



Preventing Enterprise Data Loss

Best Practices to Identify, Control and Manage Sensitive Data

Todd Graham, Senior Technologist, Office of the CTO
RSA , The Security Division of EMC

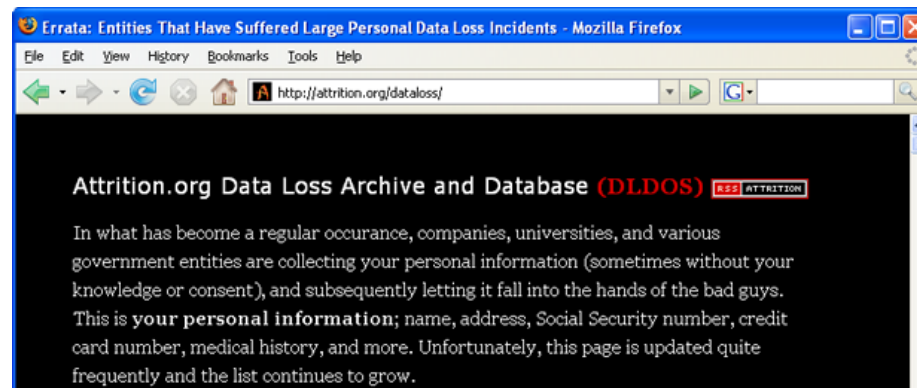
INTEROP[®]
THE LEADING BUSINESS TECHNOLOGY EVENT

DLP Defined

- Data Loss Prevention (DLP) – is technology designed to detect and potentially prevent the unauthorized transmission of information by insiders of an organization to those on the outside

