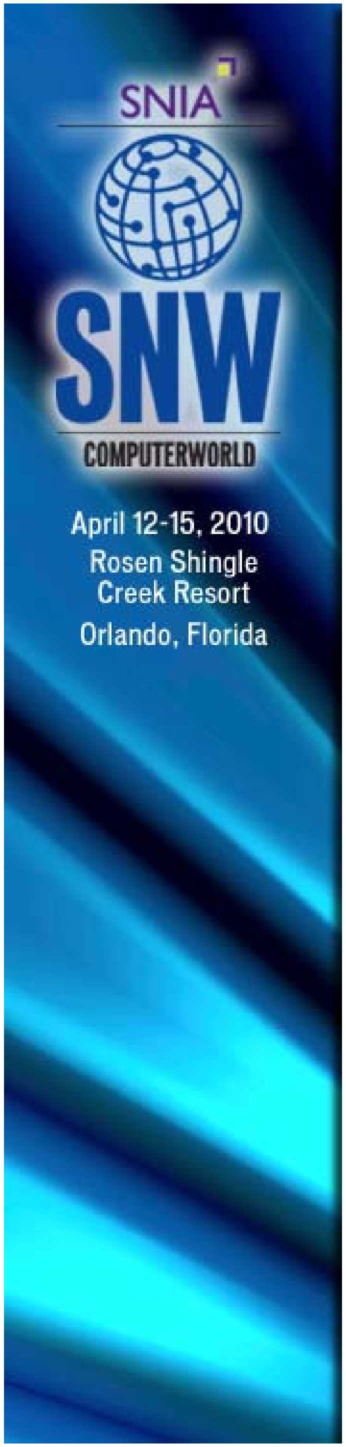


Securing Sensitive Information

Discovery, Monitoring and Control

Robert Griffin
Director, Technical Marketing
RSA, the Security Division of EMC

SNIA

SNW

COMPUTERWORLD

April 12-15, 2010
Rosen Shingle
Creek Resort
Orlando, Florida

What's Happening To Customer / Employee Data

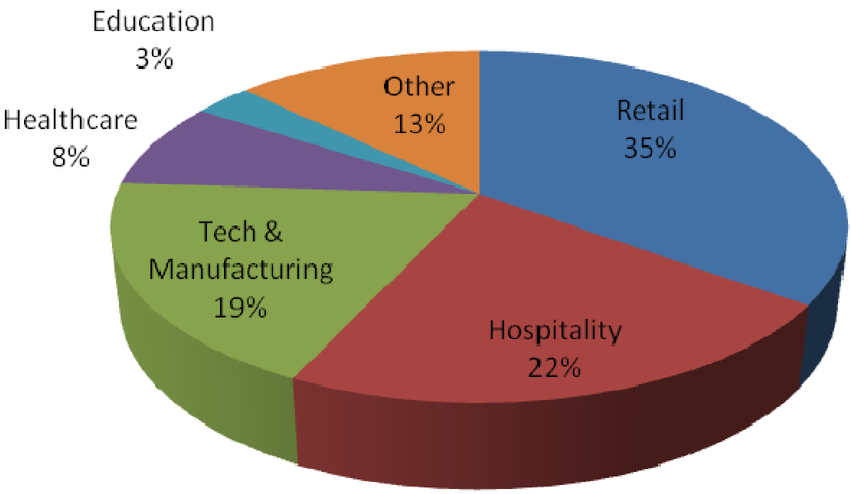
NEWS OF THE NATION

[redacted] loses data on 1.2M accounts

Finance Week Business

[redacted] loses data on 70,000 workers

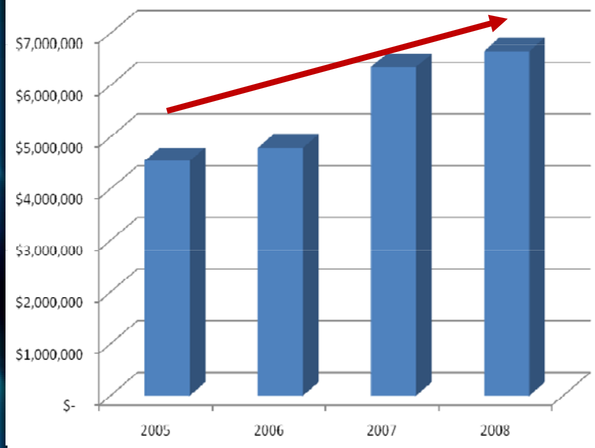
Data Leakage Incidents Between 2005-2008



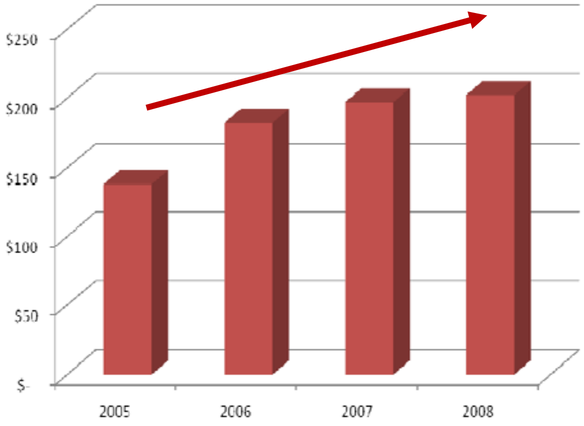
Source: Privacy Rights Clearing House, Data Loss Database, RSA Research & Analysis

Cost of Data Breaches

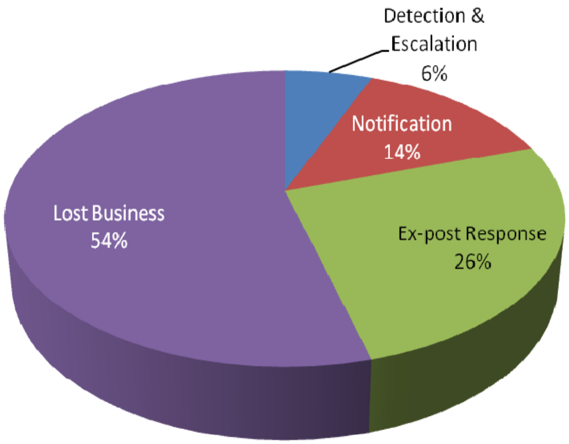
Average Cost Per Breach



Average Cost Per Breached Record



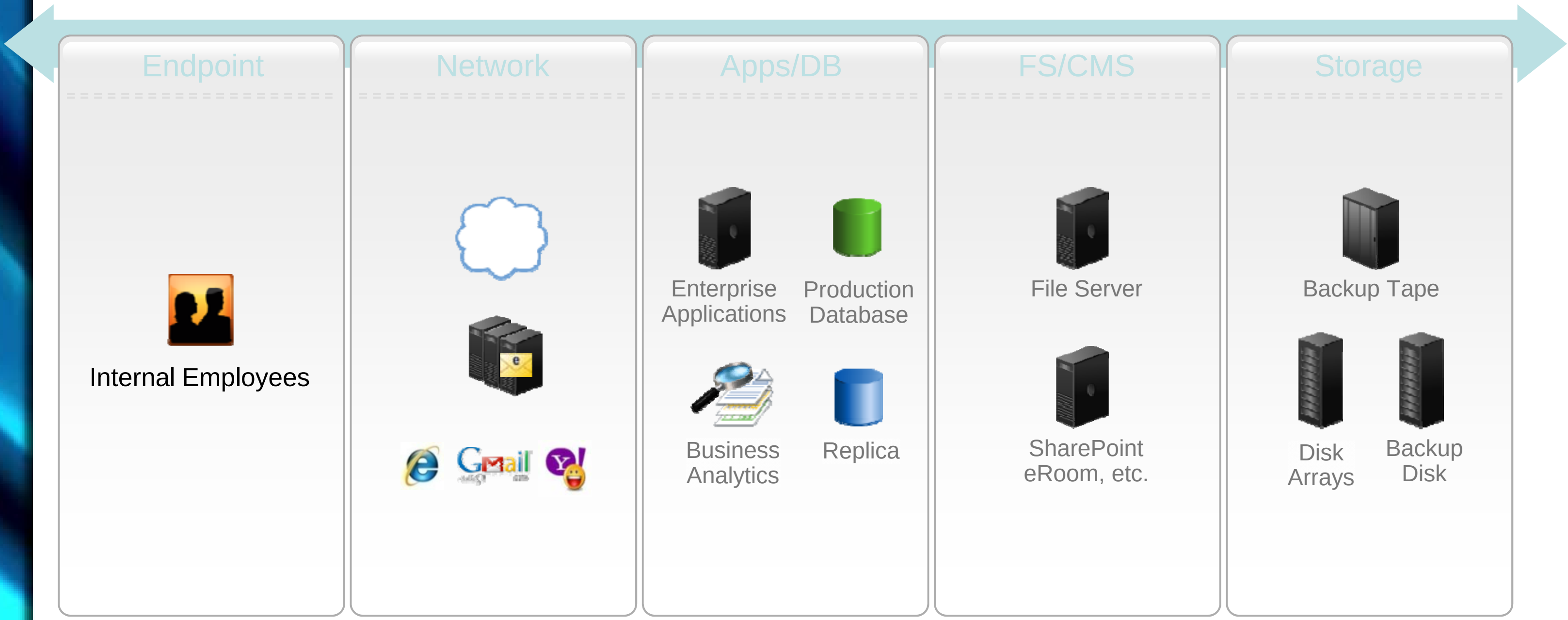
Breach Costs Break Down



- ➔Tangible financial impact
- ➔ Long-term damage to brand equity
- ➔ Total cost per breach is increasing
- ➔ 44 US States have notification laws
- ➔ EU & Australia data privacy policies

Source: Ponemon Institute 2008 Annual Study on Cost of a Data Breach

Challenge: Expanding Information



Endpoint

Internal Employees

Network

Apps/DB

Enterprise Applications

Production Database

Business Analytics

Replica

FS/CMS

File Server

SharePoint eRoom, etc.

