

Integrated Cloud Protection

An architectural perspective

Iaroslav Levkov,
Solution Architect, HP TS Consulting CIS Countries
April 2013

© Copyright 2012 Hewlett-Packard Development Company, L.P.
The information contained herein is subject to change without notice.



Agenda

1. Executive summary
2. Top threats in the cloud
3. Focus areas for cloud security
4. HP Cloud Protection Reference Architecture
5. HP Cloud Protection Program overview
6. HP Services



Executive summary

Today, everything is mobile, connected, interactive, immediate, and fluid. As business expectations are high, it mounts pressure on service delivery.

Organizations, such as yours, are required to provide technology-enabled services to the business users and customers, whenever and wherever they need them—cost-effectively, securely, and quickly.

Cloud computing can provide new levels of collaboration, agility, speed, and cost savings for enterprises of any size and type. But getting the most out of the cloud is not a simple exercise. All services are not created equal. Each has its own requirements in terms of performance, security, control, and availability.



Cloud Security

© Copyright 2012 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.



Top threats in the cloud

Top threats in the cloud
• Abuse and nefarious use of cloud computing • Vulnerable application programming interfaces • Malicious insiders • Unknown risk profile • Shared technology vulnerabilities • Data loss/leaks • Account, service, and traffic hijacking
cloudsecurityalliance.org/topthreats.html



5 focus areas for cloud security

- 1. Security of cloud access devices**
- 2. Security and availability of the cloud platform**
- 3. Identity and access management for the cloud**
- 4. Security and compliance management for the cloud**
- 5. Security impact for cloud stakeholders**



HP Cloud Protection Reference Architecture

© Copyright 2012 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.



Security of cloud access devices

- User authentication based on the combination of user ID/password, user ID/security token, or user ID/public key infrastructure (PKI) credentials, before establishing a browser connection to the cloud
- Browser connection established using a secure remote access solution (for example: based on a Secure Sockets Layer (SSL) tunnel and the associated device-level PKI credentials, and strong cryptographic algorithms)
 - Anti-malware
 - Data and Host protection



Security and availability of the cloud platform

- Classical nonvirtualized computing, networking, and storage services
- Combination of both virtualized and non-virtualized IT resources
- Malware and data protection measures
- Network and host security solutions
- Security solutions tailored to protect the virtualization layer
- IDS/IPS, firewalls, and networking protection software.
- Security management solution that can span both the physical and virtualized elements of the IT infrastructure.
- Multi-tenancy isolation requirements different tenants' data are isolated while they are processed, transmitted, or stored on the shared cloud infrastructure.
- PaaS, SaaS application-level hardening, denial-of-service protection, application-level data encryption, and integrity protection.
- PaaS secure software development and deployment.



Identity and access management for the cloud

Identity and access management services:

- Account management
- Role-based access control management
- Key and credential management (for example: through the use of a PKI)
- Authentication services and single sign on (SSO)
- Identity-level auditing
- Identity federation (secure exchange of identity attributes between different cloud environments and cloud “islands” like SSO and transparent resource access to users of such cloud service)
- Identity provisioning (automatic provisioning and de-provisioning of all user, device, and service accounts across cloud and non-cloud IT infrastructures)



4. Security and compliance management for the cloud

Security management services for the cloud consist of a set of ITIL-driven management services with security impact and services such as vulnerability, compliance, and security patch management.

Management services with security impact include change, incident, configuration, capacity, and availability management.

Security and compliance management for the cloud requires more than just security products; it also involves security-minded people, processes, policies, procedures, and proof to ensure that the environment operates at a certain security level



P5 Model (HP ISSM)

P1 People

Determines if the right staff are performing the correct roles to oversee Cloud Computing security.

P2 Policy & Procedures

Determines if the right set of policies and procedures are in place to govern the security and continuity of public / private Cloud Computing.

P3 Processes

Determines if the proper security / continuity process models are in place to safeguard the transference of data between consumers and providers of Cloud Computing.

P4 Products

Determines if appropriate defense-in-depth technologies / solutions are in place to manage/mitigate risk between consumers and providers of Cloud Computing.

P5 Proof

Determines if the correct validation methods, metrics, and / or KPIs are used to track Cloud Computing consumer and provider control effectiveness.

5. Security impact for cloud stakeholders

Three categories, of stakeholders each linked to distinct security attributes with different cloud security-related processes, procedures, and policies.

