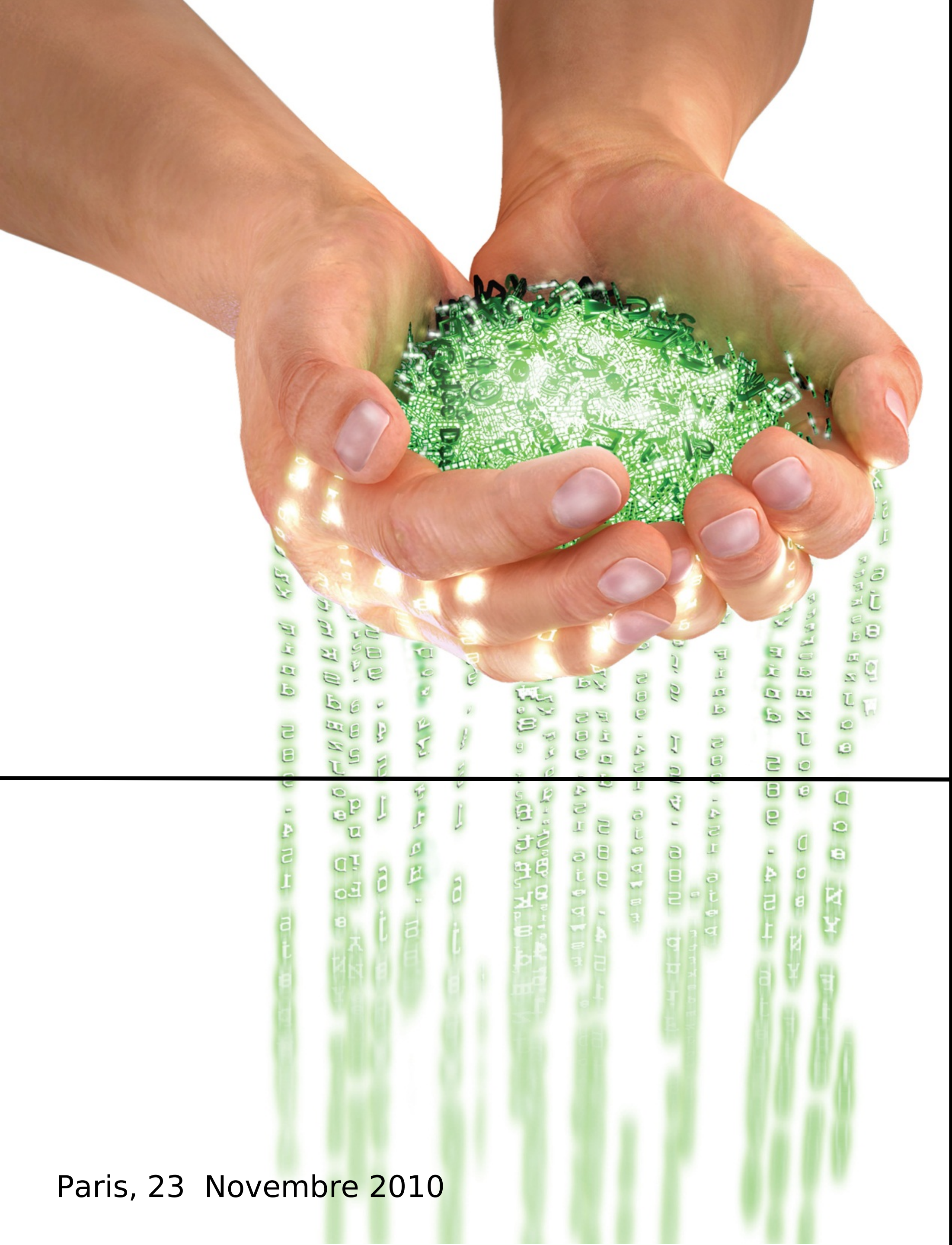


DeviceLock®

- DLP -

Des nuages à la terre ferme

Paris, 23 Novembre 2010

Agenda

- Notion de Data Leak Prevention
- Retour sur le Cloud
- Mesures de sécurité spécifiques au Cloud
- Quel est la nécéssité du DLP dans le Cloud ?
- DLP dans le Cloud et sur la terre ferme
- La protection des données en mouvement, en utilistation et stockées
- DLP Functional Split for the Cloud
- Conclusion

