Pulse

IBM SolutionsConnect 2013

Cloud Security

Enabling adoption of cloud policies within the enterprise

13/06/2013

IBM

Introductions

- Mark Johnston is a Security Solution Architect and part of IBM's Worldwide Security Tiger Team within IBM Software Group.

- Mark has over 13 years experience in the IT Industry. He has consulted with various Australian federal and state government departments, helping them to build Identity, Access, and Security monitoring solutions for their business. He has worked in a number of countries in Asia, Europe and the USA

- Mark previously worked as a consultant in the IBM Security and Privacy division and is currently developing security workshop offerings to assess the maturity of IT security controls in organisations today.

- Mark is also an open group certified Master IT Specialist and co-author of the IBM Redbook [Using the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security]

Email : markjohnston@au1.ibm.com

Twitter: markjohnston_au

LinkedIn: http://www.linkedin.com/in/markjohnstonau

Agenda

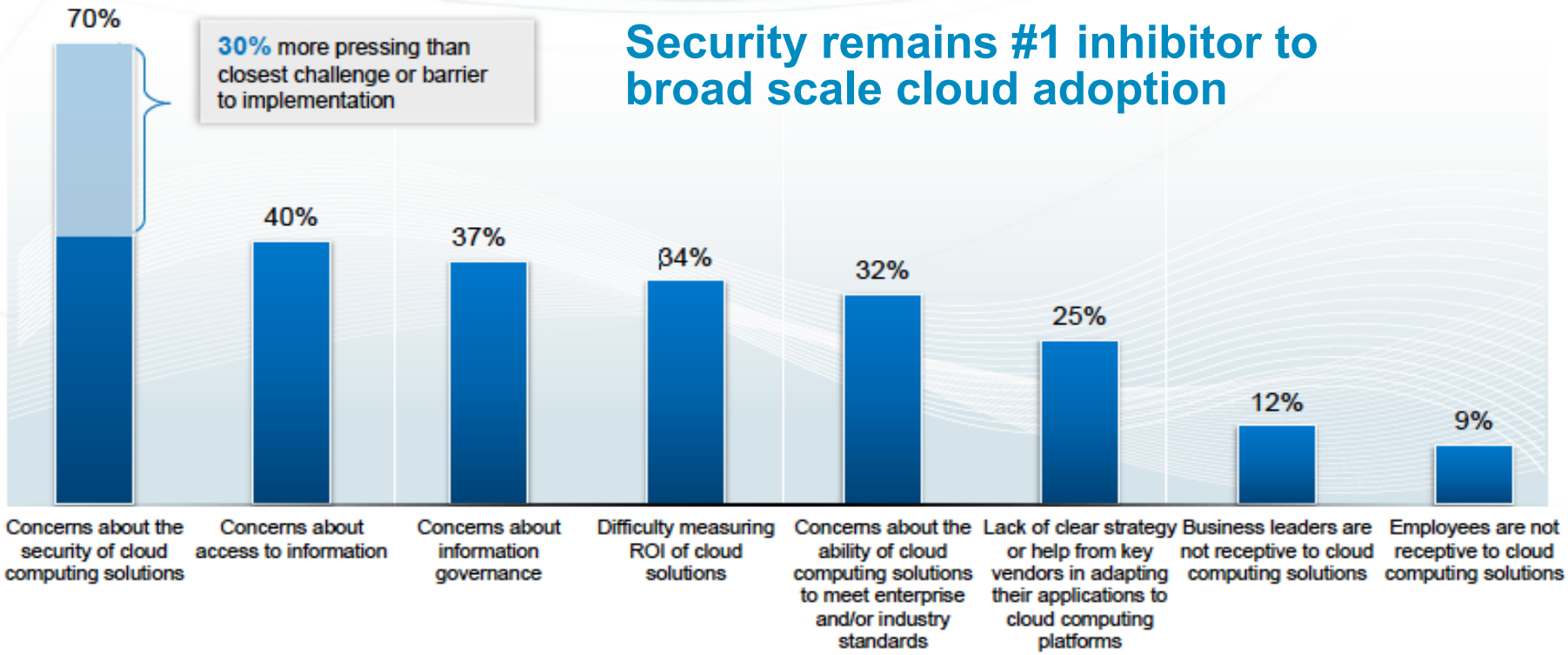
- Introduction to cloud computing
- Security challenges posed by cloud computing
- How we can address some of these challenges

- Caveats
- Cloud has many multiplicity's of deployment and consumption I do not aim to cover all of these in this presentation
- I will not be speaking about the IBM Cloud offering, more generally how you can connect and enable the enterprise to adopt cloud policies by mitigating risks.