Storage

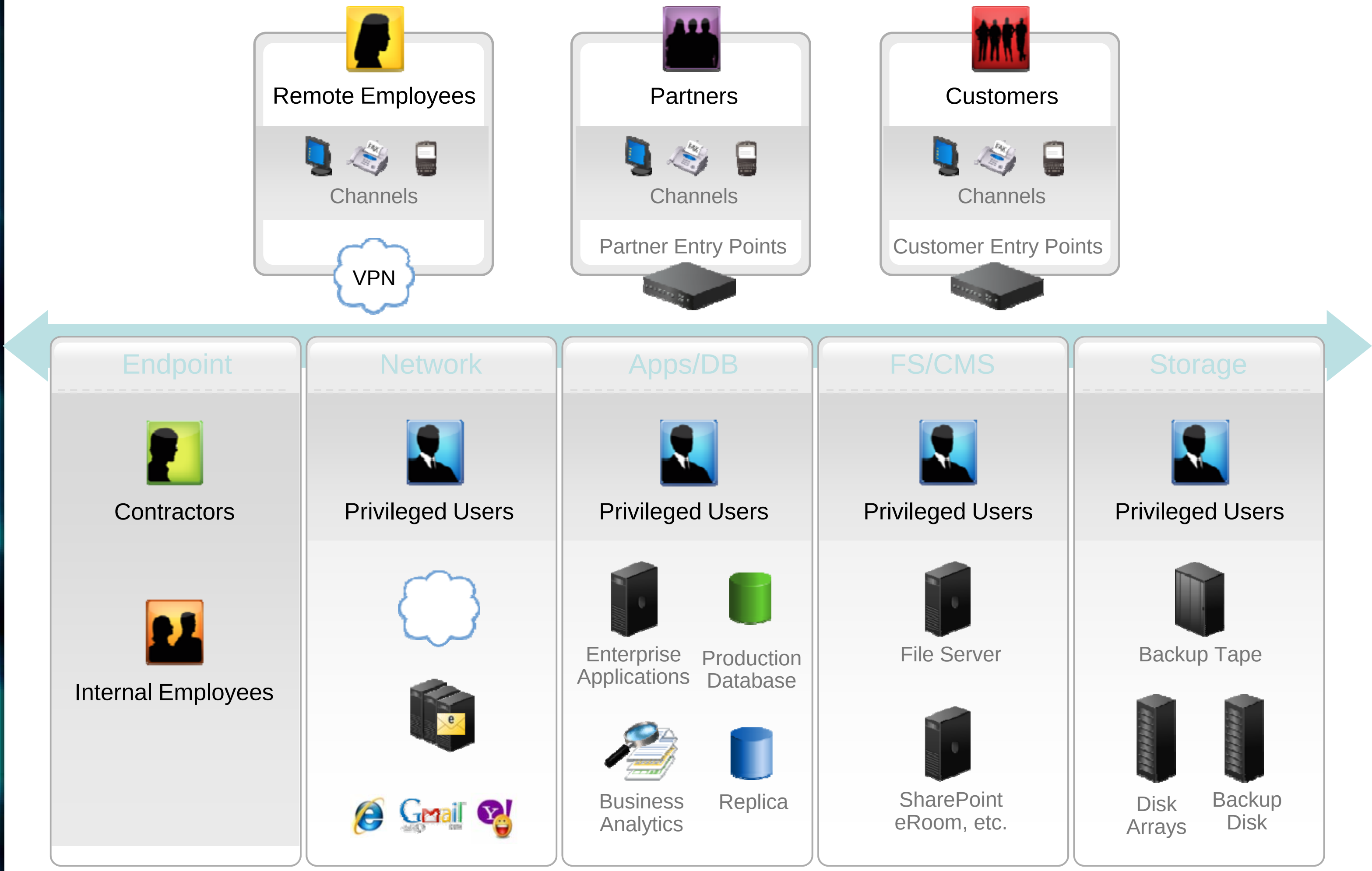
Backup Tape

Disk Arrays

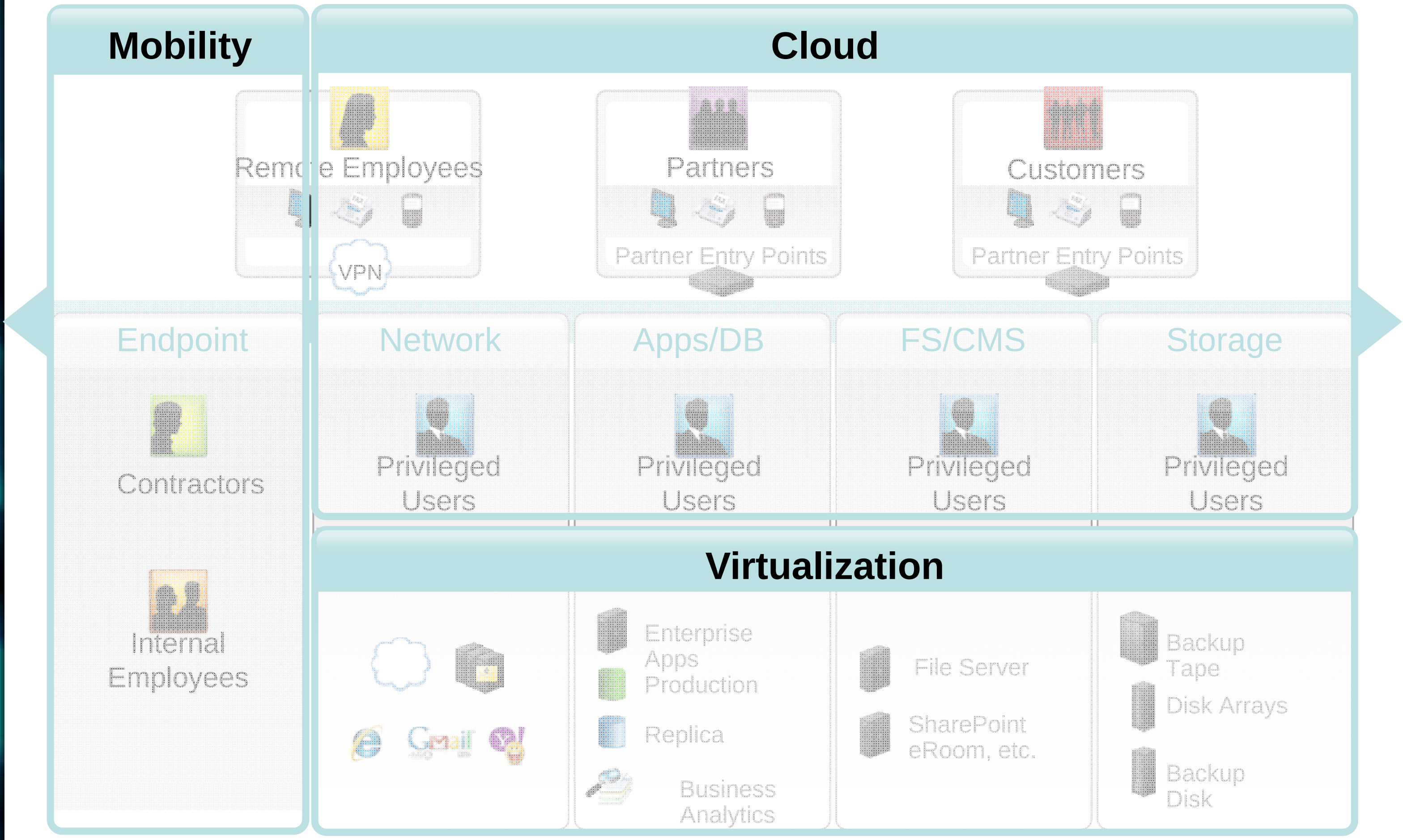
Backup Disk

SNIA SNW COMPUTERWORLD
April 12-15, 2010
Rosen Shingle Creek Resort
Orlando, Florida

Challenge: Expanding Identities



Challenge: Expanding Infrastructure



Mobility

Cloud

Remote Employees

VPN

Partners

Partner Entry Points

Customers

Partner Entry Points

Endpoint

Contractors

Internal Employees

Network

Privileged Users

Apps/DB

Privileged Users

FS/CMS

Privileged Users

Storage

Privileged Users

Virtualization

Enterprise Apps Production

Replica

Business Analytics

File Server

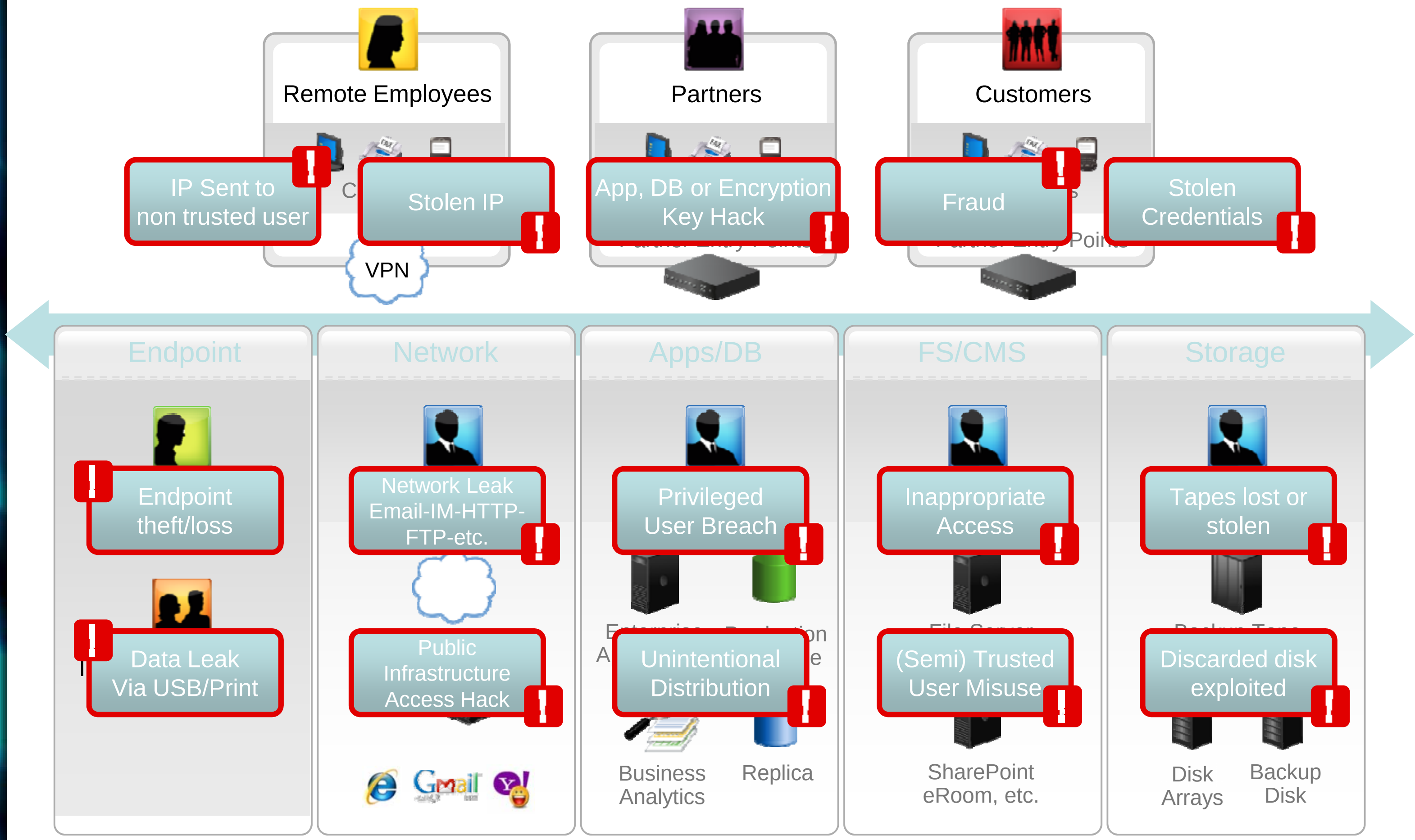
SharePoint eRoom, etc.