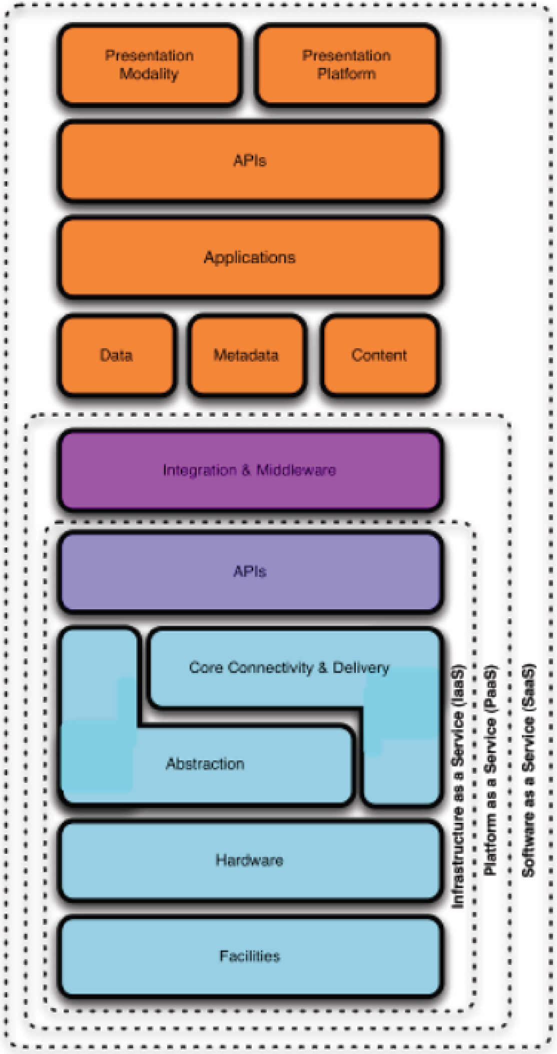
Data Leak Prevention in Brief

- Prevent unauthorized use and transfer of sensitive corporate information by protecting
  - Data in motion (DIM) – network transmissions
  - Data in use (DIU) – endpoint actions
  - Data at rest (DAR) – data storage
- Functions
  - Control of data transfer/storage operations (context-based)
  - Content monitoring and filtering (core DLP technology)
  - Content discovery & classification
  - Event logging and alerting, data shadowing
  - Incident management
  - Central administration and policy management