What is cloud computing?

- **Cloud computing** is a colloquial expression used to describe a variety of different computing concepts that involve a large number of computers that are connected through a real-time communication network (typically the Internet). Cloud Computing is a jargon term without a commonly accepted non-ambiguous scientific or technical definition.
- - Wikipedia

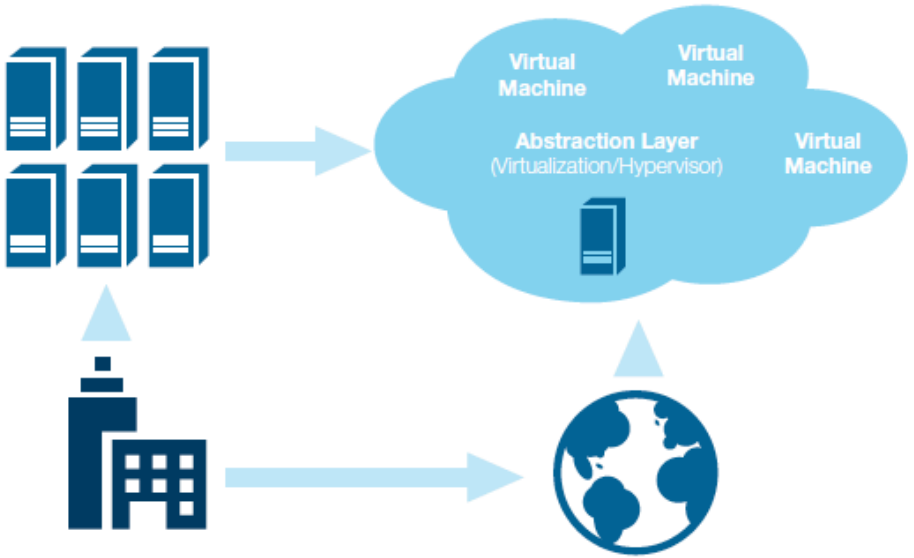
What is the concern?



Cloud environments = new challenges

Today's Data Center

- We have control
- It's located at X
- It's stored in servers Y, Z
- We have backups in place
- Our admins control access
- Our uptime is sufficient
- The auditors are happy
- Our security team is engaged



Tomorrow's Cloud

- Who has control?
- Where is it located?
- Where is it stored?
- Who backs it up?
- Who has access?
- How resilient is it?
- How do auditors observe?
- How does our security team engage?

What are the security challenges cloud introduces?

- There are existing security challenges, experienced in other computing environments, and there are new elements which are necessary to consider.

Providing Software as a service (SaaS), Infrastructure and hardware as a service (IaaS) and Platform as a service (PaaS), either individually or in different combinations

Governance

- Achieving and maintaining governance and compliance in cloud environments brings new challenges to many organizations.

- Jurisdiction and regulatory requirements
- Complying with Export/Import controls
- Compliance of the infrastructure
- Audit and reporting to regulatory obligations

Data

- Cloud places data in new and different places, not just the user data but also the application (source) code. Who has access, and what is left behind when you scale down a service?

- Data location and segregation
- Data footprints
- Backup and recovery
- Administration of cloud environment
- Data at rest

Architecture

- Standardized infrastructure and applications; increased commoditization leading to more opportunity to exploit a single vulnerability many times. Looking at the underlying architecture and infrastructure, some of the considerations include:

- Protection mechanisms
- Hypervisor vulnerabilities
- Multi-tenant environments
- Security policies
- Identity Management

Applications

- There has been a significant increase in web application vulnerabilities, so much so that these vulnerabilities make up more than half of the disclosed vulnerabilities over the past 4 years.

