



# **Business Friendly Distribution**

## **Document Security for Your Data in Motion**

- Vincera introduction
- The Challenge – Data Leakage
- Convergence in the Market
- Document Security for Your Data in Motion
- Q&A

“Our membership consists of security practitioners in diverse industries, people who are charged with the vital, formidable task of ensuring data confidentiality and integrity in their companies. The ISSA stands ready to aid these practitioners in obtaining the up-to-the-minute information data confidentiality and integrity governing and securing. Vincera’s seminal series supports these goals, and we are pleased to welcome [Vincera] as [they] expand knowledge of how Business Friendly Distribution can be used to broaden our members’ security options.”

Pamela Fusco, Presidential Advisor to the ISSA  
Guru, Information Security

- How “It” Happens (the oops factor!)
  - Accidental “Send”
  - Email Address Auto-Fill – Wrong Recipient
  - “for all you’ve done for me” Proliferation
  - Critical Document + Disgruntled (ex) Employee
  - Hacked/Compromised: External – Internal
- Top Three Risks\*
  - Portable Devices 75% (of respondents)
  - Email Attachment 63% (i.e. documents)
  - Email Content 59%
- Automatic Enforcement of Document Security Compliance\*
  - **57% Of Companies Have NO Method of Enforcement**
- Security Breach Occurrence\*\*
  - 84% Insiders Send Confidential Data Outside the Company
  - 35% Experienced An Insider “Attack” Within Last 12 Months

\* Loudhouse Research Survey, August 2006  
 \*\* Gartner CERT® Insider Threat Report, 2005

- **Bad Press**
- **Brand Name Damage\***
- **Lost Customer & Prospect Confidence**
- **Lost Partner Confidence**
- **Stock Devaluation (15% for one company)**
- **Revenue Loss (35%)\*\***
- **Intellectual Capital & Competitive Edge Loss**
- **Regulatory Consequences**

\* Gartner 2005: In Banking and Finance the losses per location exceeded \$500,000 per Incident

