# How to Lock Down Data in Motion

Tom Bowers
Managing Director
Security Constructs LLC

Technical Editor
Information Security Magazine
SearchSecurity.com

# Contents

- Business drivers
- The strategic architecture
- The content protection layers
- Evaluating technologies
- Active protections
- Enabling technology
- Passive protections
- Conclusions

# Business Drivers

- Intellectual property
- Information leakage egress points
- Forensics
- Regulations
- eDiscovery

Steptoe and Johnson International Attorneys
eCommerce Law Weekly Newsletter
www.steptoe.com/publications-signup.html

# eDiscovery – The Framework

- New Rules December 2006
- Amendment to the Federal Rules for Civil Procedure
- Prior rules were based on paper evidence which was not a good fit for electronic data
- Four Major Components
  - Document Retention Policies and Requirements
  - Electronic Discovery
  - Cost allocation of electronic discovery
  - Spoiling evidence and consequences
- Guidance Software – Encase Forensics

# eDiscovery - Data Sources

- LAN
- WAN
- Active Data
- Stored Data
- Metadata***
  - Now legally searchable
  - Likely to a huge area of legal vulnerability
- Legacy Data
  - Stored on outdated hardware or software
- Residual data***
  - Deleted data that may be retrieved via an undelete command

# Strategic Architecture

1. Policies: Practical and legal framework.
2. Procedures: Meet policy guidelines operationally.
3. Contracts: Legal framework for using corporate intellectual property.
4. Vendor selection: Standard testing protocol for vendor / product selection.
5. Auditing: Ensures that all stated policies and procedures are being followed.
6. Active protections: Those technologies and business processes that dynamically protect content (encryption, port control…).
7. Passive protections: Technologies and business process that provide monitoring, investigation or auditing of content usage.

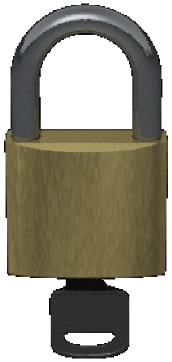
# The Technologies

- Evaluating technology
- Active Protections
- Enabling Technologies
- Passive Protections

# Evaluating Technology/Evaluation Criteria

- Installation
- Initial configuration
- Scalability
- Management/ Administration
  - *Usability, Adjustments, Helpdesk, Admin time required to operate, Training*
- Reporting
- Documentation
- Integration into other security or networking systems
- Security of the device

# Active Protection



- Encryption (Utimaco, Safeboot, GuardianEdge)
  - Full disk
  - PCMCIA encryption cards
  - TPM encryption chips
- Digital Rights Management (Authentica, Liquid Machines, Sealed Media)
- Secure Storage Devices (RedCannon, Kanguru, Kingston)

•Port Control (Safend, SecureWave)
•Mobile Device (Nokia, Credant)

# Enabling Technology

## Identity Management

- User identity across devices
- Framework for use with outsourced partners
- Easier auditing
- Better reporting

