RSA CONFERENCE CHINA 2011
NOVEMBER 2-3 | CHINA WORLD HOTEL | BEIJING

Securing Sensitive Data in the Virtual World: Instantiating DLP in the Cloud

Speaker：Bob Griffin
Job Title：Virtualization Architect
Company Name：RSA

Speaker：Mike Foley
Job Title：Chief Security Architect
Company Name：RSA

Agenda

- Using DLP to secure sensitive information
- Using DLP with VDI and virtual servers
- Using DLP in private, public and hybrid clouds

Why DLP Is Important

Comply With Regulations

PCI, HIPAA, GLBA, PIPEDA, EU Data Directive, etc.

Fines: More than $500K in fines

Burden: Quarterly audits

Legal: Lawsuits, privacy notices

Secure Your Sensitive Data

Employee & customer data (PII), corporate secrets, intellectual property

Damage: Corporate brand equity

Churn: Customer & employee

Loss: Competitive advantage

Improve Operational Efficiencies (security)

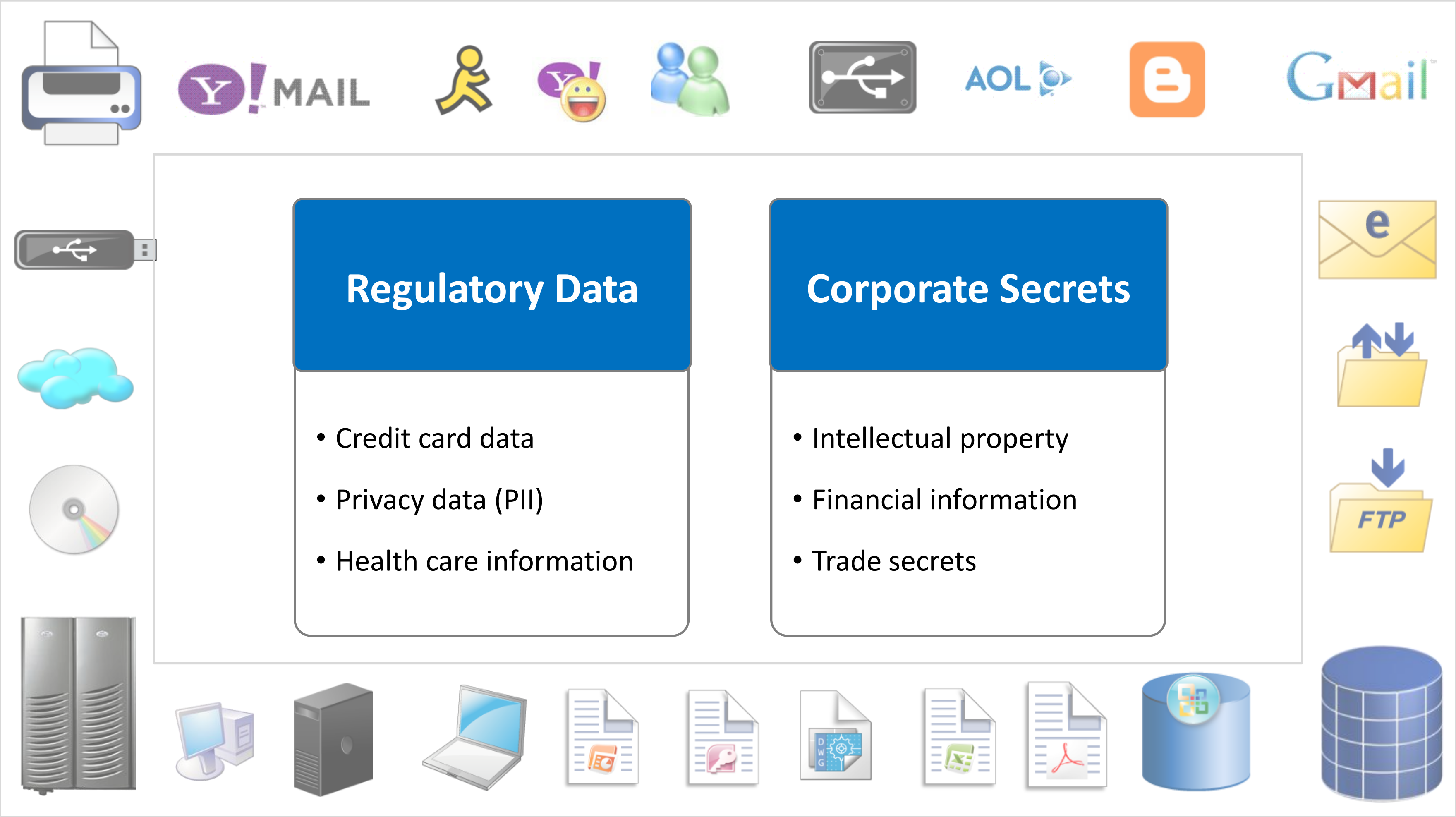
Keep security costs low and reduce impact on end users

Burden: More FTEs for security

Capital: Additional HW & SW

Cost: Higher TCO

Knowing The “D” In DLP: Sensitive Data



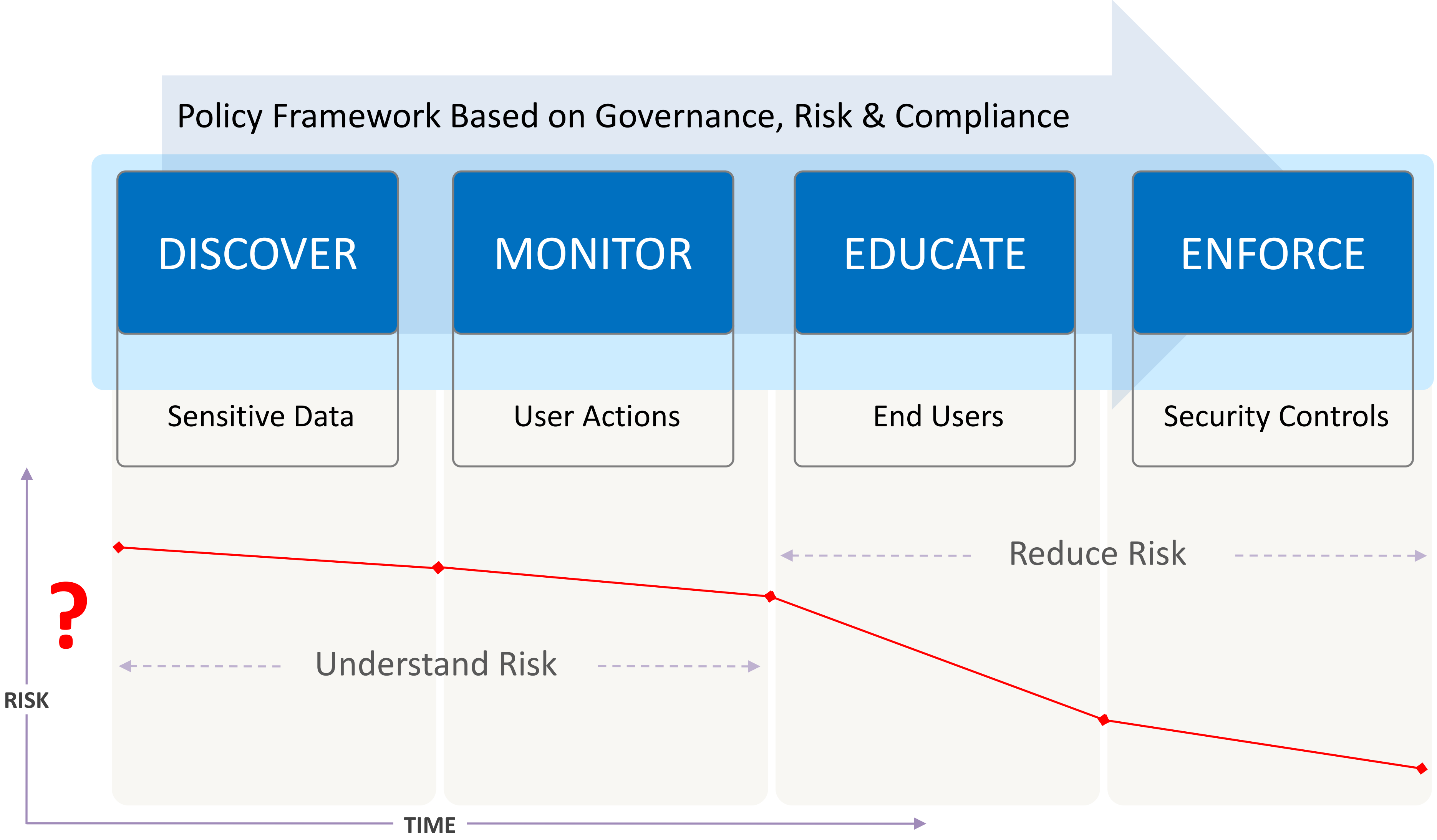
Regulatory Data

- Credit card data
- Privacy data (PII)
- Health care information

Corporate Secrets

- Intellectual property
- Financial information
- Trade secrets

Securing Sensitive Information Using DLP



Business Policy and DLP

Business Policy

Governance Team

- Establish business policy for DLP
- Investigation of DLP findings that violate policy
- Update policies to reflect changes in business, technology and threats

Requirements

•Assessment requirements

•DLP policies & rules

DLP Administrator

DLP Policies

Content: Credit Card Number, Drivers Licence number, Social Security number

DataCenter	**Endpoint**	**Network**
Move if not encrypted	e.g Block USB notify user	e.g Block, notify sender

