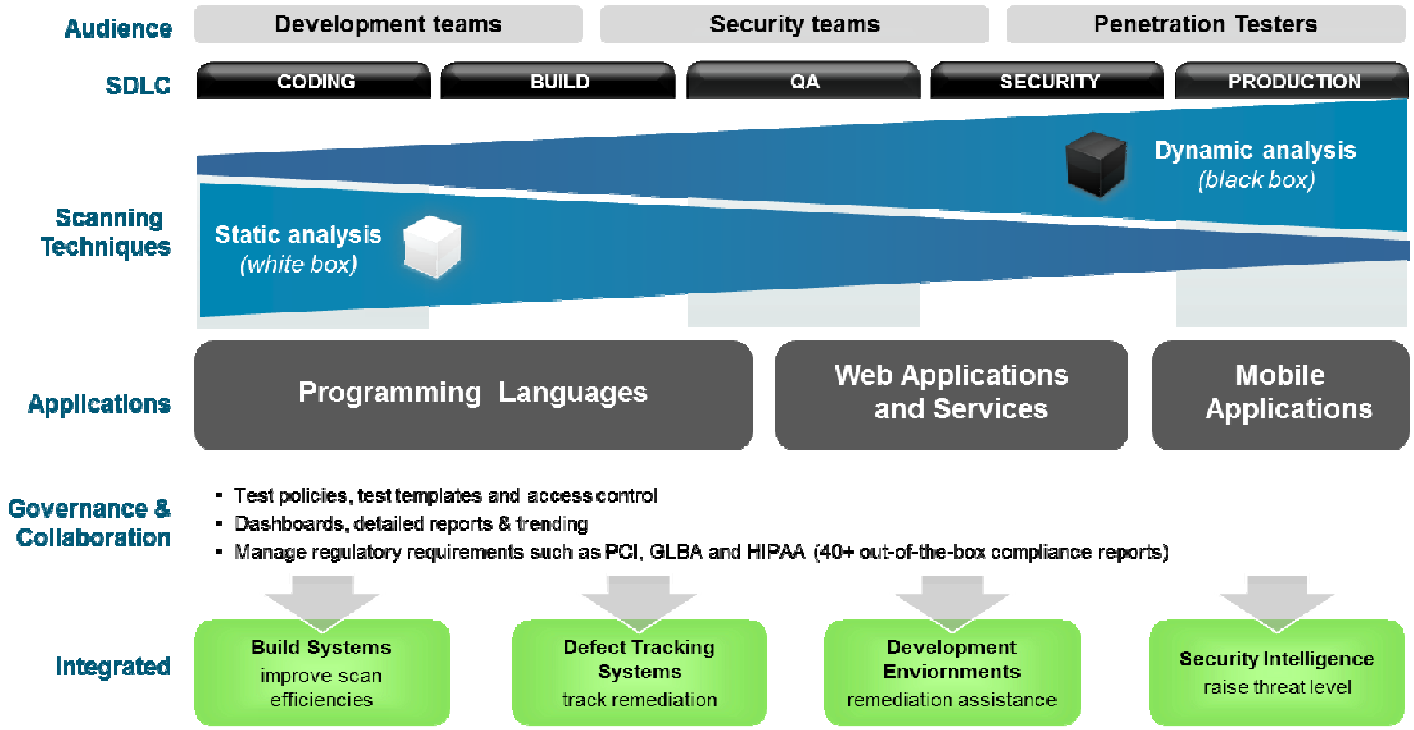
Enhanced Compliance Management

Enhanced Database Vulnerability Assessment (VA) and Database Protection Subscription Service (DPS) with improved update frequency, labels for specific regulations, and product integrations

Dynamic Data Protection

Data masking capabilities for databases (row level, role level) and for applications (pattern based, form based) to safeguard sensitive and confidential data

Application Security: Implement with best practices in mind



Key Themes

Coverage for Mobile applications and new threats

Continue to identify and reduce risk by expanding scanning capabilities to new platforms such as mobile, as well as introducing next generation dynamic analysis scanning and glass box testing

