Minimizing the Risk of Data Loss in Mobile Environments

Scott Shepard
Principal Consultant
GlassHouse Technologies
Agenda

- Data Centric Security Strategy
  - Protecting “Data of Concern”
  - Enhanced Protection for Tiers
- Data Loss Prevention (DLP) Strategy
  - Objectives
  - Requirements
- Solutions
  - Enterprise Digital Right Management (EDRM)
  - Pure-Play DLP Technology
- Lessons Learned
• Data Protection Policy
  – Policy focuses efforts on protecting “data of concern”
  – Policy drives data classification

• Data of concern
  – The small percentage of data where protection is required by law, regulation, or company policy
  – Private Data, Regulated Data, Intellectual Property / Trade Secret

10-15% is “Data of Concern”
Data-Centric Security: Protection Strategy

- Minimum security for all data regardless of asset value
- Enhanced Protection for high value assets
Data-Centric Security: Network Architecture

- VPN Tunnel
- Low Value Utility Servers
- Mobile User
- Internet Lab
- Engineering
- Data Repository
- DMZ
- End Users
- Intranet
- Internet
Agenda

• Data Centric Security Strategy
  – Protecting “Data of Concern”
  – Enhanced Protection for Tiers

• Data Loss Prevention (DLP) Strategy
  – Objectives
  – Requirements

• Solutions
  – Enterprise Digital Right Management
  – Pure-Play DLP Technology

• Lessons Learned
DLP Strategy: Objectives

- Align with Data-Centric Security strategy
- Identify data of concern
- Understand the data of concern life cycle
- Increase end user awareness and ownership
- Eventually protect it
DLP Strategy: Requirements

- Protection
  - Secure data regardless of where it resides
  - EDRM technology
    - Product design
    - Key financial information
    - Senior management communication

- Detect and Respond
  - Trust but verify
  - Pure-play DLP technology
    - Discover
    - Monitor
    - Block unauthorized disclosure
Agenda

- Data Centric Security Strategy
  - Protecting “Data of Concern”
  - Enhanced Protection for Tiers
- Data Loss Prevention (DLP) Strategy
  - Objectives
  - Requirements
- Solutions
  - Enterprise Digital Right Management (EDRM)
  - Pure-Play DLP Technology
- Lessons Learned
• Multi-tiered architecture
  - HTTP access in DMZ that allows for connectivity from business partners, mobile users
  - Connectivity to internal LDAP for authorization and authentication
• Client distributed to end points
EDRM: Key Processes

• Access and rights management
  – Limit the number of roles
    • Policy administration
    • Read and write content rights
    • Read only content rights
  – Leverage roles across all projects
• Integrate with business processes
• Validate
EDRM: Deployment

- Multiple Deployments
  - Engineering:
    - Protection of Pro/Engineer CAD through Windchill
    - CAD shared with Outsourced manufacturer
    - ERM Developed a customized wrapper around Windchill in 8 months
    - Delays associated with getting encryption technology approved
    - Completed pilot, but not scalable.
  - Finance:
    - Protection of financials
    - Successfully completed pilot, worked as advertised
EDRM: Lessons Learned

- EDRM technology still immature
  - Problem with updates to applications
  - Multiple application channels accessed data
- Delays with country encryption Laws
  - EDRM vendor was not experienced in working in a global environment.
- Worked very well with internal financial documents
- Problem protecting unstructured data
- Lacked accountability and responsibility
  - No benefit from outsourced manufacturer
  - Hindrance for internal employees
Agenda

• Data Centric Security Strategy
  – Protecting “Data of Concern”
  – Enhanced Protection for Tiers

• Data Loss Prevention (DLP) Strategy
  – Objectives
  – Requirements

• Solutions
  – Enterprise Digital Right Management (EDRM)
  – Pure-Play DLP Technology

• Lessons Learned
- Network monitoring of email and web traffic at Internet perimeter
- Future: Network monitoring at internal network segmentation border
- DLP discovery scanning of known file servers
- End Point DLP monitoring
DLP Technology:
Key Processes

- Information classification process
  - Document Tagging for unstructured data
    (Project Name, unique identifier, date)
  - Subject matter experts for free form usage of unstructured data

- Detect and response process
  - Training the monitoring team
    - Higher-skilled monitoring staff
    - Understand the business context
  - Integration with business process
  - Maintain a knowledge base
DLP Technology: Deployment

- Privacy implications for multinational organizations
  - Is it worth the effort to monitor?
  - Consult your legal department
  - Budget 3rd party council

- Legal limitations
  - Known blind spots in monitoring SSL traffic
DLP Technology: Lessons Learned

• Set Reasonable Expectations
  – May not be able to prevent leakage
• Span port noise
• Start small and controllable
• Increased Awareness
  – Driving accountability and responsibility
  – Improve understanding of privacy regulations
Conclusion

• Both technologies are maturing
  – Great deal of improvement in last 2 years
  – Monitoring has proven more successful in our environment

• In the end it is all about the person
  – Rewarding accountability and responsibility