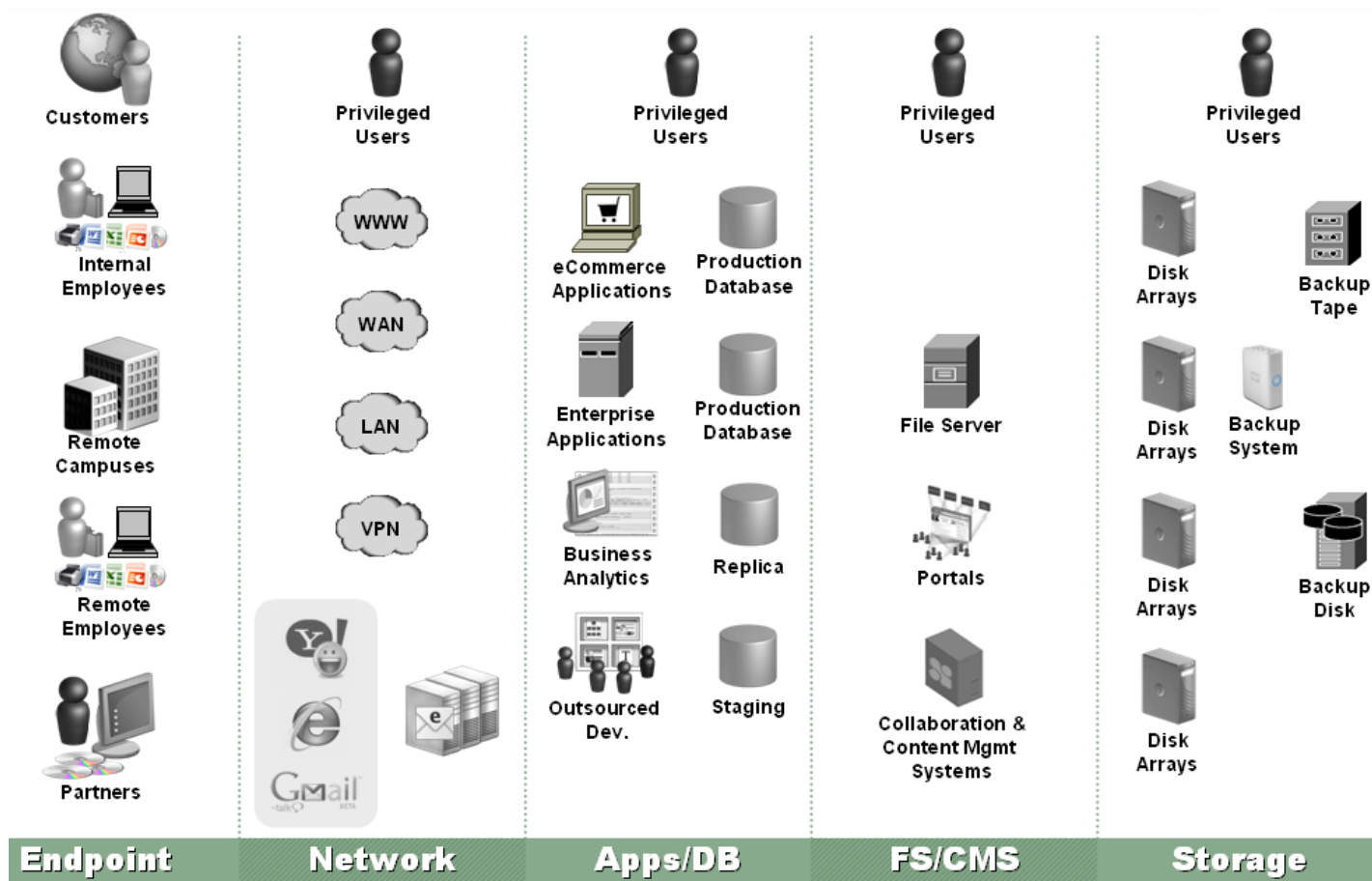
Key Business Drivers

- State Notification Laws
 - Your company's data loss is the type of coverage no one wants to see in the Wall Street Journal



- Payment Card Industry Data Security Standard (PCI DSS)

Why Is This So Hard?



Risk-based Approach



- Information-centric
 - Shows where the vulnerabilities are and clarifies business context
- Risk-based
 - Reveals a clear priority and basis for making security investments
- Framework-oriented
 - Emphasizes repeatability and re-use based on best practice frameworks

Reveals where to invest, why to invest, and how security investments map to critical business objectives

The Pay-Off

IT organizations that have taken a risk-oriented, framework-based approach have been able to reduce their number of controls by 30% to 70%*



1	Better Security Investments	Better prioritization of controls
2	Lower Compliance Costs	Fewer, more repeatable controls
3	Better Business Alignment	Shared assessment of risk

Traditional Security Model

- **Context-based**
- **Focused on external adversaries**
- **All-or-nothing approach**
- **All data treated equally**
- **Severity of threats is often binary**

*Example: if signature X on port Y then block;
or don't allow the mounting of USB drives*

Data Security Model

- **Based on the Content *and* the Context**
- **Determine the actual content affected**
- **Focused on content identification, then applying business rules to address threats**
- **Different Content *types* drive different severity and response**

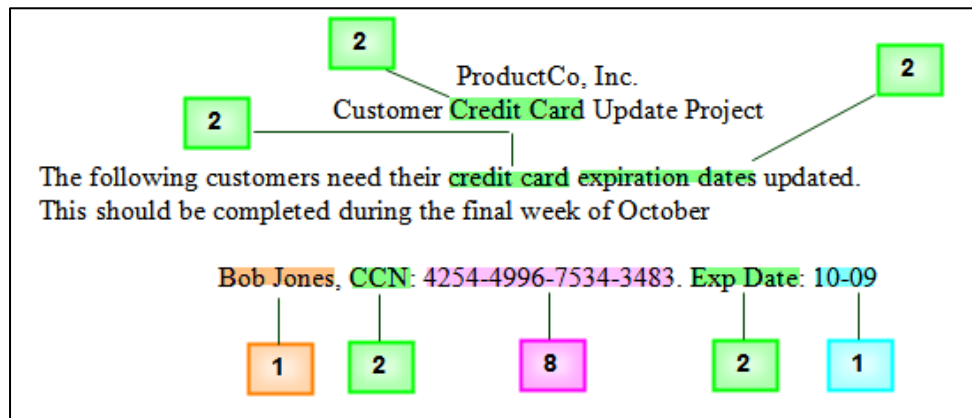
Example: if email contains PCI block; or don't allow the copying of pre-release financials to USB