Simplified interface and accelerated ROI

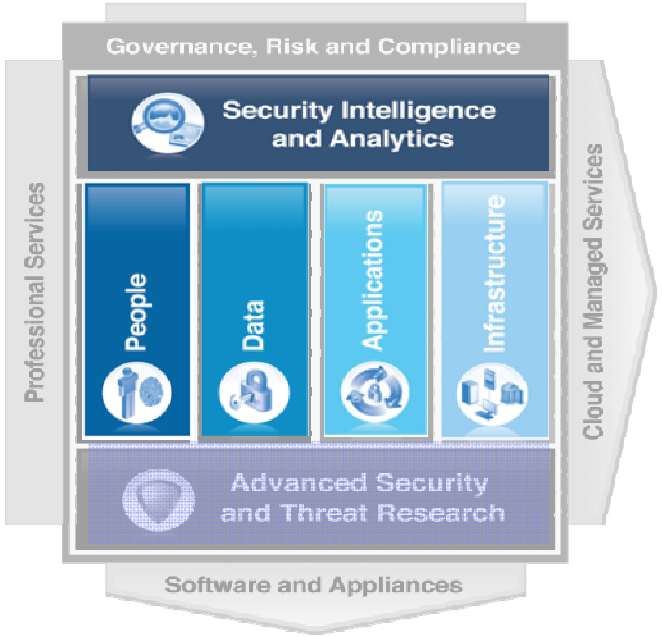
New capabilities to improve customer time to value and consumability with out-of-the-box scanning, static analysis templates and ease of use features

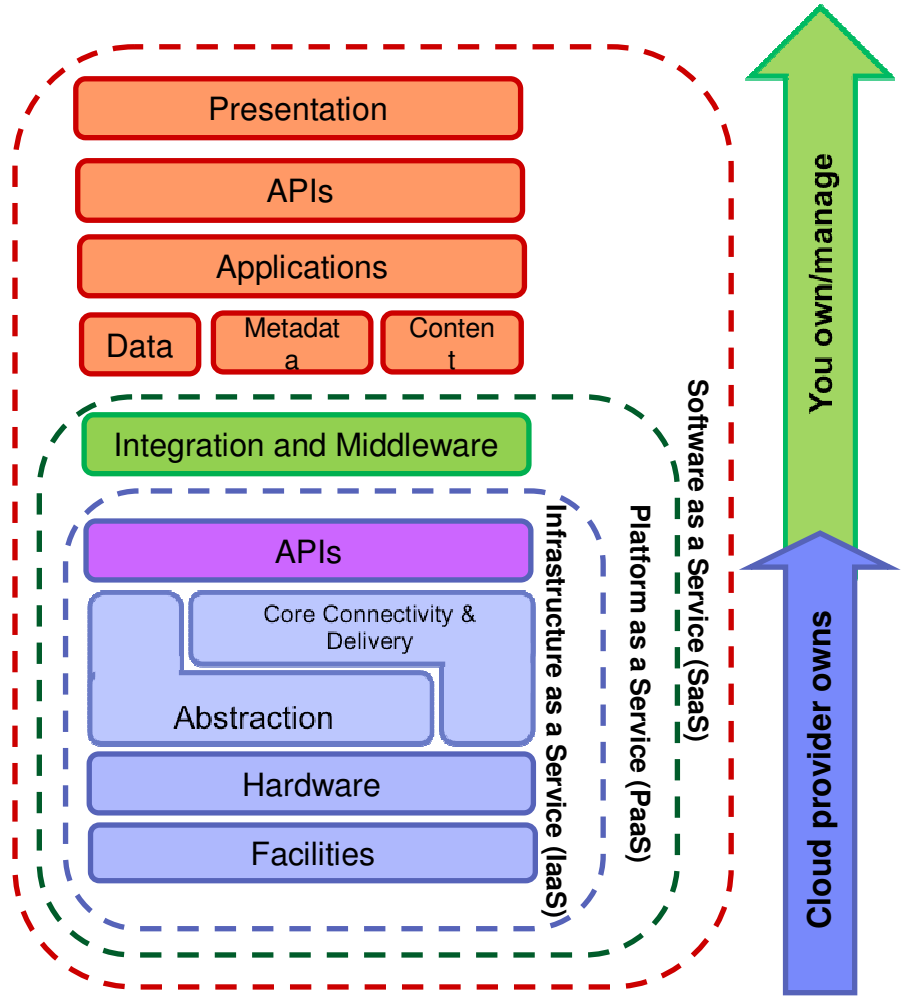
Security Intelligence Integration

Automatically adjust threat levels based on knowledge of application vulnerabilities by integrating and analyzing scan results with SiteProtector and the QRadar Security Intelligence Platform

