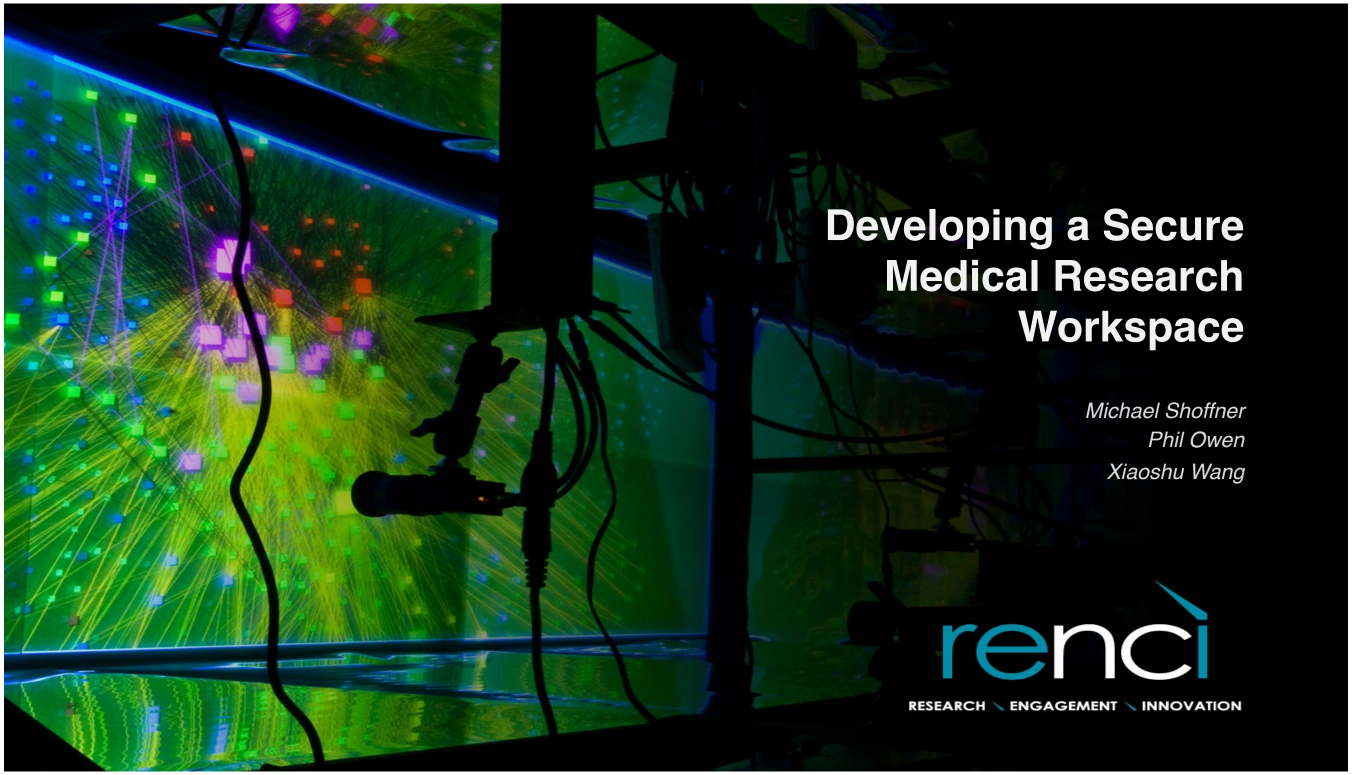


# Developing a Secure Medical Research Workspace

*Michael Shoffner*
*Phil Owen*
*Xiaoshu Wang*

renci

RESEARCH ENGAGEMENT INNOVATION

# Collaborators

CTSA Clinical & Translational Science Awards ®

NC TraCS Institute

renci

UNC School of Medicine

UNC School of Information and Library Science

UNC Hospitals

The Clinical and Translational Science Awards (CTSA) is a registered trademark of DHHS; All logos are the property of their respective owners

# Team

- Javed Mostafa (PI – SILS, NC TraCS)
- Charles Schmitt (RENCI)
- Brent Lamm (NC TraCS)
- Michael Shoffner (RENCI)
- Phil Owen (RENCI)
- Xiaoshu Wang (RENCI)
- Casey Averill (RENCI)
- Ray Diorio (NC TraCS)
- Ken Langley (SOM)
- Erik Scott (RENCI)