Consumers :

- A set of credentials (ID and authentication factors)
- A cloud-level role (defining the privileges and access rights of the consumer in the cloud)
- A security domain (or classification level defining consumer access to a sub-portion(s) of the cloud)

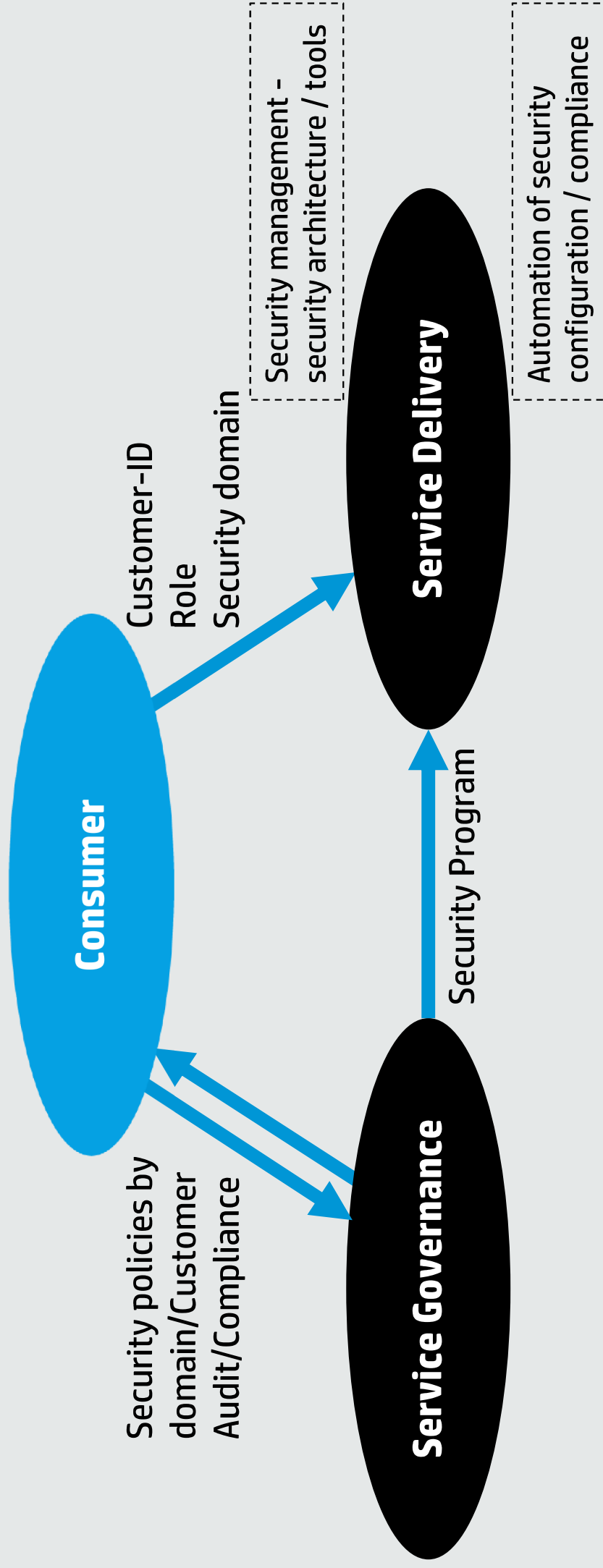
Service delivery personnel ensure proper security configuration and operation of the cloud and its resources. Cloud service delivery personnel include administrators, developers, architects, and security administrators

Service governance stakeholders set the overall security levels and direction for the cloud and ensure that the security posture of the cloud is aligned with organizational, industry, or governmental regulations (audit and compliance). Service governance stakeholders include the IT manager, business manager, security officer, and security auditor.