Describing Data

- Technique of “describing” content using linguistic evidence
- Content Blades use described content techniques
 - Detection Rules
 - Context Rules
- Detection Rules are if/then rules
 - If the document contains “such-and-such” then it *might* be sensitive
 - Words and Phrases
 - Regular Expressions
 - Entities
 - What evidence is in the documents?
- Context Rules leverage contextual evidence
 - How does the evidence appear within the documents?

Data in Context

- Context Rules: How does the evidence appear within the document?

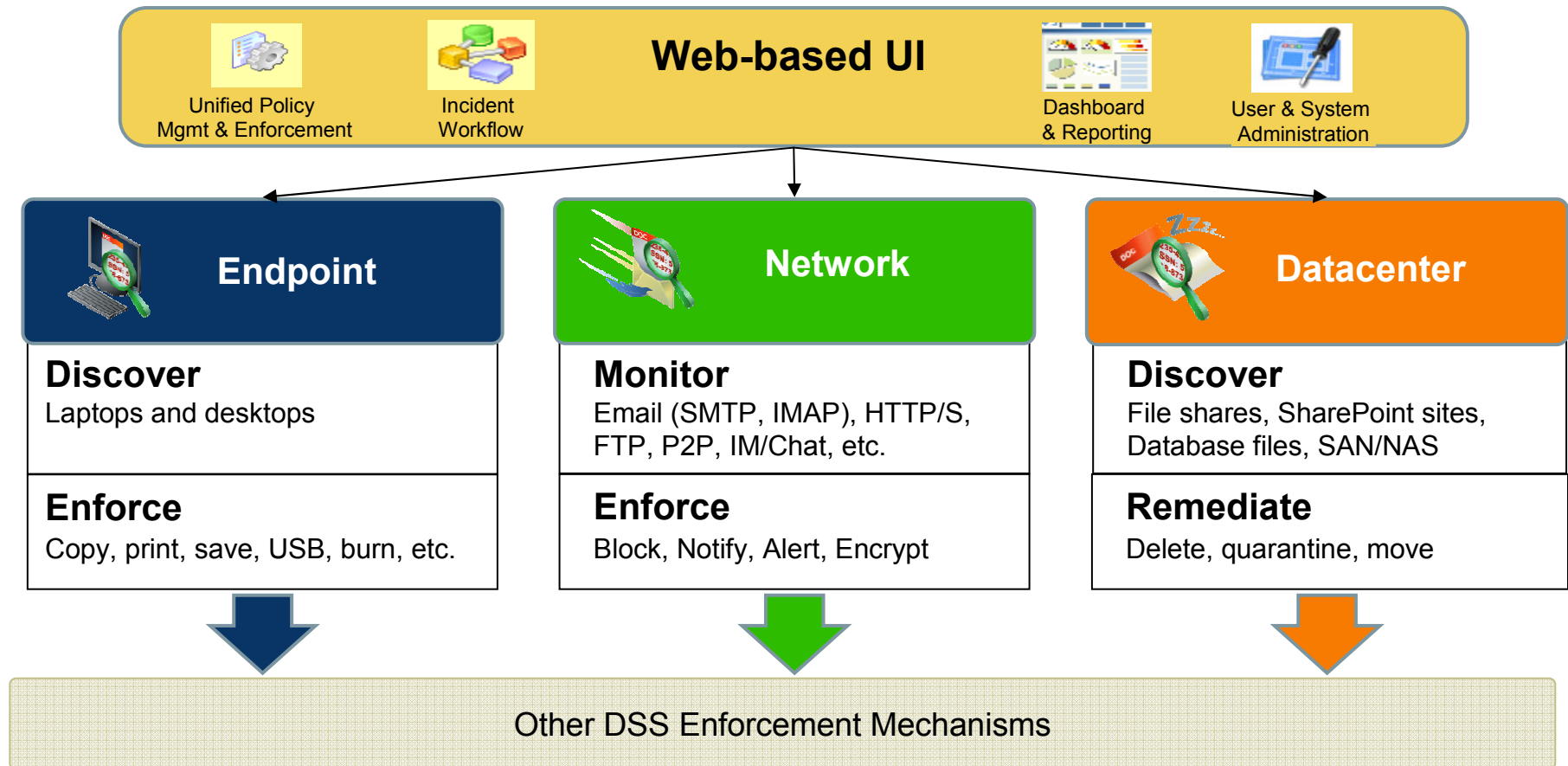


- Proximity
- Weighting
 - Document Thresholds
- Grouping detection rules
 - Minimum Unique Matches
 - Required Matches

The Toolset

- **Discovery – Data At Rest**
 - Scan laptops, desktops, and file servers for sensitive information
 - Locate and remediate sensitive content stored across enterprise
 - Determine proper access controls, and encryption strategy
- **Network – Data In Motion**
 - Monitor and secure content moving across the network
 - Multiple protocol inspection (email, web, IM, etc.) for sensitive information
 - Block policy violations based on content exiting the enterprise
 - Opportunistically encrypt information as it leaves – limit user impact
- **Desktop – Data In Use**
 - Monitor and control sensitive content in use on workstations
 - Transparently enforce policies based on content
 - Coverage for actions like print, screen capture, burn to CD/DVD, copy to USB, etc.
 - Integration with secure devices and encryption technologies to enforce written policies

DLP Architecture



The Process

- Most enterprises...
 - know they have data
 - believe there is value associated with their data
 - suspect they know what data is valuable
 - know where core valuable information is probably stored
- Most enterprises do not...
 - know the different values assigned to data by disparate groups
 - know who's creating the data
 - where all the data is being stored
 - how derivatives are being used
 - where their data is at risk

The Process continued

- Not all data created by an enterprise is equal and shouldn't all be treated the same