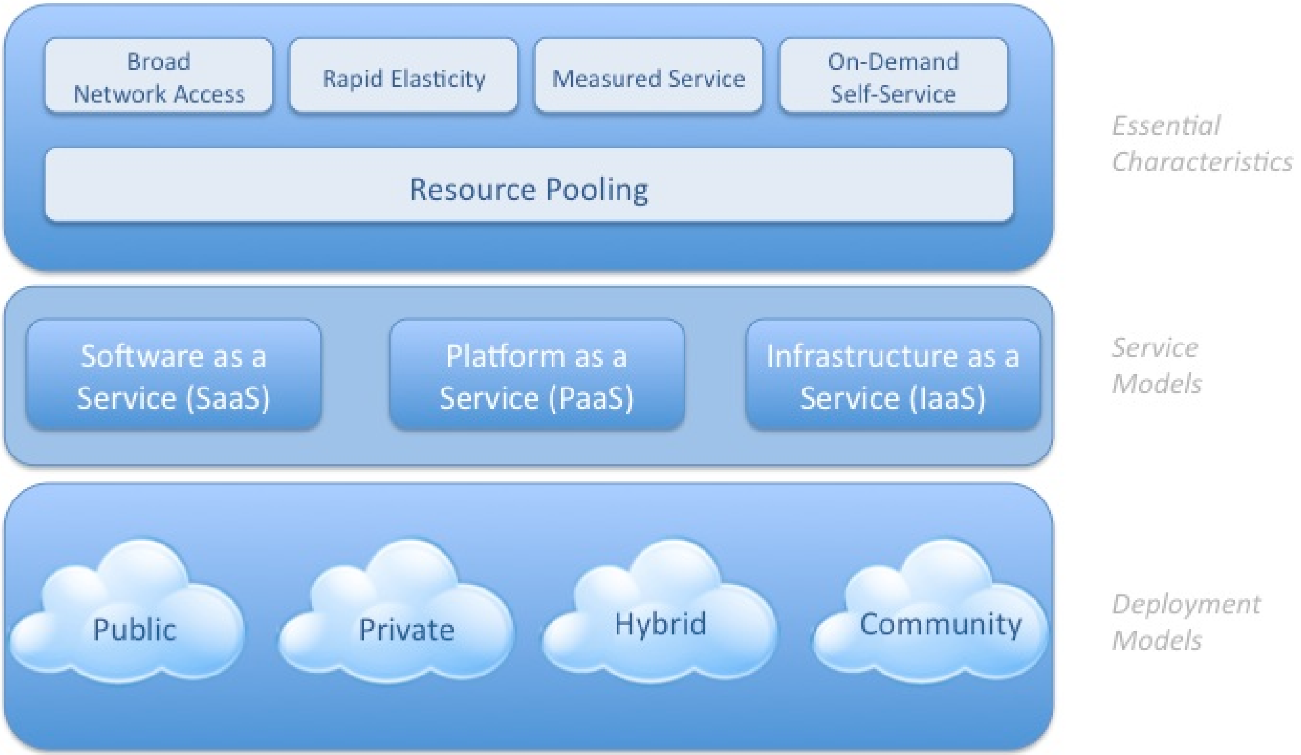
Data Leak Prevention in Brief (*cont.*)

- DLP types
  - Network-based (DLP appliances)
    - Perimeter control of data transmissions from/to internal PCs and servers in the office
    - High performance processing
    - Most effective and unique for email content filtering
  - Endpoint (host-resident software DLP agents)
    - Desktops, laptops, netbooks, tablets, smartphones
    - Control over local data channels
    - DLP for remote and mobile computers
  - Hybrid
    - Combine unique features of both network-based and endpoint DLP components
    - Functionally most complete

Cloud Computing At-a-Glance



- Cloud computing is an implementation of the “IT as a utility” dream for a modern enterprise
  - Reference model of Cloud computing stack (left)
  - Visual Cloud computing definition (below)