\*\* KPMG Industry-Wide Security Study, 2005

## Enterprise Information Security

Data at Rest

storage,  
raw data

native files, databases,  
spreadsheets

physical,  
technical

**Confidentiality**

**Integrity**

**Availability**

**Use Control**

**Accountability**

## Enterprise Information Security

Data Security  
for  
Data at Rest

storage,  
raw data

native files, databases,  
spreadsheets

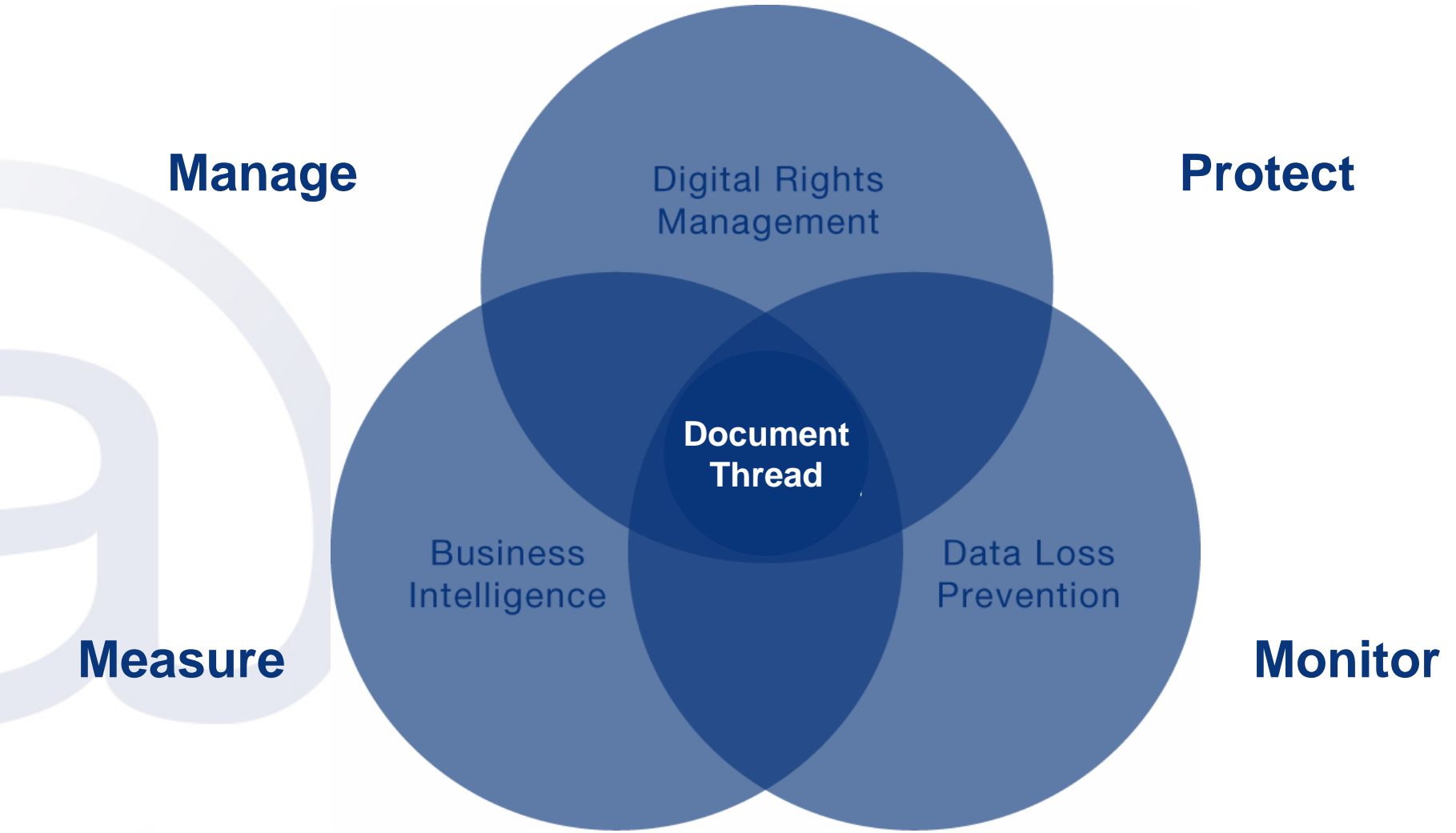
physical,  
technical

Document Security  
for  
Data in Motion

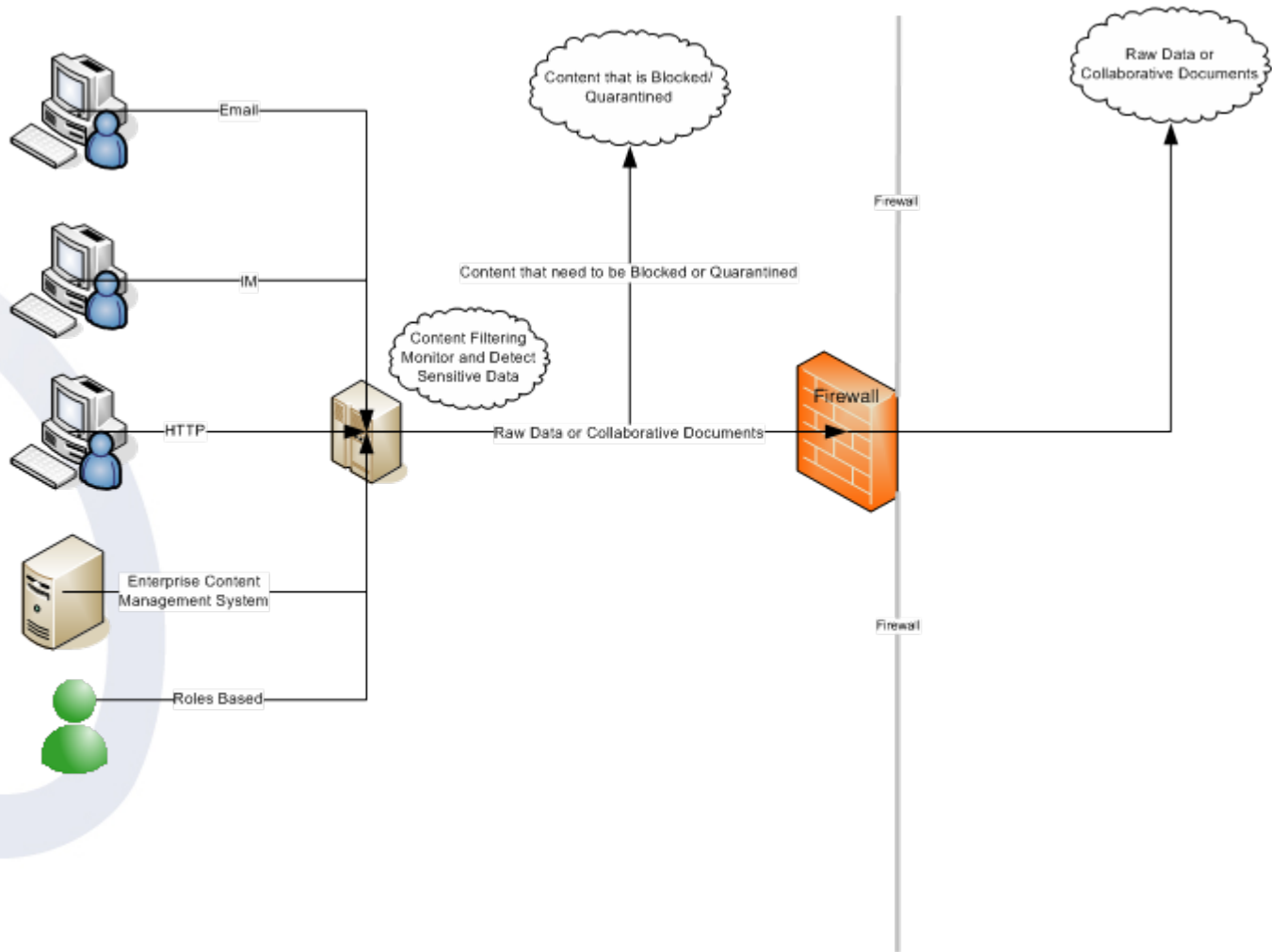
PDF,  
highly portable

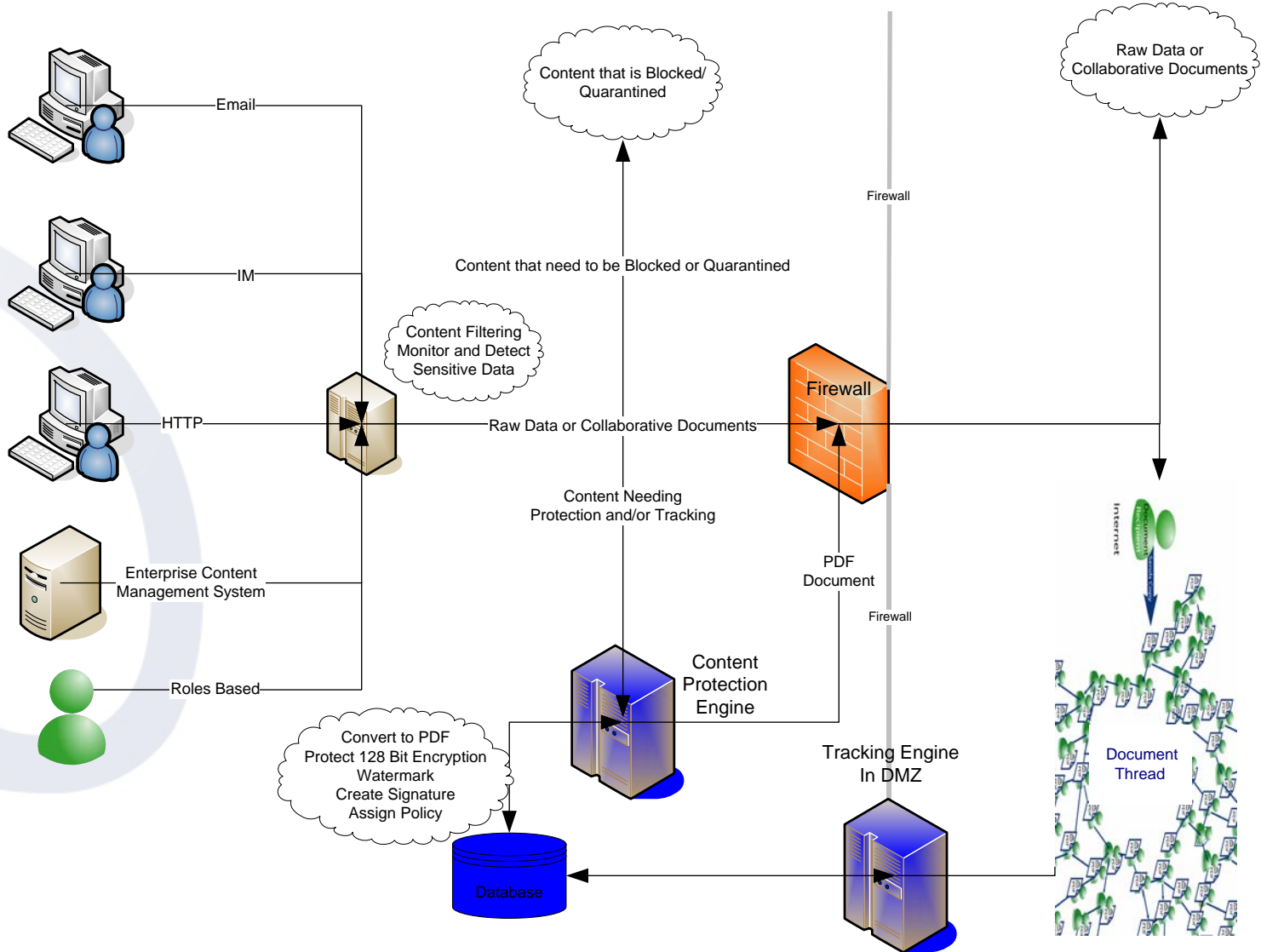
legal, HR, IP, PII,  
sensitive information