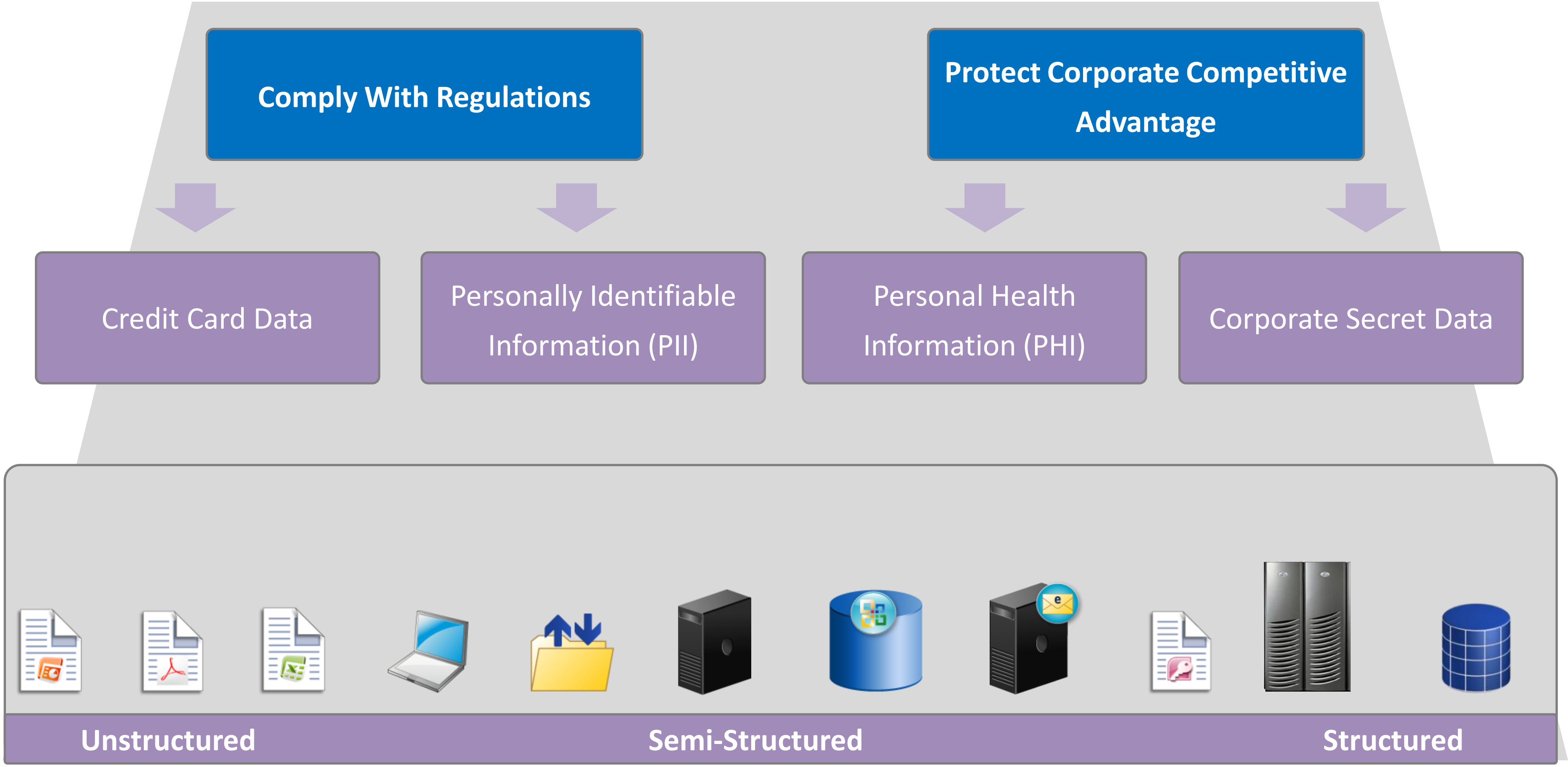
Status & Exceptions

•Assessment findings

•Escalated incidents

Discover Your Sensitive Data

Reduce uncertainty and understand risk from the data you own



Comply With Regulations

Protect Corporate Competitive Advantage

Credit Card Data

Personally Identifiable Information (PII)

Personal Health Information (PHI)

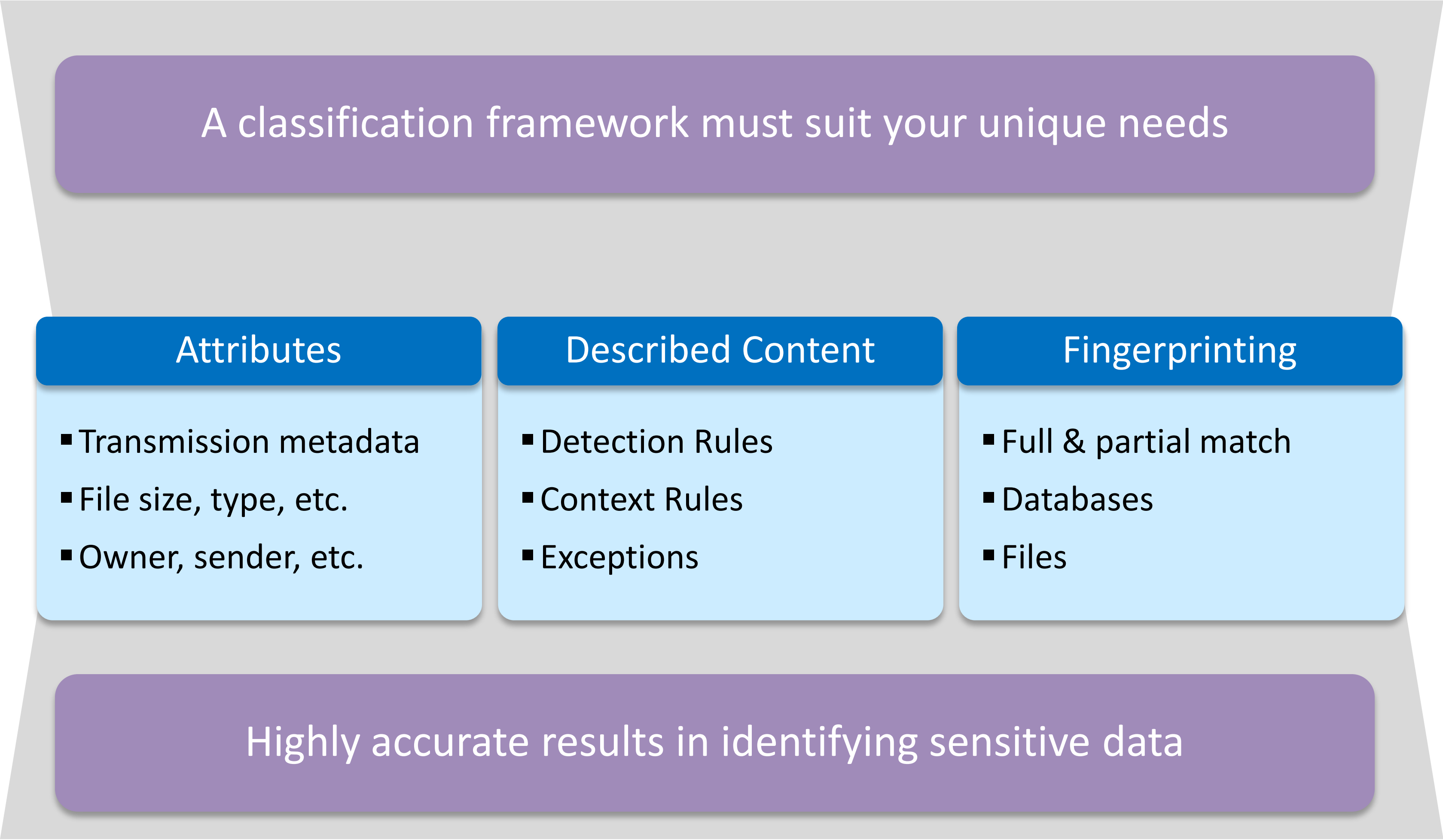
Corporate Secret Data

Unstructured

Semi-Structured

Structured

Classification Framework



A classification framework must suit your unique needs

Attributes

- Transmission metadata
- File size, type, etc.
- Owner, sender, etc.