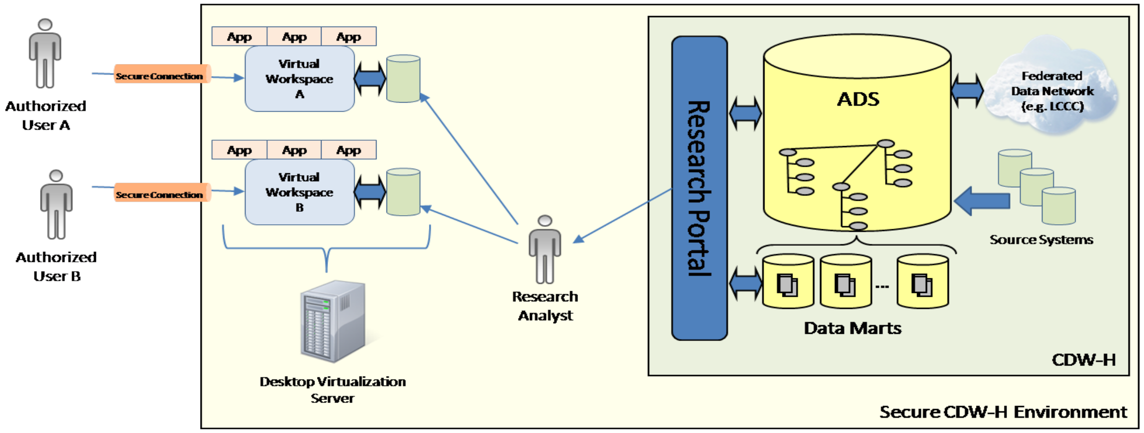
# Drivers

❑ Protected Health Information (PHI) data must always be protected.

❑ Lack of a security solution for working with PHI impedes medical and translational research.

# Vision (I)

Provide convenient, secure access to PHI CDW-H for UNC healthcare professionals and researchers.



# Vision (II)

Produce a model system plan and architecture for dissemination.

photo: guy schmidt

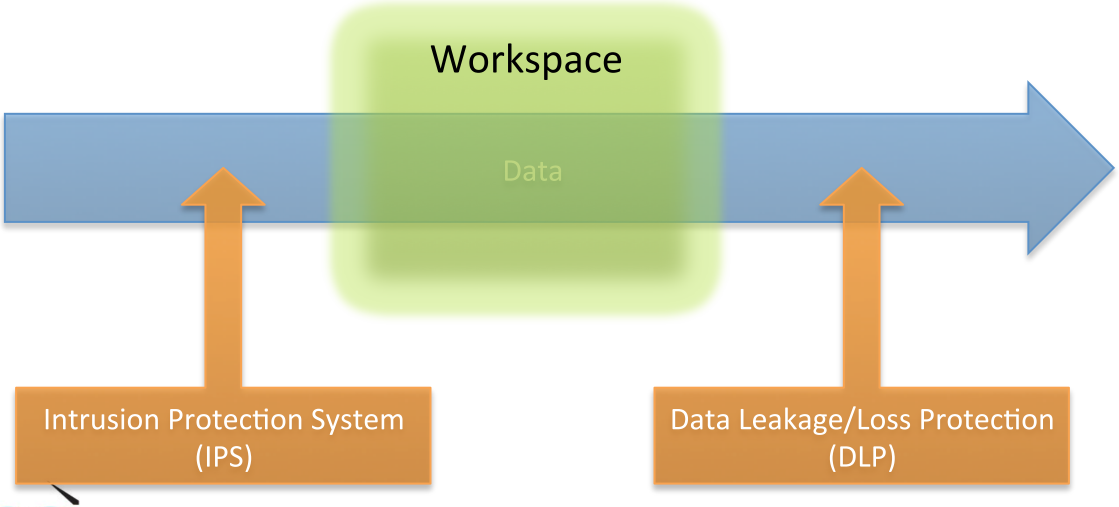
# Vision (III)

- Maintain a testbed for ongoing development
  - – In partnership with NC TraCS, SOM, ISD, and ITS.