contextual,  
business

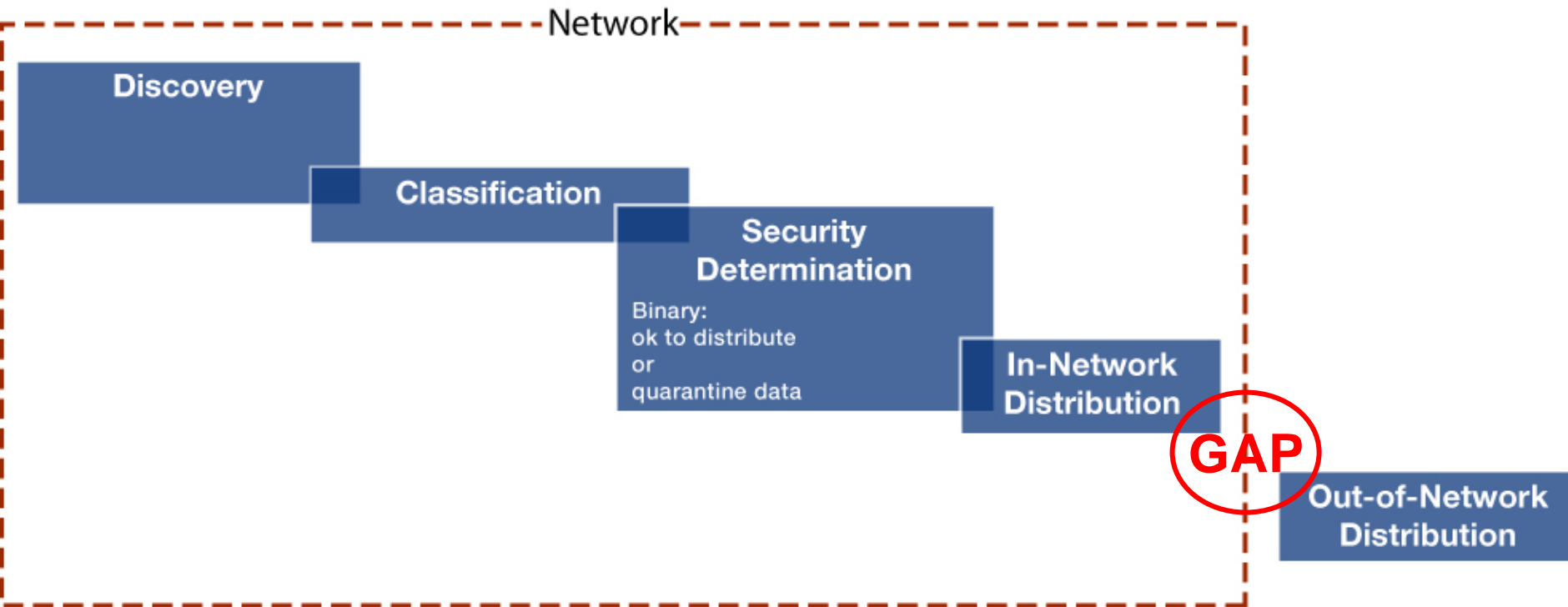


- DLP applies rules to **identify** sensitive data
- BFD applies **security policies** based on sensitivity
- DLP discovers data in motion and **scans** it
- BFD **protects and monitors** data in motion
- DLP **classifies** data in motion based on sensitivity
- BFD **leverages classification** as a security policy
- DLP extends to **end-points** creating monitored network
- BFD monitors the **document thread**, even in the “wild”



