Bezpečnosť dát v HP Cloude

Ochrana dát a súkromia v cloudových službách

Február 2013

Agenda

TRENDY

RIEŠENIA HP

PRÍKLADY

Security awareness at board level

Security leadership is under immense pressure

Cyber threat	**56%** of organisations have been the target of a nation state cyber attack
Extended supply chain	**44%** of all data breach involved third-party mistakes
Financial loss	**$675m** average cost associated with data breach
Reputation damage	**30%** market cap reduction due to recent events
Cost of protection	**11%** of total it budget spent on security

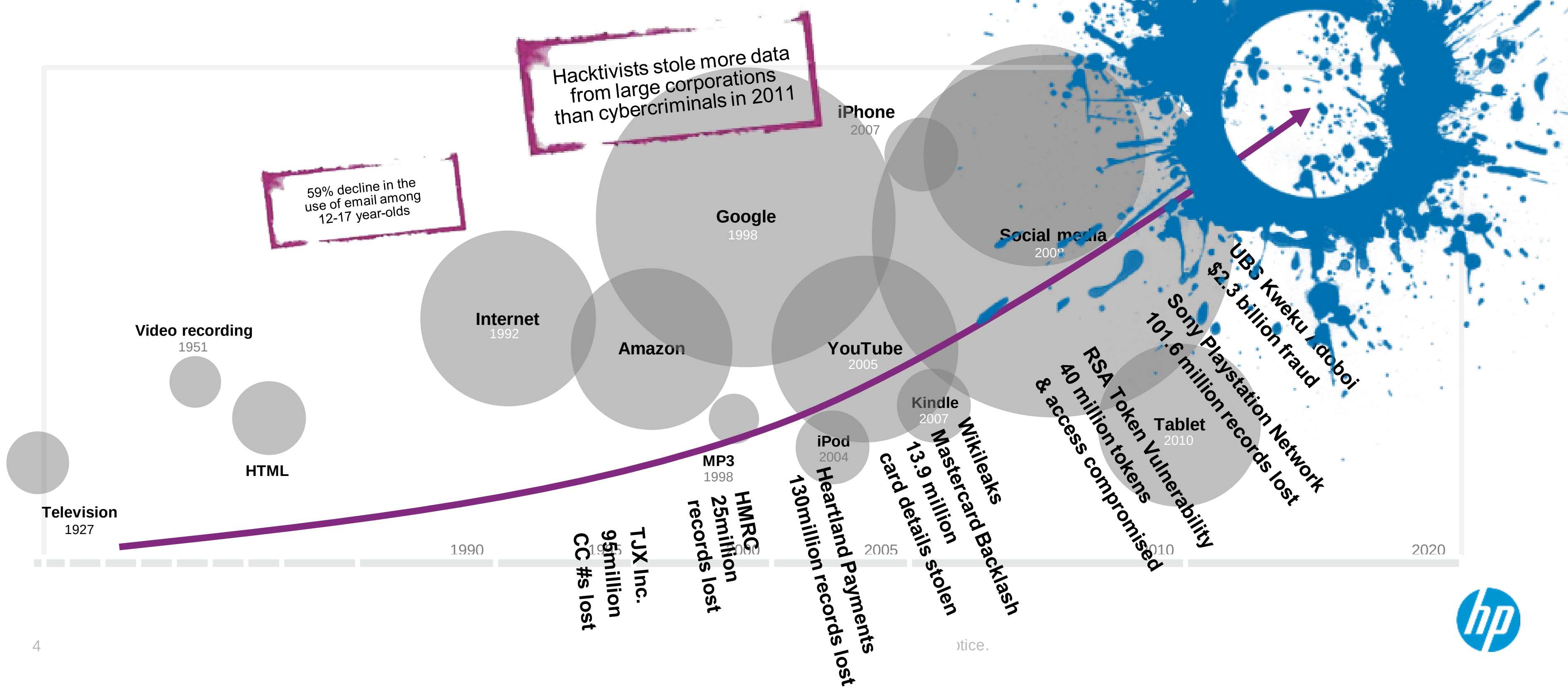
TRUST
sits at heart of
the enterprise security
response

Source: HP internal data, Forrester Research, Ponemon Institute

ce.

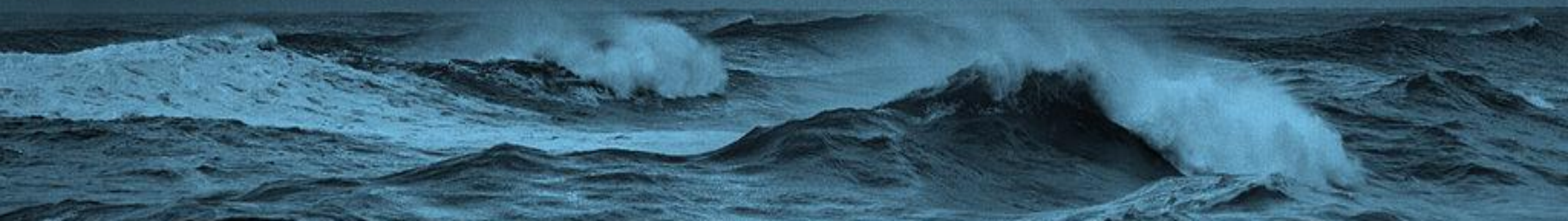
Technology & security timeline

Data freedom, cyber threat, tech complexity & IP value



A New Threat Landscape …

Old world	Traditional IT	Attacks for fame	Regulation
New world	Mobile, cloud, social, information	Attacks for shame, Attacks for gain, cyber warfare	Increasing cost and complexity



China Goverment hacking UNIT 61398

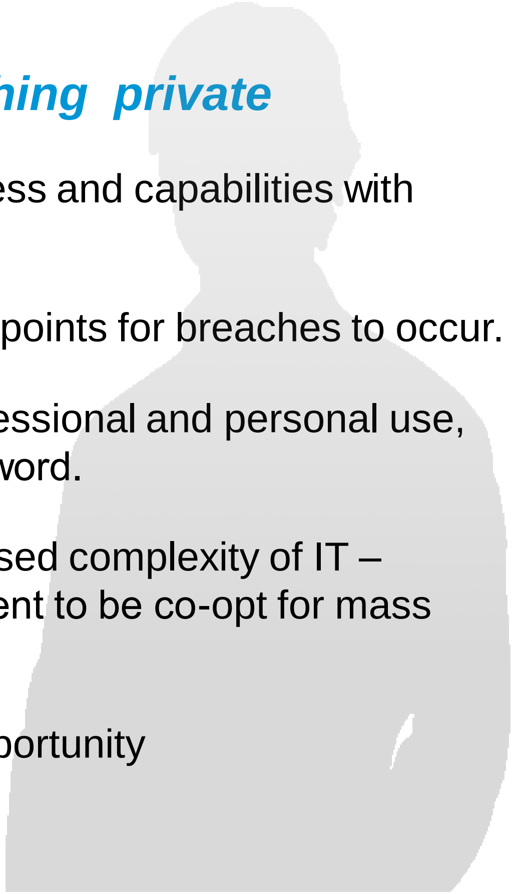
Goverment sponsored „Advanced Persistent Threat“ group

Cybersecurity firm – Mandiant

- believed to be the 2nd Bureau of the People’s Liberation Army (PLA) General Staff Department’s (GSD) 3rd Department, which is most commonly known by its Military Unit Cover Designator (MUCD) as Unit 61398.