Described Content

- Detection Rules
- Context Rules
- Exceptions

Fingerprinting

- Full & partial match
- Databases
- Files

Highly accurate results in identifying sensitive data

Mapping Risk to Sensitive Information

- VISBILITY INTO INFORMATION RISK FOR ASSETS

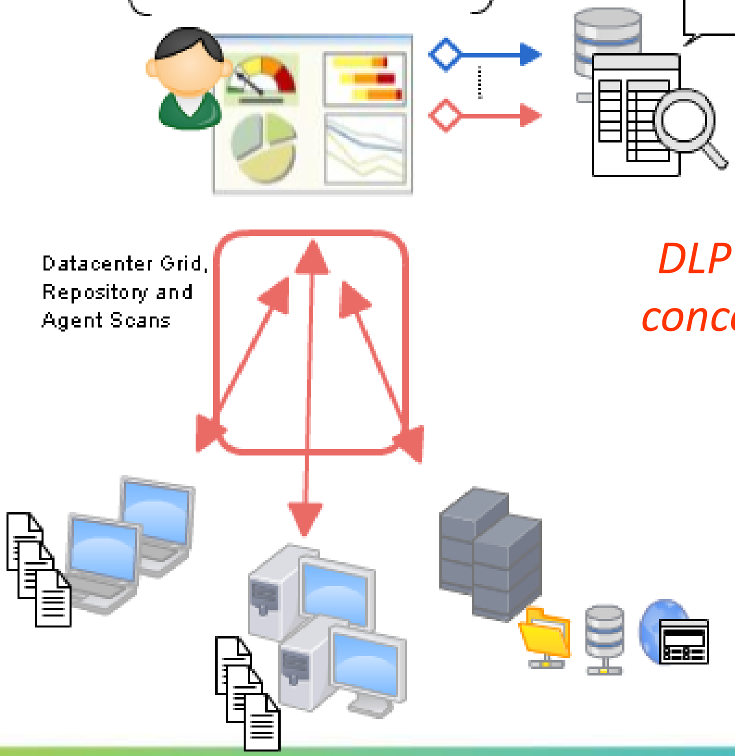
- DLP's view into Information Risk contributes to overall Security Risk at the assets

- Report shows the most current state of information risk at assets

- Assets refreshed with new values after scan

PCI DSS

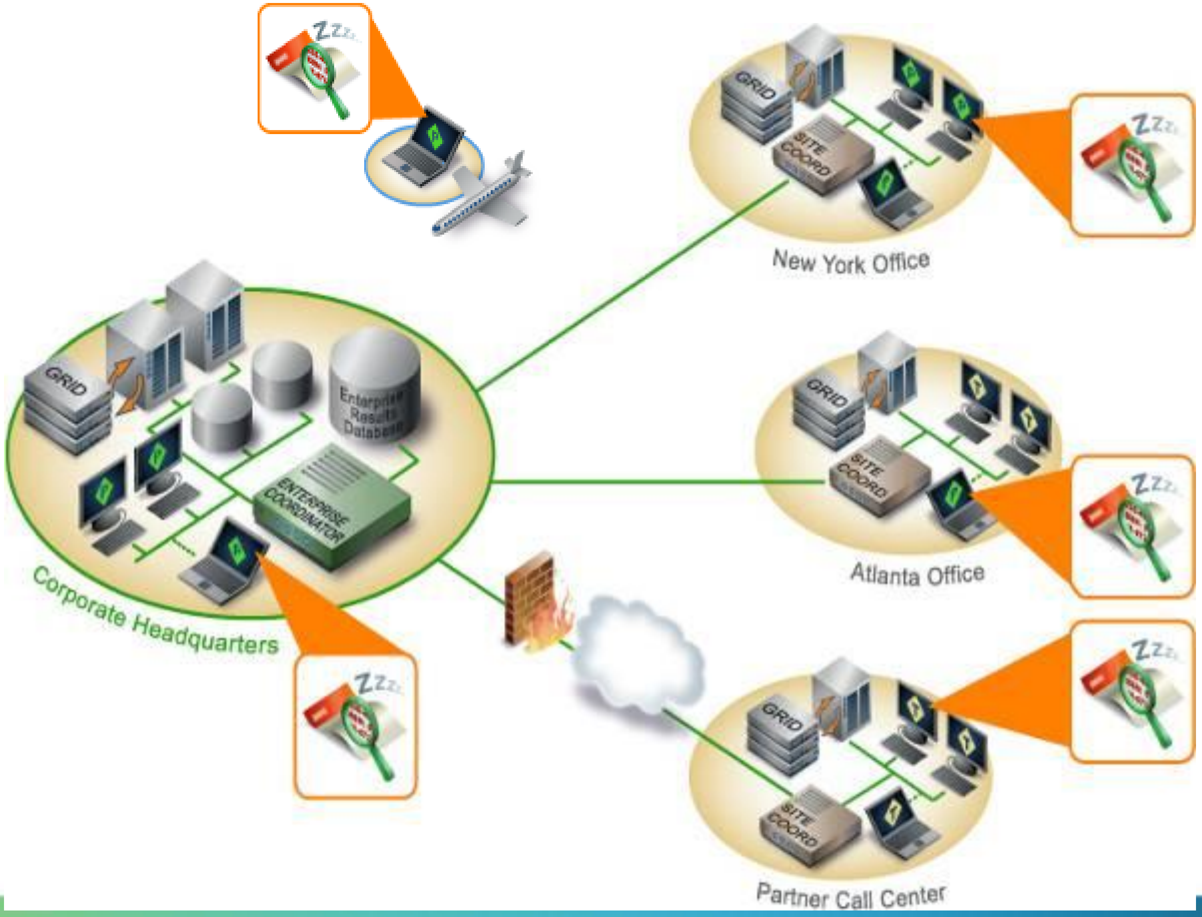
	Severity	Match Count
Client1.rsa.com	🟥	150
Client2.rsa.com	🟨	30
SharePoint1.rsa.com	🟧	100
Database.rsa.com	⬜	0



DLP heat maps provide the Information risk (or concern) index for assets within the organization

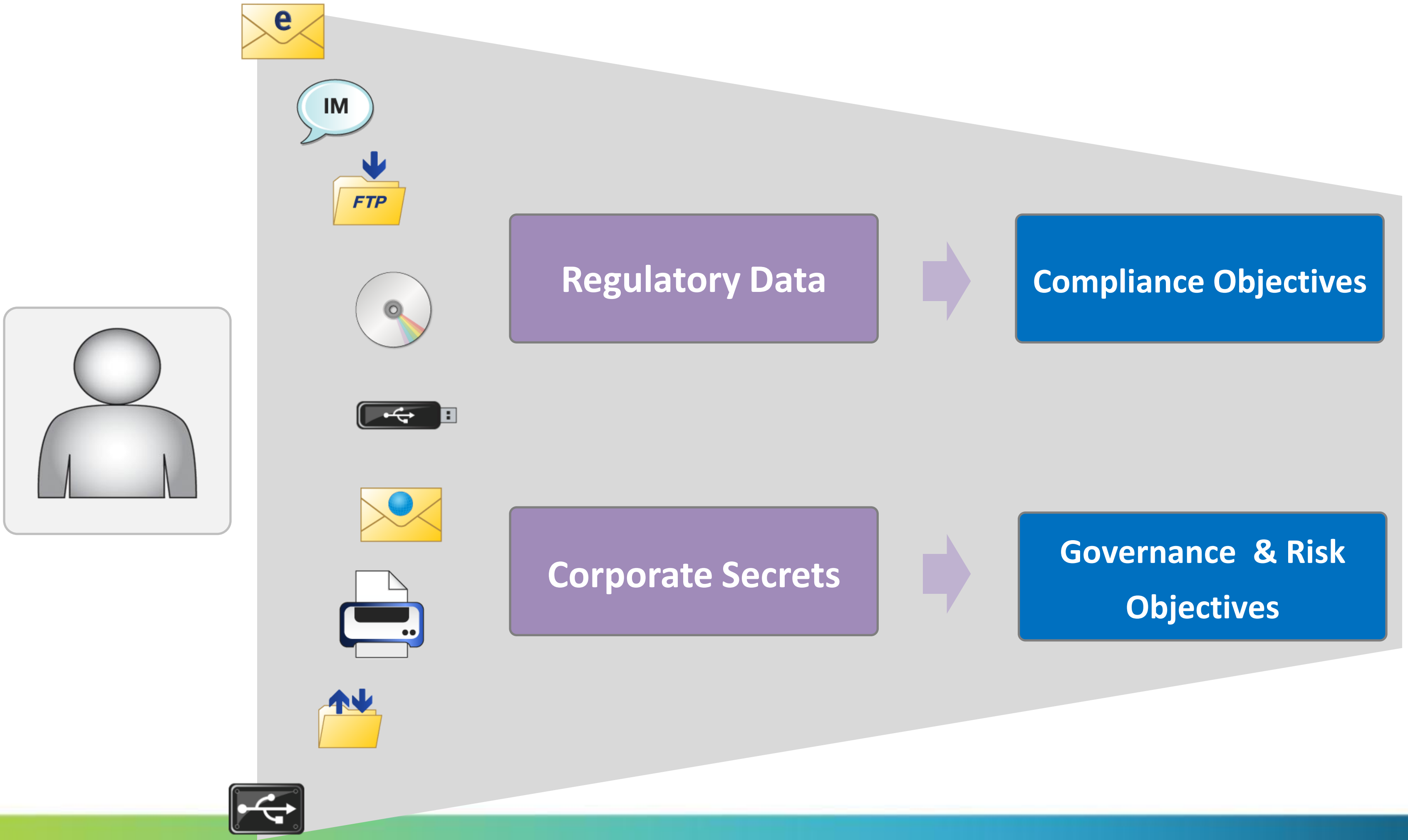
Use Case: Information Discovery

Analyst gets full picture of where sensitive information is located and how it is protected