# Strategy

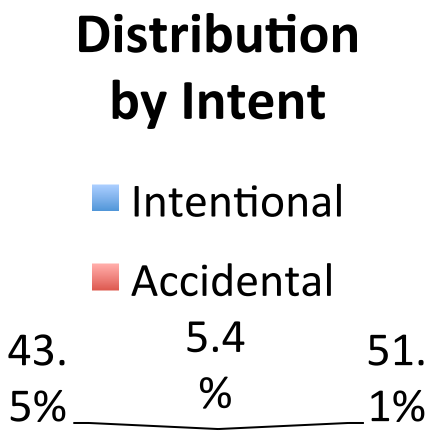
- "Defense in Depth" philosophy
- Development
  - Prefer COTS/vendor solutions
  - Integrate (limited) custom code
- Track ongoing security research
- Test, test, and test again

# Security Landscape


Workspace
Data
Intrusion Protection System (IPS)
Data Leakage/Loss Protection (DLP)

# Definitions

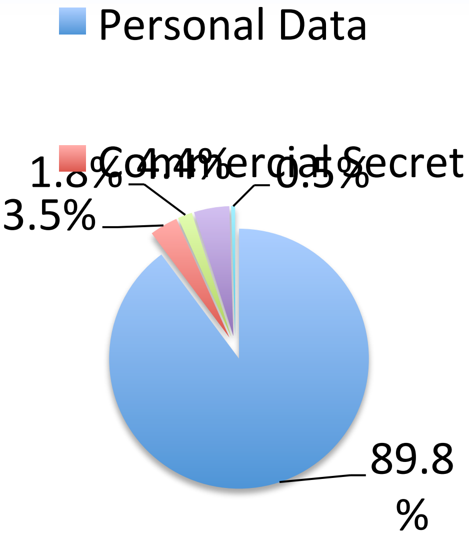
- **Data Leakage**: *Unauthorized* transmission of data from within an organization to an external destination or recipient.
  - Unauthorized ≠ Intentional or malicious
  - Unintentional or inadvertent leakage is also unauthorized



*Infowatch.com: Global Data Leakage Report 2009*

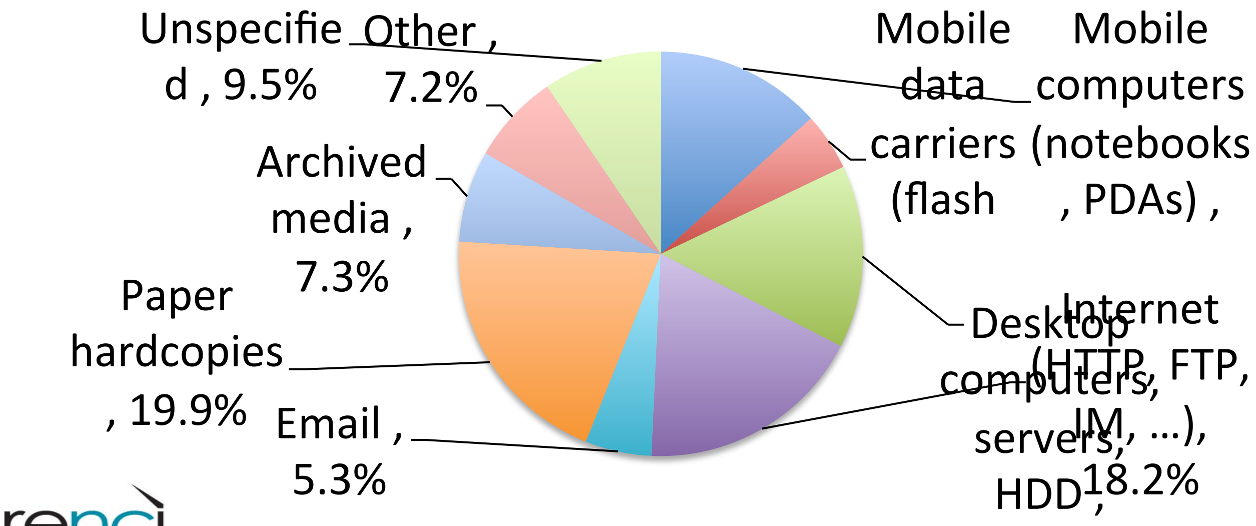
# Types of Leaked Data

- Private identifiable information (PII)
  - Private but not secretive
  - Examples: SSN, Patient’s medical billing code
- Intellectual Property
  - Things of secretive nature
  - Example: source code, design, pricing information