- Software vulnerabilities
- Patch management
- Application systems

Assurance

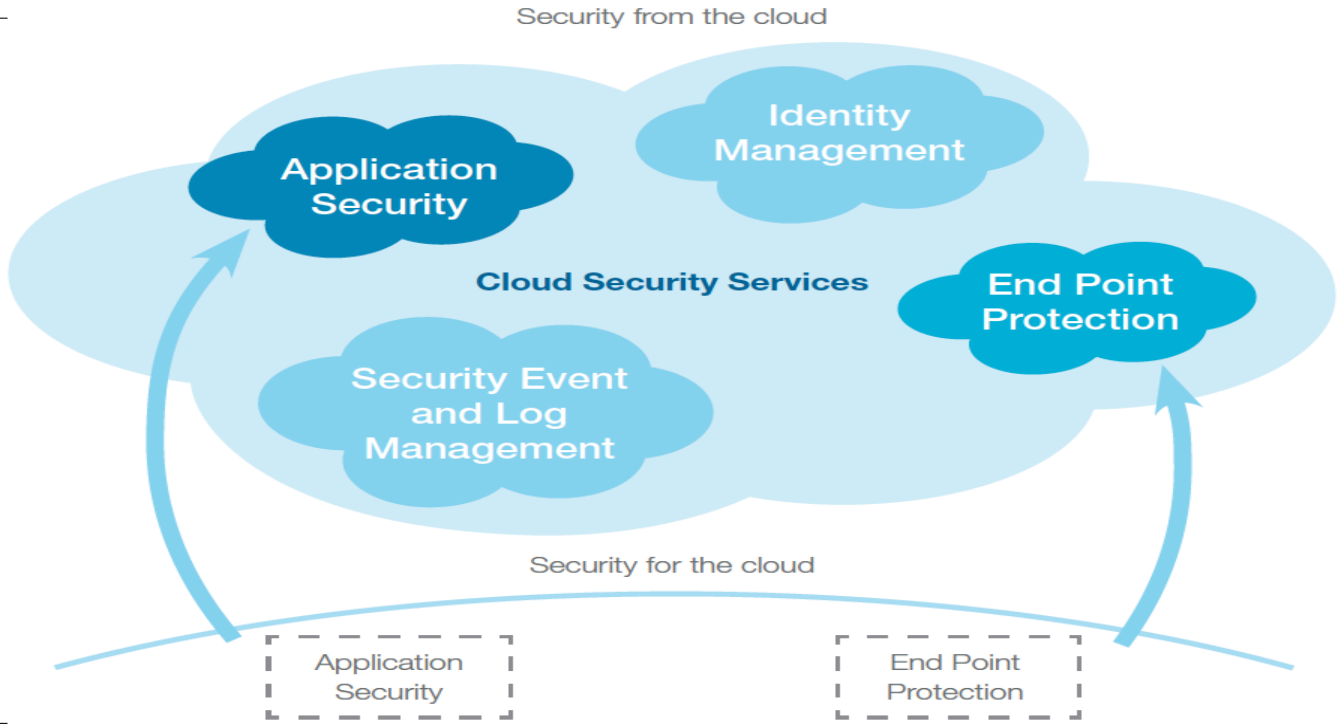
- Challenges exist for testing and assuring the infrastructure, especially when there is no easy way for data center visits or penetration tests.

- Operational oversight
- Audit and assurance
- Investigating an incident
- Experience of new cloud providers

Building trust with cloud delivery models

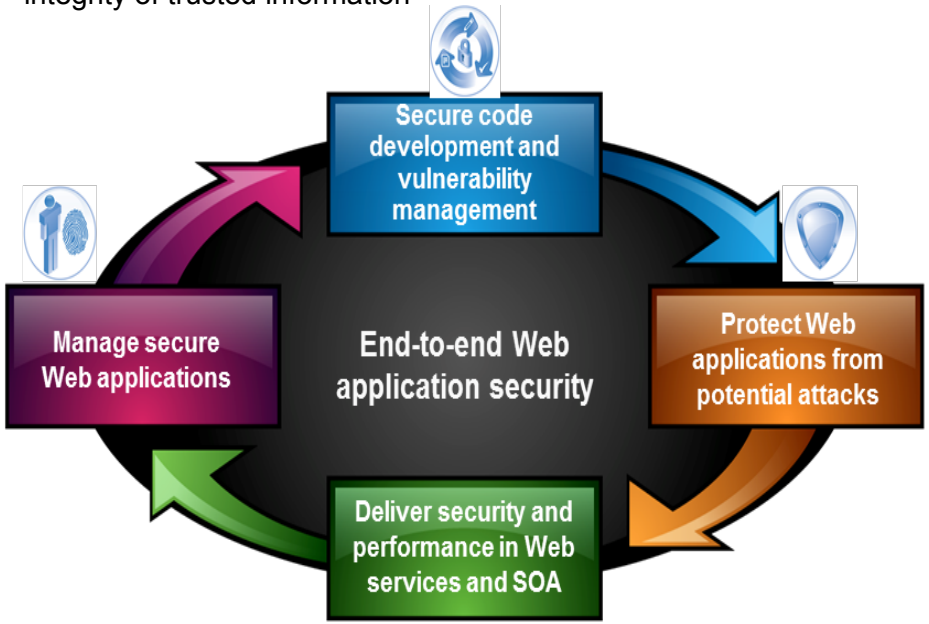
Governance, Risk Management and Compliance