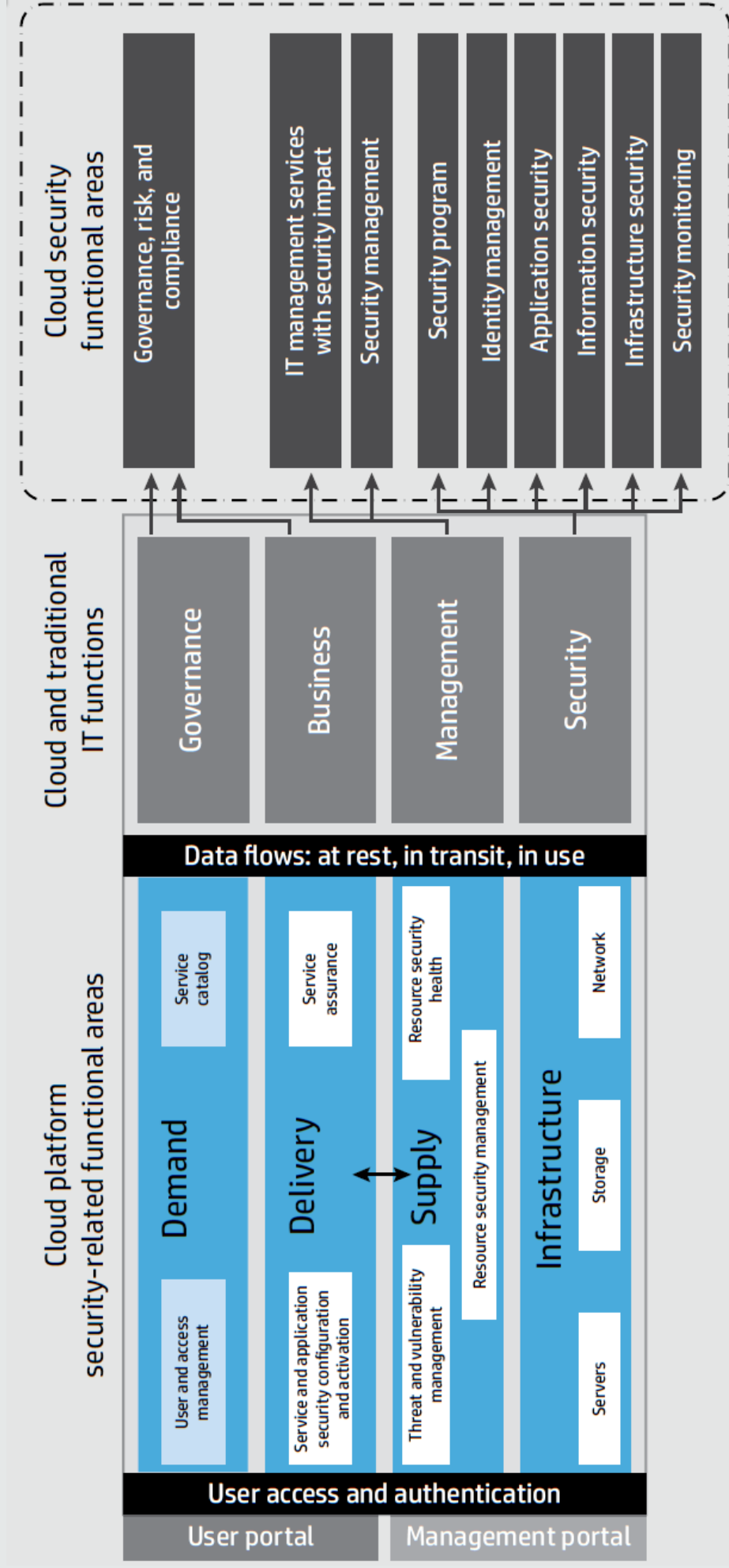


Security stakeholders:

Functional interlock - governance



HP Cloud Protection Reference Architecture



Functional to technical subcomponents

Cloud security functional areas

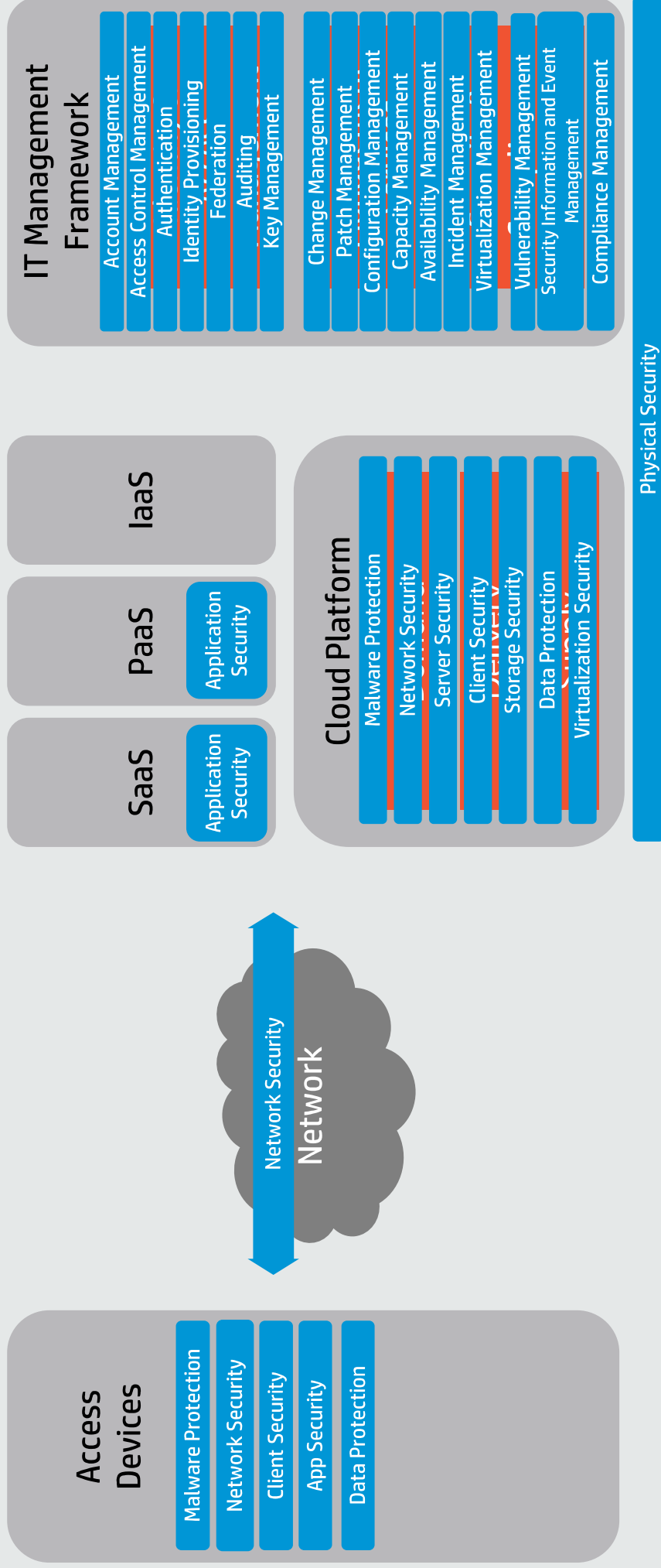
Governance, Risk & Compliance
Security Management
Security Program
Identity Management
Application Security
Information Security
Infrastructure Security
Security Monitoring

Cloud security technology components (P4: Products)

GRC Tool
Policy Based Management & Automation
Change Management
Patch Management
Configuration Management
Vulnerability Management
Security Service Portal
Account Management
Access Control Enforcement
Identity Provisioning
Authentication
Auditing
Federation
Code Scanning & Remediation
Secure Application Development Tools
Data Loss Protection
Data Recovery
e-Discovery
Data Privacy
Rights Management
Data Encryption
Virtualization Security
Malware Protection
Client Security
Server Security
Network Security
Storage Security
SIEM Tool
Intrusion Detection & Prevention
Vulnerability Scanning



HP Cloud Protection Reference Architecture: Technical View

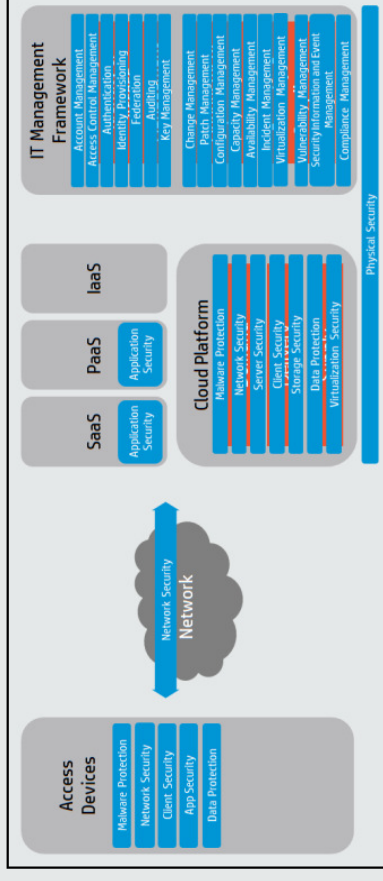
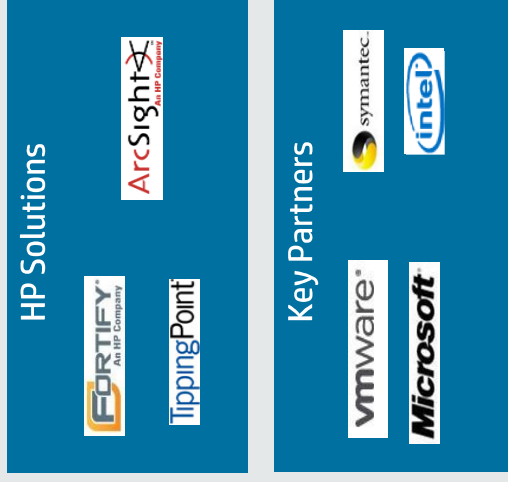