Cloud Security Considerations: Infrastructure as a Service (IaaS)

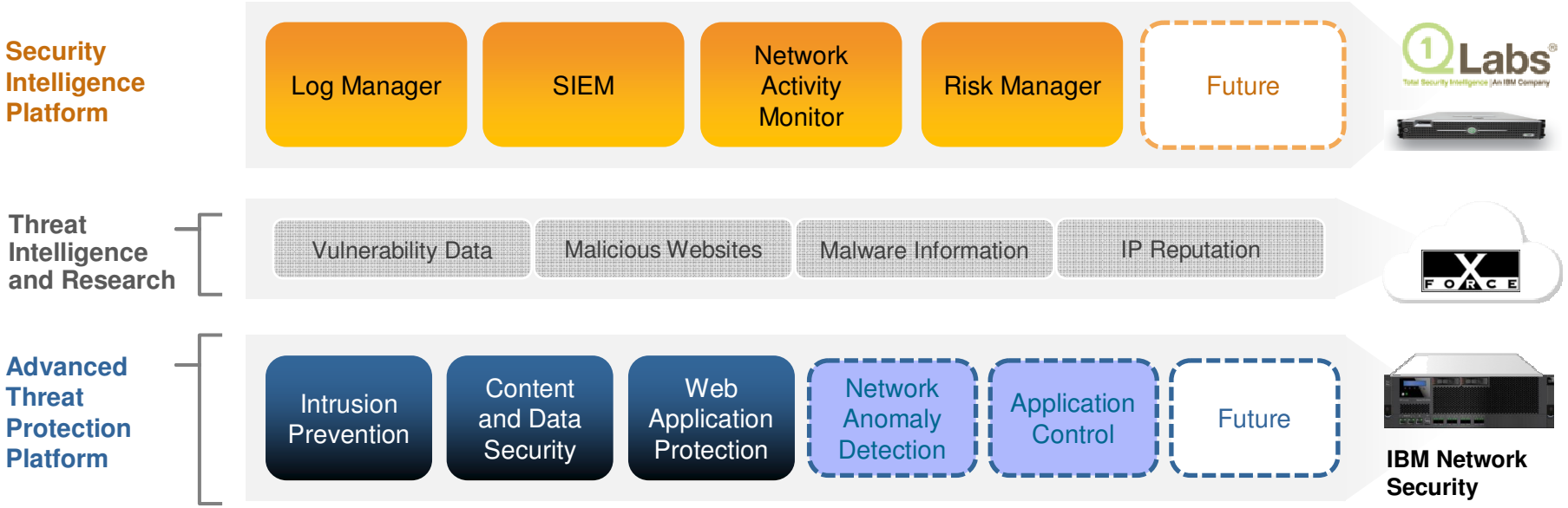
- Cloud provider delivers virtual infrastructure
- You provide OS, middleware, and application
- Same access entitlements, security intelligence, data and application security requirements
- Now, you must secure the virtual infrastructure and manage real-world threats





IBM's Vision For Threat Protection (Part 1 of 2)

Integrated Solutions.



Advanced Threat Protection Platform

Ability to 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

Expanded X-Force Threat Intelligence

Increased coverage of world-wide threat intelligence harvested by X-Force and the consumption of this data to make smarter and more accurate security decisions across the IBM portfolio

Security Intelligence Integration

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

IBM's Vision For Threat Protection (Part 2 of 2)

Integrated Research.

Stay ahead of the changing threat landscape

The X-Force team is one of the best-known commercial security research groups in the world. These security experts research vulnerabilities and security issues, collect worldwide threat data and develop countermeasure technologies for IBM products

Examples of integrated X-Force research

- X-Force Database - 63,000+ unique vulnerabilities, threats and security checks
- Virtual Patch - Eliminates fire drills for new threats by mitigating vulnerabilities through network intrusion prevention
- X-Force Hosted threat analysis service - offers threat information collected from globally networked security operations centers