- APT1 has systematically stolen hundreds of terabytes of data from at least 141 organizations.
- APT1 focuses on compromising organizations across a broad range of industries in English-speaking countries.
- APT1 maintains an extensive infrastructure of computer systems around the world.
- poor operational security choices, facilitating our research and allowing us to track their activities

Increasing security & privacy threats



Requires new approach = *everything secure, everything private*

- **Affiliated & organized crime groups** are gaining increasing access and capabilities with which to breach security & privacy.

- **Proliferation of mobile devices** increases the number of access points for breaches to occur.

- **Consumerization of IT,** the mixed usage of IT equipment for professional and personal use, increases the potential for breaches – and the use of 'same' password.

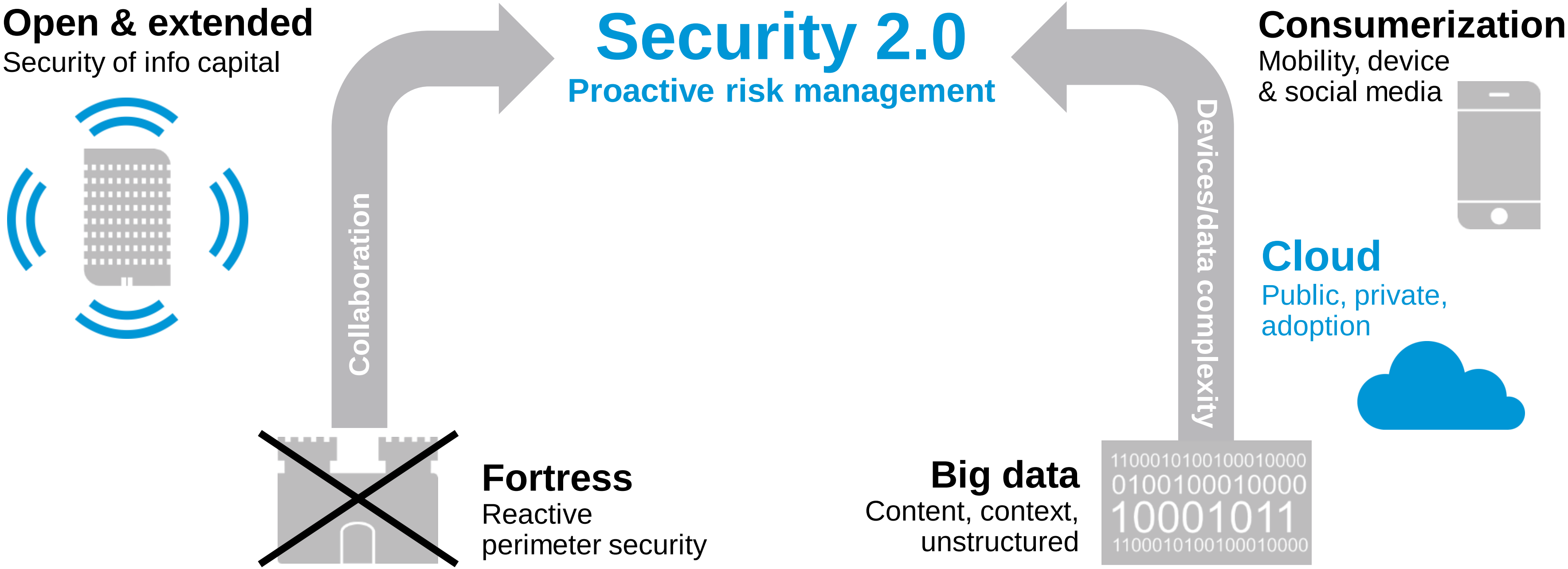
- **Relative lack of sophistication of IT users**: in part due to increased complexity of IT – increases their vulnerability and the opportunity for user's equipment to be co-opt for mass attacks.

- **Ubiquitous use of Social Networking** gives rise to increased opportunity for social engineering exploitation.

Security Industry Challenges

USER ORIENTATION	Identity & Authentication, User Awareness, Traditional Apps/Infrastructure – ID/Profiles/Roles (IAM)
SECURITY BUILT-IN	Virtual, Device & HW level (Trusted Computing)
ANALYTICS & DYNAMIC MONITORING	Event Monitoring, Pattern & Correlation, Volume
CYBER & HACKTIVISM	Collaboration – Industry, Nation, Cybercrime, Hacktivist
SECURITY RISK & COMPLIANCE	Policy, Single View, Integration of Services
MOBILITY / CLOUD	Devices, Web Software & Services, Public/Private Services

Cloud is just one of many disruptive tech trends



Open & extended
Security of info capital

Security 2.0
Proactive risk management

Consumerization
Mobility, device
& social media

Cloud
Public, private,
adoption

Fortress
Reactive
perimeter security

Big data
Content, context,
unstructured

Cloud services: adoption is tempered by uncertainty

Scalability

Security

Auditing

Control

Governance

Data security
& protection

LOB/IT
CIO

Performanc
e

Cost

Reliability

Service levels

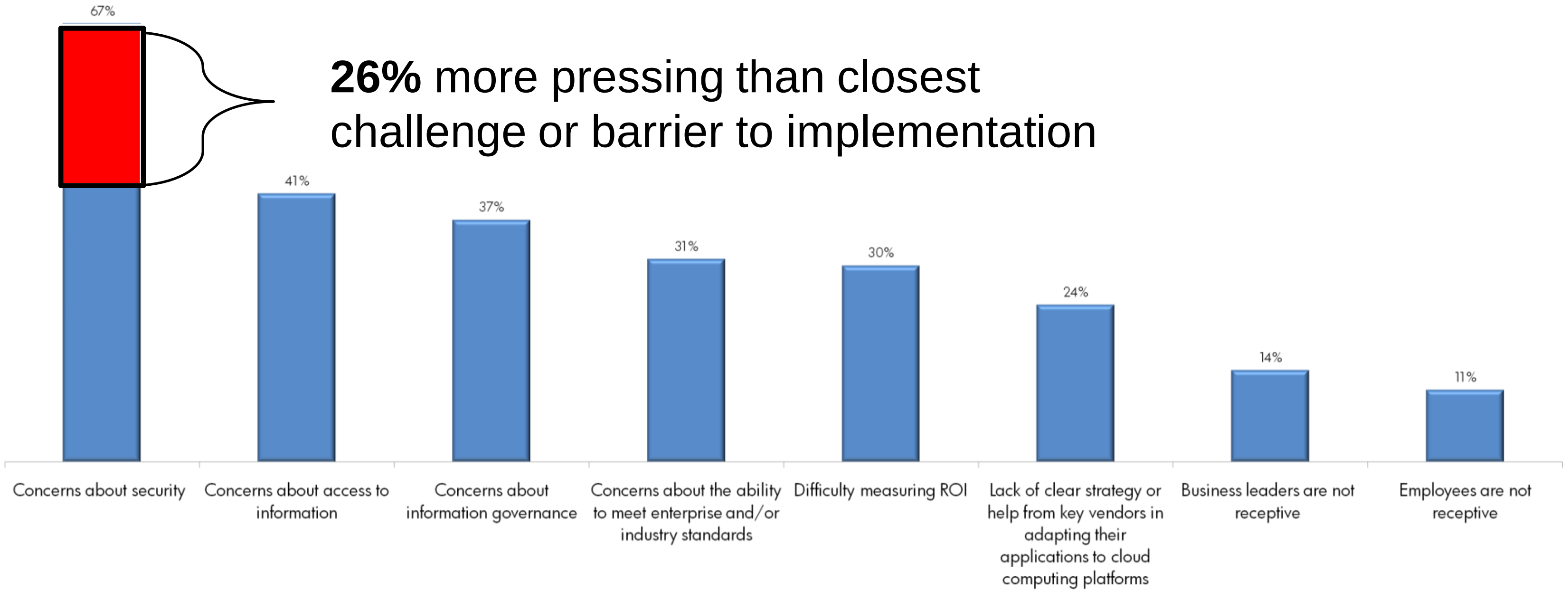
Availability

Compliance

Security or related component is #1 concern/issue for most enterprises

Security is a major CIO challenge

Security concerns prevent movement to the cloud



26% more pressing than closest challenge or barrier to implementation

What do we mean by “cloud security”?