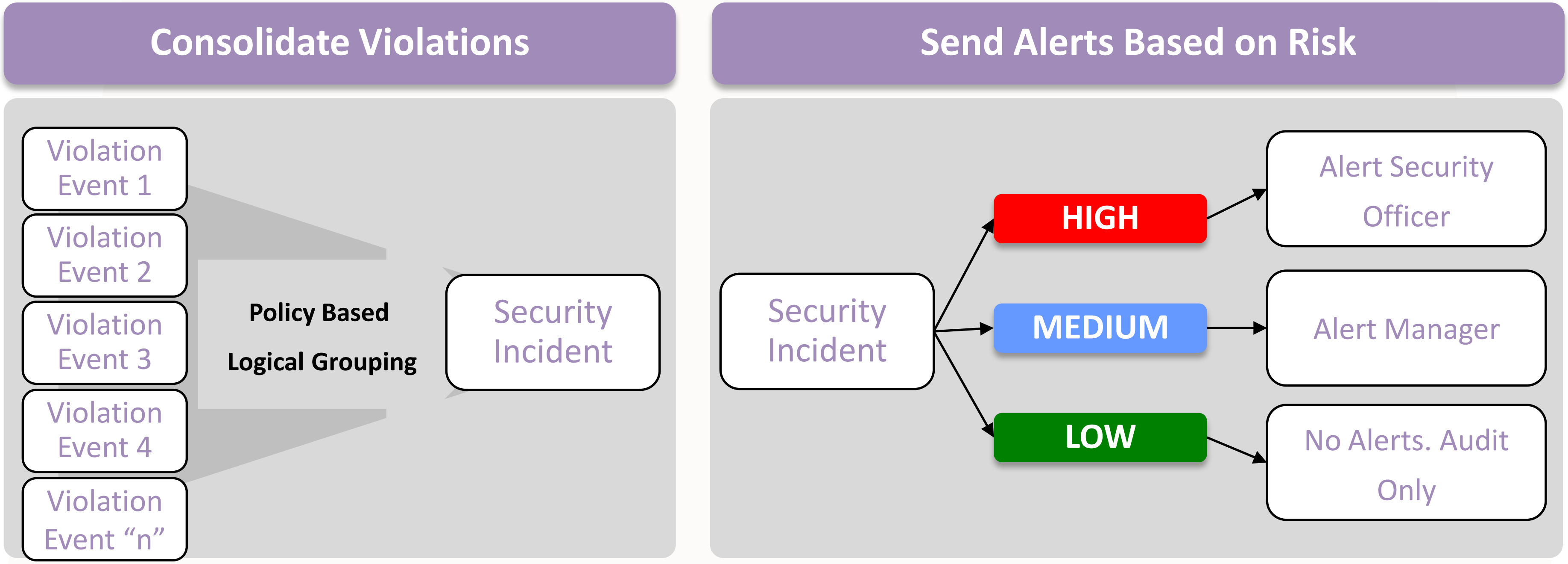
Monitor Your Sensitive Information

Understand how your user actions impact your corporate objectives



Incident Workflow to Manage Violations

Reduce noise, prioritize incidents and manage workflow



Consolidate Violations

Violation Event 1

Violation Event 2

Violation Event 3

Violation Event 4

Violation Event “n”

Policy Based

Logical Grouping

Security Incident

Send Alerts Based on Risk

Security Incident

HIGH

MEDIUM

LOW

Alert Security Officer

Alert Manager

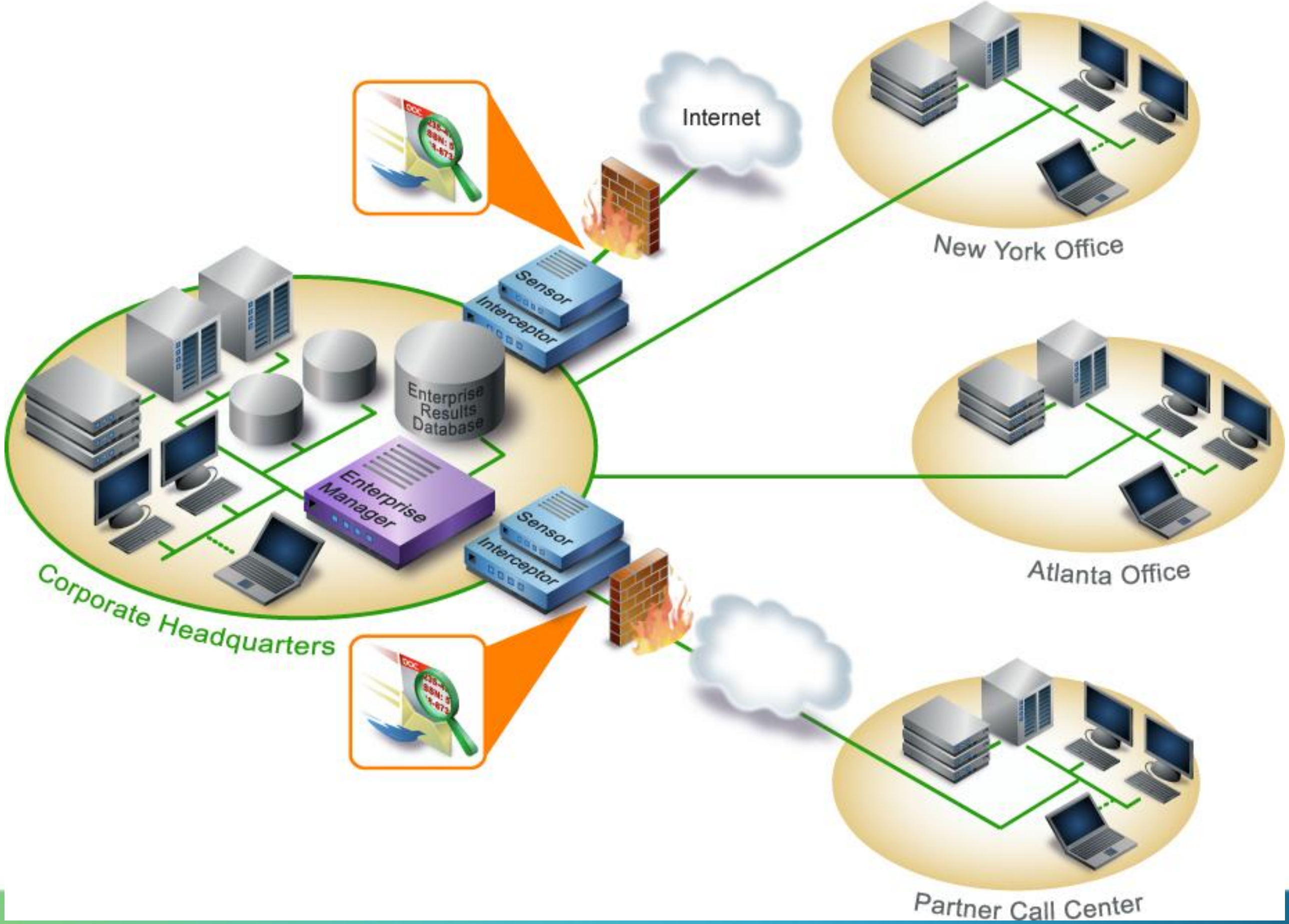
No Alerts. Audit Only

intelligent alerts and prioritization

Use Case: Security Investigation

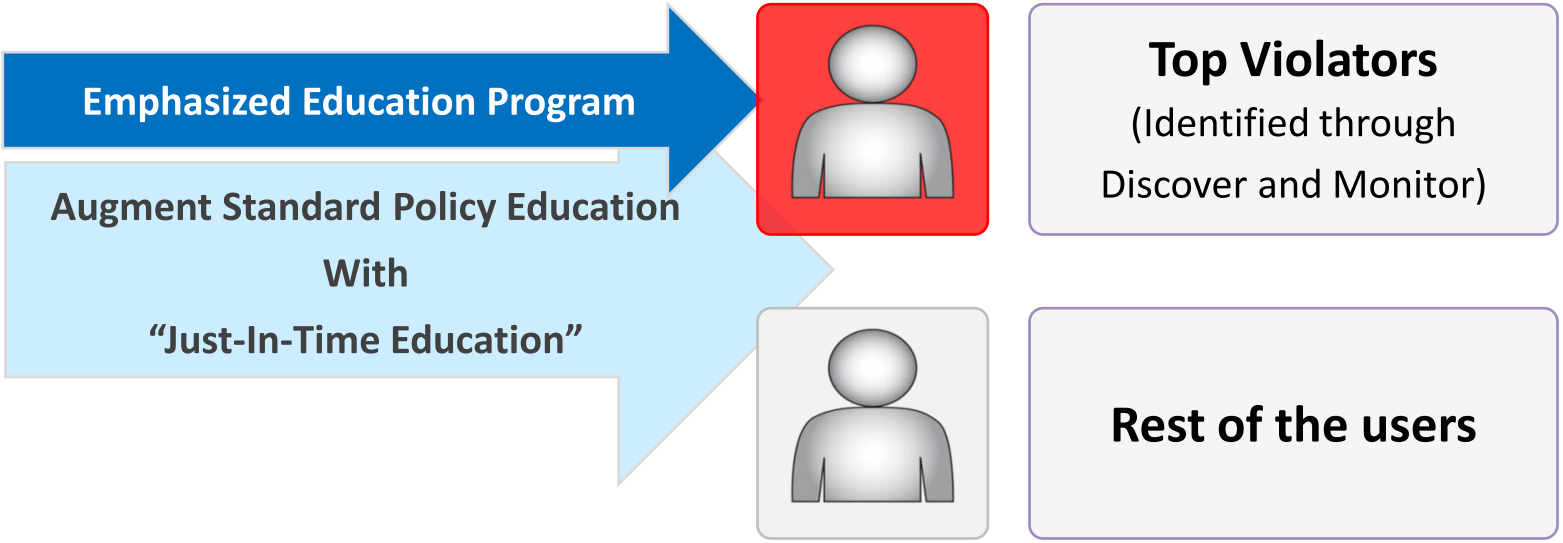
Analyst investigates malware outbreak

DLP detects if confidential Information is leaving network



Educate End Users

Educate end users on policies and violations to reduce risk

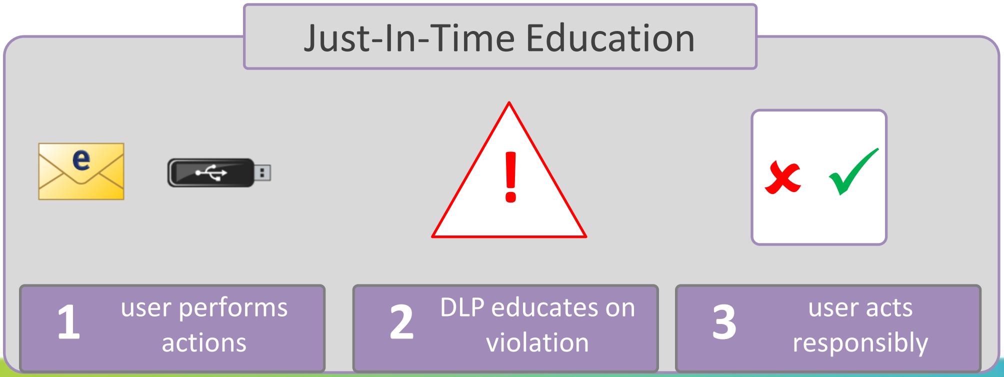


Emphasized Education Program

Augment Standard Policy Education
With
“Just-In-Time Education”