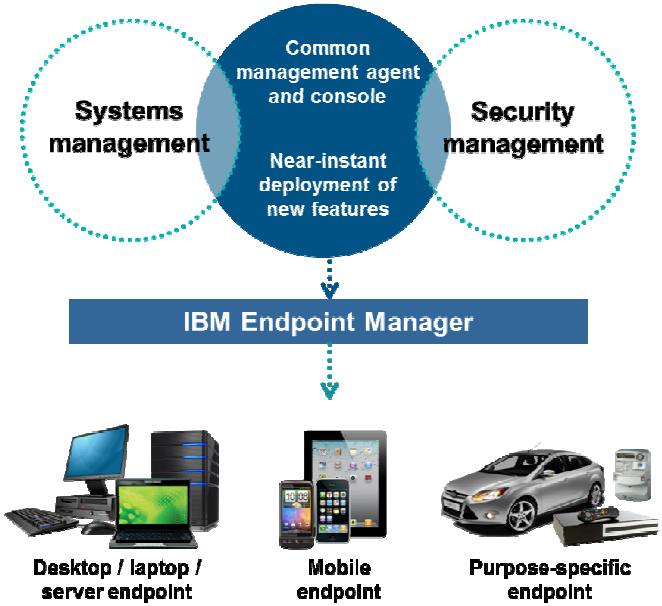
Intelligence to assess and harden databases

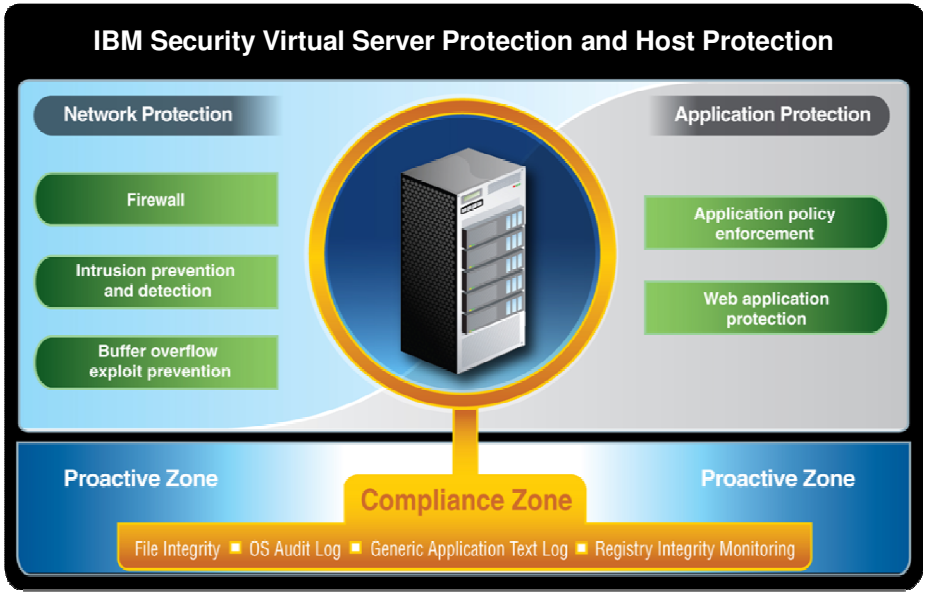
Guardium contains hundreds of preconfigured vulnerability tests, encompassing CIS and STIG best practices, updated regularly through IBM's Knowledge Base service

Detect the latest web application vulnerabilities

Information on the latest threats, updated automatically when you launch a AppScan product – including OWASP and SANS top vulnerabilities

Infrastructure Protection: Endpoint & Server management





Key Themes

Security for Mobile Devices

Provide security for and manage traditional endpoints alongside mobile devices such as Apple iOS, Google Android, Symbian, and Microsoft Windows Phone - using a single platform