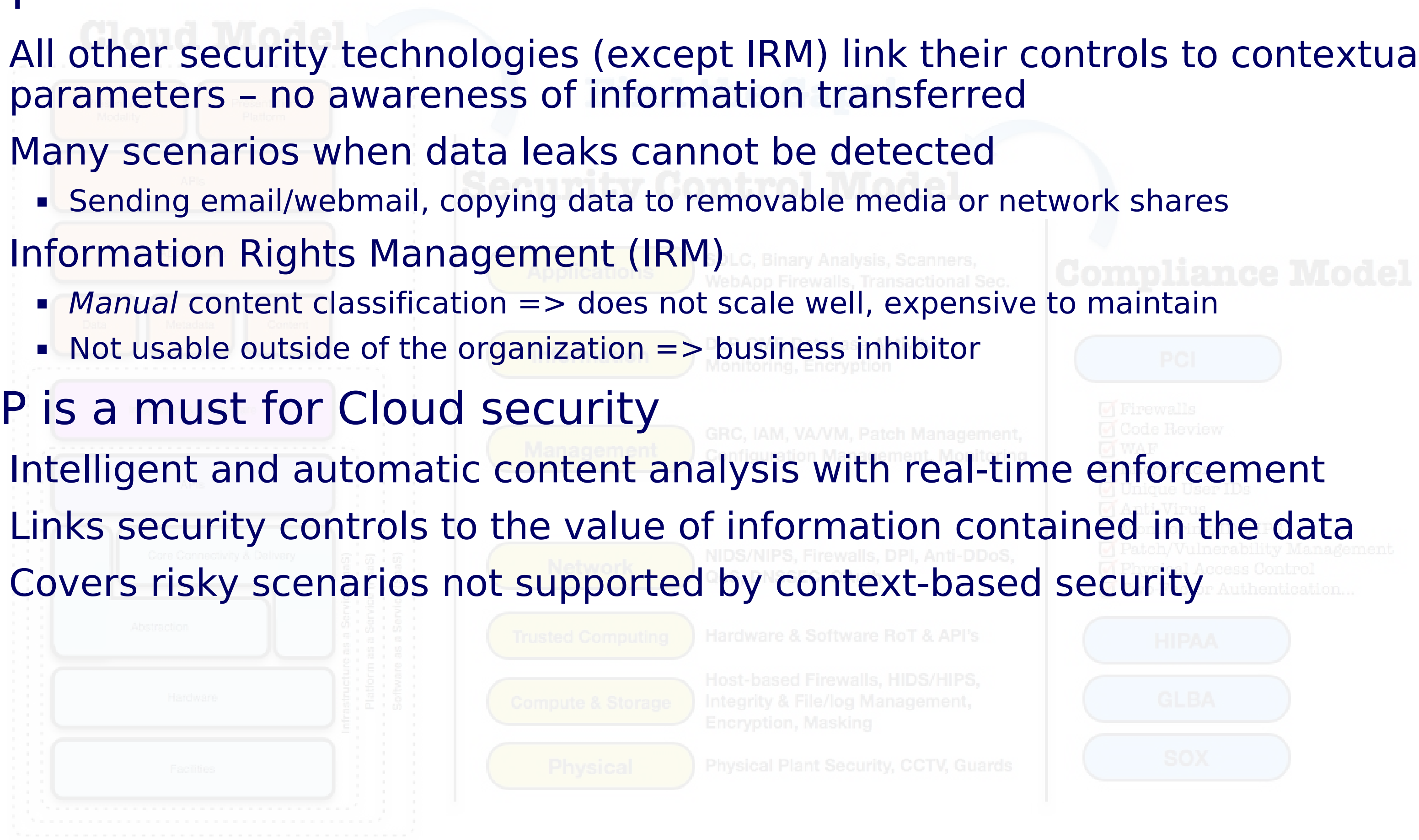
Source: Cloud Security Alliance Guidance Version 2.1 (2009)
NIST Visual Model of Cloud Computing Definition (2009)

Cloud Security Specifics

- Factors
  - Multi-tenancy
    - Data & apps from different customers share the same computing resources
  - Virtualization
    - Data, applications, OS, virtual machines and networks can dynamically move in the Cloud
    - Computing & network resources abstracted to the highest degree possible
  - No physical separation & control, no static perimeter to protect
  - Data location is distributed, undetectable, and may move any time
  - Split of operational responsibilities between customer and provider(s)
  - Lack of trust: between customer and provider, between different tenants
- Consequences
  - Specific threat profile - different from those of conventional IT models
  - Information-centric security becomes the core IT security principle
    - Links security controls to information contained in the data
    - Effectively implements risk-based approach to corporate IT security