1 **Security for the cloud?** → Securely use cloud

(consumers)

2 →

- **Security from the cloud?** Security-as-a-Service

3 →

- **Security in the cloud?** Embedded security (providers)

4 →

- **Security across clouds?** Hybrid models, interoperability

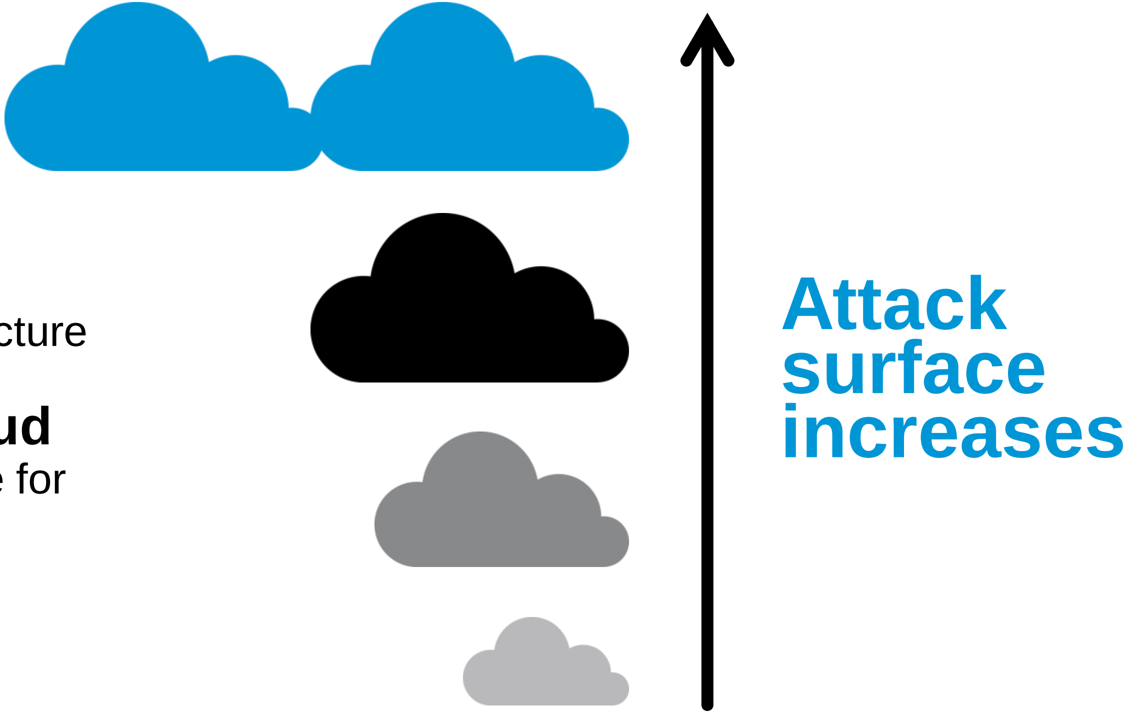
Cloud models require different security solutions…

Hybrid cloud
composition of two
or more clouds

Public cloud
Sold to the public,
mega-scale infrastructure

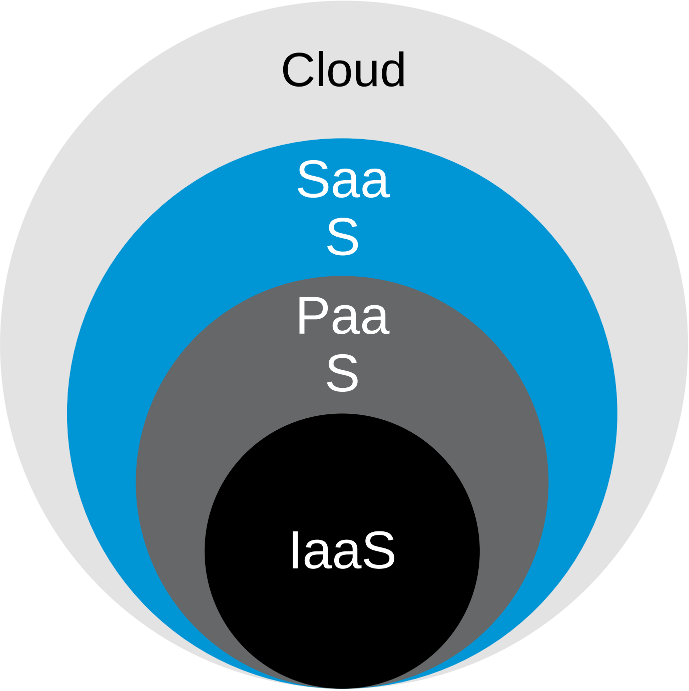
Community cloud
Shared infrastructure for
specific community

Private cloud
Enterprise-owned
or leased



Attack surface increases

… and different roles & responsibilities regarding security



SaaS: Software as a Service, generally provides application, data and infrastructure security, with varying degrees of compliance

PaaS: Platform as a Service, may provide some additional security functions for IDM and secure application development – security falls to app developer and customer IT operations

IaaS: Infrastructure as a Service – providers generally offer basic network & infrastructure security, firewalls, some tools – but customer is generally responsible for implementation, operations, monitoring

But what is really new about “cloud security”?

Many traditional security concerns are recast as a “cloud problem”. . .

- Many “cloud security incidents“ are issues with **web apps and data-hosting,** but at greater scale…
  - e.g. Phishing, downtime, data loss, weak passwords, compromised hosts running botnets, etc …
- **Unexpected side channels** and covert channels arising from shared-resource environments in public services
  - Activity patterns need to be protected in addition to apps and data
- **Reputation fate sharing:** possible blacklisting or service disruption due to “bad neighbors”
  - Need “mutual auditability” (providers need to audit/monitor users)
- **Longer trust chains:** {SaaS to PaaS to IaaS}

Y.Chen, et.al, “What’s New About Cloud Computing Security?” UC Berkeley, Jan.20, 2010

Are your applications & data…

Design apps to
run in cloud

The path of least resistance?