Backup Tape

Disk Arrays

Backup Disk

Challenge: Increasing Threats



SNIA

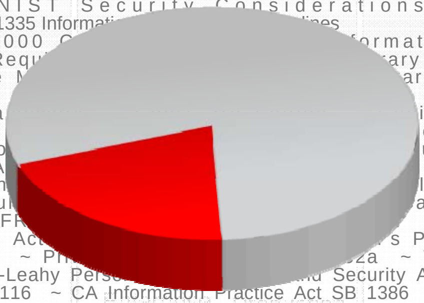
SNW

COMPUTERWORLD

April 12-15, 2010
Rosen Shingle
Creek Resort
Orlando, Florida

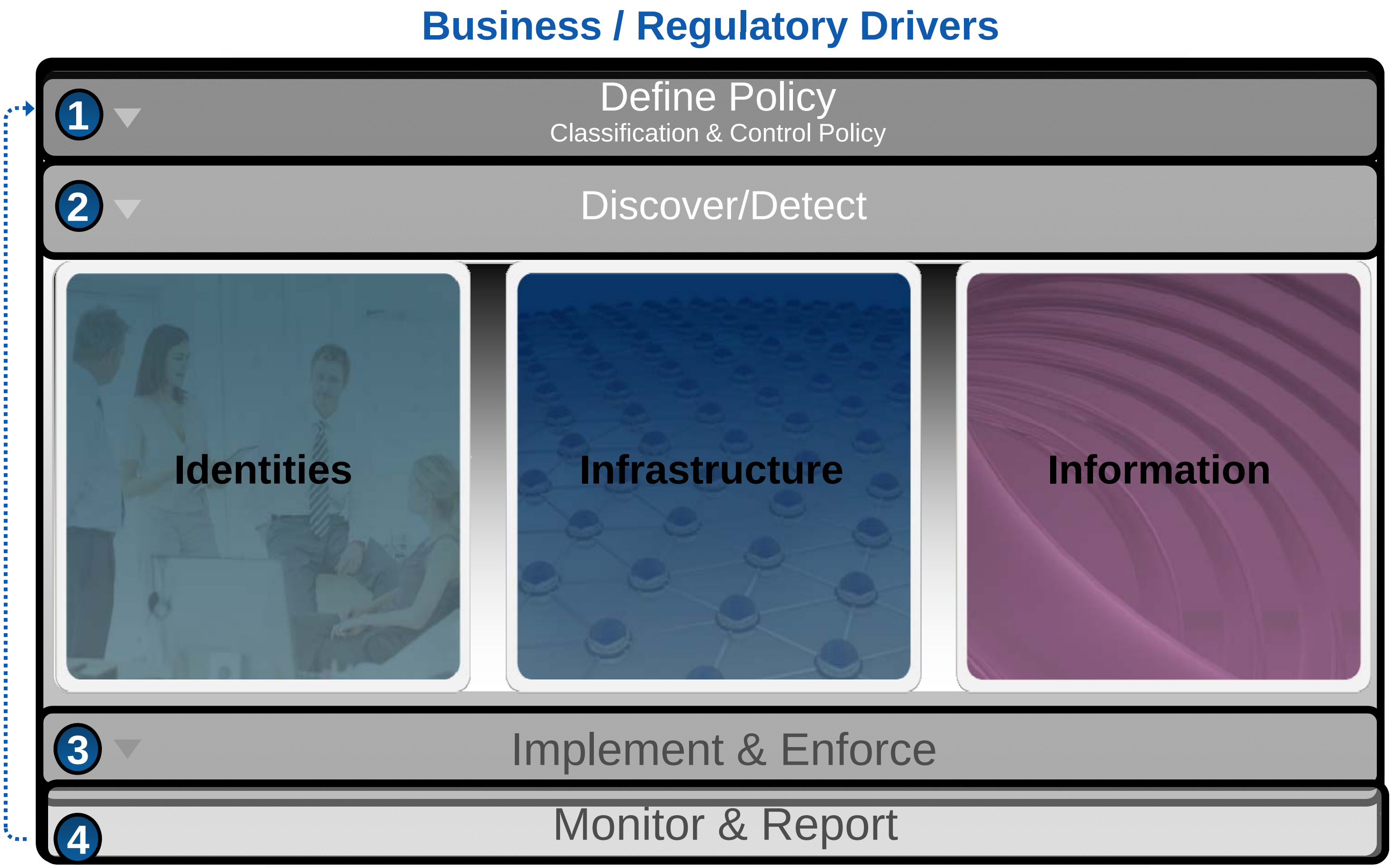
Challenge: Increasing Regulation

Sarbanes-Oxley Act (SOX) ~ PCAOB ~ SAS 94 ~ AICPA/CICA Privacy Framework ~ AICPA Suitable Trust Services Criteria ~ SEC Retention of Records, 17 CFR 210.2-06 ~ SEC Controls and Procedures, 17 CFR 240.15d-15 ~ SEC Reporting Transactions and Holdings, 17 CFR 240.16a-3 ~ Basel II ~ BIS Sound Practices for the Management and Supervision of Operational Risk ~ Gramm-Leach-Bliley Act (GLB) ~ Standards for Safeguarding Customer Information, FTC 16 CFR 314 ~ Privacy of Consumer Financial Information Rule ~ Safety and Soundness Standards, Appendix of 12 CFR 30 ~ FFIEC Information Security ~ FFIEC Development Acquisition ~ FFIEC Business Continuity Planning ~ FFIEC Audit ~ FFIEC Management ~ FFIEC Operations ~ NASD ~ NYSE ~ Recordkeeping rule for securities exchanges, SEC 17 CFR 240.17a-1 ~ Records to be made by exchange members, SEC 17 CFR 240.17a-3 ~ Records to be preserved by exchange members, SEC 17 CFR 240.17a-4 ~ Recordkeeping, SEC 17 CFR 240.17Ad-6 ~ Record retention, SEC 17 CFR 240.17Ad-7 ~ HIPAA (Health Insurance Portability and Accountability Act) ~ HIPAA HCFA Internet Security Policy ~ NIST Introductory Resource Guide for [HIPAA] (800-66) ~ CMS Core Security Requirements (CSR) ~ CMS Information Security Acceptable Risk Safeguards (ARS) ~ CMS Information Security Certification & Accreditation (C&A) ~ FDA Electronic Records; Electronic Signatures 21 CFR Part 11+D1 ~ Federal Energy Regulatory Commission (FERC) ~ North American Electric Reliability Council (NERC) ~ VISA CISP (Cardholder Information Security Program) ~ Mastercard SDP (Site Data Protection) Program ~ American Express DSS (Data Security Standard) ~ PCI DSS (Payment Card Industry Data Security Standard) ~ FTC ESIGN (Electronic Signatures in Global and National Commerce Act) ~ Uniform Electronic Transactions Act (UETA) ~ FISMA (Federal Information Security Management Act) ~ FISCAM (Federal Information System Controls Audit Manual) ~ FIPS Security Requirements for Cryptographic Modules 140-2 ~ FIPS Guideline for the Analysis of LAN Security 191 ~ FIPS Application Profile for GILS 192 ~ Clinger-Cohen Act (Information Technology Management Reform Act) ~ National Strategy to Secure Cyberspace ~ GAO Financial Audit Manual ~ DOD ...Standard for Electronic Records Management Software...5015-2 ~ CISWG Report on the Best Practices Subgroup ~ CISWG Information Security Program Elements ~ NCUA Guidelines for Safeguarding Member Information 12 CFR 748 ~ IRS Revenue Procedure: Retention of books and records 97-22 ~ IRS Revenue Procedure: Record retention: automatic data processing... 98-25 ~ IRS Internal Revenue Code Section 501(c)(3) ~ Federal Rules of Civil Procedure ~ Uniform Rules of Civil Procedure ~ ISO 15489-1 Information and Documentation: Records management: General ~ ISO 15489-2 Information and Documentation: Records management: Guidelines ~ DIRKS: A Strategic Approach to Managing Business Information ~ Sedona Principles Addressing Electronic Document Production ~ NIST ...Principles and Practices for Securing IT Systems 800-14 ~ NIST ...Developing Security Plans for Federal Information Systems 800-18 ~ NIST Security Self-Assessment Guide... 800-26 ~ NIST Risk Management Guide... 800-30 ~ NIST Contingency Planning Guide... 800-34 ~ NIST ...Patch and Vulnerability Management Program 800-40 ~ NIST Guidelines on Firewalls and Firewall Policy 800-41 ~ NIST Security Controls for Federal Information Systems 800-53 ~ NIST ... Mapping...Information and ... Systems to Security Categories 800-60 ~ NIST Computer Security Incident Handling Guide 800-61 ~ NIST Security Considerations in...Information System Development 800-64 ~ ISO 73:2002 Risk management -- Vocabulary ~ ISO 1335 Informati lines for management of IT Security ~ ISO 17799:2000 C formation Security Management ~ ISO 27001:2005 ...Information Security Management Systems -- Requ ary (ITIL) Planning to Implement Service Management ~ IT Information Library (ITIL) ICT Infrastructure M ary (ITIL) Service Delivery ~ IT Information Library (ITIL) Service Support ~ IT Information Library IT Information Library (ITIL) Security Management ~ COSO Enterprise Risk Management (ERM) Fra iT 4th Edition ~ ISACA IS Standards, Guidelines, and Procedures for Auditing and Control... ency Management and Business Continuity... ~ Information Security Forum (ISF) Standard o urity Forum (ISF) Security Audit of Networks ~ A Risk Management Standard, jointly issued by A Continuity Institute (BCI) Good Practice Guidelines ~ IIA Global Technology Audit Guide - Information lly Accepted Information Security Principles (GAISP) ~ CERT Operationally Critical Threat, Asset & Vul able Communications Privacy Act Title 47 § 551 ~ Telemarketing Sales Rule (TSR) amendment 16 CFR ~ Children's Online Privacy Protection Act (COPPA) 16 CFR 312 ~ Children's Online Privacy Protection Act s Privacy Protection Act (DPPA) 18 USC 2721 ~ Family Education Rights Privacy Act (FERPA) 20 USC 1232 ~ Pri 52a ~ Telemarketing Sales Rule (TSR) 16 CFR 310 ~ Video Privacy Protection Act (VPPA) 18 USC 2710 ~ Specter-Leahy Perso and Security Act ~ AR Personal Information Protection Act SB 1167 ~ AZ Amendment to Arizona Revised Statutes 13-2001 HB 2116 ~ CA Information Practice Act SB 1386 ~ CA General Security Standard for Businesses AB 1950 ~ CA Public Records Military Veteran Discharge Documents AB 1798 ~ CA OPP Recommended Practices on Notification of Security Breach ~ CO Prohibition against Using Identity Information for Unlawful Purpose HB 1134 ~ CO Consumer Credit Solicitation Protection HB 1274 ~ CO Prohibiting Inclusion of Social Security Number HB 1311 ~ CT Requiring Consumer Credit Bureaus to Offer Security Freezes SB 650 ~ CT Concerning Nondisclosure of Private Tenant Information HB 5184 ~ DE Computer Security Breaches HB 116 ~ FL Personal Identification Information/Unlawful Use HB 481 ~ GA Consumer Reporting Agencies SB 230 ~ GA Public employees; Fraud, Waste, and Abuse HB 656 ~ HI Exempting disclosure of Social Security numbers HB 2674 ~ IL Personal Information Protection Act HB 1633 ~ IN Release of Social Security Number, Notice of Security Breach SB 503 ~ LA Database Security Breach Notification Law SB 205 Act 499 ~ ME To Protect Maine Citizens from Identity Theft LD 1671 ~ MN Data Warehouses; Notice Required for Certain Disclosures HF 2121 ~ MO HB 957 ~ MT To Implement Individual Privacy and to Prevent Identity Theft HB 732 ~ NJ Identity Theft Prevention Act A4001/S1914 ~ NY A4254, A3492 [no title] ~ NV SB 347 [no title] ~ NC Security Breach Notification Law (Identity Theft Protection Act) SB 1048 ~ ND Personal information protection act SB 2251 ~ OH Personal information -- contact if unauthorized access HB 104 ~ RI Security Breach Notification Law H 6191 ~ TN Security Breach Notification SB 2220 ~ TX Identity Theft Enforcement and Protection Act SB 122 ~ VT Relating to Identity Theft HB 327 ~ VA Identity theft; penalty; restitution; victim assistance HB 872 ~ WA Notice of a breach of the security SB 6043 ~ EU Directive on Privacy and Electronic Communications 2002/58/EC ~ EU Directive on Data Protection 95/46/EC ~ US Department of Commerce EU Safe Harbor Privacy Principles ~ ...Consumer Interests in the Telecommunications Market Act No. 661 ~ Directive On Privacy And Electronic Communications 2002.58.EC ~ OECD Technology Risk Checklist ~ OECD Guidelines on...Privacy and Transborder Flows of Personal Data ~ UN Guidelines for the Regulation of Computerized Personal Data Files (1990) ~ ISACA Cross-border Privacy Impact Assessment ~ The Combined Code on Corporate Governance ~ Turnbull Guidance on Internal Control, UK FRC ~ Smith Guidance on Audit Committees Combined Code, UK FRC ~ UK Data Protection Act of 1998 ~ BS 15000-1 IT Service Management Standard ~ BS 15000-2 IT Service Management Standard - Code of Practice ~ Canada Keeping the Promise for a Strong Economy Act Bill 198 ~ Canada Personal Information Protection and Electronic Documents Act ~ Canada Privacy Policy and Principles ~ Argentina Personal Data Protection Act ~ Mexico Federal Personal Data Protection Law ~ Austria Data Protection Act ~ Austria Telecommunications Act ~ Bosnia Law on Protection of Personal Data ~ Czech Republic Personal Data Protection Act ~ Denmark Act on Competitive Conditions and Consumer Interests ~ Finland Personal Data Protection Act ~ Finland Amendment of the Personal Data Act ~ France Data Protection Act ~ German Federal Data Protection Act ~ Greece Law on Personal Data Protection ~ Hungary Protection of Personal Data and Disclosure of Data of Public Interest ~ Iceland Protection of Privacy as regards the Processing of Personal Data ~ Ireland

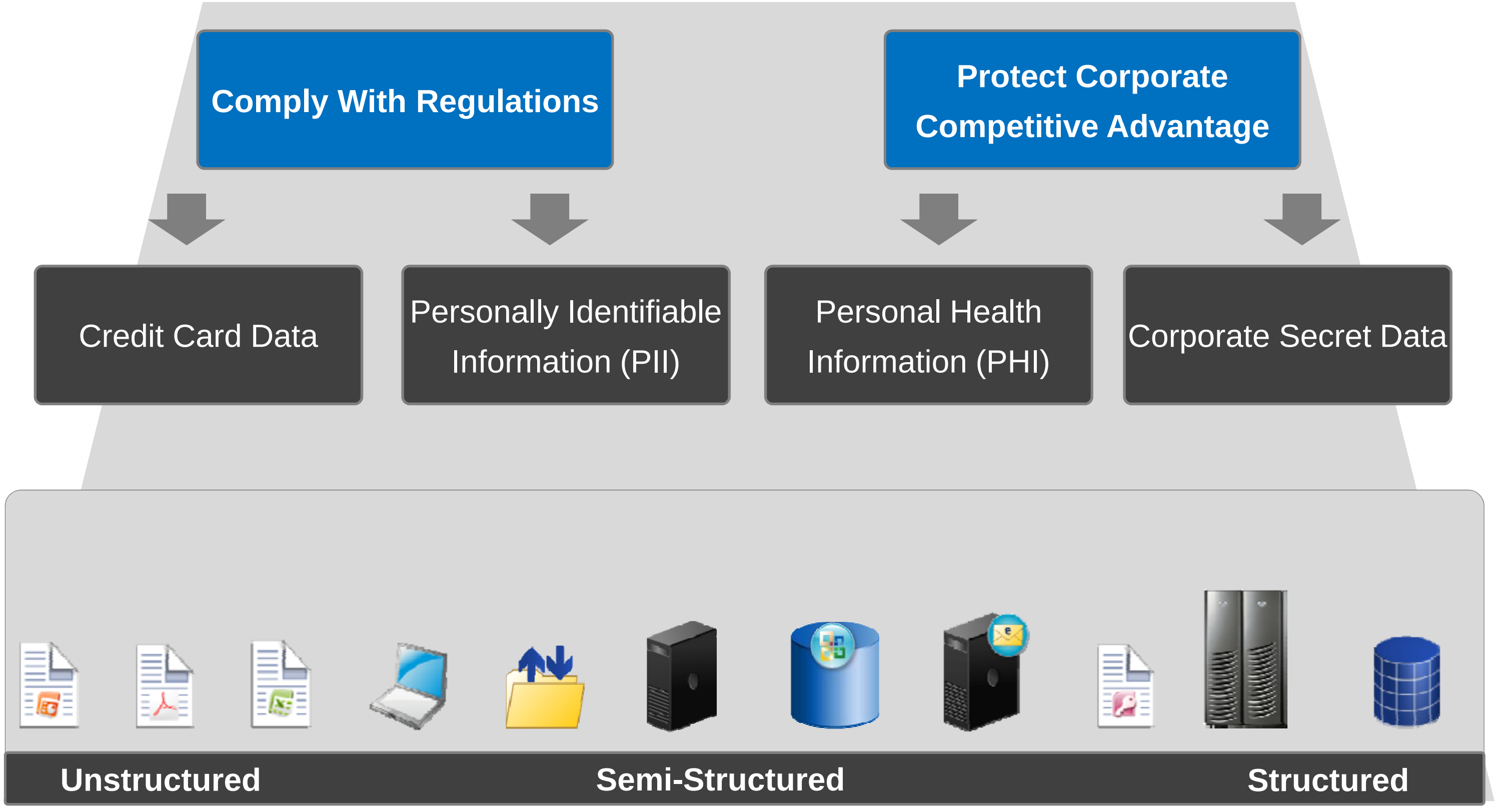


20% of IT staff time

Information Risk Management



Discover Your Sensitive Data



Comply With Regulations

Protect Corporate Competitive Advantage

Credit Card Data

Personally Identifiable Information (PII)

Personal Health Information (PHI)