Expansion of Security Content

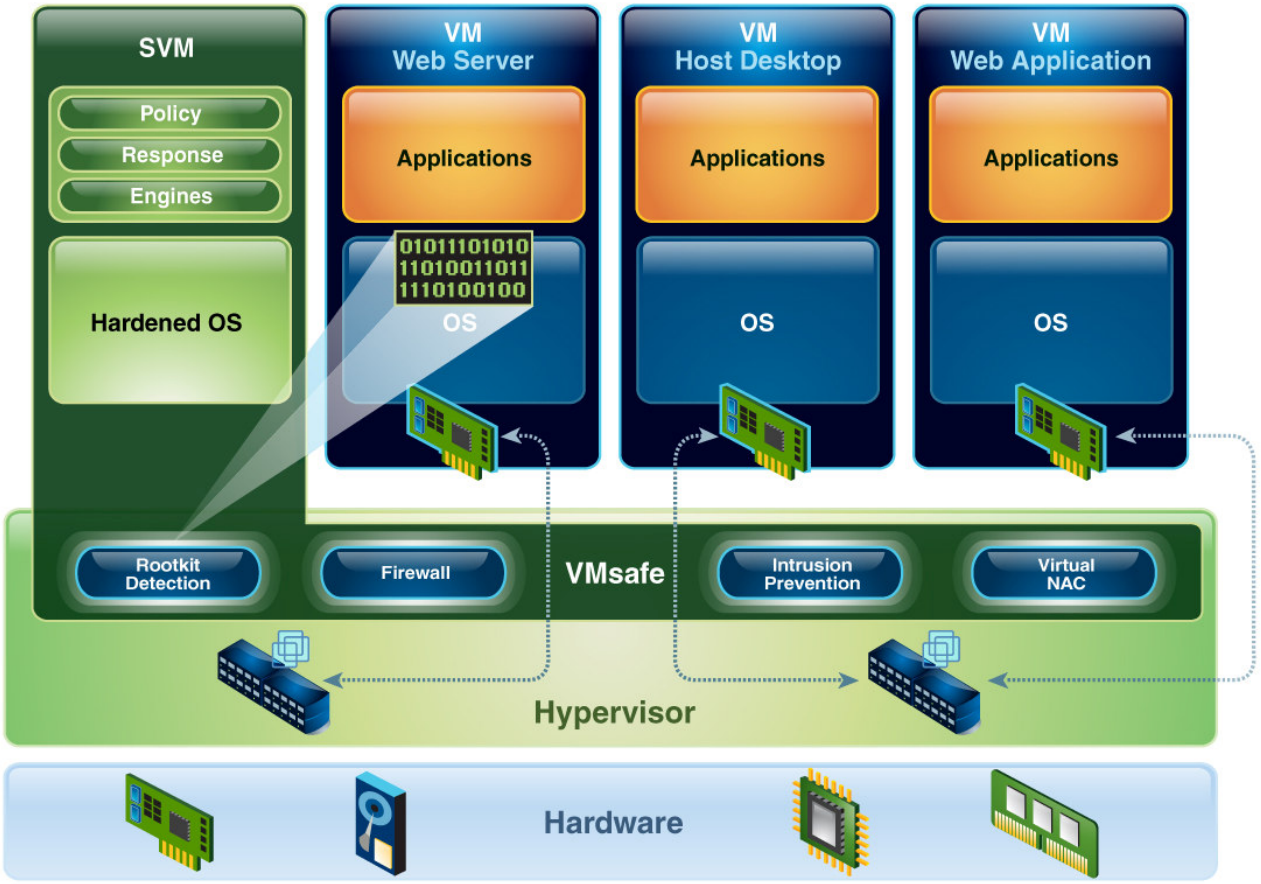
Continued expansion of security configuration and vulnerability content to increase coverage for applications, operating systems, and industry best practices

Security Intelligence Integration

Improved usage of analytics - providing valuable insights to meet compliance and IT security objectives, as well as further integration with SiteProtector and the QRadar Security Intelligence Platform

Virtual Server Protection for VMWare:
Integrated threat protection for VMware vSphere

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



- 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

Conclusions

Benefits Of IBM Security Solutions In The Cloud

IBM Cloud Security helps customers regain visibility and control

QRadar Security Intelligence
Deep visibility into virtual environments

IBM Security Identity and Access Management Suite
Identity integration, provision users to SaaS applications
Desktop single sign on supporting desktop virtualization

IBM Security AppScan Suite
Scan cloud based web applications for vulnerabilities

Securing Cloud with IBM Security Systems

Security Intelligence ● People ● Data ● Apps ● Infrastructure

IBM InfoSphere Guardium Suite
Protect and monitor access to shared databases

IBM Security Network IPS
Guard cloud users and apps from network attacks

IBM Endpoint Manager
Patch and configuration management of VMs

IBM Security Virtual Server Protection for VMware
Protect VMs from advanced threats

Award Winning IBM Cloud Security

End-to-end security for private, hybrid and public clouds

IBM is the only vendor with security products, services and expertise that span all critical dimensions of cloud - **users, data, applications** and **virtualized infrastructure.**

- **Enterprise-class** security across all cloud domains
- **Visibility** into the security of cloud environments
- **Control access** to cloud applications
- **Data protection** for in motion and at rest
- **Threat and vulnerability management** solutions for applications and infrastructure
- **Security Services** specifically designed for the cloud

Best Cloud Computing Security