HP Enterprise Security

Security Intelligence Platform

HP Enterprise Security

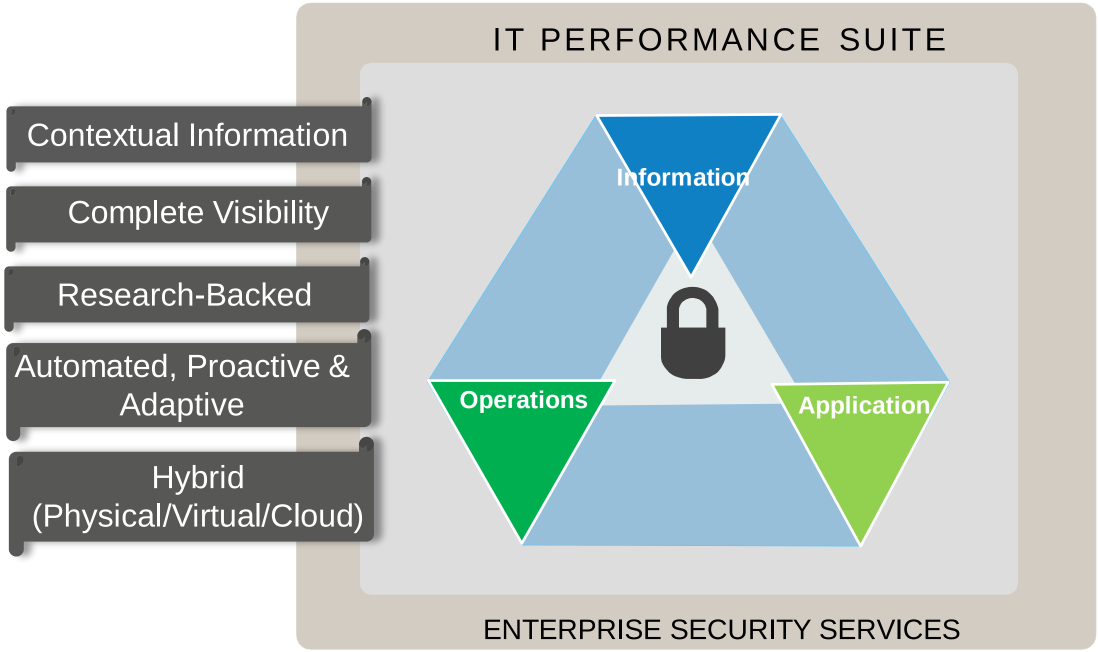
Market leading products and services

- Security Information and Event Management
- Log Management
- Application Security
- Network Security
- Data Protection
- Threat Research
- Security Services

One Team, One Vision
hp
DVLabs
TippingPoint
ArcSight
VISTORM
ATALLA
DATA SECURITY
FORTIFY
SPI DYNAMICS
secure. protect. inspect.

HP Security Intelligence Platform

The only security intelligence platform that gives clients the insight to proactively manage their specific enterprise security threats and risks



IT PERFORMANCE SUITE

- Contextual Information
- Complete Visibility
- Research-Backed
- Automated, Proactive & Adaptive
- Hybrid (Physical/Virtual/Cloud)

ENTERPRISE SECURITY SERVICES

Establish complete visibility across all applications and systems

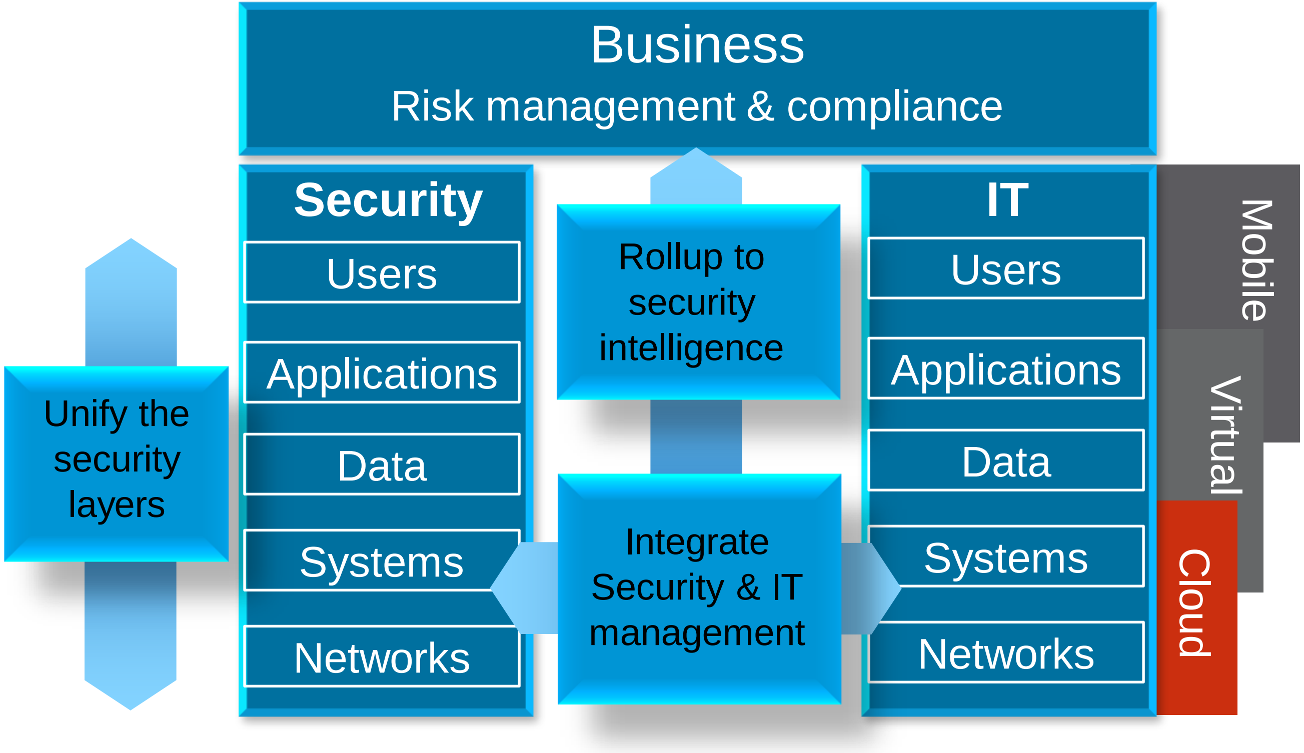
Analyze vulnerabilities in applications and operations to understand risk

Respond adaptively to build defenses against the exploitation of vulnerabilities

Measure security effectiveness and risk across people, process, and technology to improve over time