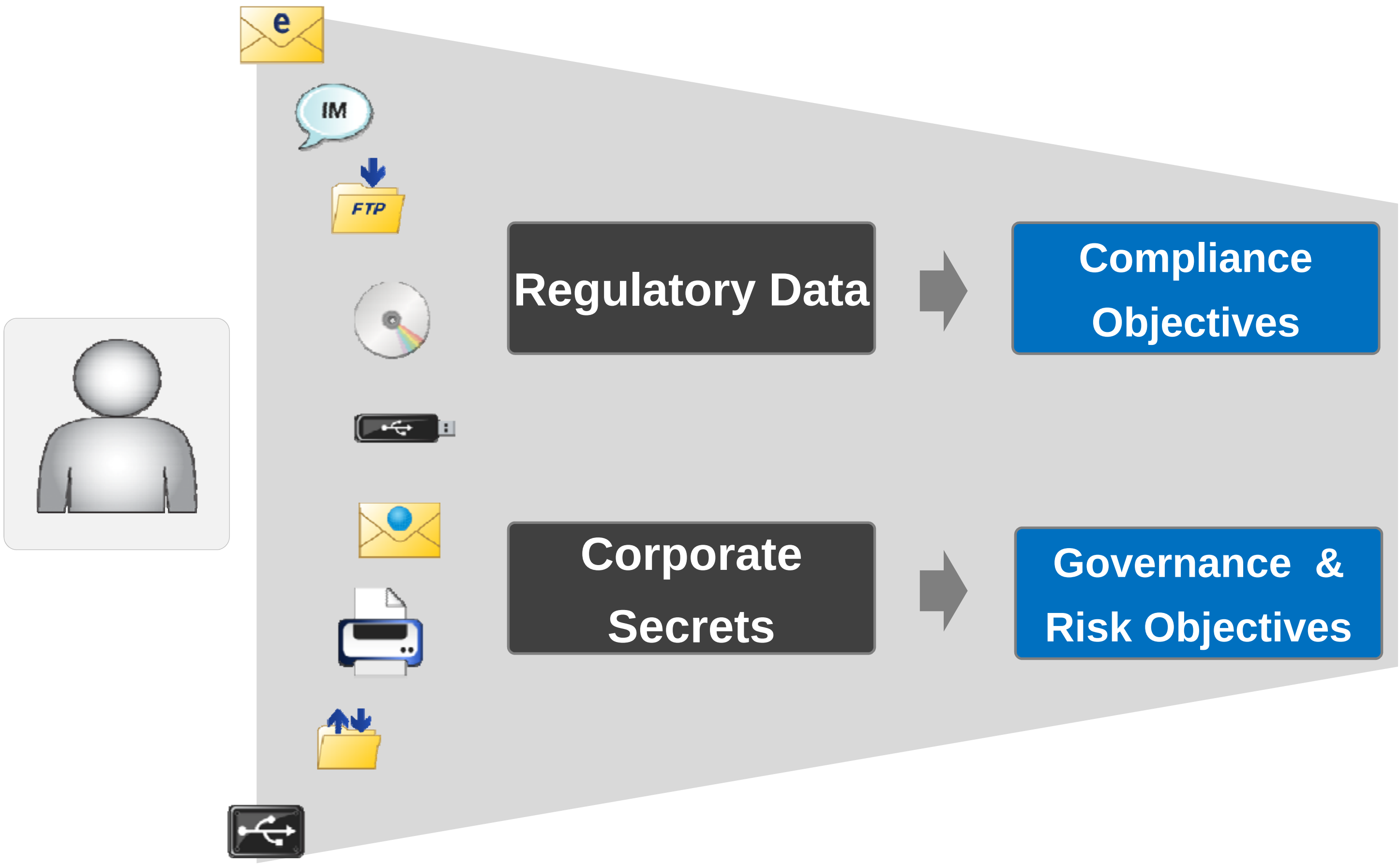
Corporate Secret Data

Unstructured

Semi-Structured

Structured

Monitor Your Sensitive Data



Regulatory Data → Compliance Objectives

Corporate Secrets → Governance & Risk Objectives

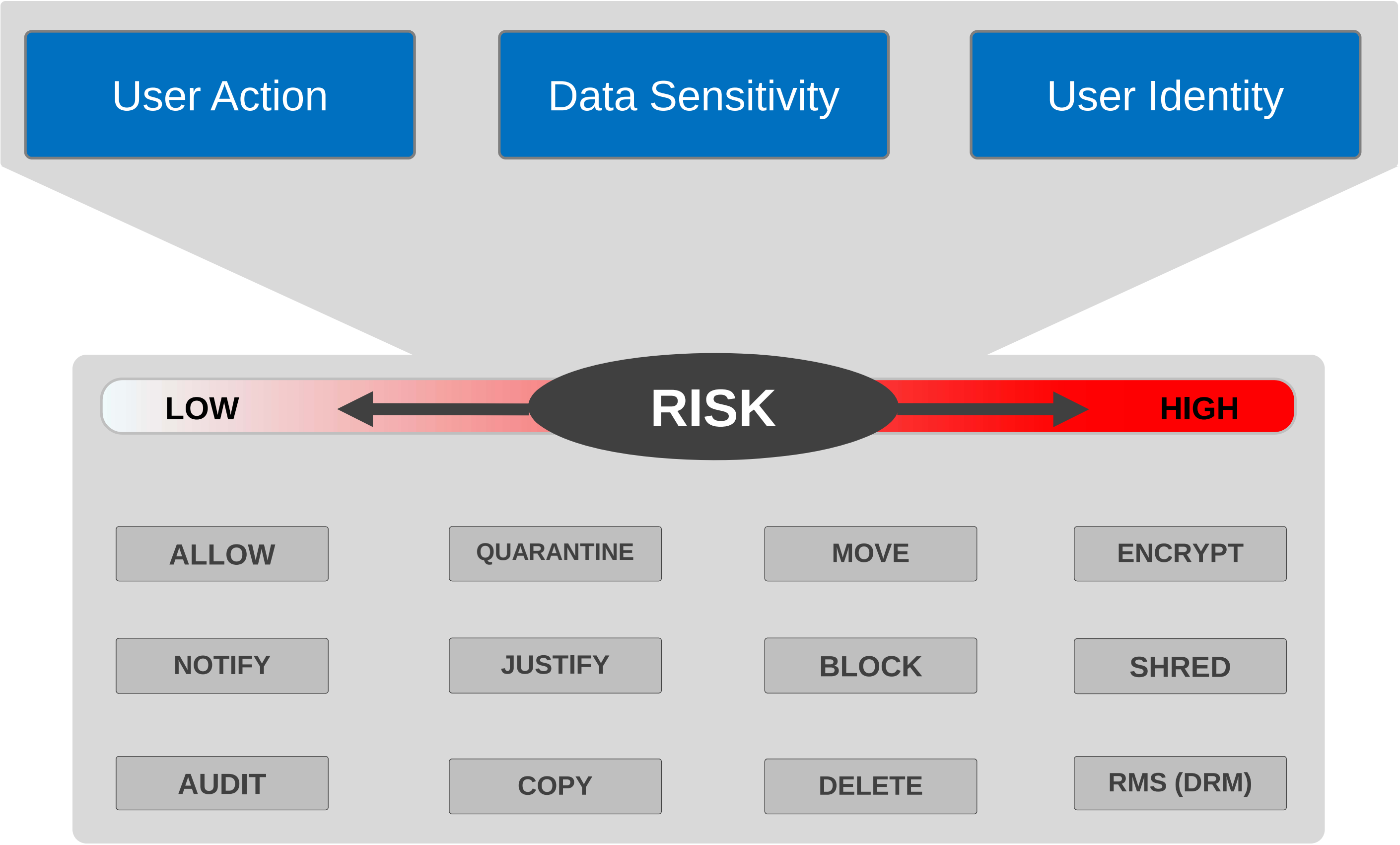
SNIA

SNW

COMPUTERWORLD

April 12-15, 2010
Rosen Shingle
Creek Resort
Orlando, Florida

Secure Your Sensitive Data



User Action

Data Sensitivity

User Identity

LOW

RISK

HIGH

ALLOW	QUARANTINE	MOVE	ENCRYPT
NOTIFY	JUSTIFY	BLOCK	SHRED
AUDIT	COPY	DELETE	RMS (DRM)

SNIA

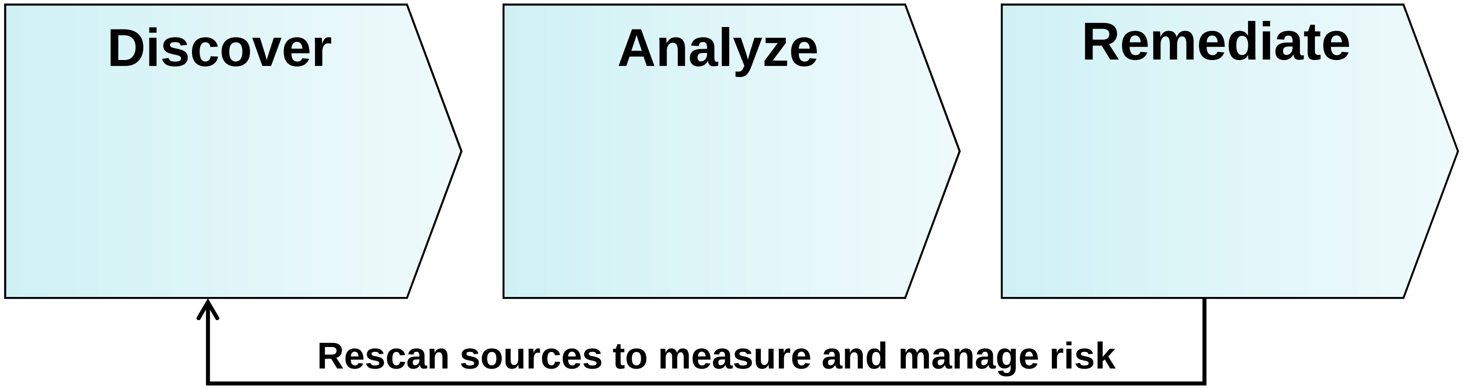
SNW

COMPUTERWORLD

April 12-15, 2010
Rosen Shingle
Creek Resort
Orlando, Florida

Discovering Sensitive Information

Reducing Your Sources of Risk: Data at Rest



File shares, Servers,

- Windows file shares
- Unix file shares
- NAS / SAN storage
- Windows 2000, 2003
- Windows XP, Vista

300+ File types

- Microsoft Office Files
- PDFs, PSTs
- Zip files
- CATIA files

Databases & Repositories

- SharePoint
- Documentum
- Microsoft Access
- Oracle, SQL
- Content Mgmt systems

Remediation

- Secure Delete
- Manual/Auto Move
- Manual/Auto Quarantine
- Notifications
- eDRM

Business Policy to Information Discovery

Business Policy

Governance Team

- Establish business policy for DLP discovery
- 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 blades: Credit Card Number, Drivers Licence number, Social Security number

DataCenter
Move if not encrypted

Endpoint
e.g Block USB notify user

Network
e.g Block, notify sender

Status & Exceptions

•Assessment findings

•Escalated incidents

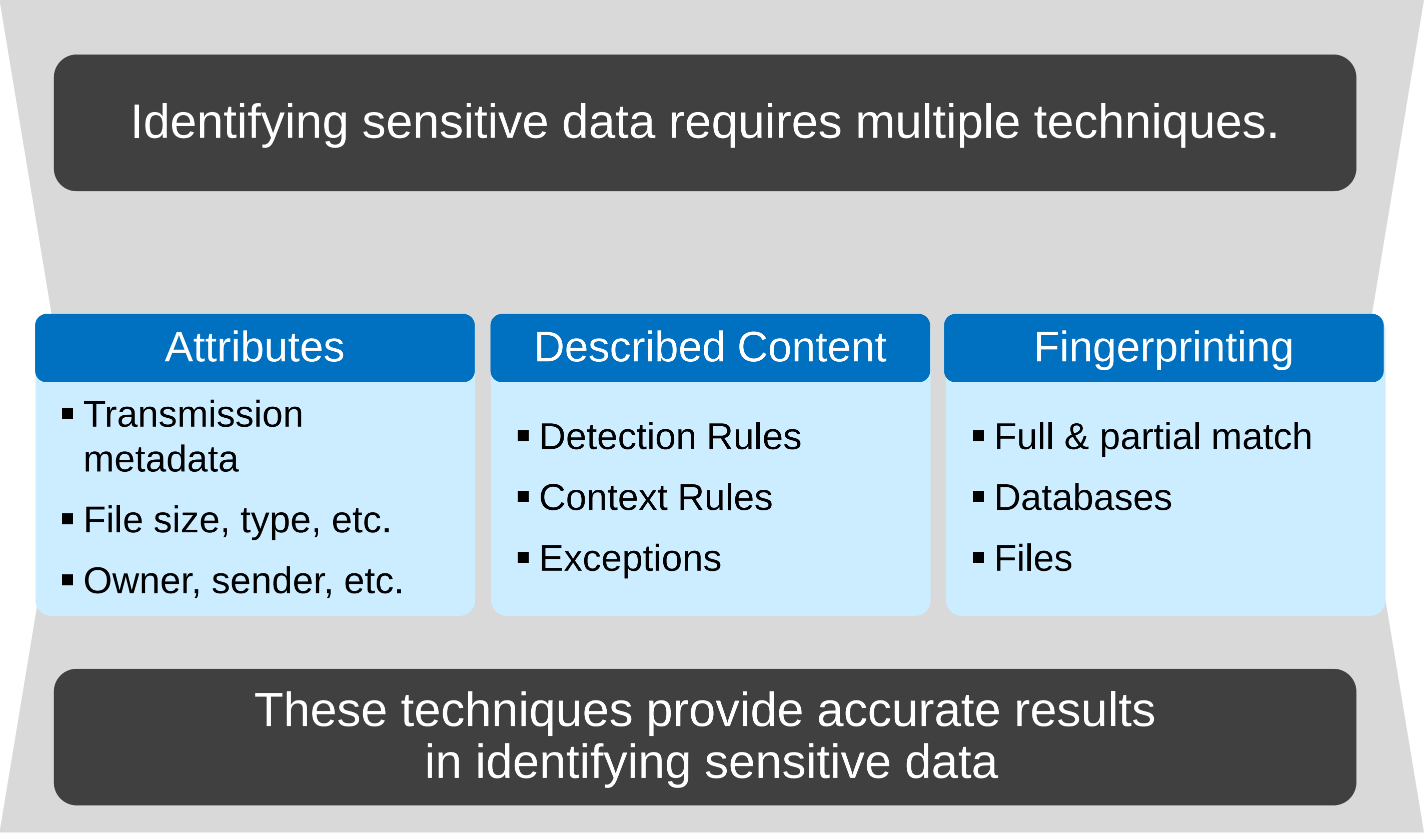
DLP Policies

1
Identification
2
Notification
3
Remediation

1. Policies identify a violation by specifying
   - What: the identification of content is done by Content Blades. You can further manage this by specifying attributes like file type, file size
   - Who: same content might be a violation for some people or AD groups, departments, while perfectly ok for others.
   - Where: in the network, datacenter, endpoint or all; or in a particular subset of scans identified by a scan group (which can represent a BU, geography); or a specific user action (at copy or at print).
2. Policies set up notification by defining
   - Who: who is responsible for handling the incident (the user creating it, the administrator, the user's manager)
   - What: what is in the notification (eg. notification customized per AD group or policy, include links)
   - How: Send an email, pop up a window, integrate into Remedy or SIEM solution
3. Remediation
   - What: different remediation options including encryption, quarantine, block, copy, move, delete, apply rights management.
   - How: thru automated actions at the time of the incident; thru workflow that can leverage AD hierarchy; facilitated actions, or manual actions with incident management

SNIA
SNW
COMPUTERWORLD
April 12-15, 2010
Rosen Shingle Creek Resort
Orlando, Florida

Data Identification



Identifying sensitive data requires multiple techniques.