How can you start to build to a position of trust and risk management when setting up cloud computing for your organization?



Application Security

Developing secure applications and assuring the privacy and integrity of trusted information



IBM Portfolio Overview

AppScan Enterprise

- Enterprise-class solution for implementing and managing an application security program, includes high-level dashboards, test policies, scan templates and issue management capabilities
- Multi-user solution providing simultaneous security scanning and centralized reporting

AppScan Standard

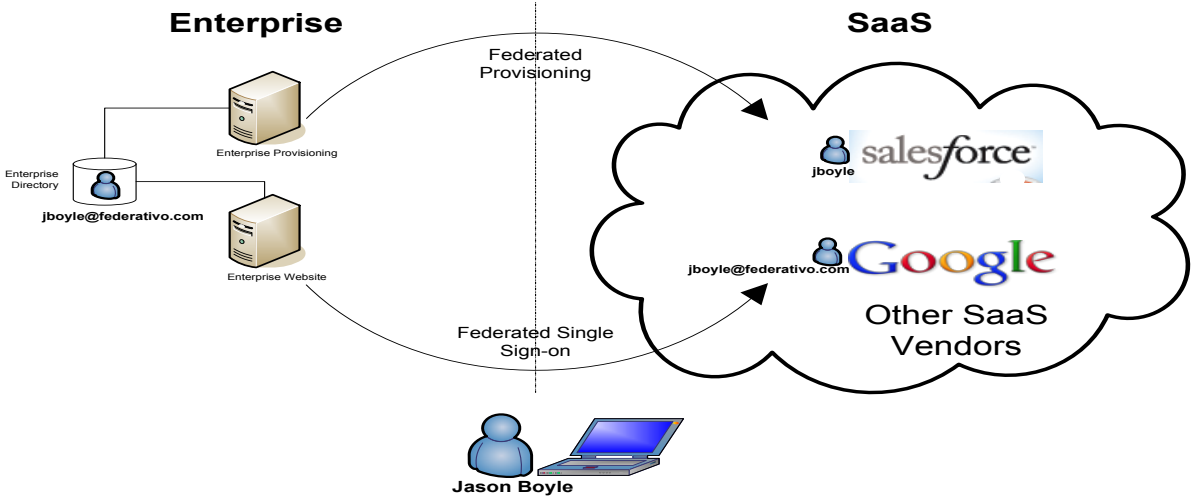
- Desktop solution to Dynamic Application Security testing for IT Security, auditors, and penetration testers

AppScan Source

- Static application security testing to identify vulnerabilities at the line of code. Enables early detection within the development life cycle.

Identity Management

- Pattern: Adopting Software as a Service
  - Salesforce, GoogleApps, Workday, etc
- Target: B2E
- Technologies: Federated Provisioning and Single Sign-on