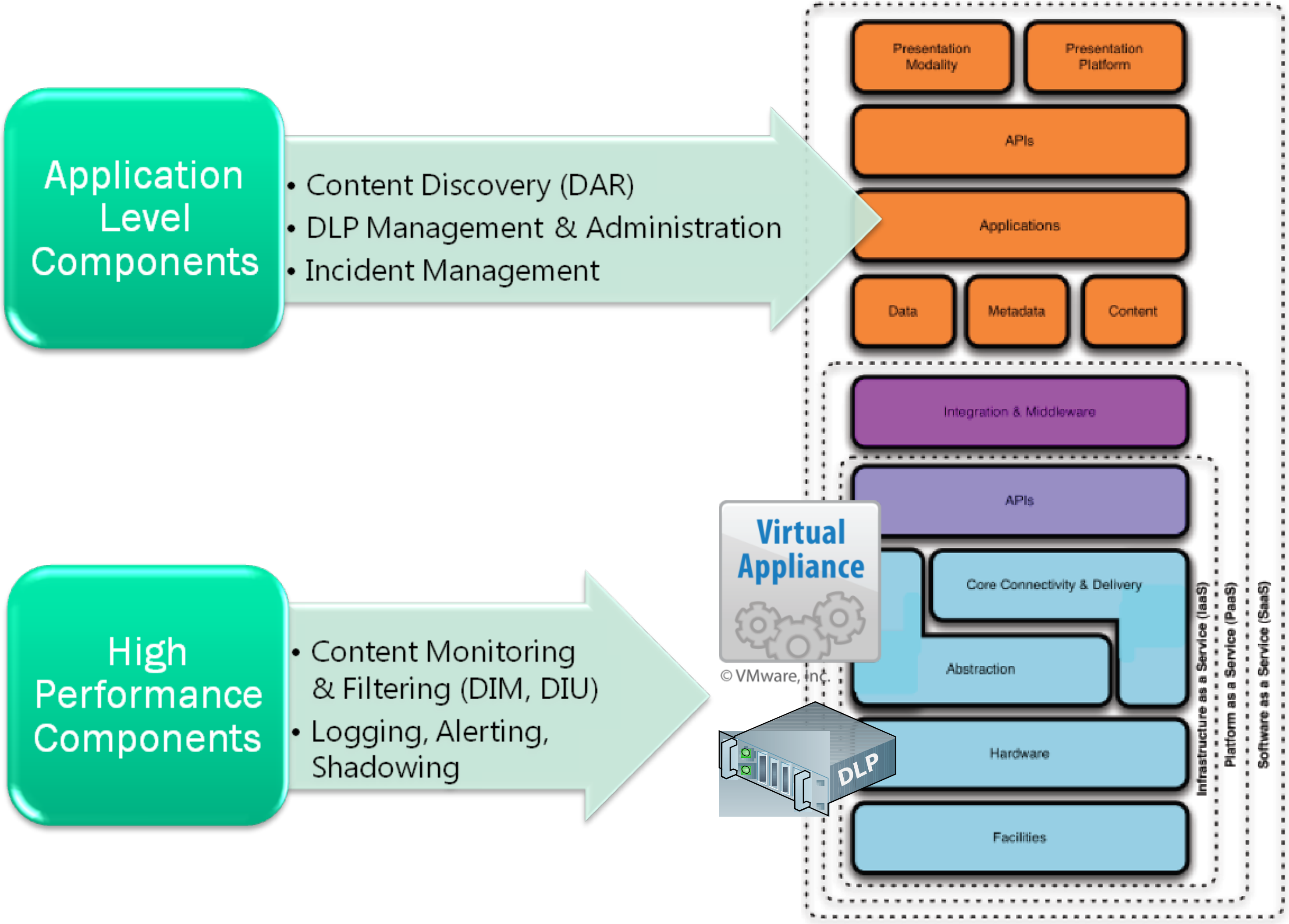
Is DLP Necessary for the Cloud?

- Many other infosecurity mechanism used in the Cloud
- BUT
  - All other security technologies (except IRM) link their controls to contextual parameters – no awareness of information transferred
  - Many scenarios when data leaks cannot be detected
    - Sending email/webmail, copying data to removable media or network shares
  - Information Rights Management (IRM)
    - *Manual* content classification => does not scale well, expensive to maintain
    - Not usable outside of the organization => business inhibitor
- DLP is a must for Cloud security
  - Intelligent and automatic content analysis with real-time enforcement
  - Links security controls to the value of information contained in the data
  - Covers risky scenarios not supported by context-based security