Attributes

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

Described Content

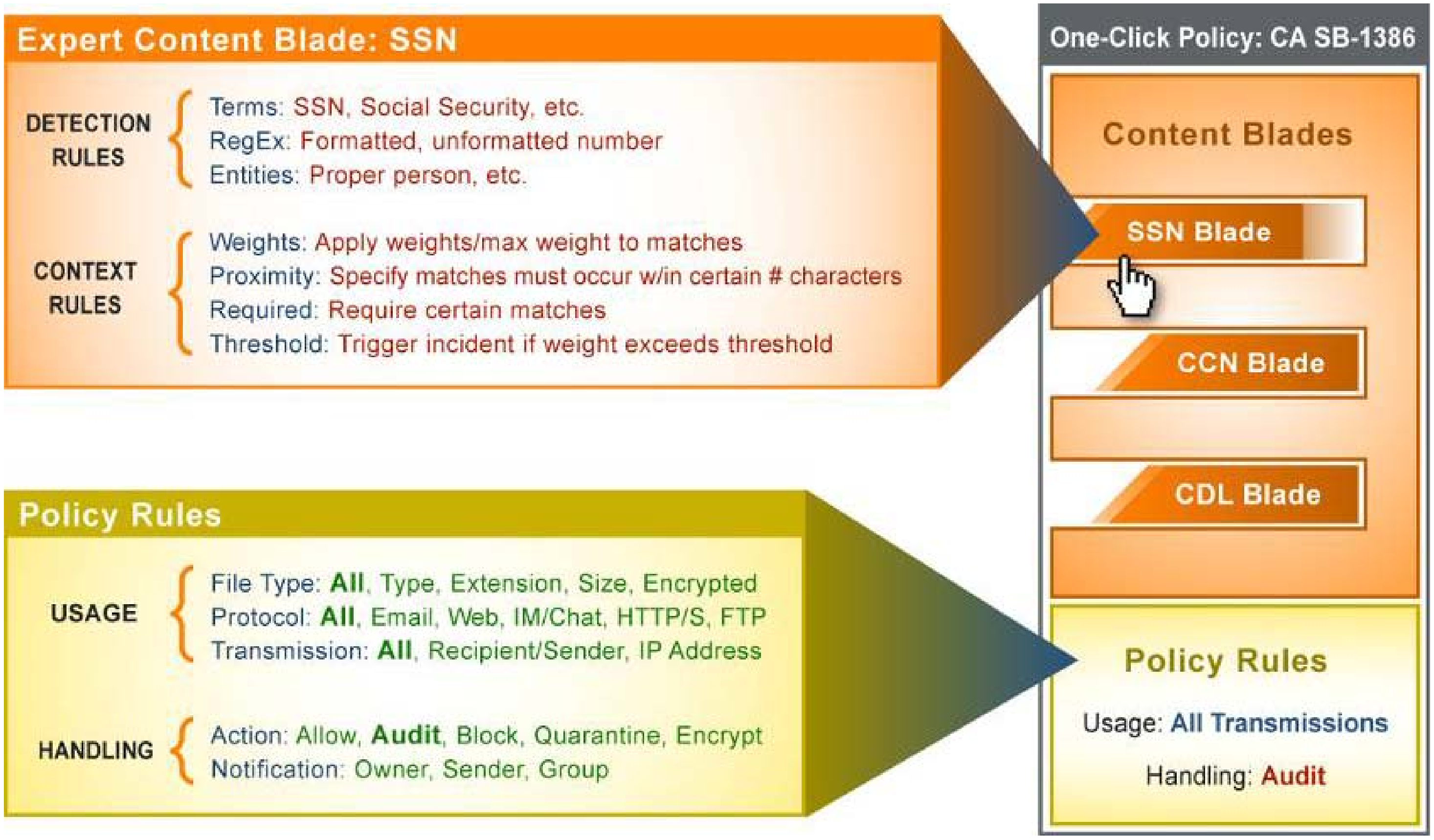
- Detection Rules
- Context Rules
- Exceptions

Fingerprinting

- Full & partial match
- Databases
- Files

These techniques provide accurate results
in identifying sensitive data

Data Discovery and Remediation



Expert Content Blade: SSN

DETECTION RULES
- Terms: SSN, Social Security, etc.
- RegEx: Formatted, unformatted number
- Entities: Proper person, etc.

CONTEXT RULES
- Weights: Apply weights/max weight to matches
- Proximity: Specify matches must occur w/in certain # characters
- Required: Require certain matches
- Threshold: Trigger incident if weight exceeds threshold

Policy Rules

USAGE
- File Type: **All**, Type, Extension, Size, Encrypted
- Protocol: **All**, Email, Web, IM/Chat, HTTP/S, FTP
- Transmission: **All**, Recipient/Sender, IP Address

HANDLING
- Action: Allow, **Audit**, Block, Quarantine, Encrypt
- Notification: Owner, Sender, Group

One-Click Policy: CA SB-1386

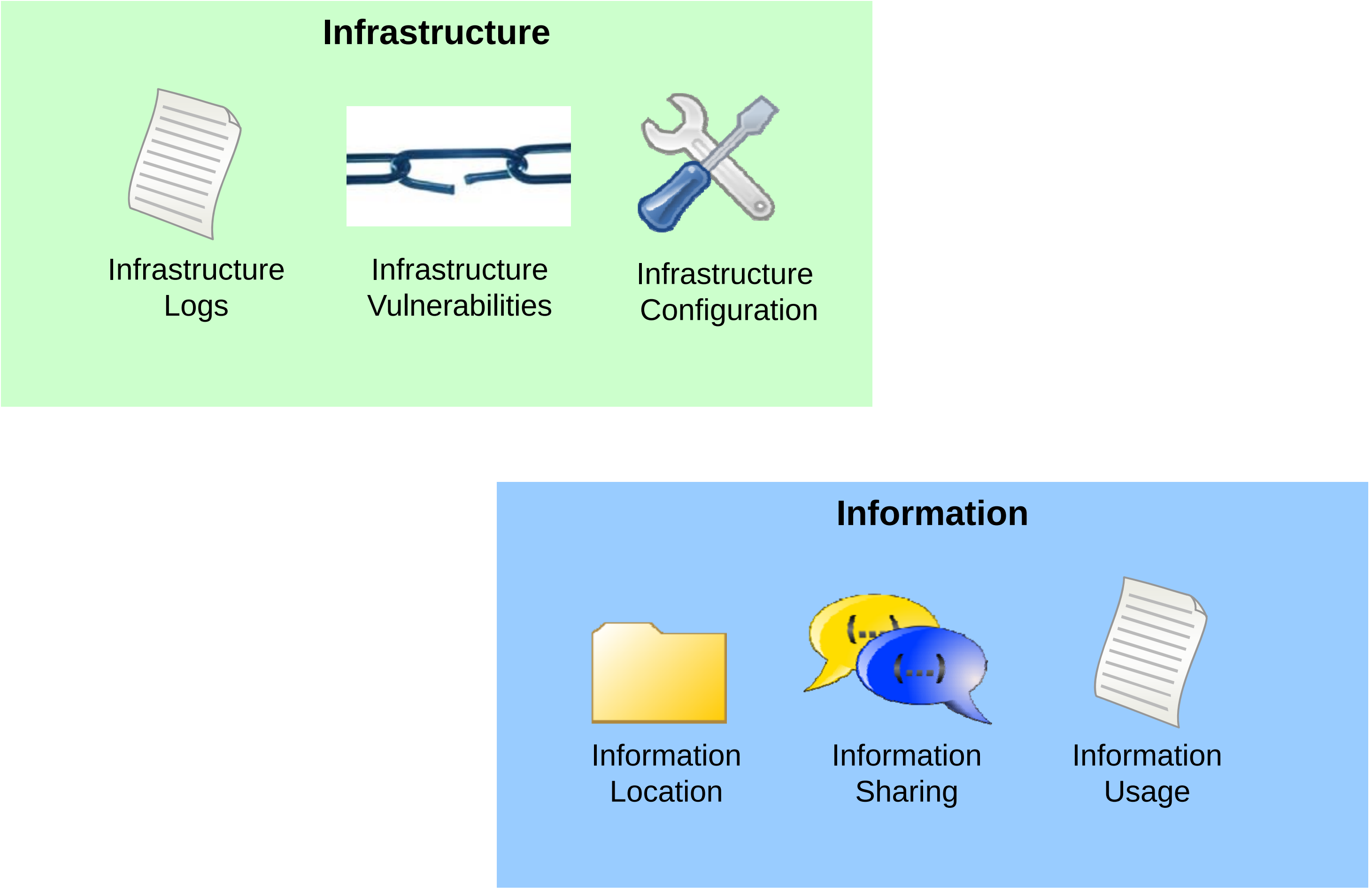
Content Blades
- SSN Blade
- CCN Blade
- CDL Blade

Policy Rules

Usage: **All Transmissions**

Handling: **Audit**

Configuration Analysis



Infrastructure

Infrastructure Logs

Infrastructure Vulnerabilities

Infrastructure Configuration

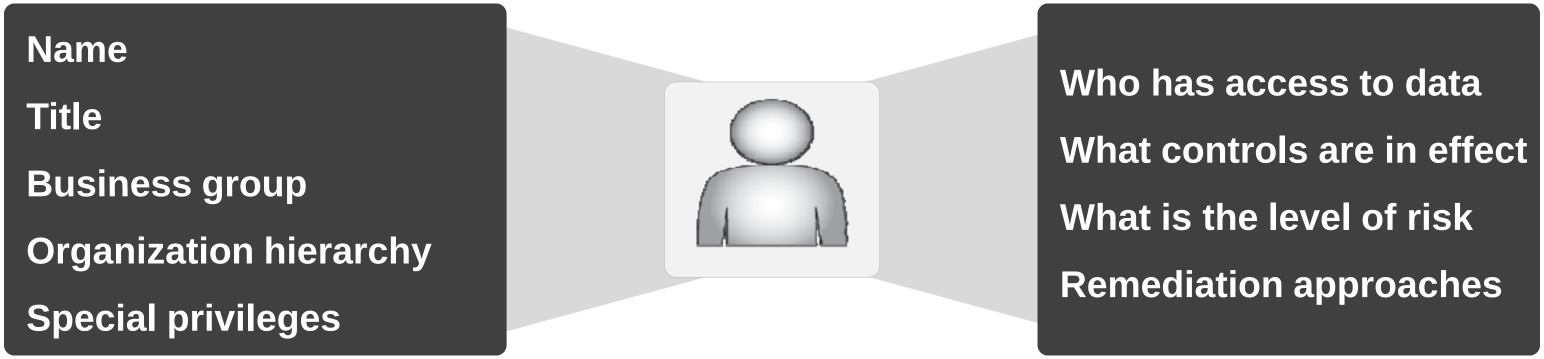
Information

Information Location

Information Sharing

Information Usage

User Identity Analysis



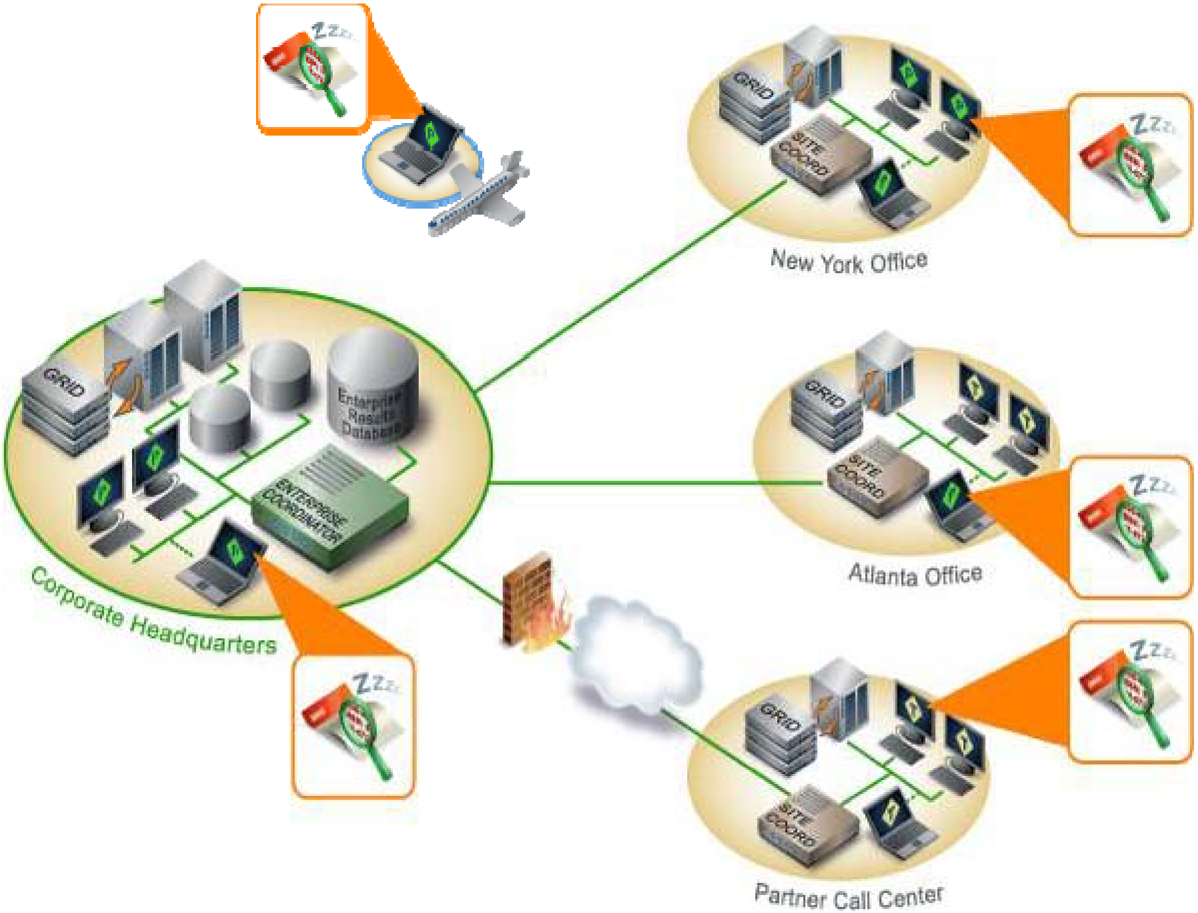
- Name
- Title
- Business group
- Organization hierarchy
- Special privileges