- Solution
  - ISIM
  - ISAM for Cloud

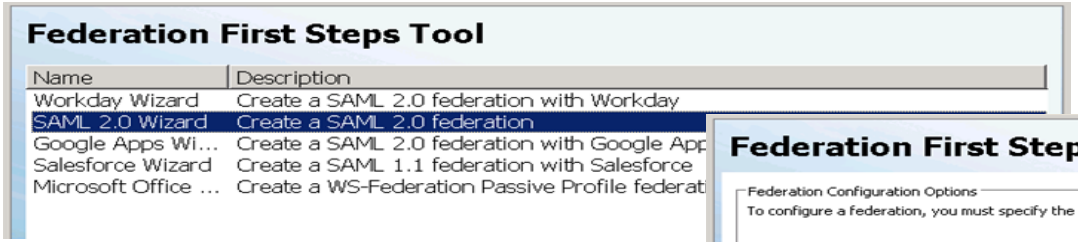
ISAM for Cloud also…

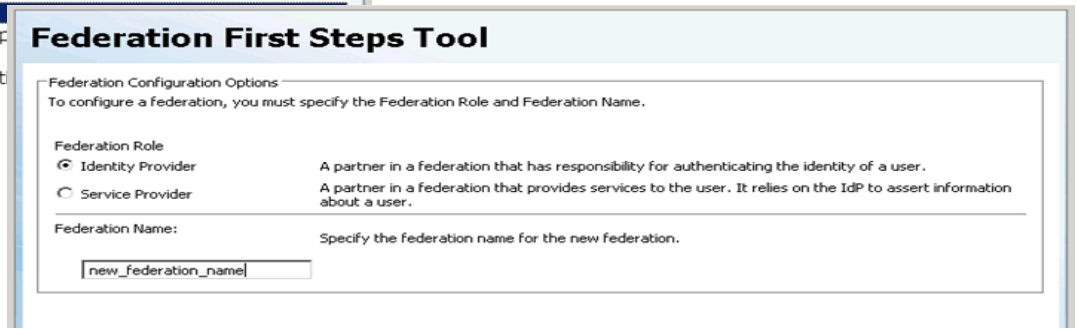
- **Ships with Wizards for creation of federations**
  - Called “Federation Fist Steps”, introduced with latest feature pack (#4, Dec 2012)
  - Simplifies/reduces effort to setup a federation
  - Currently have;

    SAML 2.0,

    Workday (SAML 2.0),

    Google Apps (SAML 2.0),

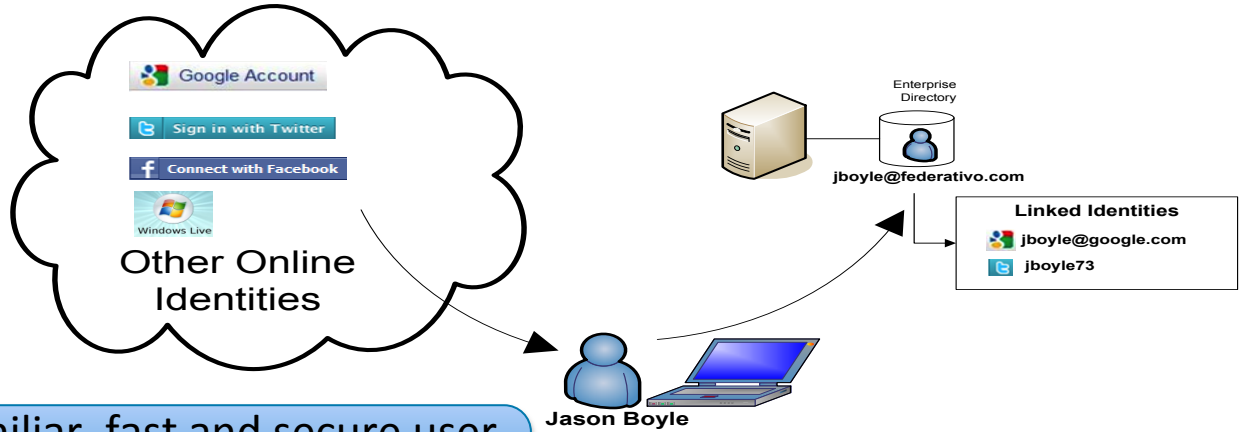




IAM from the cloud

- Pattern: Bring your own identity (BYO-Id)
  - LinkedIn, Facebook, Twitter, Google, Yahoo, Government ID's
- Target: B2C
- Technologies: Self-registration, Single Sign-on, User self-care