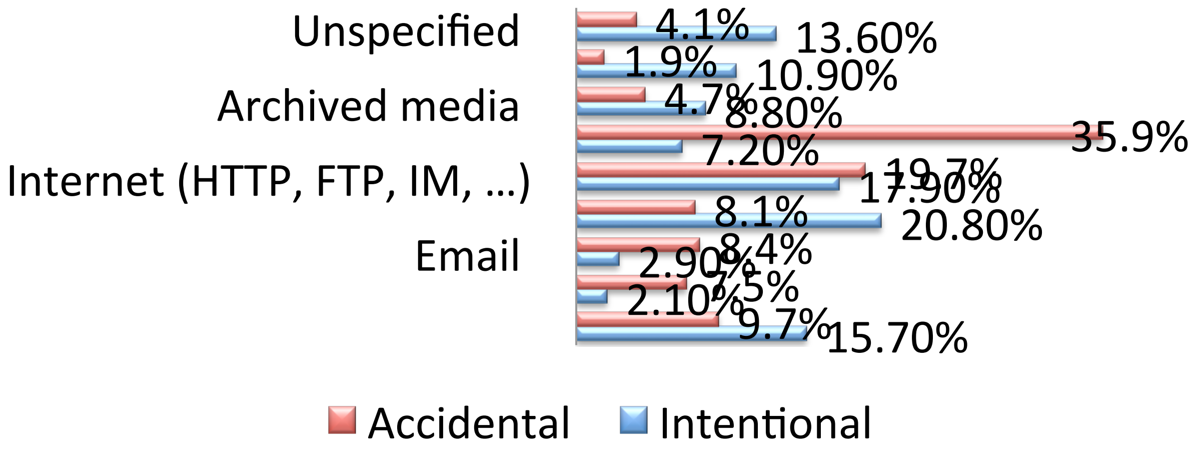
*Infowatch.com: Global Data Leakage Report 2009*