- Who has access to data
- What controls are in effect
- What is the level of risk
- Remediation approaches

SNIA
SNW
COMPUTERWORLD
April 12-15, 2010
Rosen Shingle
Creek Resort
Orlando, Florida

Use Case: Information Discovery

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



SNIA

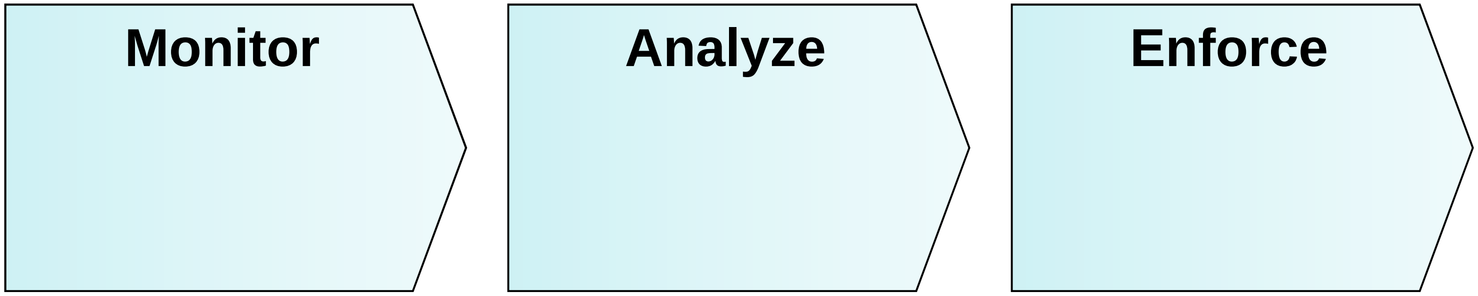
SNW

COMPUTERWORLD

April 12-15, 2010
Rosen Shingle
Creek Resort
Orlando, Florida

Monitoring Sensitive Information

Protecting Data in the Network: Data in Motion



Email

- SMTP email
- Exchange, Lotus, etc.
- Webmail
- Text and attachments

Instant Messages

- Yahoo IM
- MSN Messenger
- AOL Messenger

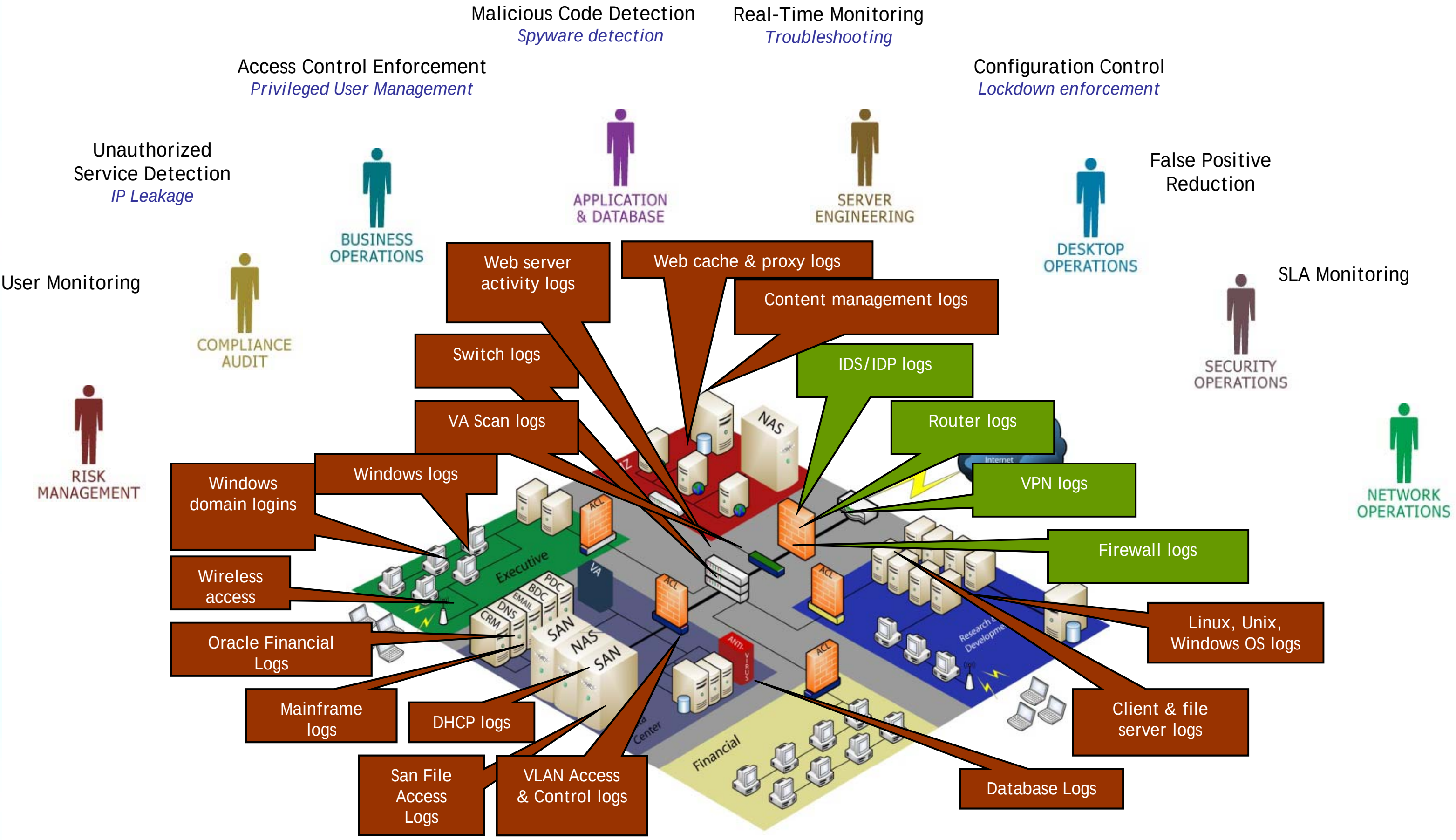
Web Traffic

- FTP
- HTTP
- HTTPS
- TCP/IP

Remediation

- Audit
- Block
- Encrypt
- Log

Correlating Event Information



Malicious Code Detection
Spyware detection

Real-Time Monitoring
Troubleshooting

Access Control Enforcement
Privileged User Management

Configuration Control
Lockdown enforcement

Unauthorized Service Detection
IP Leakage

False Positive Reduction

User Monitoring

SLA Monitoring

BUSINESS OPERATIONS

APPLICATION & DATABASE

SERVER ENGINEERING

DESKTOP OPERATIONS

COMPLIANCE AUDIT

SECURITY OPERATIONS

RISK MANAGEMENT

NETWORK OPERATIONS

Web server activity logs

Web cache & proxy logs

Content management logs

Switch logs

IDS/IDP logs

VA Scan logs

Router logs

Windows domain logins

Windows logs

VPN logs

Firewall logs

Wireless access

Linux, Unix, Windows OS logs

Oracle Financial Logs

Mainframe logs

DHCP logs

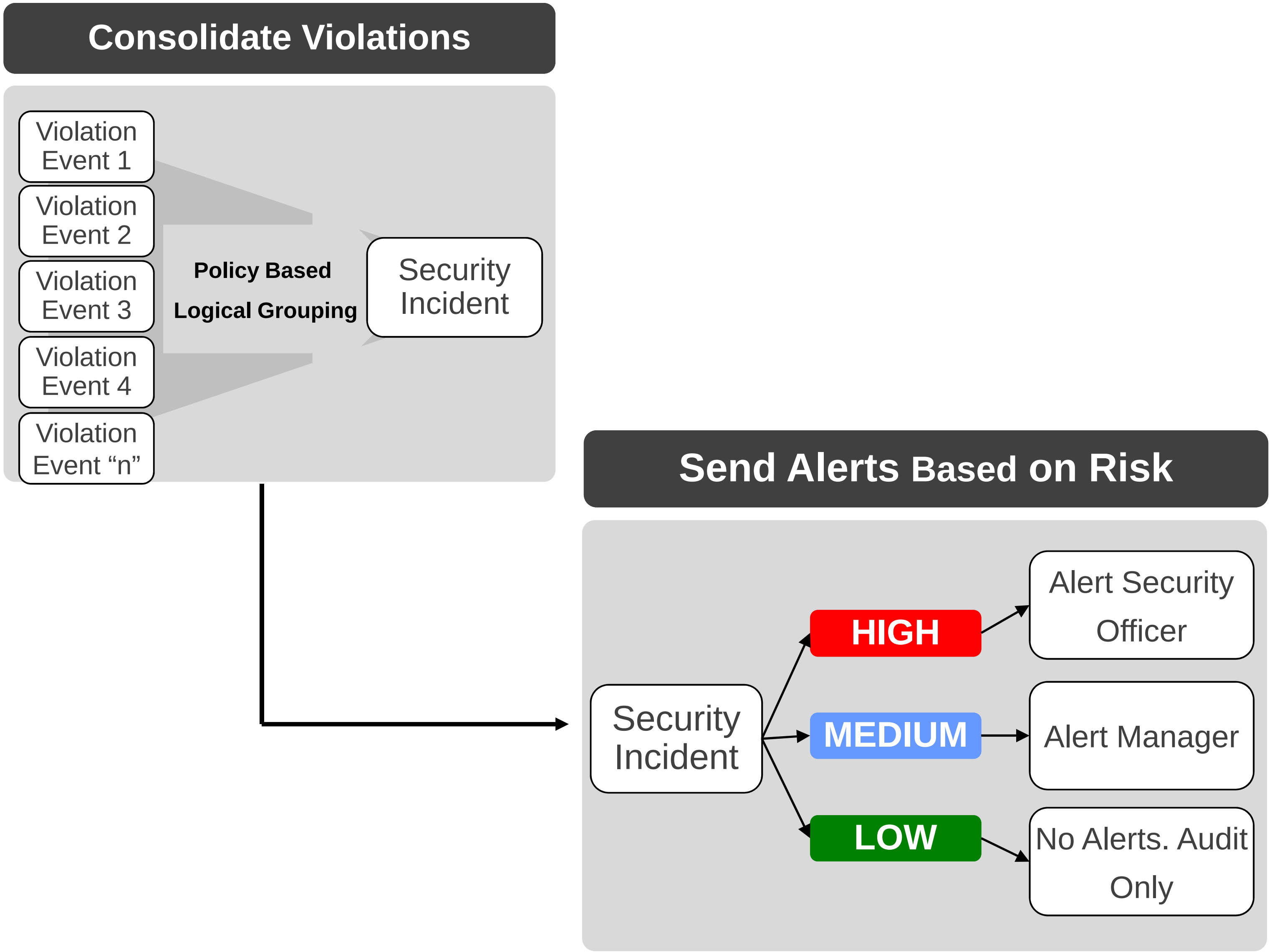
Client & file server logs

San File Access Logs

VLAN Access & Control logs

Database Logs