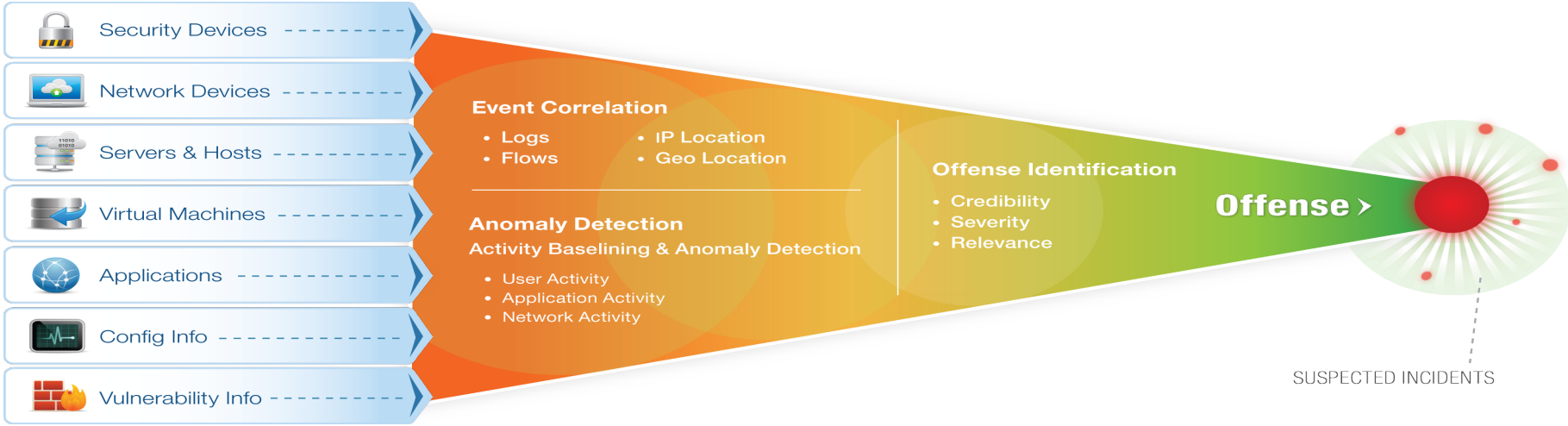
- Solution
  - ISAM for Cloud



"Making access easy, with a familiar, fast and secure user experience is key to attaining and retaining new customers."

SIEM / SELM

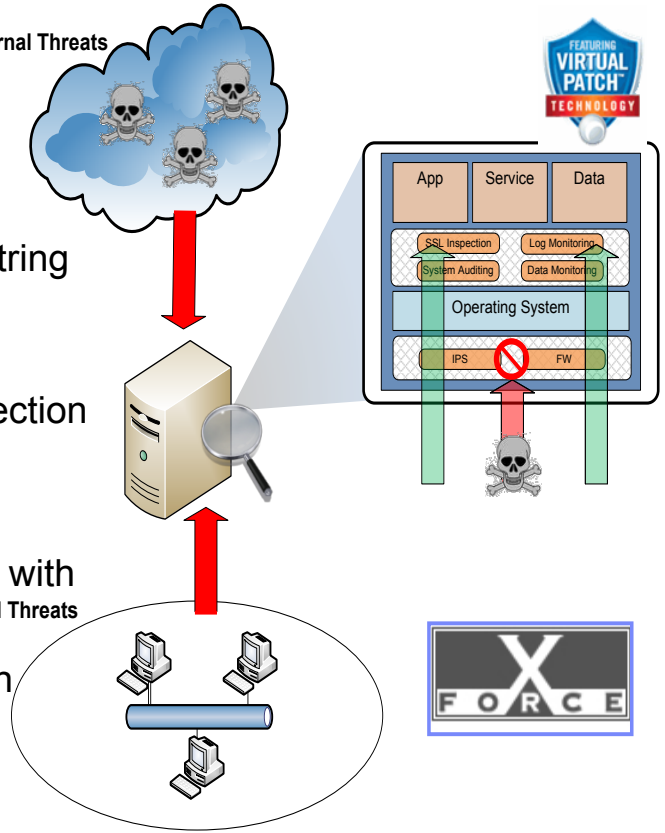
- Provides support for compliance through Accountability, Transparency and Measurability of actions on a system.
- IBM QRadar monitors logs and network flows for anomaly detection.
- Privileged User Monitoring



Extensive Data Sources + **Deep Intelligence** = **Exceptionally Accurate and Actionable Insight**