# Leakage by Channels

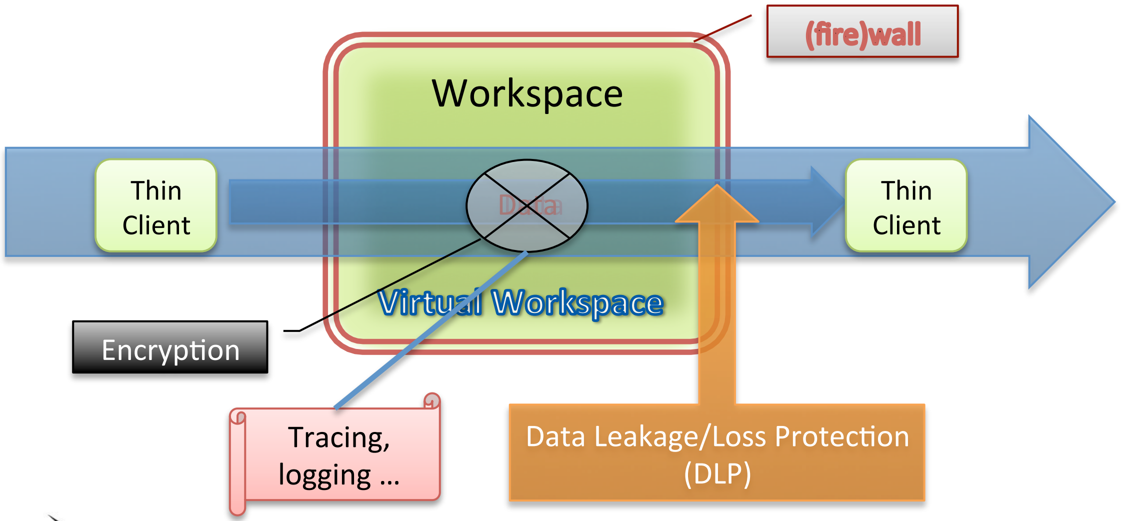


*Infowatch.com: Global Data Leakage Report 2009*

# Leakage by Channel/Intent



# Counter Measures



(fire)wall

Workspace

Thin Client

Data

Thin Client

Virtual Workspace

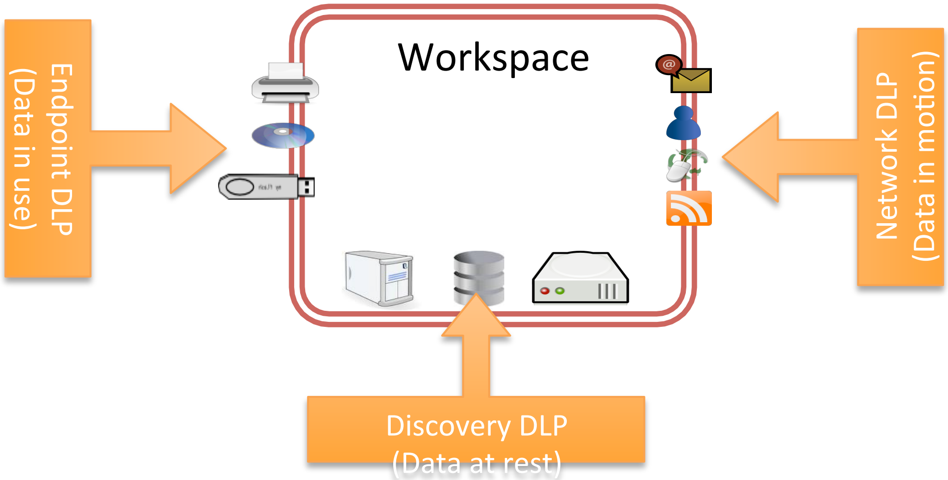
Encryption

Tracing, logging …

Data Leakage/Loss Protection (DLP)

renci

# DLP Channels



Workspace

Endpoint DLP
(Data in use)

Network DLP
(Data in motion)

Discovery DLP
(Data at rest)

# Network DLP

- Bridge-based
  - Inspected at the packet level
  - Protocol agnostic
  - Ineffective b/c limited action
- Proxy-based
  - Message queued at proxy for inspection
  - Respond properly according to different protocols
  - Integrates with existing web gateway via iCAP

# Discovery DLP

- Scan sensitive data on
  - Servers
  - Databases
  - File servers
  - SAN and NAS
- Server or Agent based
- Discovery DLP is not just a scan, it can react according to predefined policies

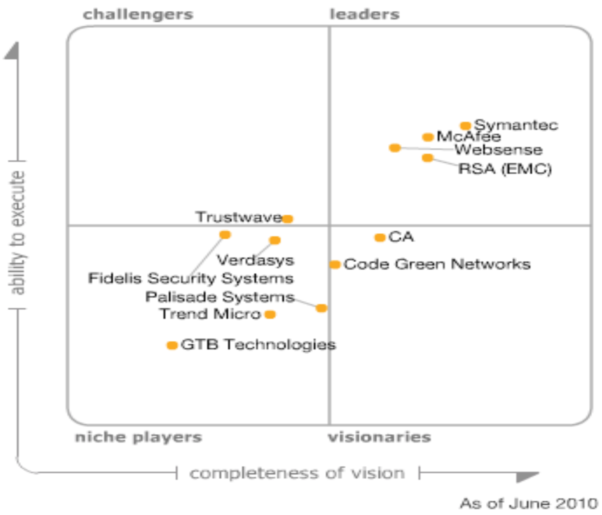
# Endpoint DLP

- Enforces policies at the endpoint
- Monitors and prevents data movement to common vectors
- Endpoint DLP plugs into OS kernel to monitor
  - File movement
  - Copy/paste
  - Printing
  - Etc.

# DLP Method

- Understand
  - Data transportation protocols
  - Data formats
  - Encryption/Decryption techniques
- Algorithms
  - Keywords
  - Regular Expressions
  - Fingerprinting (Full, partial hash matching)
  - Statistical analysis
  - Conceptual Lexicons

# Vendors



*Gartner Report: Magic Quadrant of DLP Vendors*

# SMRW Environment and Technology

Objective:

- Provide and facilitate a working environment for researchers that protects sensitive healthcare information.