Top Violators
(Identified through
Discover and Monitor)

Rest of the users



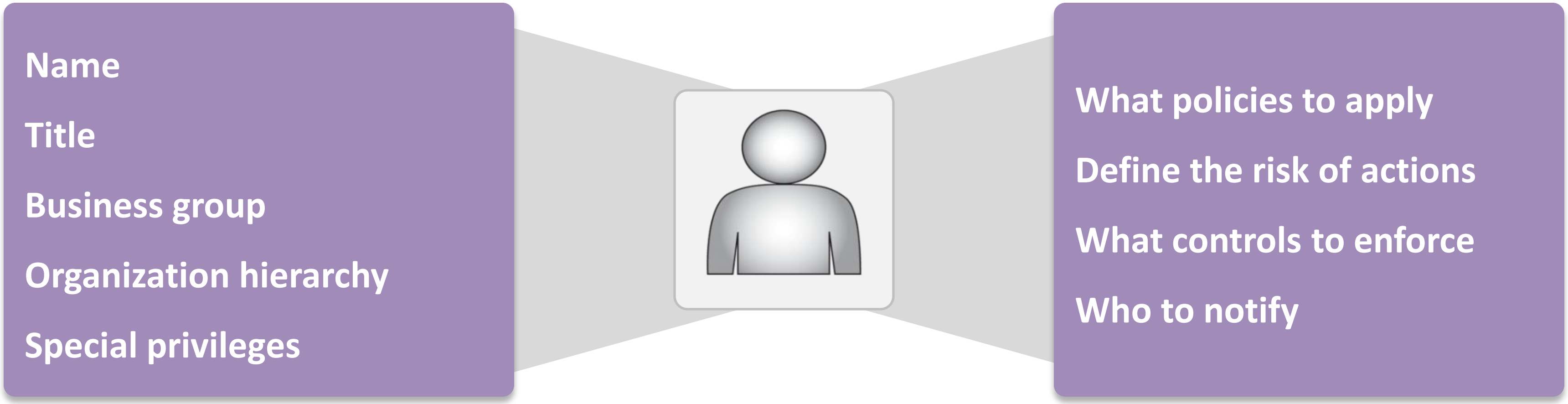
Just-In-Time Education

1 user performs actions

2 DLP educates on violation

3 user acts responsibly

User Identity Analysis



Name

Title

Business group

Organization hierarchy

Special privileges

What policies to apply

Define the risk of actions

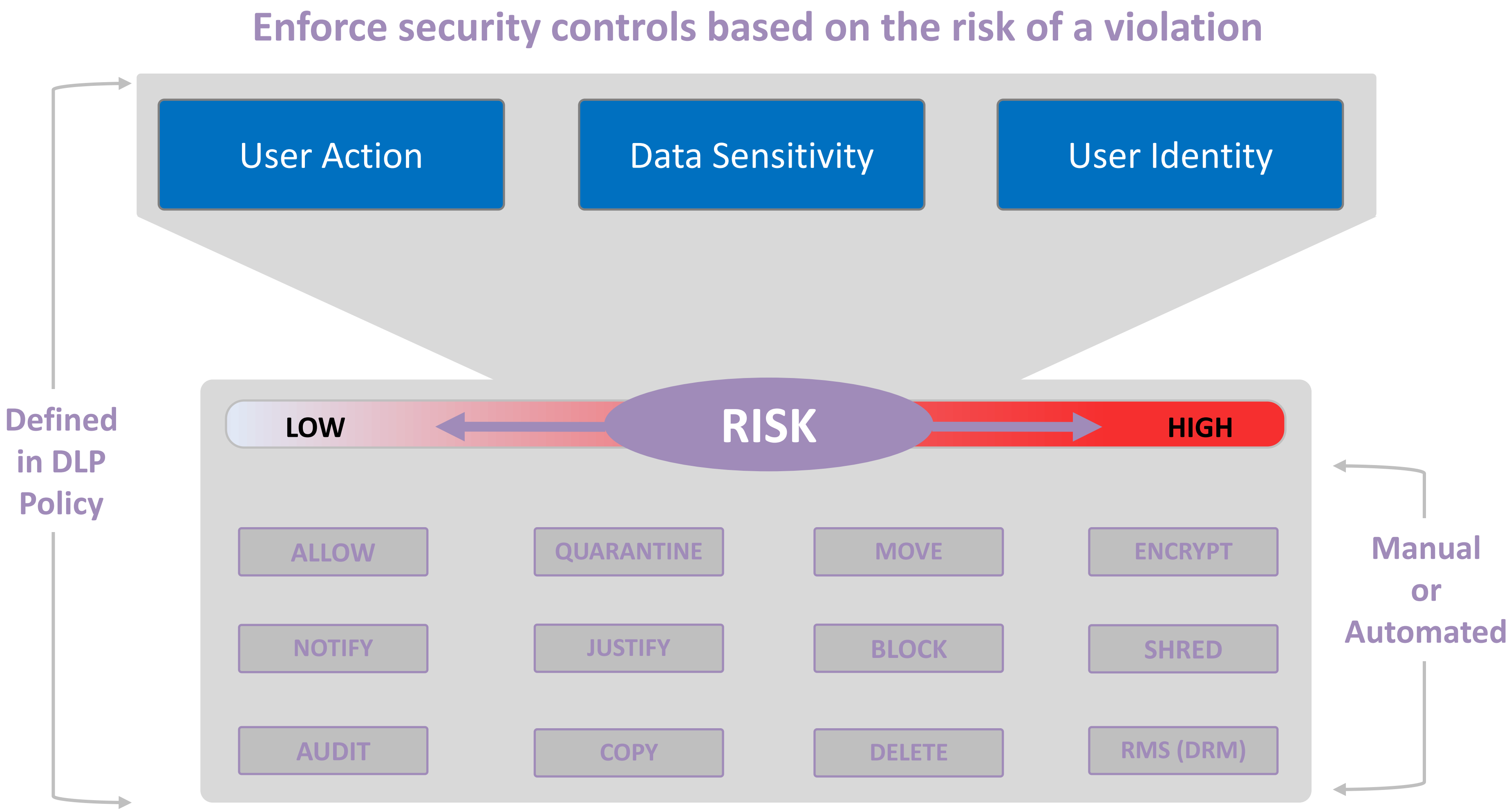
What controls to enforce

Who to notify

Real-time data from your Windows Active Directory

Used across all phases of DLP

Enforce Controls to Prevent Data Loss

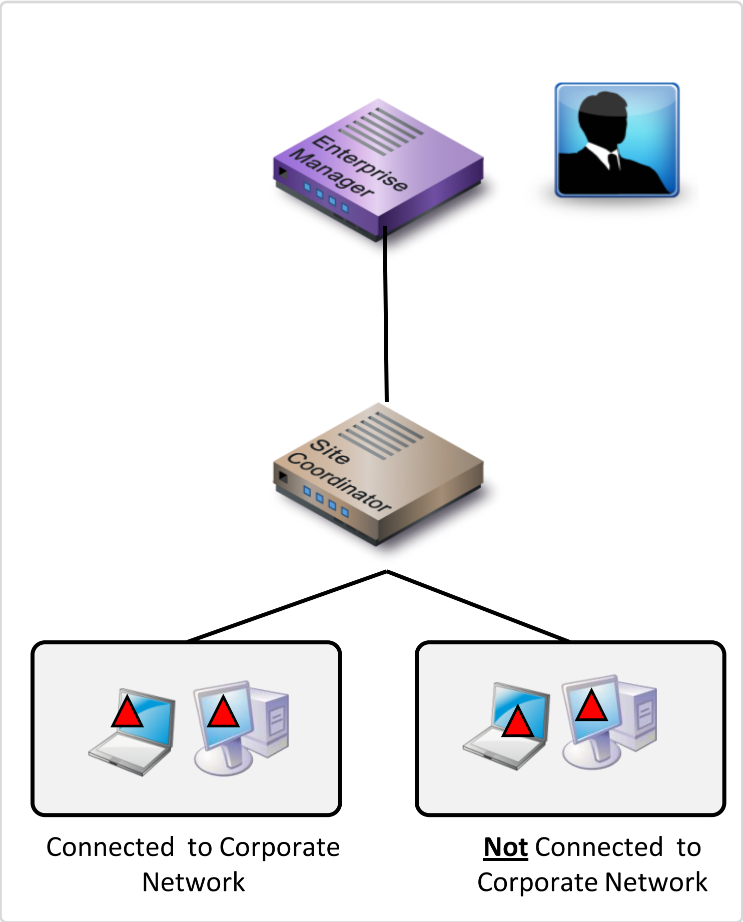


Secure Sensitive Information on Endpoints

Mitigate risk from end user actions on endpoints

Connected or Disconnected from Corporate Network

	Monitor	Educate	Enforce
💿	✓	✓	✓
🔌	✓	✓	✓
🖨	✓	✓	✓
🔌	✓	✓	✓
2.0GB SD	✓	✓	✓
⚡	✓	✓	✓
📁	✓	✓	✓
✉	✓	✓	✓
IM	✓	✓	✓