Incident 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

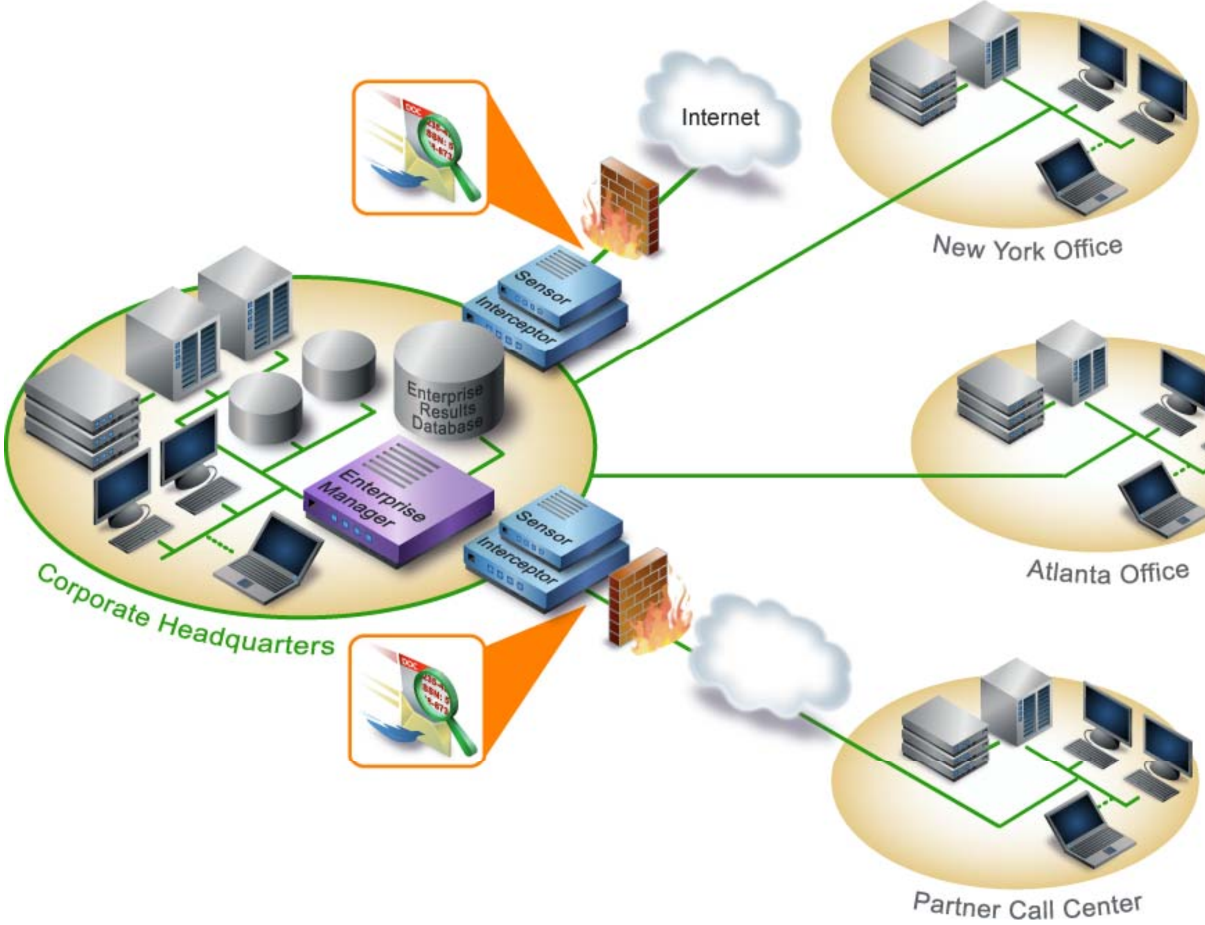
Alert Manager

No Alerts. Audit Only

Use Case: Security Incident

Analyst investigates malware outbreak

DLP detects if confidential Information is leaving network



SNIA

SNW

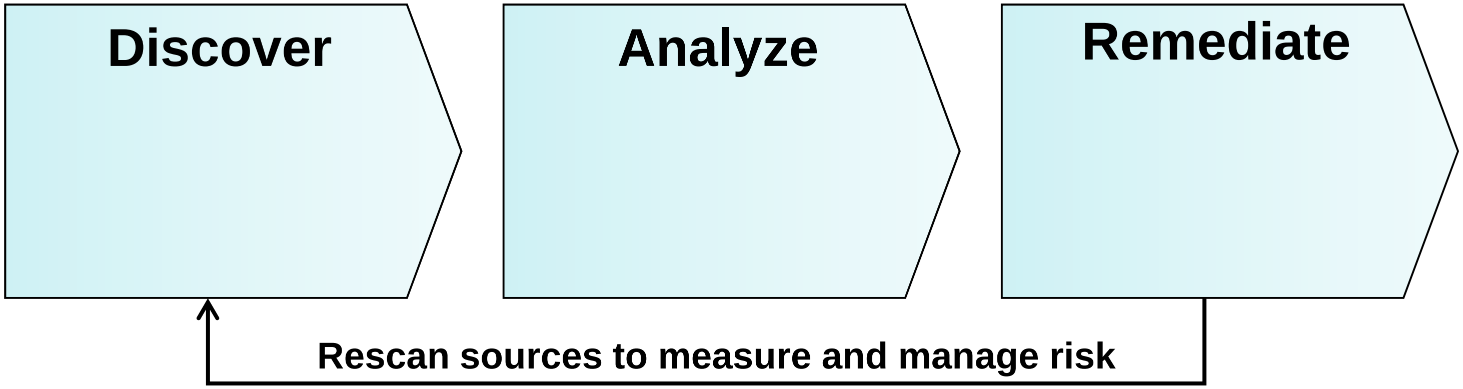
COMPUTERWORLD

April 12-15, 2010
Rosen Shingle
Creek Resort
Orlando, Florida

Securing Sensitive Information

Reducing Your Sources of Risk:

Data at Rest



File shares, Servers,

- •Windows file shares
- •Unix file shares
- •NAS / SAN storage
- •Windows 2000, 2003
- •Windows XP, Vista

300+ File types

- •Microsoft Office Files
- •PDFs, PSTs
- •Zip files
- •CATIA files

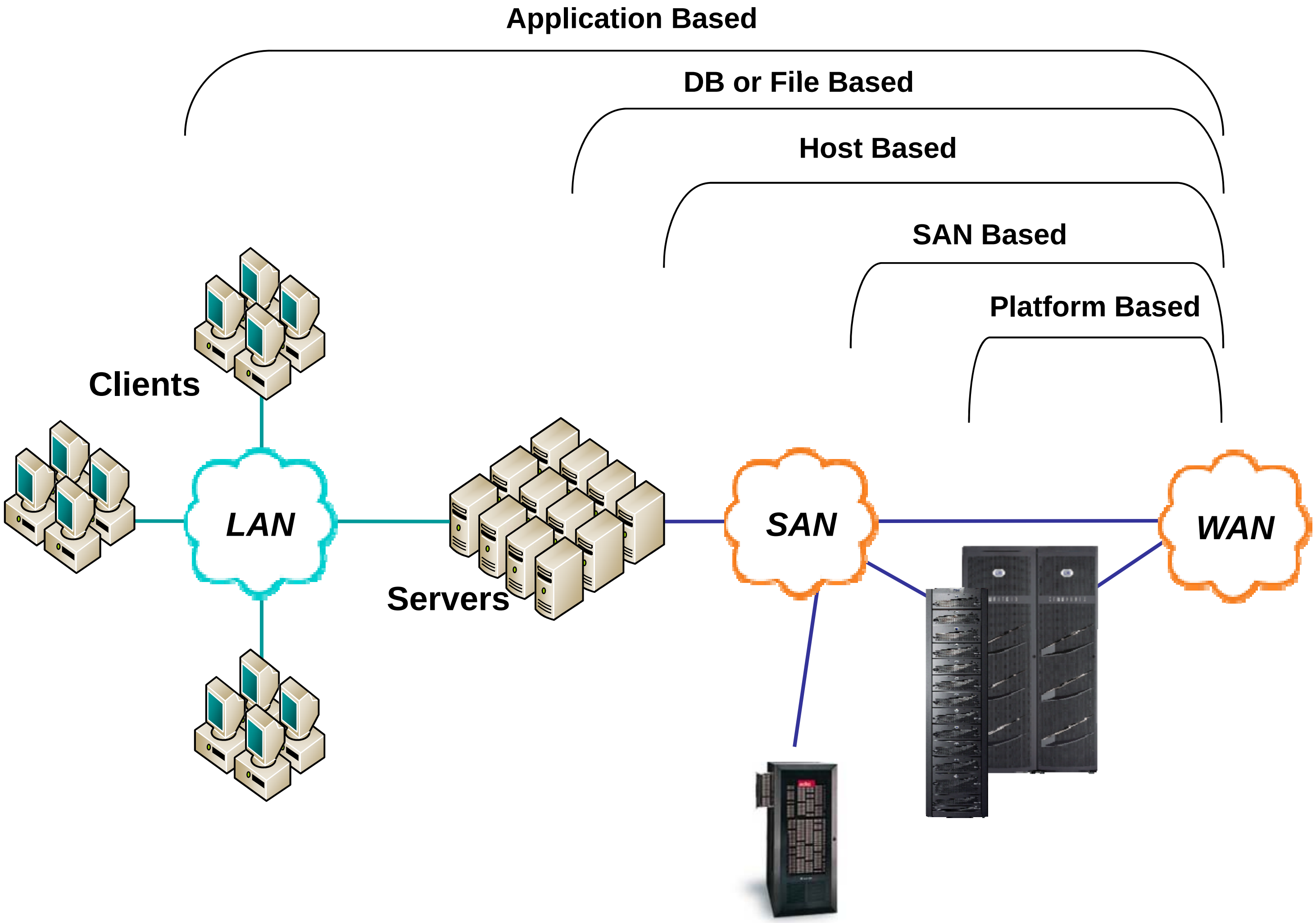
Databases & Repositories

- •SharePoint
- •Documentum
- •Microsoft Access
- •Oracle, SQL
- •Content Mgmt systems

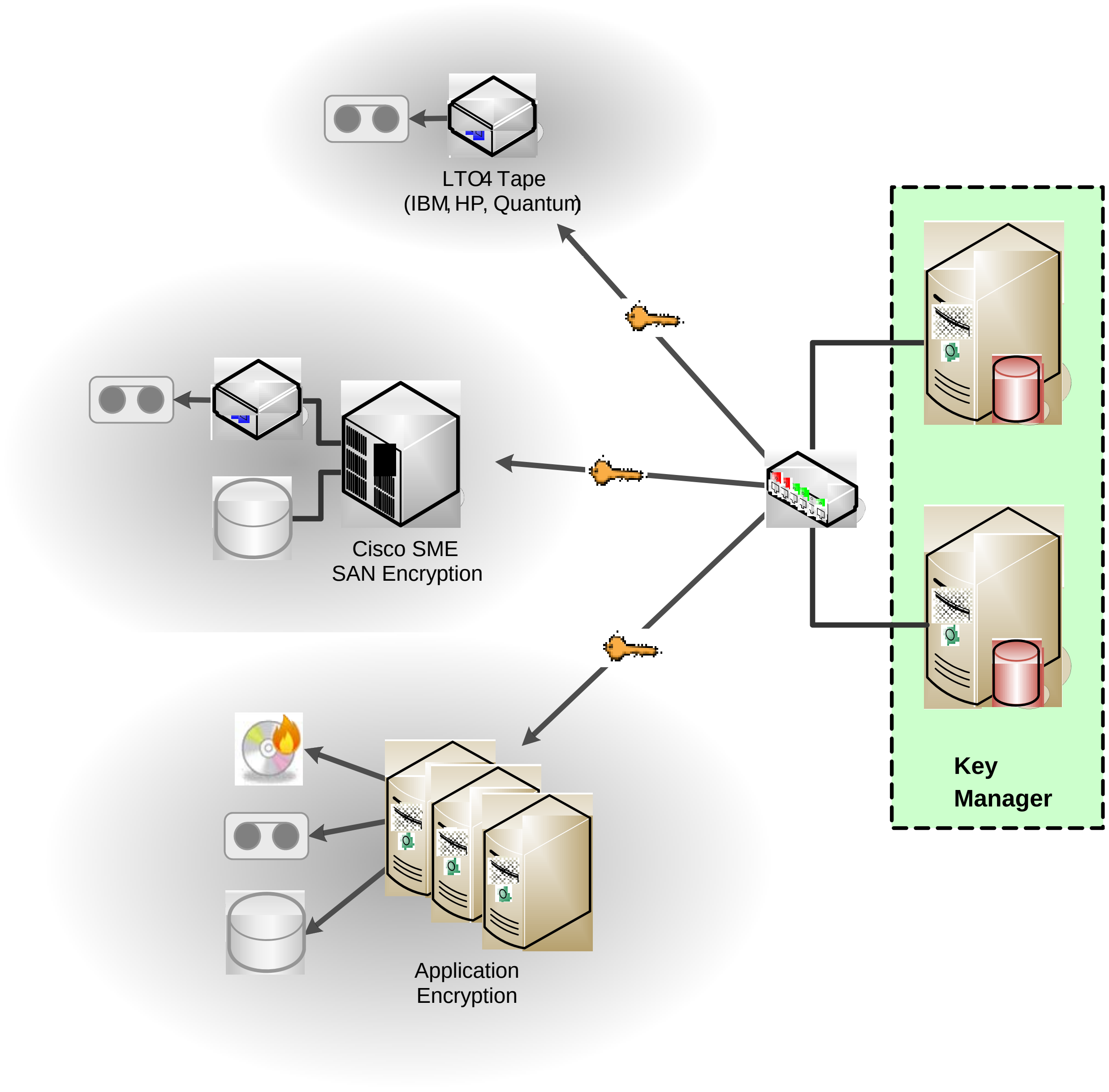
Remediation

- • Secure Delete
- • Manual/Auto Move
- • Manual/Auto Quarantine
- • Notifications
- • eDRM

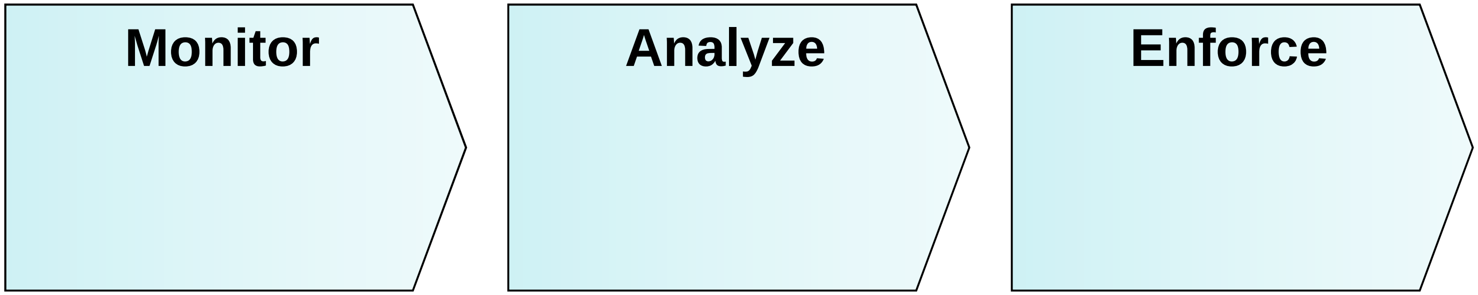
Using Encryption to Secure Data at Rest



Enterprise Key Management



Protecting Data in the Network: Data in Motion



Email

- SMTP email
- Exchange, Lotus, etc.
- Webmail
- Text and attachments

Instant Messages

- Yahoo IM
- MSN Messenger
- AOL Messenger

Web Traffic

- FTP
- HTTP
- HTTPS
- TCP/IP

Remediation

- Audit
- Block
- Encrypt
- Log

SNIA

SNW

COMPUTERWORLD

April 12-15, 2010
Rosen Shingle
Creek Resort
Orlando, Florida

Securing Data in Motion

Monitor Risk Exposure for Data in Motion

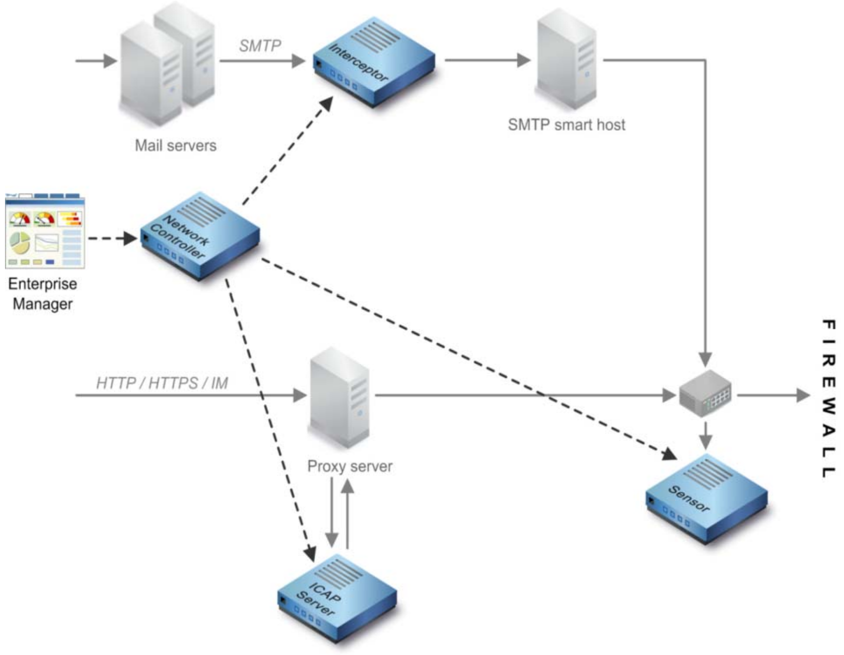
- Audit data in motion
- Notify sender of inappropriate communication
- Notify and escalate to senders manager