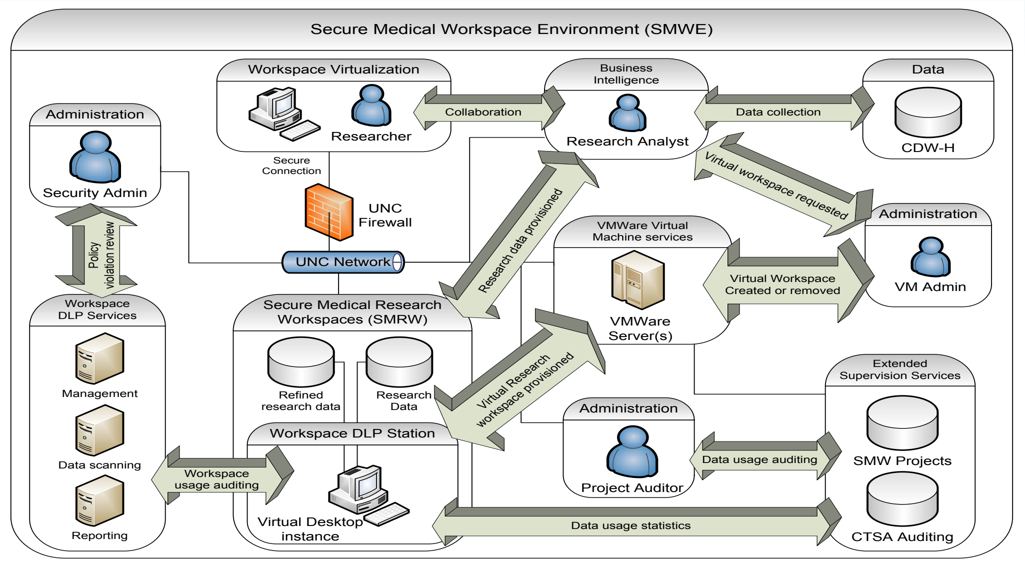
The workspace environment will provide the researcher with:

- A protected environment.
- Provisioned information gathered from various sources.
- Tools to work with the provisioned data.

The workspace will provide analysts and administrators:

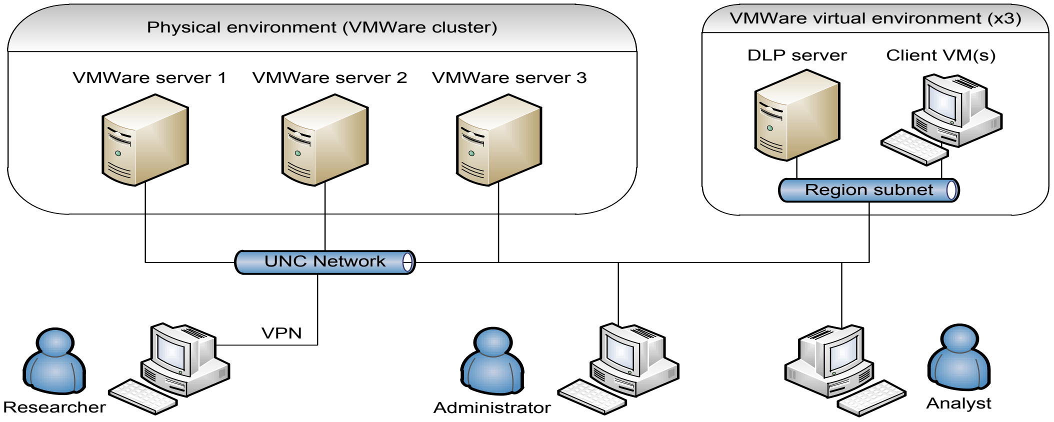
- Security auditing capabilities.
- Research data usage metrics.

# Logical Architecture

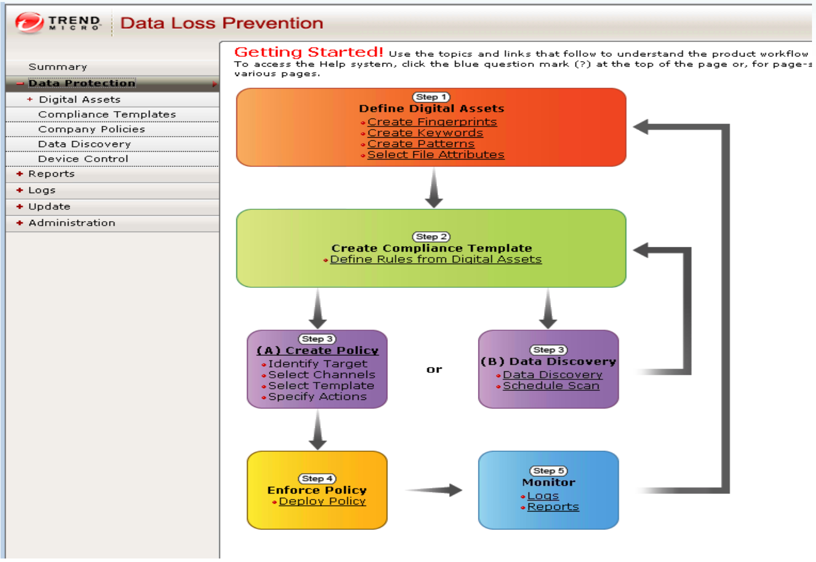


renci

# Physical Layout



# Screenshot – Trend Micro server



Getting Started! Use the topics and links that follow to understand the product workflow
To access the Help system, click the blue question mark (?) at the top of the page or, for page-s
various pages.