Cloud Model
APIs
Data
Metadata
Content
Core Connectivity & Delivery
Abstraction
Hardware
Facilities
Infrastructure as a Service
Platform as a Service
Software as a Service
Security Control Model
Applications
SDLC, Binary Analysis, Scanners, WebApp Firewalls, Transactional Sec.
Information
Monitoring, Encryption
Management
GRC, IAM, VA/VM, Patch Management, Configuration Management, Monitoring
Network
NIDS/NIPS, Firewalls, DPI, Anti-DDoS,
Trusted Computing
Hardware & Software RoT & API's
Compute & Storage
Host-based Firewalls, HIDS/HIPS, Integrity & File/log Management, Encryption, Masking
Physical
Physical Plant Security, CCTV, Guards
Compliance Model
PCI
Firewalls
Code Review
WAF
Unique User IDs
Anti-Virus
Patch/Vulnerability Management
Physical Access Control
HIPAA
GLBA
SOX

Source: Cloud Security Alliance Guidance Version 2.1 (2009)

DLP Position in the Cloud



Application Level Components

- Content Discovery (DAR)
- DLP Management & Administration
- Incident Management

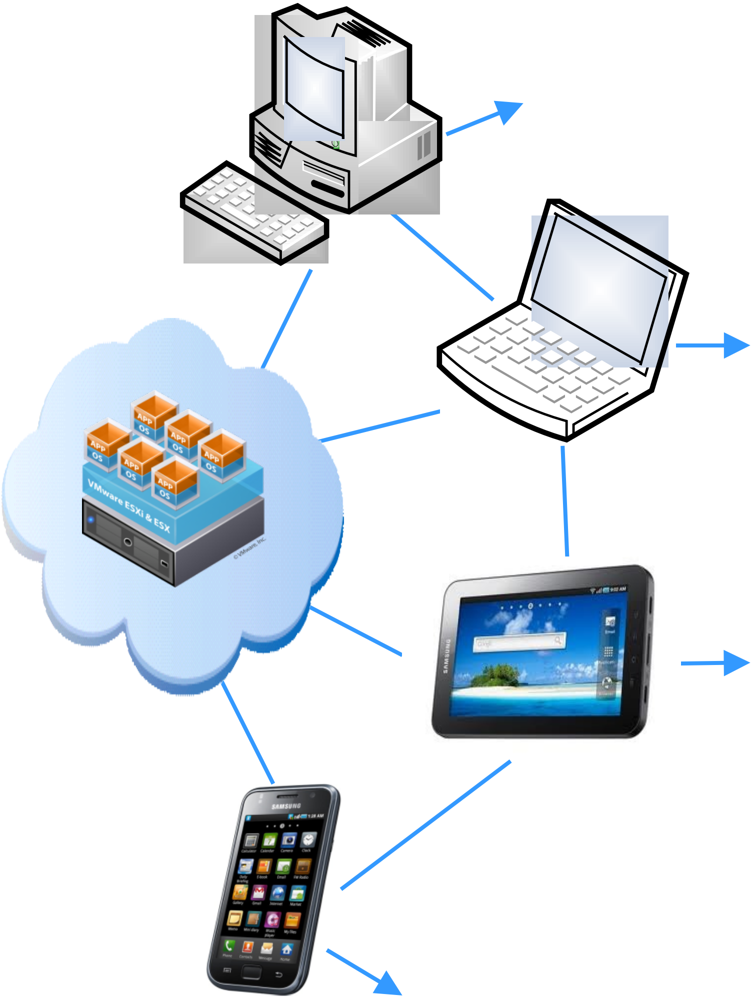
High Performance Components

- Content Monitoring & Filtering (DIM, DIU)
- Logging, Alerting, Shadowing

© VMware, Inc.