HP Cloud Protection Reference Architecture

Reference architecture components:

- Business, functional, technical & implementation Views (HP GM ITSA)
- Integrated ITSM-ISSM P5 Reference Model
- Detailed threat matrix with technology solution mapping
- CSA threats with technology solution mapping
- Hybrid cloud security processes with context of threats, controls and technology solution

HP solutions augmented with best-of-breed HP partner solutions:



Summary content available in public white paper



HP Cloud Protection Program overview

Integrated security and compliance in the cloud

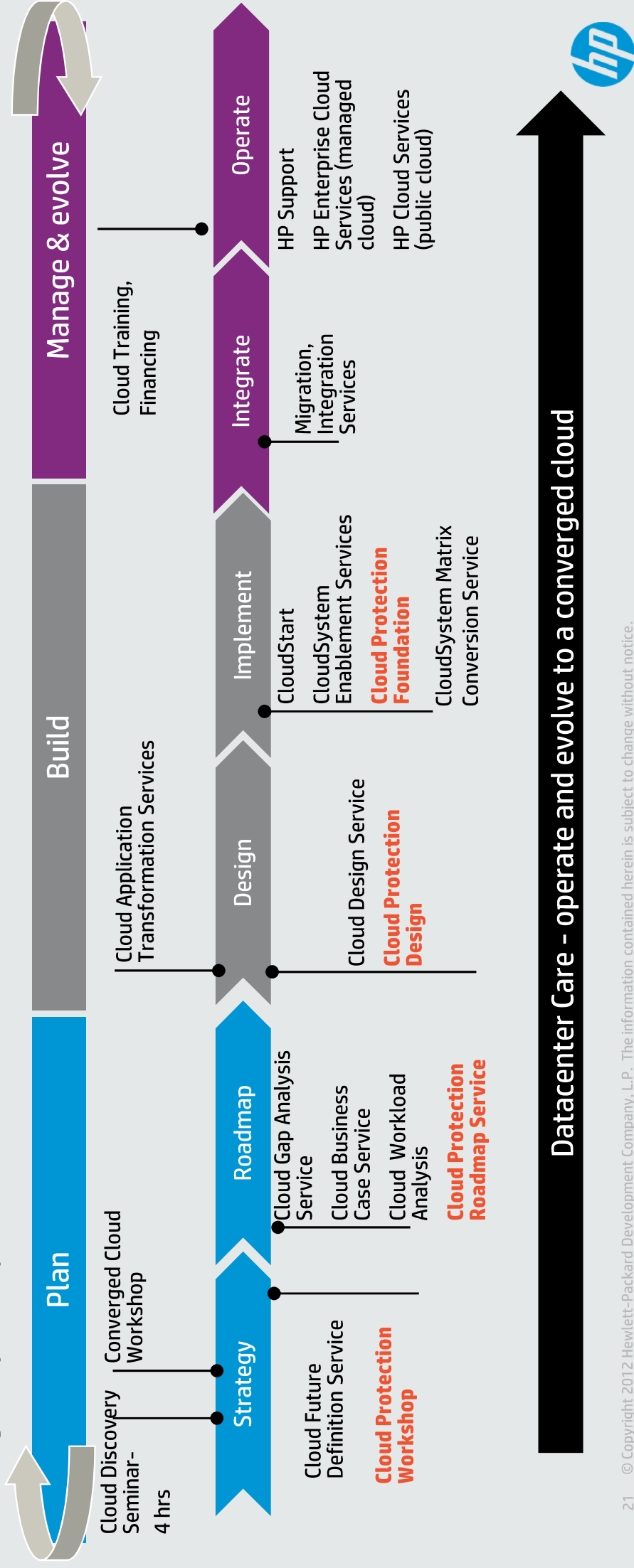
**Confidently mitigate threats defined by
Cloud Security Alliance across policy,
people, process and technology**

**Faster security technology
deployment based on proven experience
and building block approach**



HP services for planning, building, managing, & evolving your converged cloud

Guiding the journey- detailed view



Thank you

© Copyright 2012 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