HP Business Risk Management Strategy

Using Security Intelligence Platform



Business

Risk management & compliance

Security

Users

Applications

Data

Systems

Networks

Unify the security layers

Rollup to security intelligence

Integrate Security & IT management

IT

Users

Applications

Data

Systems

Networks

Mobile

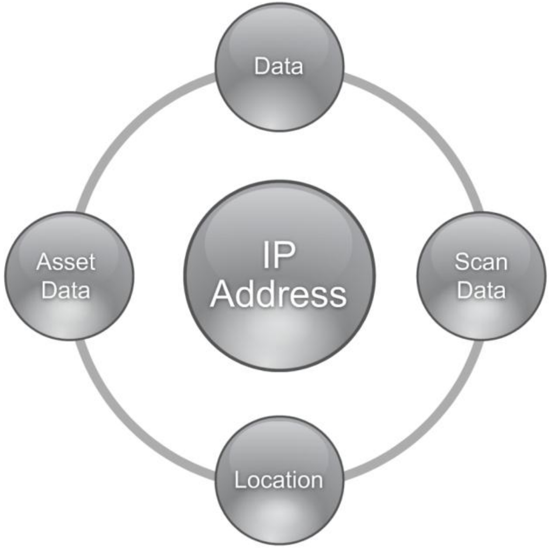
Virtual

Cloud

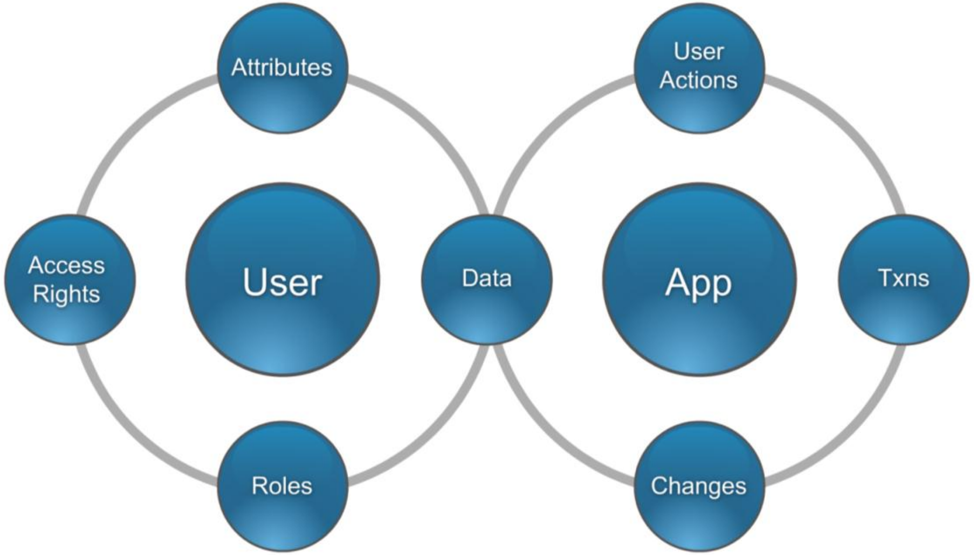
Unify the security layers

Provides Situational Awareness

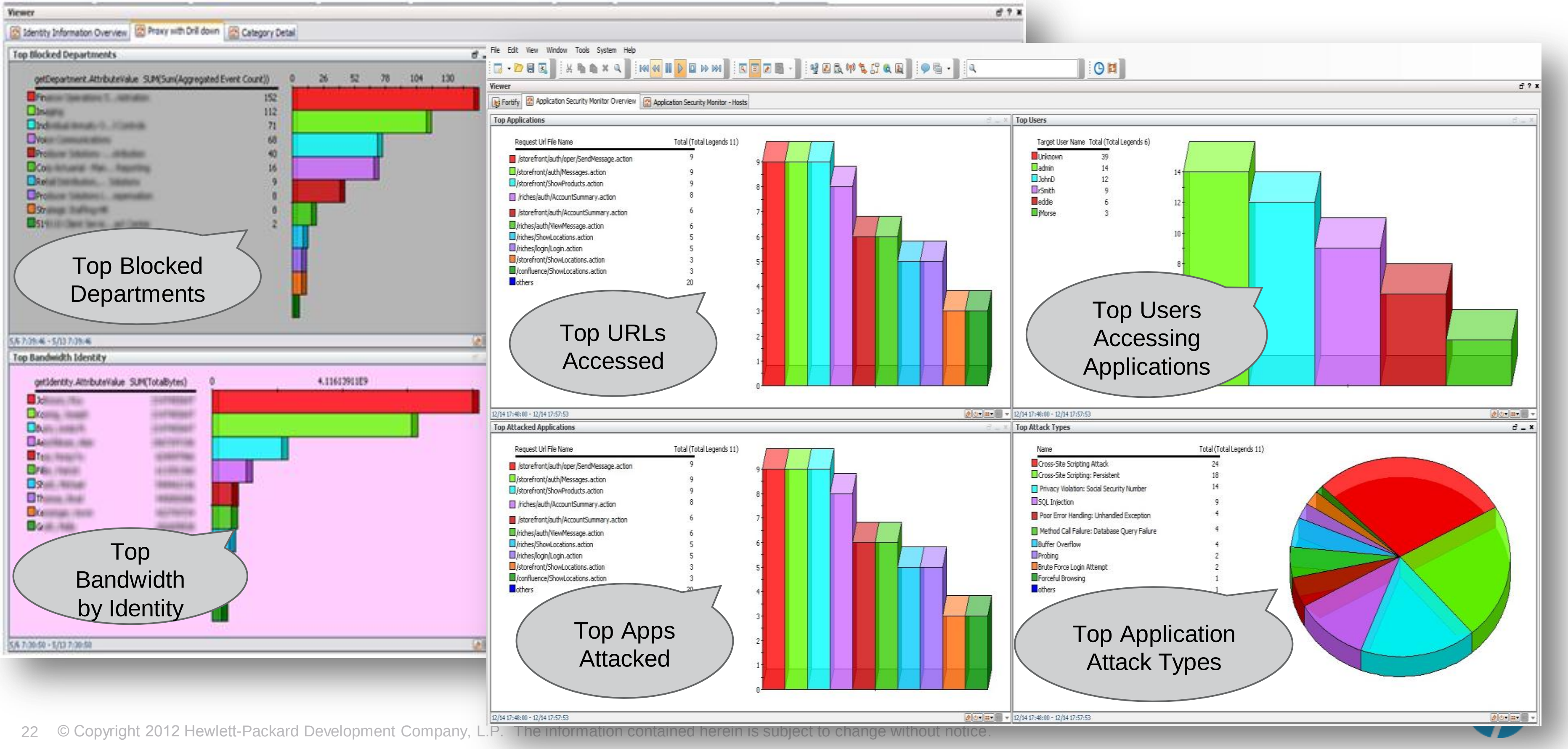
Traditional Security Monitoring



Hybrid Security Monitoring



User and Application Risk Monitoring



Top Blocked Departments

getDepartment.AttributeValue	SUM(Sum(Aggregated Event Count))
🟥 [illegible]	152
🟩 [illegible]	112
🟦 [illegible]	71
🟪 [illegible]	68
🟥 [illegible]	40
🟩 [illegible]	16
🟦 [illegible]	9
🟪 [illegible]	8
🟧 [illegible]	8
🟩 [illegible]	2

5/6 7:39:46 - 5/13 7:39:46

Top Blocked Departments

Top Bandwidth Identity

getIdentity.AttributeValue	SUM(TotalBytes)
🟥 [illegible]	[illegible]
🟩 [illegible]	[illegible]
🟦 [illegible]	[illegible]
🟪 [illegible]	[illegible]
🟥 [illegible]	[illegible]
🟩 [illegible]	[illegible]
🟦 [illegible]	[illegible]
🟪 [illegible]	[illegible]
🟧 [illegible]	[illegible]
🟩 [illegible]	[illegible]

5/6 7:30:50 - 5/13 7:30:50

Top Bandwidth by Identity

Top Applications

Request Url File Name	Total (Total Legends 11)
🟥 /storefront/auth/oper/SendMessage.action	9
🟩 /storefront/auth/Messages.action	9
🟦 /storefront/ShowProducts.action	9
🟪 /riches/auth/AccountSummary.action	8
🟥 /storefront/auth/AccountSummary.action	6
🟩 /riches/auth/ViewMessage.action	6
🟦 /riches/ShowLocations.action	5
🟪 /riches/login/Login.action	5
🟧 /storefront/ShowLocations.action	3
🟩 /confluence/ShowLocations.action	3
🟦 others	20

12/14 17:48:00 - 12/14 17:57:53

Top URLs Accessed

Top Users

Target User Name	Total (Total Legends 6)
🟥 Unknown	39
🟩 admin	14
🟦 JohnD	12
🟪 rSmith	9
🟥 eddie	6
🟩 jMorse	3

12/14 17:48:00 - 12/14 17:57:53

Top Users Accessing Applications

Top Attacked Applications

Request Url File Name	Total (Total Legends 11)
🟥 /storefront/auth/oper/SendMessage.action	9
🟩 /storefront/auth/Messages.action	9
🟦 /storefront/ShowProducts.action	9
🟪 /riches/auth/AccountSummary.action	8
🟥 /storefront/auth/AccountSummary.action	6
🟩 /riches/auth/ViewMessage.action	6
🟦 /riches/ShowLocations.action	5
🟪 /riches/login/Login.action	5
🟧 /storefront/ShowLocations.action	3
🟩 /confluence/ShowLocations.action	3
🟦 others	20