Step 1
**Define Digital Assets**
- Create Fingerprints
- Create Keywords
- Create Patterns
- Select File Attributes

Step 2
**Create Compliance Template**
- Define Rules from Digital Assets

Step 3
**(A) Create Policy**
- Identify Target
- Select Channels
- Select Template
- Specify Actions

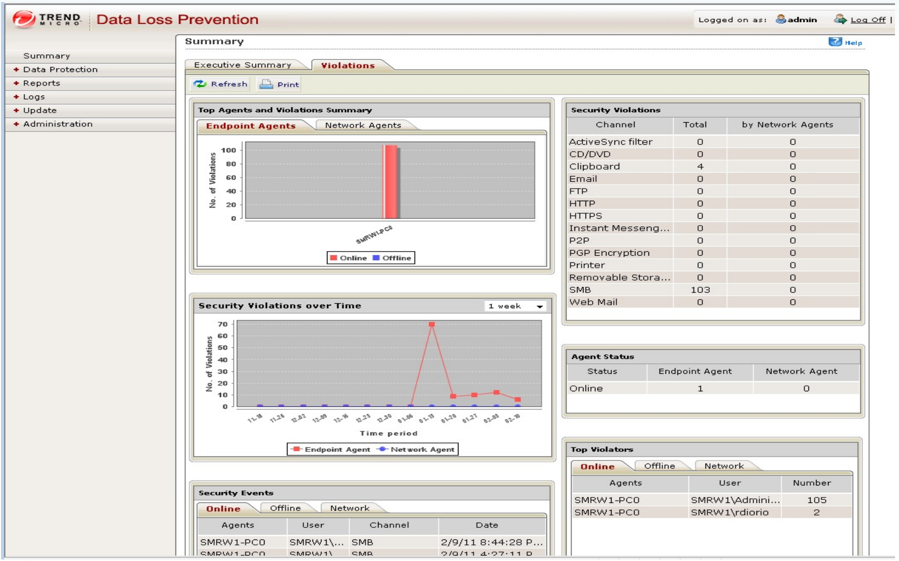
or

Step 3
**(B) Data Discovery**
- Data Discovery
- Schedule Scan

Step 4
**Enforce Policy**
- Deploy Policy

Step 5
**Monitor**
- Logs
- Reports

# Screenshot – Trend Micro server



**Security Violations**

| Channel | Total | by Network Agents |
|---|---|---|
| ActiveSync filter | 0 | 0 |
| CD/DVD | 0 | 0 |
| Clipboard | 4 | 0 |
| Email | 0 | 0 |
| FTP | 0 | 0 |
| HTTP | 0 | 0 |
| HTTPS | 0 | 0 |
| Instant Messeng... | 0 | 0 |
| P2P | 0 | 0 |
| PGP Encryption | 0 | 0 |
| Printer | 0 | 0 |
| Removable Stora... | 0 | 0 |
| SMB | 103 | 0 |
| Web Mail | 0 | 0 |

**Agent Status**

| Status | Endpoint Agent | Network Agent |
|---|---|---|
| Online | 1 | 0 |

**Top Violators**

| Agents | User | Number |
|---|---|---|
| SMRW1-PC0 | SMRW1\Admini... | 105 |
| SMRW1-PC0 | SMRW1\rdiorio | 2 |

**Security Events**

| Agents | User | Channel | Date |
|---|---|---|---|
| SMRW1-PC0 | SMRW1\... | SMB | 2/9/11 8:44:28 P... |
| SMRW1-PC0 | SMRW1\ | SMB | 2/9/11 4:27:11 P |

# Future Directions

- Automated virtual environment creation capabilities.
- Fabian Monrose (UNC CS)
  - Auditing
  - Security and forensics
- Elisa Bertino (Perdue CS, CERIAS)
  - Security policies

# Wrap-up

- Questions and comments