# Passive Protection

## Content Monitoring – What to Evaluate

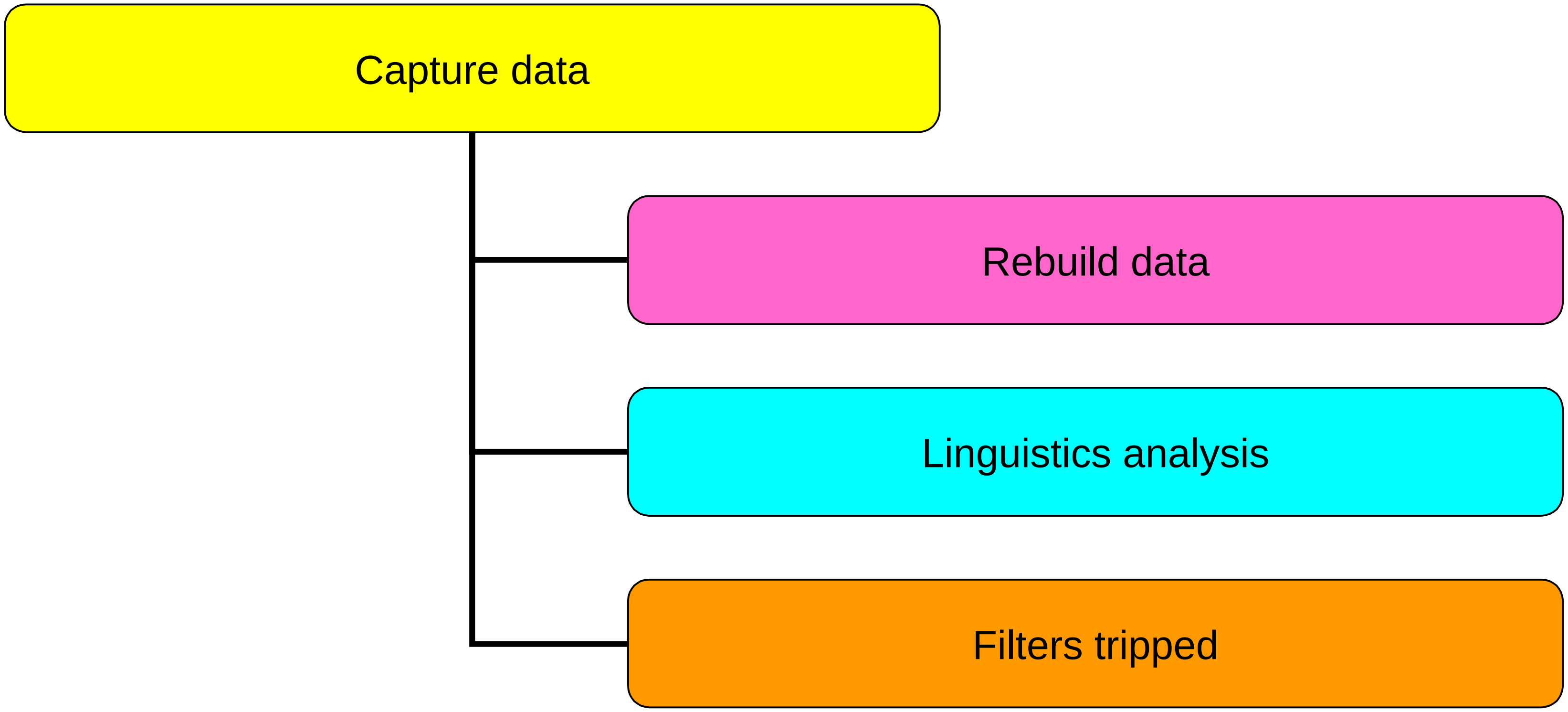
- Percentage of internet traffic monitored
- Internal versus external network
- Ports agnostic
- Linguistics analysis
- Forensic capability
- Policies and filters
- Reports
- Ease of use

Vendors to watch:
Reconnex
Code Green
GTTB
Tablus (now RSA)
Vericept

Where it all began:
Vontu (Symantec?)

# The Specifics

## Content Monitoring Overview



Capture data

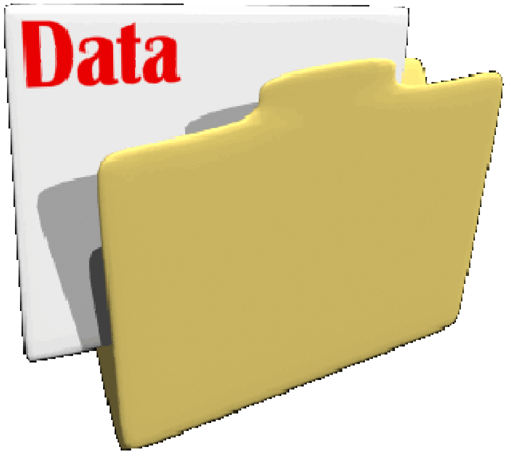
Rebuild data

Linguistics analysis

Filters tripped

# Content Monitoring Overview

## Protocols and Data Types



- HTTP
- HTTPS
- Telnet
- SSH
- SMTP
- POP3
- Webmail
- PCAnywhere
- VNC
- IM
- Citrix
- FTP...

- DOC
- PPT
- PDF
- XLS
- ASCII
- JPEG
- GIF
- BMP
- MPEG...

# Conclusions

- Wide range of business drivers
- Review the new eDiscovery rules
- Build your architecture
- Use both innovative and mature technologies
- Technologies covers both information security and regulatory needs

# Questions?

Tom.Bowers@securityconstructs.com

or

Information Security Magazine / SearchSecurity.com

Security CONSTRUCTS
FROM VISION TO ACTION