12/14 17:48:00 - 12/14 17:57:53

Top Apps Attacked

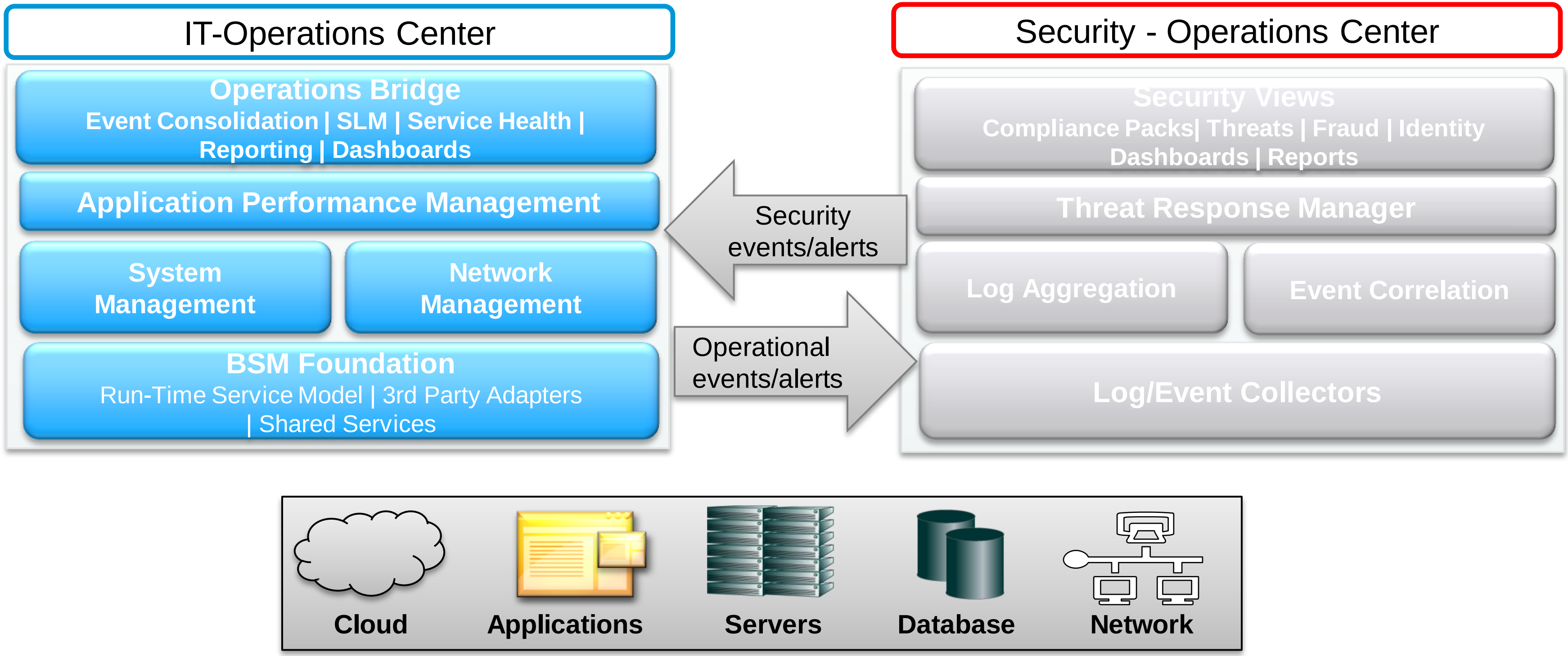
Top Attack Types

Name	Total (Total Legends 11)
🟥 Cross-Site Scripting Attack	24
🟩 Cross-Site Scripting: Persistent	18
🟦 Privacy Violation: Social Security Number	14
🟪 SQL Injection	9
🟥 Poor Error Handling: Unhandled Exception	4
🟩 Method Call Failure: Database Query Failure	4
🟦 Buffer Overflow	4
🟪 Probing	2
🟧 Brute Force Login Attempt	2
🟩 Forceful Browsing	1
🟦 others	1

12/14 17:48:00 - 12/14 17:57:53

Top Application Attack Types

Integrate Security and IT Management



IT-Operations Center

Operations Bridge
Event Consolidation | SLM | Service Health | Reporting | Dashboards

Application Performance Management

System Management

Network Management

BSM Foundation
Run-Time Service Model | 3rd Party Adapters | Shared Services

Security events/alerts

Operational events/alerts

Security - Operations Center

Security Views
Compliance Packs| Threats | Fraud | Identity Dashboards | Reports

Threat Response Manager

Log Aggregation

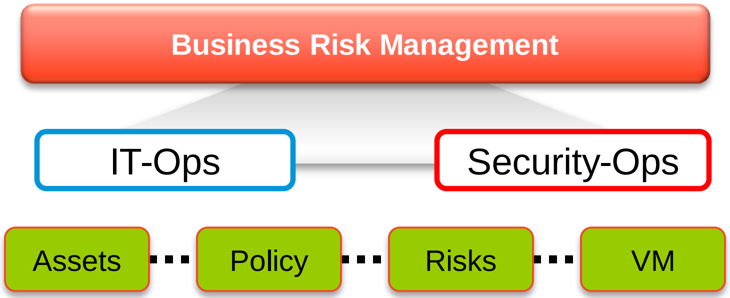
Event Correlation

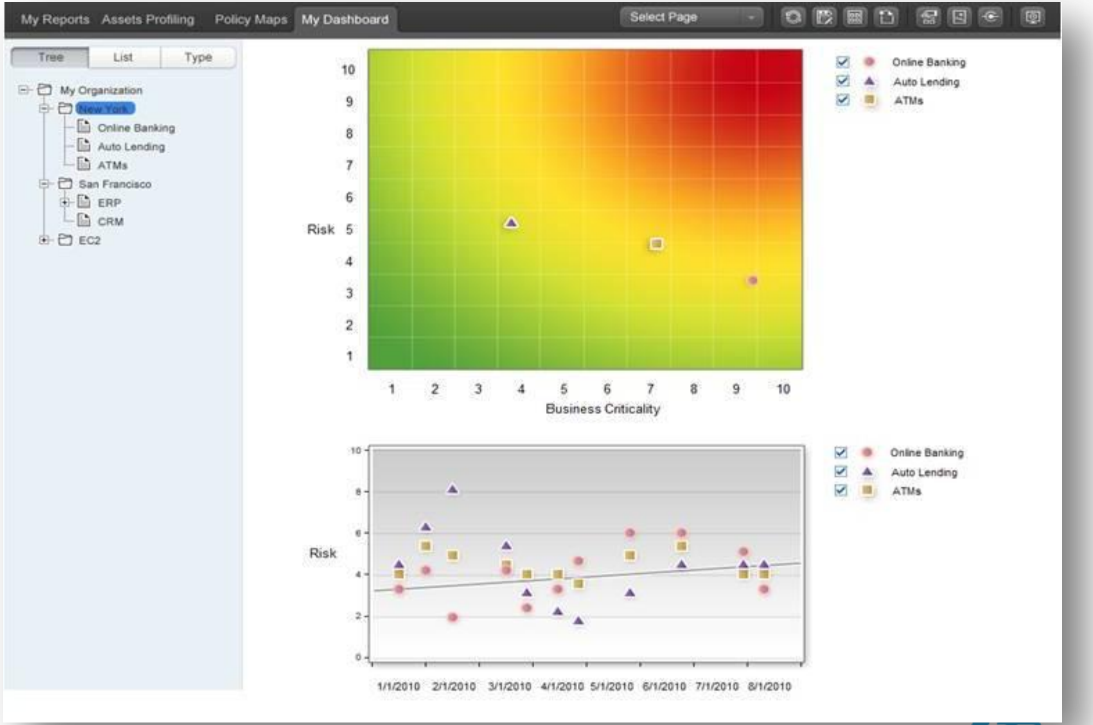
Log/Event Collectors

Cloud **Applications** **Servers** **Database** **Network**

Pro-Active Business Risk Management

Are We ~~Secure~~ at Risk?