Source: Cloud Security Alliance Guidance Version 2.1 (2009)

DLP Around the Cloud



- Corporate endpoints
  - Desktop, laptop, tablet, smartphone/PDA
- Communicate and interact with
  - Corporate Cloud
  - Each other directly (Internet)
  - External users and services
- Host-resident DLP agents is a *must* to protect corporate endpoints from many data leak vectors
  - Network communications
  - Local channels – removable media, printing, connected smartphones/PDAs

Cloud: Protecting *Data In Motion*

- Network communications control and content filtering
- Controlled by cloud-based DLP *only*
  - Cloud ⇔ Cloud(s)
  - External user ⇔ Cloud
  - External server ⇔ Cloud
- Controlled by both cloud-based DLP and endpoint DLP agent
  - Internal User ⇔ Cloud
  - Internal user ⇔ Cloud ⇔ internal user
    - Corporate email, IM, social networking
- Controlled by endpoint DLP agent *only* (“Around the Cloud”)
  - Internal user ⇔ internal user (non-corporate email/webmail, IM, P2P, etc.)
  - Internal user ⇔ external user
  - Internal user ⇔ external server

Cloud: Protecting *Data In Use*

- Endpoint scenarios (“Around the Cloud”)
  - Data accessed or transferred from/to/inside the endpoint computer through local channels
    - Removable media, printing, connected smartphones/PDAs, clipboard
  - Can be controlled by the endpoint DLP agent *only*
    - Both context-based control and content filtering
- DIU scenarios for “pure” Cloud client
  - No data transfer from/to the endpoint computer running the Cloud client
    - All applications operate in the Cloud (e.g. Google Docs)
    - All *data in use* operations are *virtually local* to the Cloud
  - Open/save (read/write) a document in a cloud-based word processor to a data store, drive, media in the Cloud
  - Can be fully controlled by cloud-based DLP (gateway, server) *only*
    - Endpoint DLP agent can control DIU cloud operations at the context-level only
    - By proxying Cloud client’s operations – questionable approach (too many apps to proxy)

Cloud: Protecting *Data At Rest*

- Content discovery
  - Data stores, repositories, databases, file systems
- In the Cloud
  - By cloud-based discovery tools
    - Most effective
  - By endpoint tools
    - Cloud-based file shares accessible via CIFS/SMB, WebDAV
- On corporate endpoints
  - By endpoint DLP agents
    - Optimal
  - By cloud-based discovery tools
    - Much less effective, sometimes impossible

DLP Functional Split for the Cloud

DLP Functions / Service Models	**IaaS**		**PaaS**		**SaaS**	
	Customer	*Provider*	*Customer*	*Provider*	*Customer*	*Provider*
Data in Motion Protection	+	+ (Cloud)	+ (Endpoint)	+ (Cloud)	+ (Cloud)	+ (Endpoint)
Data in Use Protection	+		+ (Endpoint)	+ (C-client)	+ (Endpoint)	+ (C-client)
Data at Rest Protection	+		+ (Endpoint)	+ (Cloud)	+ (Endpoint)	+ (Cloud)
Alerting, Logging, Shadowing	+	+ (Cloud)	+ (Endpoint)	+ (Cloud)	+ (Endpoint)	+ (Cloud)
Incident Management	+	Integrate, Support	+	Integrate, Support	+	Integrate, Support
	+		+		+	

Conclusions

- As the most information-centric security technology, DLP is an indispensable part of the cloud-based IT security architecture
- DLP functions and components will be split between CSP and customer
  - Performance-sensitive network-based DLP functions will be integrated in the core fabric of all service models including IaaS
  - Application-level network DLP functions may be implemented either by customers or CSP depending on Cloud service model and provider
  - Endpoint DLP agents, DLP management & administration, incident management will remain under the customer’s control
- DLP will become a key element of value-added cloud security services – standard for SaaS and PaaS, expected in IaaS
  - Delivery models may very from CSPs to add-on services by 3rd parties

Conclusions (cont.)

- Successful Cloud DLP services should include
  - The entire set of network-based DLP functions
  - Management API’s for centralized DLP management & administration
    - From customer’s or provider-supplied DLP management platform
  - Flexible integration with customer’s incident management, as well as alerting, logging, data shadowing solutions
  - Contractual support of security compliance auditing, incident investigations and forensic procedures
  - DLP-related professional services (consulting, policy development/revision, security administrator training)
- DLP vendors will port
  - DLP agents to tablets and smartphones (Android, iOS)
  - DLP appliances and management to dominant Cloud platforms

DeviceLock

Merci de votre attention

Paris, 23 Novembre 2010