Connected to Corporate Network

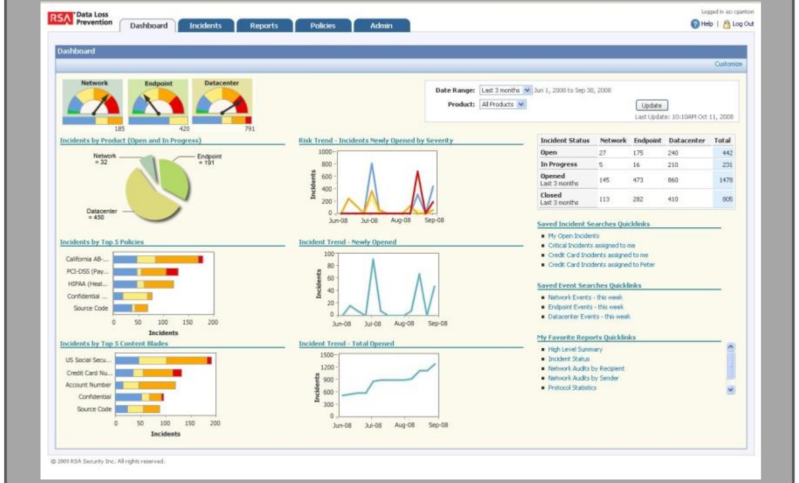
Not Connected to Corporate Network

Connecting DLP With Your Business

POLICY

INFRASTRUCTURE

Your DLP Deployment



Logged in as: cgarrison

Dashboard

Date Range: Last 3 months Jun 1, 2008 to Sep 30, 2008

Product: All Products

Last Update: 10:10AM Oct 11, 2008

Incidents by Product (Open and In Progress)

Risk Trend - Incidents Newly Opened by Severity

Incident Status	Network	Endpoint	Datacenter	Total
Open	27	175	240	442
In Progress	5	16	210	231
Opened Last 3 months	145	473	860	1478
Closed Last 3 months	113	282	410	805

Saved Incident Searches Quicklinks

- My Open Incidents
- Critical Incidents assigned to me
- Credit Card Incidents assigned to me
- Credit Card Incidents assigned to Peter

Incidents by Top 5 Policies

Incident Trend - Newly Opened

Saved Event Searches Quicklinks

- Network Events - this week
- Endpoint Events - this week
- Datacenter Events - this week

Incidents by Top 5 Content Blades

Incident Trend - Total Opened

My Favorite Reports Quicklinks

- High Level Summary
- Incident Status
- Network Audits by Recipient
- Network Audits by Sender
- Protocol Statistics

© 2009 RSA Security Inc. All rights reserved.

INCIDENTS

CONTROLS

Agenda

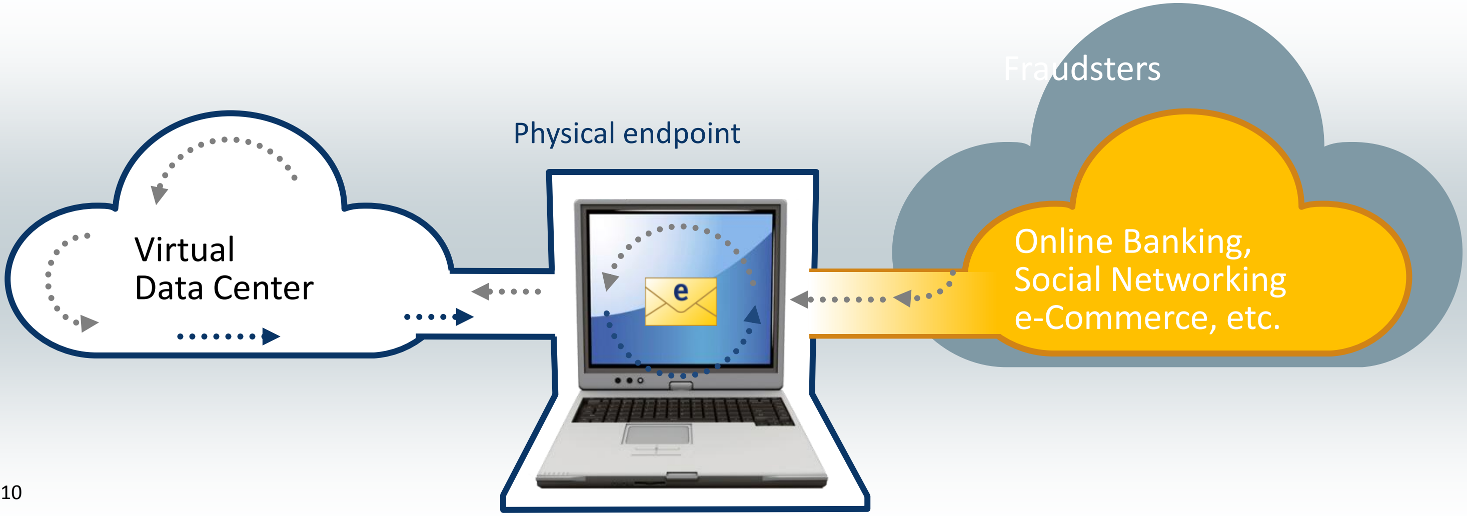
- Using DLP to secure sensitive information
- Using DLP with VDI and virtual servers
- Using DLP in private, public and hybrid clouds

It starts with infrastructure

- How do I get to “Cloud”?
  - Start with a secure infrastructure (e.g.: Private Cloud)
  - Before pushing out to the public cloud
    - Work out your user experience locally
    - Work out security best practices
  - Leverage automation and orchestration to provide consistent, measurable tasks
    - This helps to focus on “out of policy” actions, bringing them to the forefront

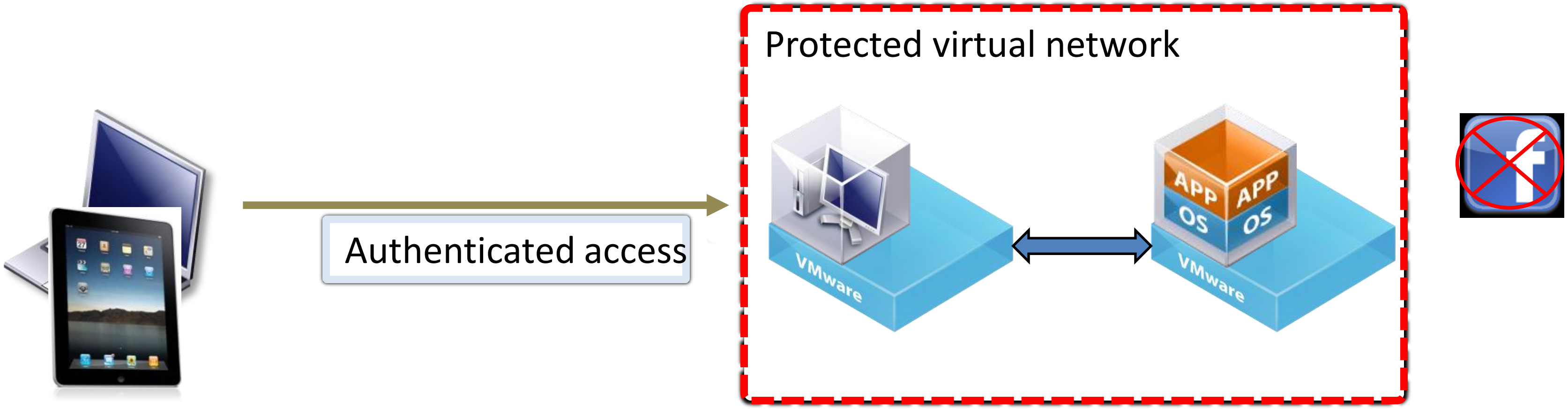
Today's Endpoint Security Challenges

- Expensive but still vulnerable
  - 60% of the security budget is consumed by endpoint security software[1]
  - Lost or stolen laptops is the largest single source of breaches[2]
  - Only 30% of business encrypt laptops[6]
- Gateway to infection and theft
  - 35% of infected PCs had up-to-date antivirus software installed[3]
  - Malware contributed to 82% of records compromised in 2009[4]
  - 88% of Fortune 500 companies have employees infected with Trojans…. and don't know about them![5]
  - 95% of lost laptops are never returned[6]



Source:
(1) Gartner, Inc.
(2) OSF Data loss DB
(3) Panda Labs
(4) Verizon Business
(5) RSA Fraud Action Lab
(6) Ponemon Institute 2010

Using DLP in the Virtual Environment



Authenticated access

Protected virtual network

Ensure no sensitive Information is on the device

- The endpoint is changing
  - Mac
  - iPhone/iPad
  - Android phones and tablets
  - BYOC

Allow Virtual Desktop with access to sensitive data

- No USB or only secure USB allowed via DLP
- All aspects of desktop interaction, including DLP information, monitored by the infrastructure

Application with sensitive data

- Identify applications containing sensitive information
- Restrict applications available through VDI
- Sensitive information doesn't leave the datacenter