Business Risk centric:

- Heat maps - real-time analysis
- Long-term trending

HP Enterprise Security

Solutions for Cloud Security

Use-Cases: ESP Cloud Security Solution

HP ESP solutions can support use-cases #1 & #2 now, and #3 in the fut

1. **Monitor user access to SaaS applications (e.g. SalesForce.com)**

   Employee access from within enterprise network via corporate gateway

   Remote worker access directly to SaaS service provider

2. **Monitor infrastructure hosted in Hybrid cloud environment (e.g. company data center)**

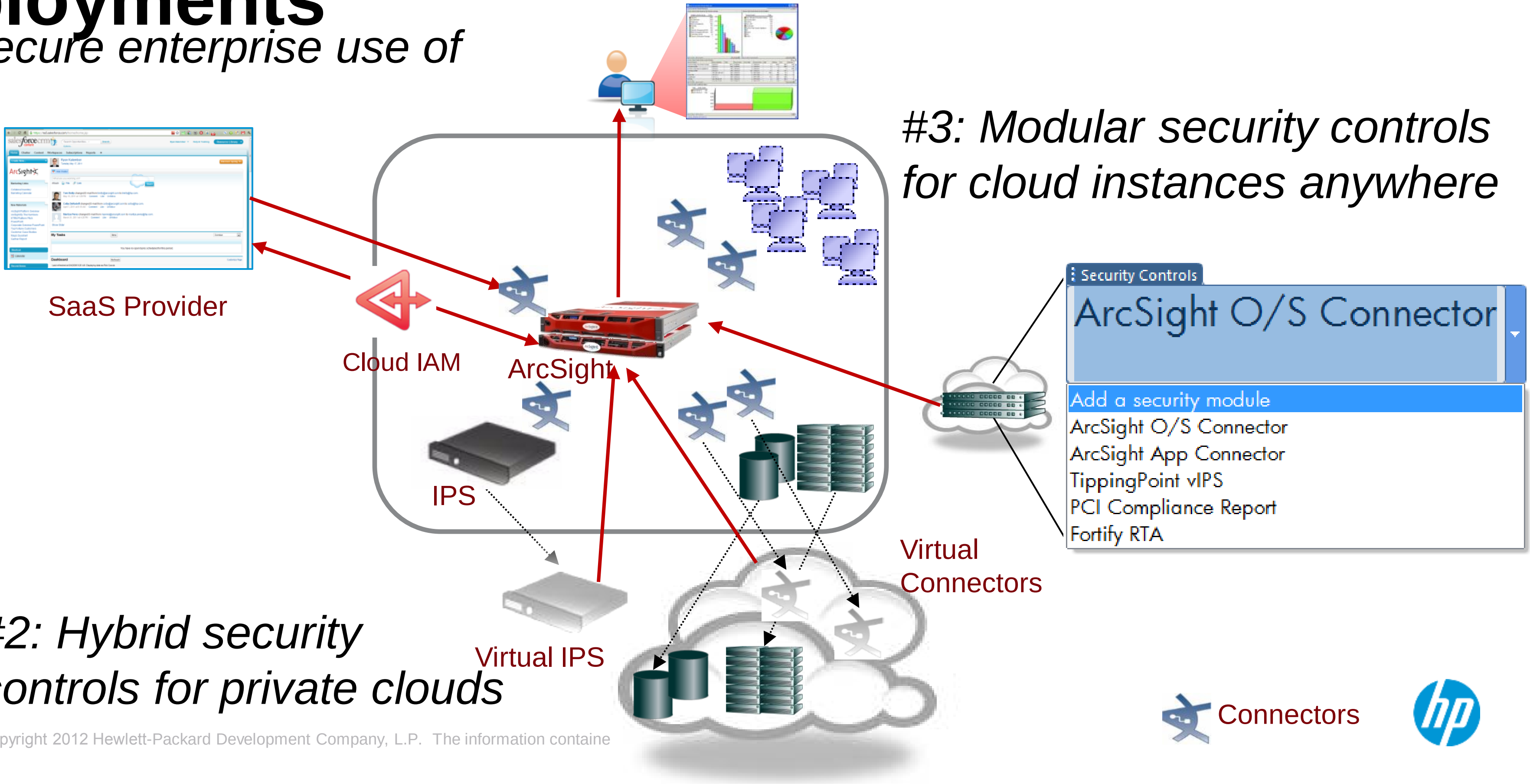
   Employee access from within enterprise network to applications hosted in private cloud

3. **Monitor infrastructure hosted in Public cloud (e.g. Amazon EC2)**

   Employee access to application stack (LAMP: Linux, Apache, MySQL, Php)

HP Security Solutions for Cloud Deployments

#1: Secure enterprise use of SaaS



#3: Modular security controls for cloud instances anywhere

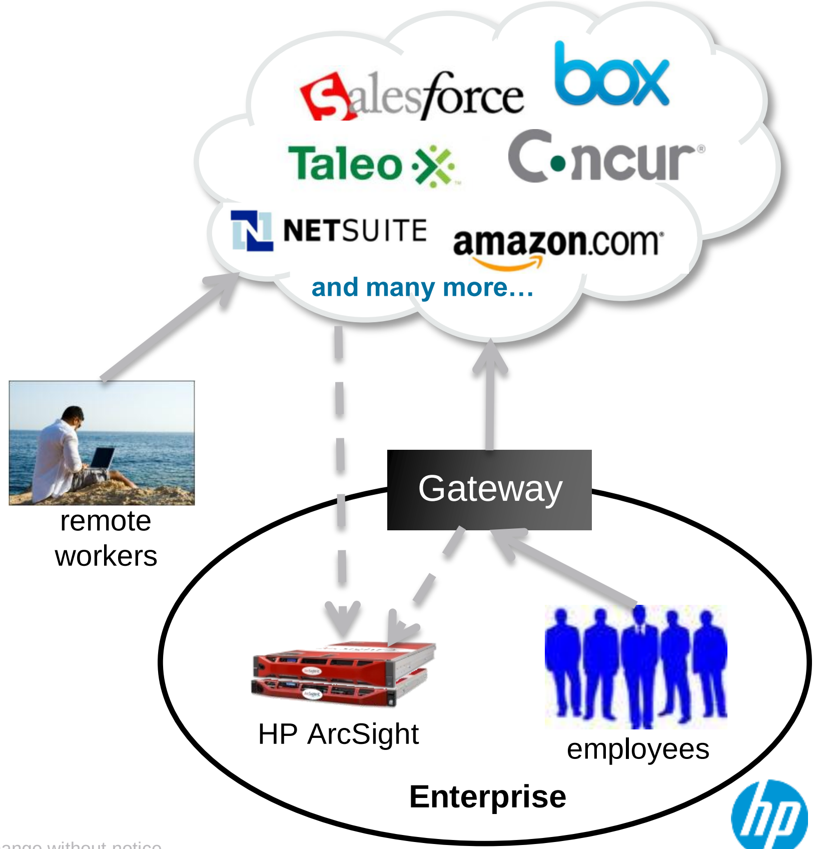
#2: Hybrid security controls for private clouds