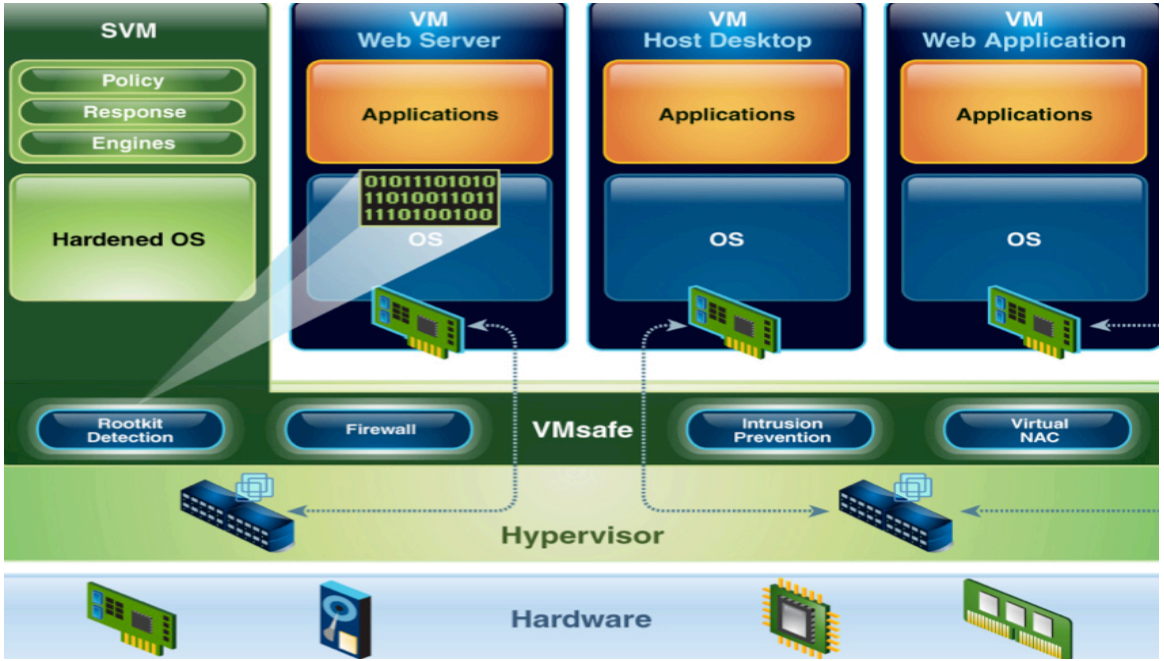
Endpoint Protection – Host IPS

- Software with multi-layered protection to guard against internal and external threats
  - **Data Security**
    Provides historical data on the origin of a change, breach, or string of behavior
  - **Threat Protection**
    Fueled by X-Force R&D, our award winning IPS provides protection without interrupting legitimate server activity
  - **Compliance**
    Provides host-level controls that allow organizations to comply with security standards such as PCI's DSS
    Provides the reporting necessary to prove the who, what, when where of user/admin behavior
- Comprehensive platform coverage with central management
  - Windows, Linux, AIX, Solaris, and VMware



Virtual server protection for VMware

- 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



Privileged Identity Management

Centralised management of privileged and shared identities

Addressing insider threat with privileged users access management

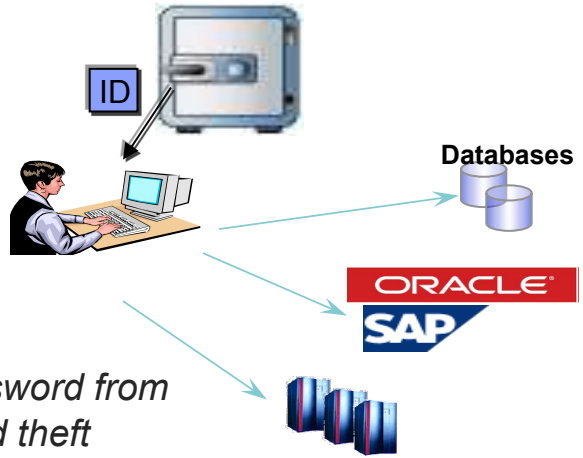
Business challenge

Track and audit activities of privileged users (e.g. root, financial app administrators) for effective governance

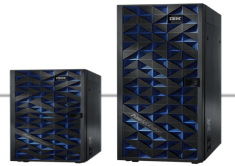
Key solution highlights

- ***Control shared access to sensitive userids***
  - Checkin/checkout using secure credential vault
- ***Request, approve and re-validate privileged access***
  - Reduce Risk, enhance compliance
- ***Track usage of shared identities***
  - Provide accountability
- ***Automated password management***
  -In conjunction with ISAM-ESSO, automate checkout of ids, hide password from requesting employee, automate password reset to eliminate password theft