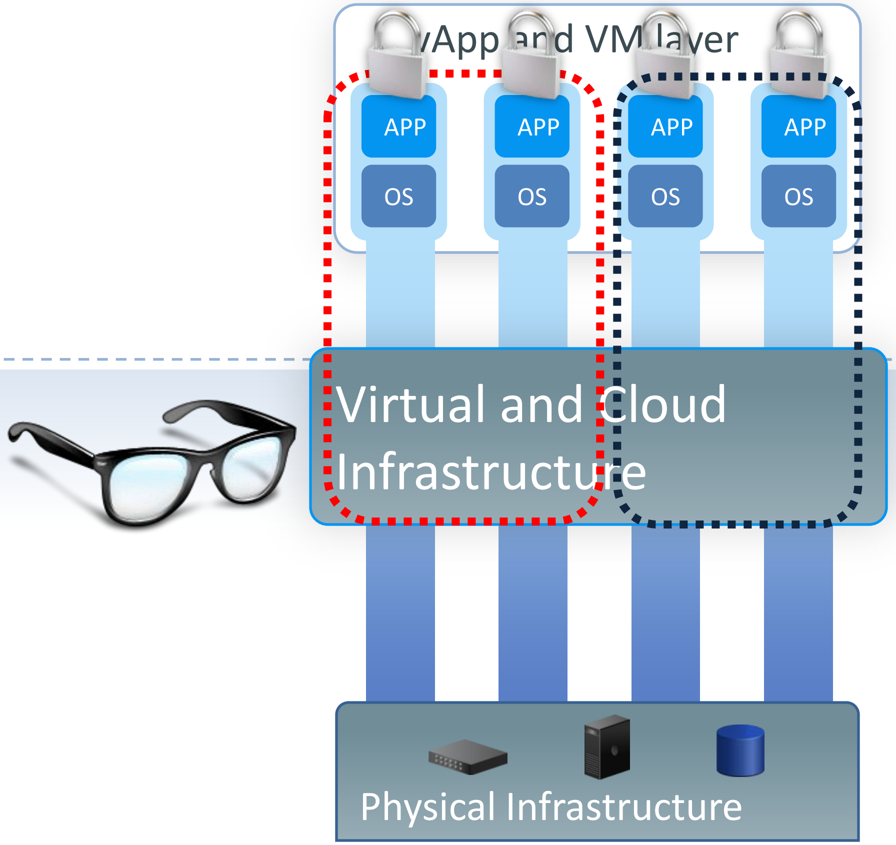
More Effective Security by Pushing Enforcement Down the Stack

Today most security is enforced by the OS and application stack. This is:

- Ineffective

Building in information security enforcement in the infrastructure layer ensures:

- Consistency
- Simplified security management
- Much higher level of visibility into security operations

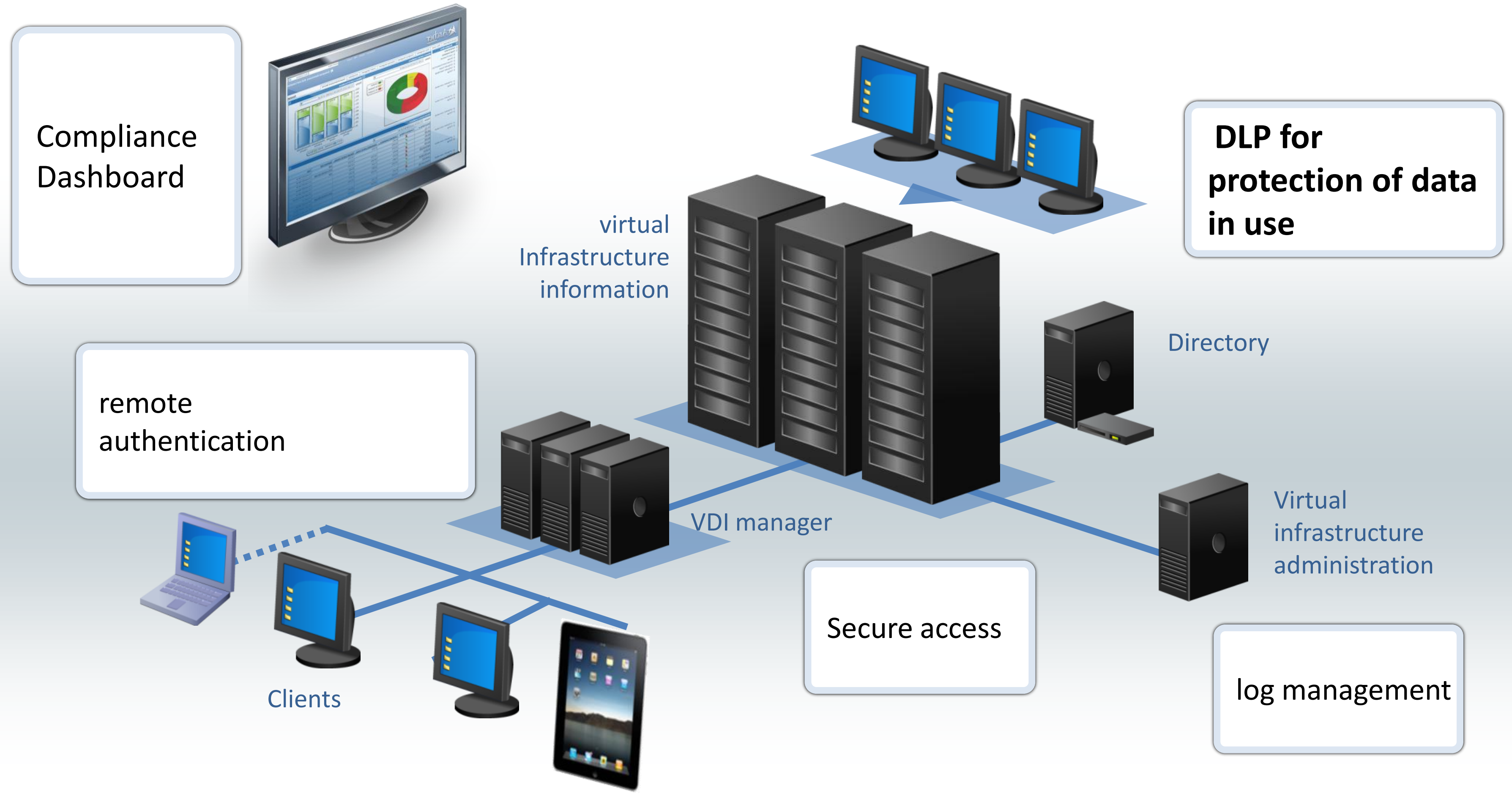


Complementing Virtual Zones with DLP

Discovery of sensitive data at the virtualization layer

	DLP	Virtual Zone
Discover sensitive data	☑	☑
Endpoint enforcement of policies at application	☑	☒
Network enforcement of policies	☑	☒
Scanning of SharePoint or Lotus Notes	☑	☒
Fingerprint files and databases	☑	☒
Custom content discovery	☑	☒

DLP within a VDI Solution


Compliance Dashboard
DLP for protection of data in use
virtual Infrastructure information
Directory
remote authentication
VDI manager
Virtual infrastructure administration
Clients
Secure access
log management

Agenda

- Using DLP to secure sensitive information
- Using DLP with VDI and virtual servers
- Using DLP in private, public and hybrid clouds

Cloud Security Alliance - Guidance

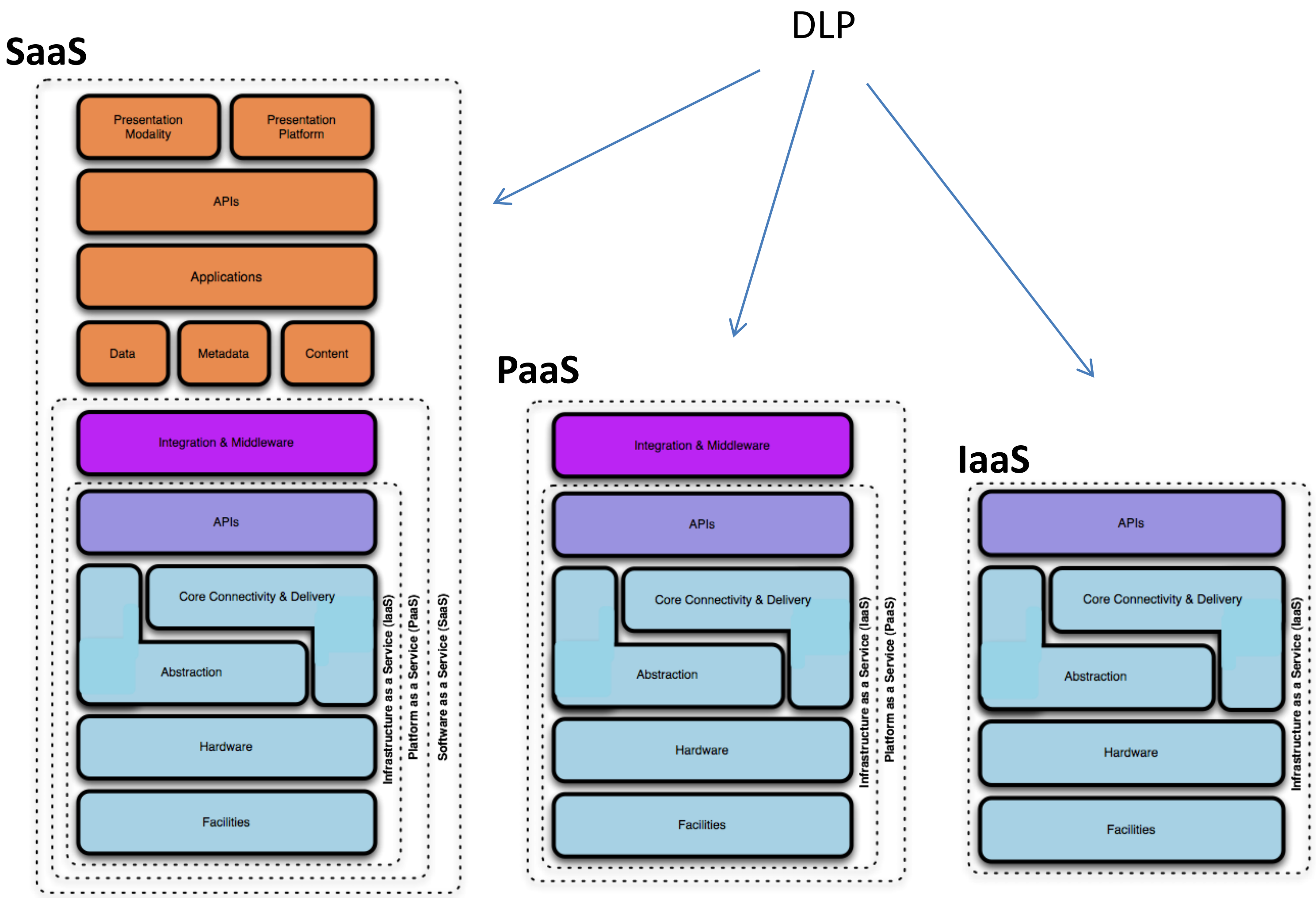
The Cloud Security Alliance’s 13 Critical Areas Of Focus for Cloud:

1. Architecture & Framework	
Governing the Cloud	*Operating the Cloud*
2. Governance & Risk Mgmt	8. Traditional BCM, DR
3. Legal & Electronic Discovery	9. Datacenter Operations
5. Compliance & Audit	10. Incident Response
6. Information Lifecycle Mgmt	11. Application Security
7. Portability & Interoperability	12. Encryption & Key Mgmt
	13. Identity & Access Mgmt

cloud security alliance
CSA

www.cloudsecurityalliance.org

DLP has a role in each cloud model



DLP

SaaS

Presentation Modality

Presentation Platform

APIs

Applications

Data

Metadata

Content

Integration & Middleware

APIs

Core Connectivity & Delivery

Abstraction

Hardware

Facilities

Infrastructure as a Service (IaaS)

Platform as a Service (PaaS)

Software as a Service (SaaS)

PaaS

Integration & Middleware

APIs

Core Connectivity & Delivery

Abstraction

Hardware

Facilities

Infrastructure as a Service (IaaS)

Platform as a Service (PaaS)

IaaS

APIs

Core Connectivity & Delivery

Abstraction

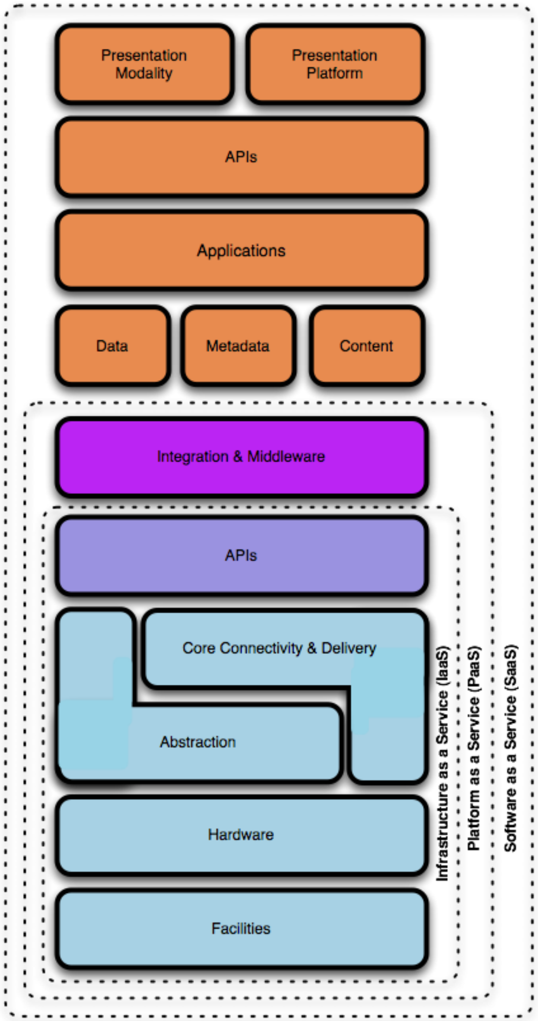
Hardware

Facilities

Infrastructure as a Service (IaaS)

Mapping the Model to the Metal

Cloud Model



Find the Gaps!

Security Control Model

Applications	SDLC, Binary Analysis, Scanners, WebApp Firewalls, Transactional Sec.
Information	DLP, CMF, Database Activity Monitoring, Encryption
Management	GRC, IAM, VA/VM, Patch Management, Configuration Management, Monitoring
Network	NIDS/NIPS, Firewalls, DPI, Anti-DDoS, QoS, DNSSEC, OAuth
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

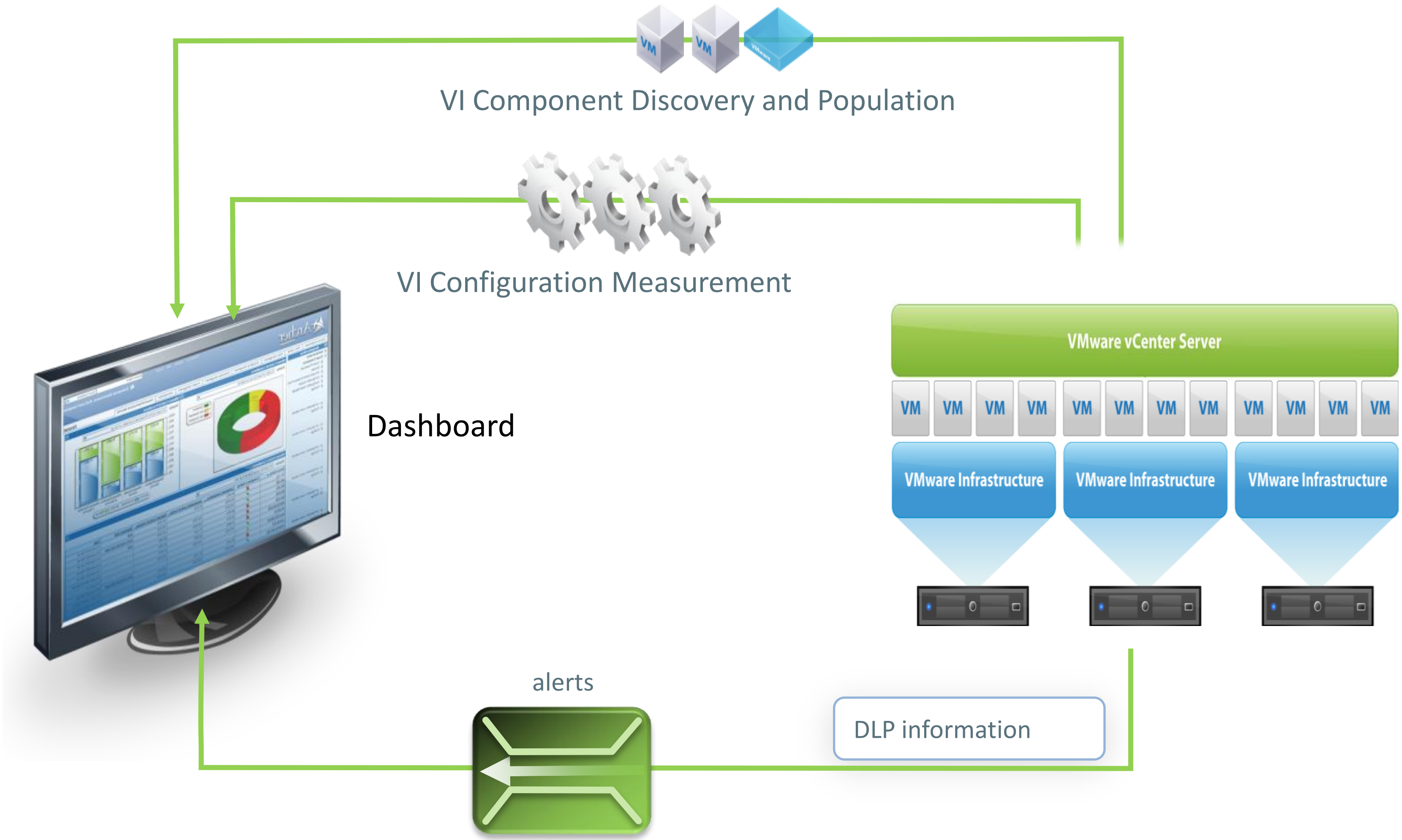
- ☑ Firewalls
- ☑ Code Review
- ☑ WAF
- ☑ Encryption
- ☑ Unique User IDs
- ☑ Anti-Virus
- ☑ Monitoring/IDS/IPS
- ☑ Patch/Vulnerability Management
- ☑ Physical Access Control
- ☑ Two-Factor Authentication...

HIPAA

GLBA

SOX

Cloud Security and Compliance



VI Component Discovery and Population

VI Configuration Measurement

Dashboard

alerts

DLP information

Thank you for joining us!

mike.foley@emc.com

robert.griffin@rsa.com