#1 Monitoring SaaS applications

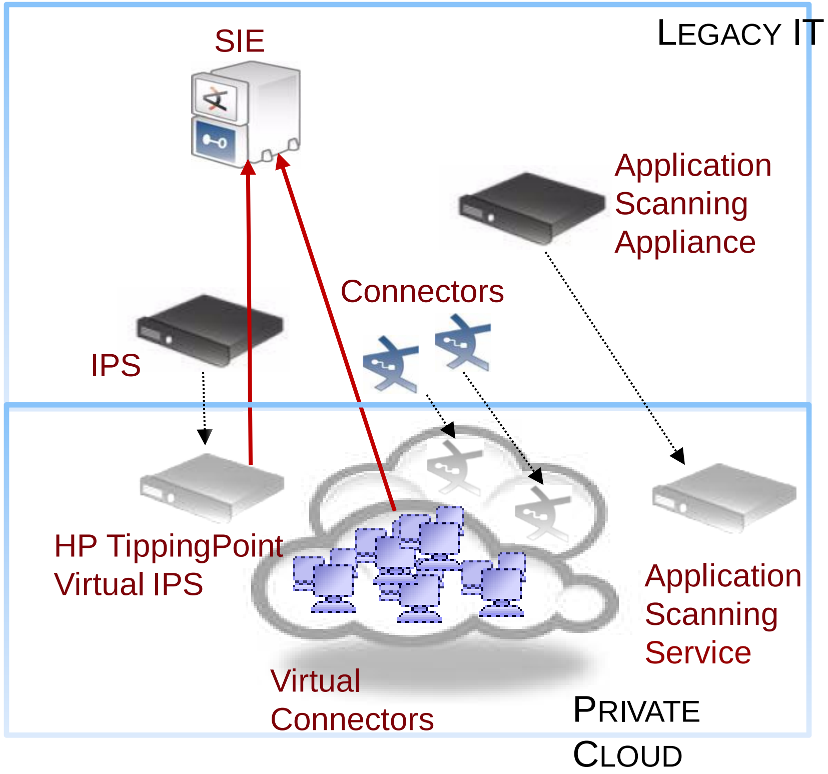
HP Cloud Connections Partners

HP ArcSight monitors SaaS applications:

- Employee access via gateways (e.g. PingIdentity, Layer7, etc.)
- Remote worker access via API's provided by SaaS vendors (e.g. SalesForce)



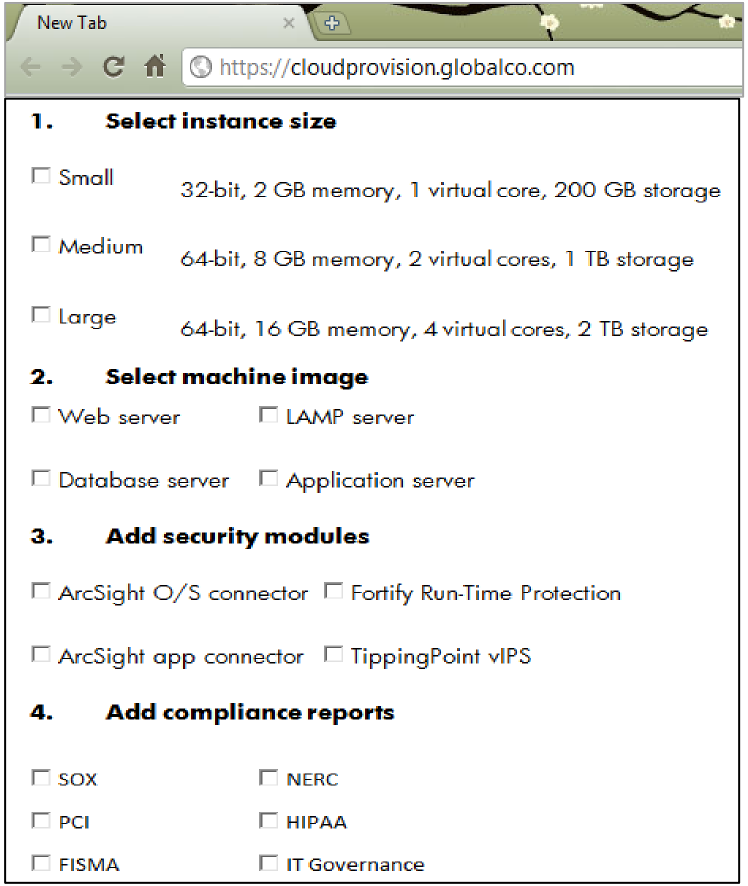
#2 Hybrid security controls


LEGACY IT
SIE
Application Scanning Appliance
Connectors
IPS
HP TippingPoint Virtual IPS
Application Scanning Service
Virtual Connectors
PRIVATE CLOUD

#3 Modular Security Controls

The future

- **Follows standard dev/ops process**
- **Select instance size/image to provision**
  - Add security modules
    - Connectors for log syndication and SIEM
    - Virtual IPS for network protection
    - Fortify RTA for run-time app protection
  - Add compliance controls/reporting
    - Reports driven by connectors
    - Controls link to security modules
- **Cloud controls integrate with legacy environment security controls**



https://cloudprovision.globalco.com

1. Select instance size

□ Small	32-bit, 2 GB memory, 1 virtual core, 200 GB storage
□ Medium	64-bit, 8 GB memory, 2 virtual cores, 1 TB storage
□ Large	64-bit, 16 GB memory, 4 virtual cores, 2 TB storage

2. Select machine image

□ Web server □ LAMP server

□ Database server □ Application server

3. Add security modules

□ ArcSight O/S connector □ Fortify Run-Time Protection

□ ArcSight app connector □ TippingPoint vIPS

4. Add compliance reports

□ SOX □ NERC

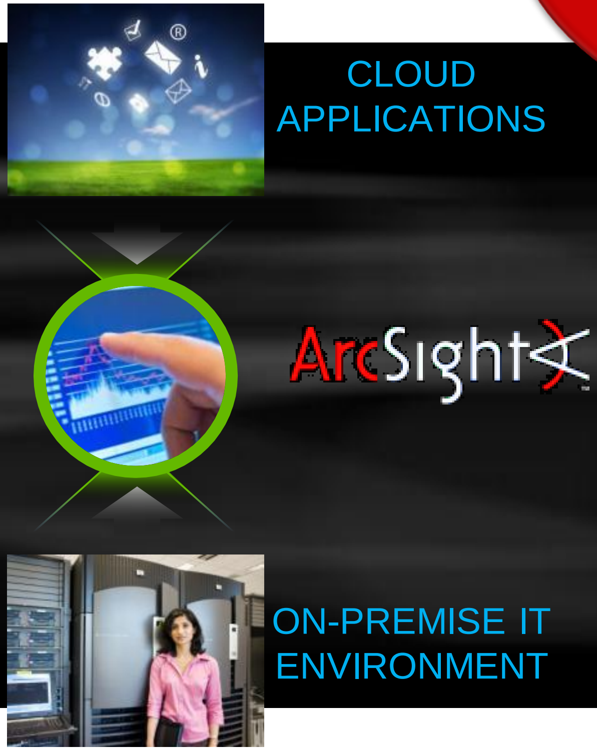
□ PCI □ HIPAA

□ FISMA □ IT Governance

HP Enterprise Security
Cloud Connections Partner Program

NEW

- HP is launching the Cloud Connections Partner Program enabling users of HP ArcSight ESM to view user activity in cloud based applications
- Hybrid analytics provide centralized views, security and compliance reporting across on-premise and cloud-based environments as customers deploy hybrid environments
- Initial partners: Salesforce.com, Box and Okta



Summary

Summary: A CISO’s path to the cloud

Approach cloud security strategically, starting with quick wins

Start with by securing enterprise use of SaaS

- Cloud identity and access management
- SaaS event monitoring

Next, establish hybrid controls:

- Log syndication
- Application scanning

Long term, add modular security controls to all clouds

Connectors for security monitoring and compliance reporting

Virtual IPS modules for virtual and physical network security

Run-time protection against application vulnerabilities

Thank you

Peter Mikeska (CiSA, CiSM, RHCE)

Technology Services

peter.mikeska@hp.com