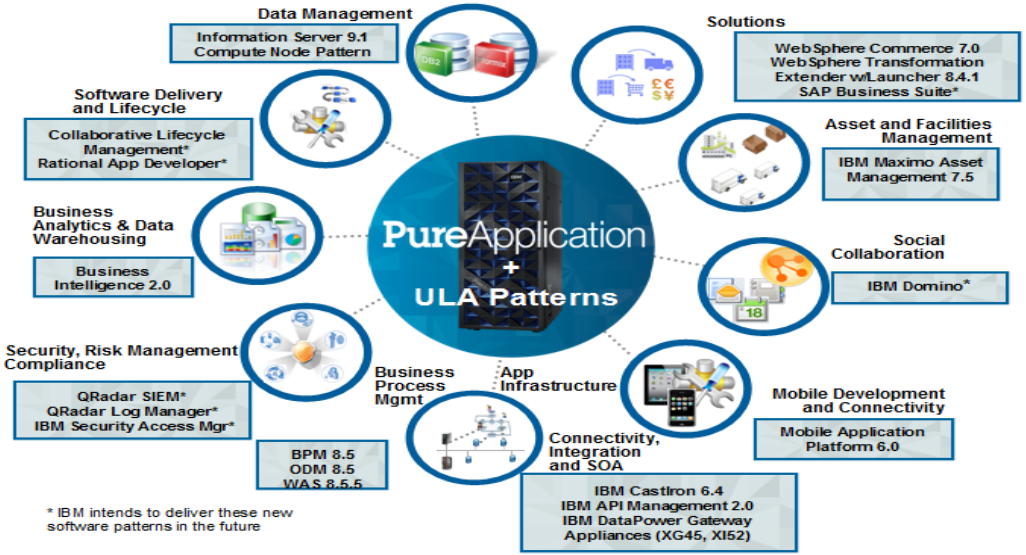
IBM Security Privileged Identity Management



IBM Security on PureApplication Systems



- IBM intends to deliver in the future the following software to run on PureApplication System.
- **IBM Security Access Manager for Web (ISAM)** for deployment on the IBM PureApplication System.
- **IBM Security QRadar SIEM** and **IBM Security QRadar Log Manager** for deployment on the IBM PureApplication System.



PureSystems ISAM and QRadar Video

Conclusion

- Application security testing is a fundamental security function that provides risk mitigations on one of the weak links in a cloud ecosystem. (Web Apps are vulnerable!)
- Identity and access management is a logical starting point for integrating on-premise and cloud security services, this is based on mature open standards.
- Identity and access can be demonstrated as an enabler for cloud adoption, not just a ‘control’ driven by risk and compliance.
- Enterprise SELM / SIEM is fundamental component of gaining visibility into who, what, when details on cloud environments and supporting adherence to governance guidelines in realtime.
- Privileged User Monitoring and Privileged Access Management are focus area for assurance.

Questions?

Thank You

gracias
merci
obrigado
obrigada
graciñas
dank
thank
mèsi
grâces
gràcie
tesekkur
gratias
mamnun
pers
terima
aabhar
much
salamat
tapadh
plural
takk
khun
asante
murakoze
vala
hmat
kasih
kié
ruuru
formal
ingular
minderit
dhanyavad
asko
cám
mercé
manana
kiitos
maita
mersi
dankon
akpé
deu
nanni
bedankt
beacôp
milesker
Allahu
khob
leat
chnorakaloutioun
dziękuję
go
grazie
krap
najis
ederim
leibh
edirem
shukriya
mochchakkeram
enkosi
faafetai
didi
kyay
nirringrazzjak
arigatò
grazzi
bayarlalaa
blagodaram
dhanyavaad
dhanyabaad
dhanyavad
diakuiu
dakujem
sana
kha
dankie
danke
po
pa
sag
ago
hamnida
akun
sobodi
dankewol
ngiyabonga
dziakuju
ko
ni
je
chai
kop
ačiū
misaotra
meharbani
ju
aguyjé
gratzias
familiar
täna
informa
saha
fyri
nandri
agat
raibh
kam
lava
paldies
köszönöm
chokrane
dieuf
děkuji
marahaba
efharisto
barkal
northern
djiere
eskerrik
fiik
motashakkeram
danki
côps
basque
mulțumesc
Barak
maith
dhanyavadagalu

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT SYSTEMS AND PRODUCTS ARE IMMUNE FROM THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

ibm.com/security