Prevent Risk Exposure for Data in Motion

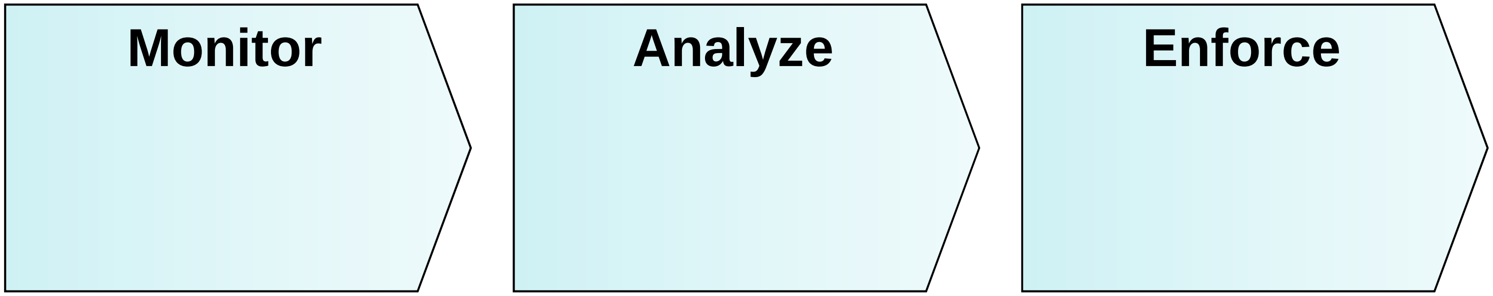
- Real-Time Blocking of Transmissions
  - Email active mode
  - Web, Secure Web and FTP active mode via Proxy's

Remediate Risk Exposure for Data in Motion

- Quarantine
  - Hold till Approved by manager, SOC, etc.
  - Sender Self Remediation (justify actions)
  - Automated timed release to prevent business impact
- Encrypt
  - Redirect to perimeter encryption engine (PGP, IronPort, etc)
- Block



Protecting Data at the Endpoint: Data in Use


Monitor

Analyze

Enforce

Print & Burn

- Local printers
- Network printers
- Burn to CDs/DVDs

USB

- External hard drives
- Memory sticks
- Removable media

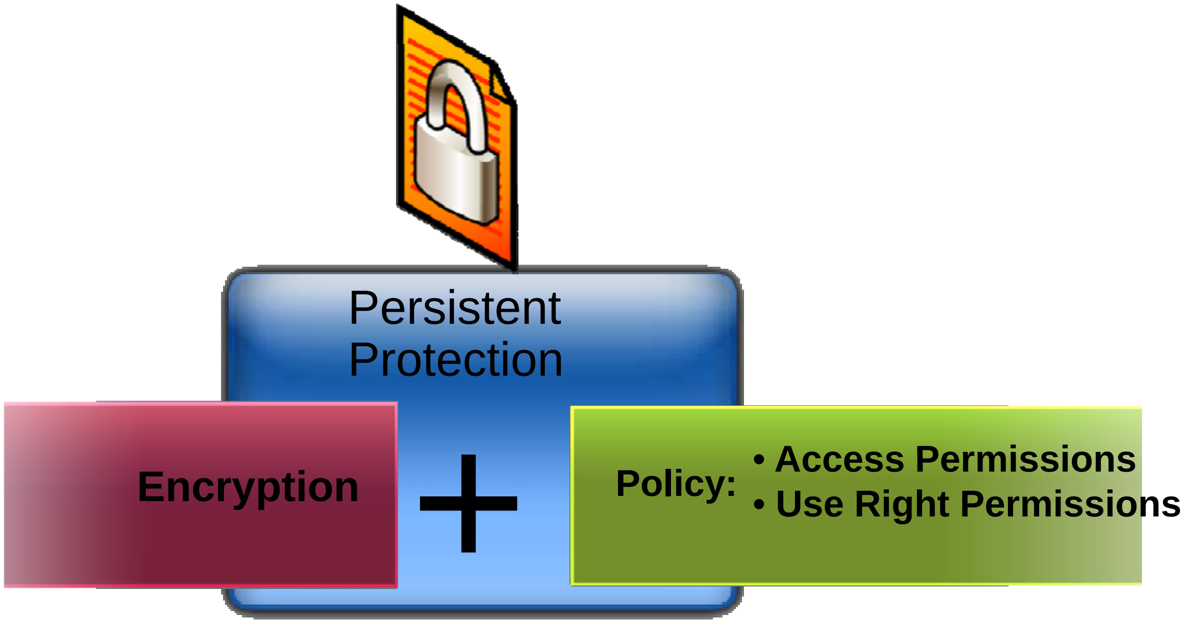
Copy and Save As

- Copy to Network shares
- Copy to external drives
- Save As to external drives

Actions & Controls

- Allow
- Justify
- Block
- Audit & Log

Rights Management Services



Persistent Protection

Encryption

+

Policy:

- Access Permissions
- Use Right Permissions

Use Case:
Protecting Data with Rights Management

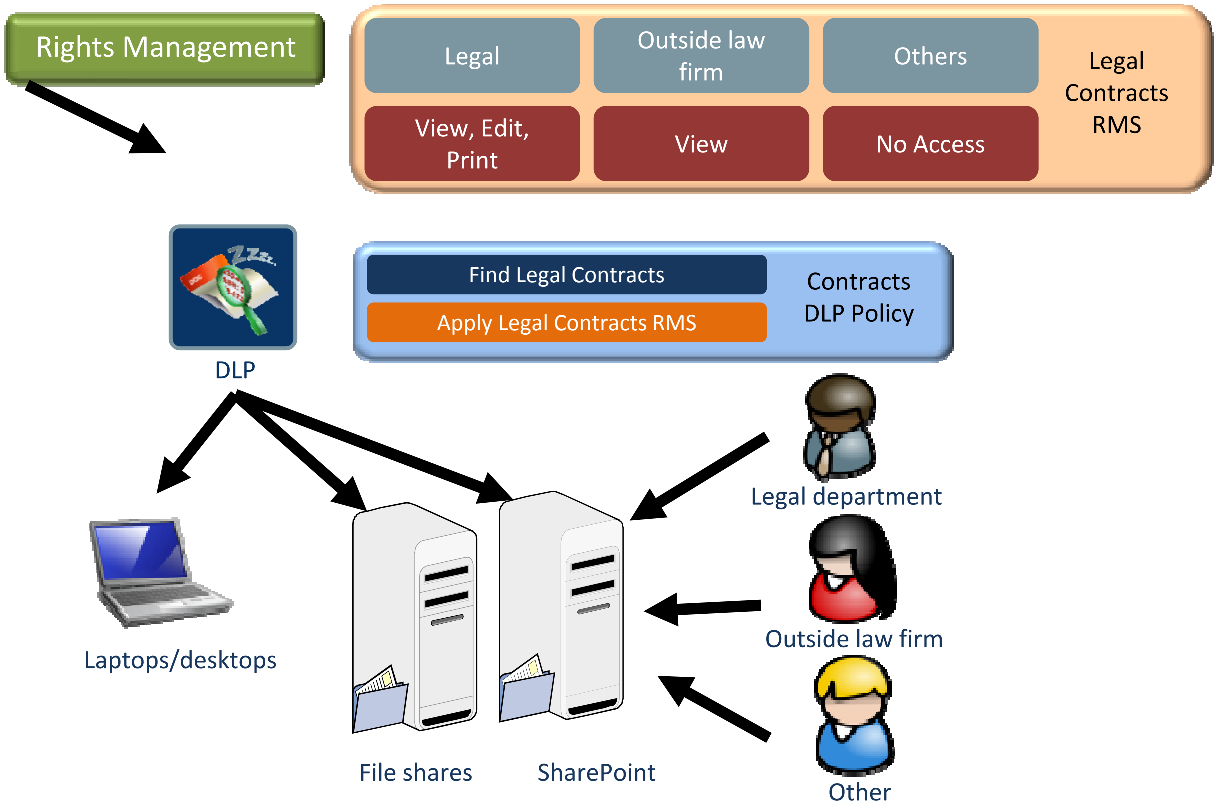
1. RMS admin creates RMS templates for data protection

2. DLP admin designs policies to find sensitive data and protect it using RMS

3. DLP discovers and classifies sensitive files

4. DLP applies RMS controls based on policy

5. Users request files - RMS provides policy based access



Rights Management

Legal	Outside law firm	Others	Legal Contracts RMS
View, Edit, Print	View	No Access	

DLP

Find Legal Contracts	Contracts DLP Policy
Apply Legal Contracts RMS	

Laptops/desktops

File shares

SharePoint

Legal department

Outside law firm

Other

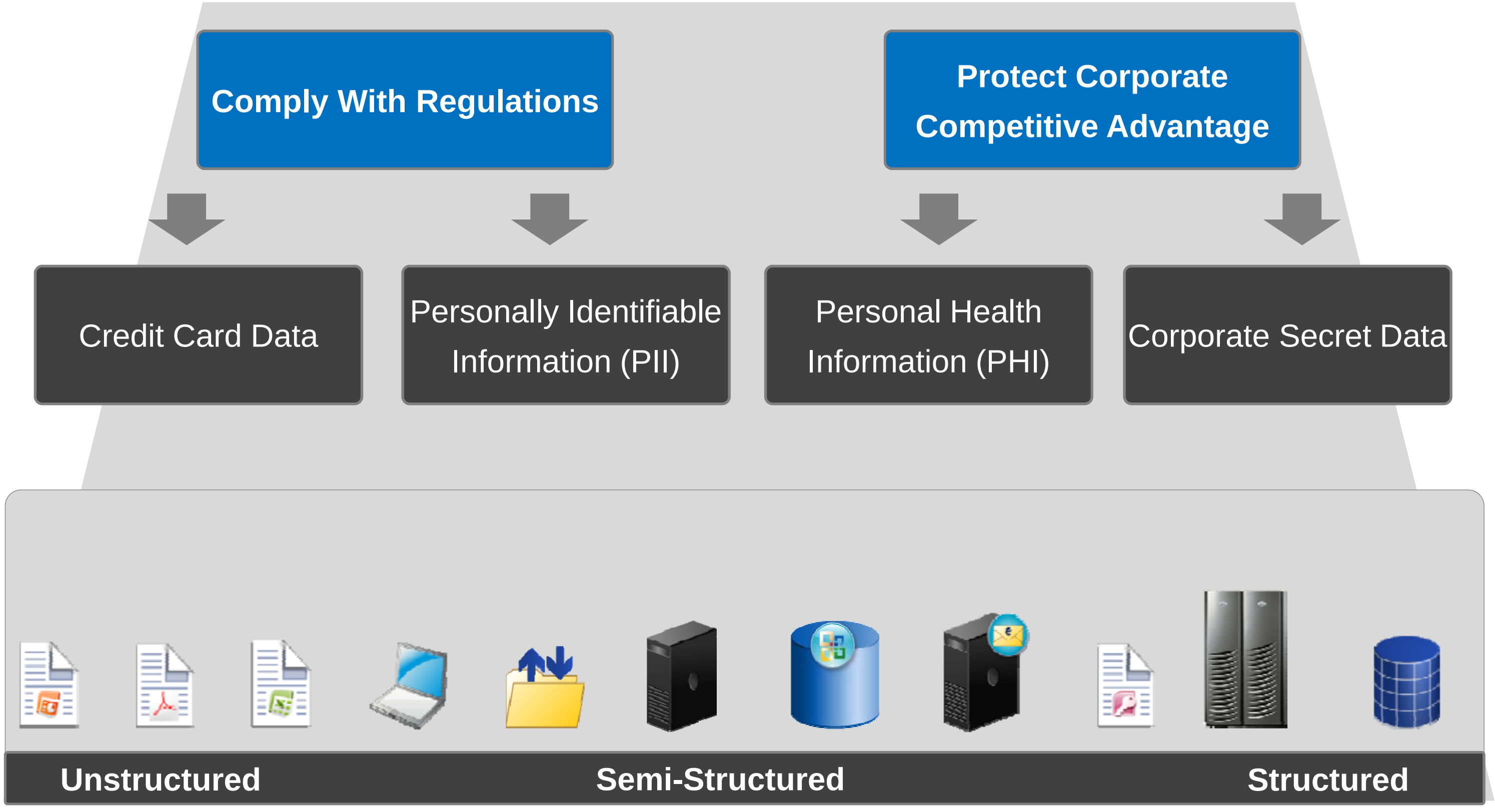
SNIA

SNW

COMPUTERWORLD

April 12-15, 2010
Rosen Shingle
Creek Resort
Orlando, Florida

Discovering, Monitoring and Managing Your Sensitive Data



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

SNIA

SNW

COMPUTERWORLD

April 12-15, 2010
Rosen Shingle
Creek Resort
Orlando, Florida

Questions?