- Engagement with business units is critical to determine their sensitive data – it may surprise you
- Simple litmus test: if this left the organization would you be worried? To what degree?
- Refine and bucket cross-organization data types
- Initial focus on the highest risk data bucket
- With organizational buy-in remediation is easier

Case Study 1

Challenge

- Protecting HBI (high business impact) data
 - PII, PCI & Intellectual Property
- Concerned with competitive risk and regulatory exposure
- Exponential growth has scattered data throughout the company
 - 30,000 file shares,
120,000 SharePoint sites

Results

- Leveraged Discovery technology
 - Scanned 12 TB of data on all file shares in 9 days
 - Completed follow-up incremental scan completed in 1/2 day
- Established proactive and continuous process for locating and protecting confidential data (HBI)
- Reduced competitive risk and regulatory exposure
- Confident executive reporting and employee protection

Case Study 2

Challenge

- Level 1 Processor of credit cards, concerned with risk of PCI-DSS non-compliance
- Impending PCI audit, must demonstrate compliance
- Transmit 1M+ emails per day, ~2,000 contain sensitive data
- Must protect high visibility brand

Results

- Deployed network DLP w/encryption for email
- Consistently achieve 99.8% accuracy detecting PCI data
- Automatically encrypt email transmissions containing PCI data
- Effectively passed PCI audit

A Pragmatic Approach

- **Determine which regulations and policies are driving you**
 - Don't try to boil the ocean; pick a handful of high impact areas of concern
 - What will get (or has) budget is the best place to start
- **Tackle the different areas of loss in a sequential, strategic manner**
 - Discovery
 - Network
 - Desktop
- **Deploy a POC**
 - Actually use the tools in that time
 - Understand the management impact
 - Tune policies and expectations
- **Don't bother with any of this unless your organization is willing to change!**

A Parting Thought...



"We've considered every potential risk except the risks of avoiding all risks."

Thank You

Questions?

todd.graham@rsa.com

INTEROP