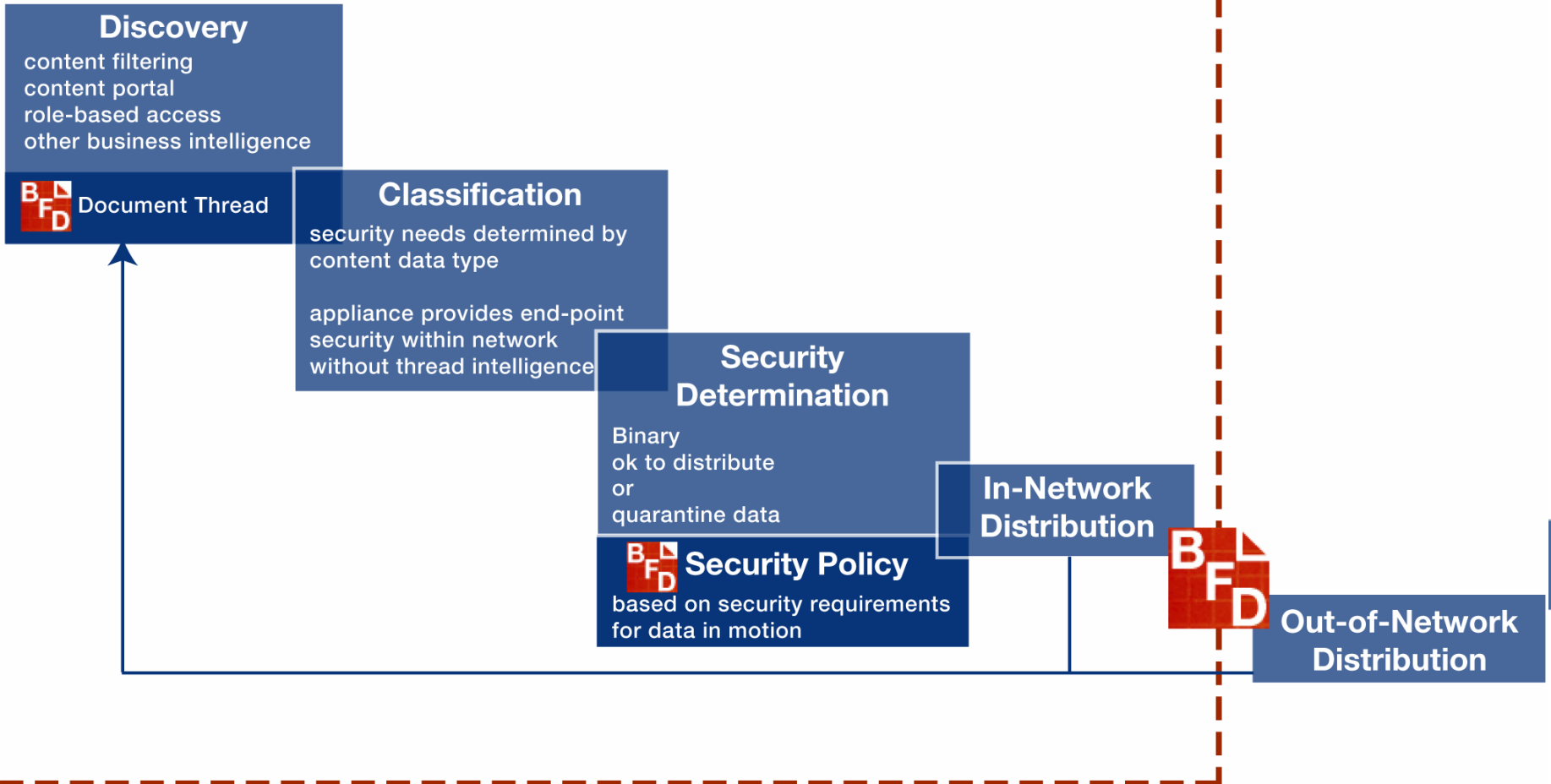


## Data Loss Prevention



## Data Loss Prevention with

Network



- DRM enforces **who has rights** to content
- BFD focuses on **what security policy applies**
- DRM embodies **workflow and collaboration**
- BFD targets **business-ready** digital assets (end-state)
- DRM protects **source formats** like word or CAD
- BFD converts all source formats to **Adobe's PDF**
- DRM **restricts** the distribution of content
- BFD enables knowledge of the **document thread**

Knowledge

**F  
U  
N  
C  
T  
I  
O  
N  
S**

Audit Trail (simple)

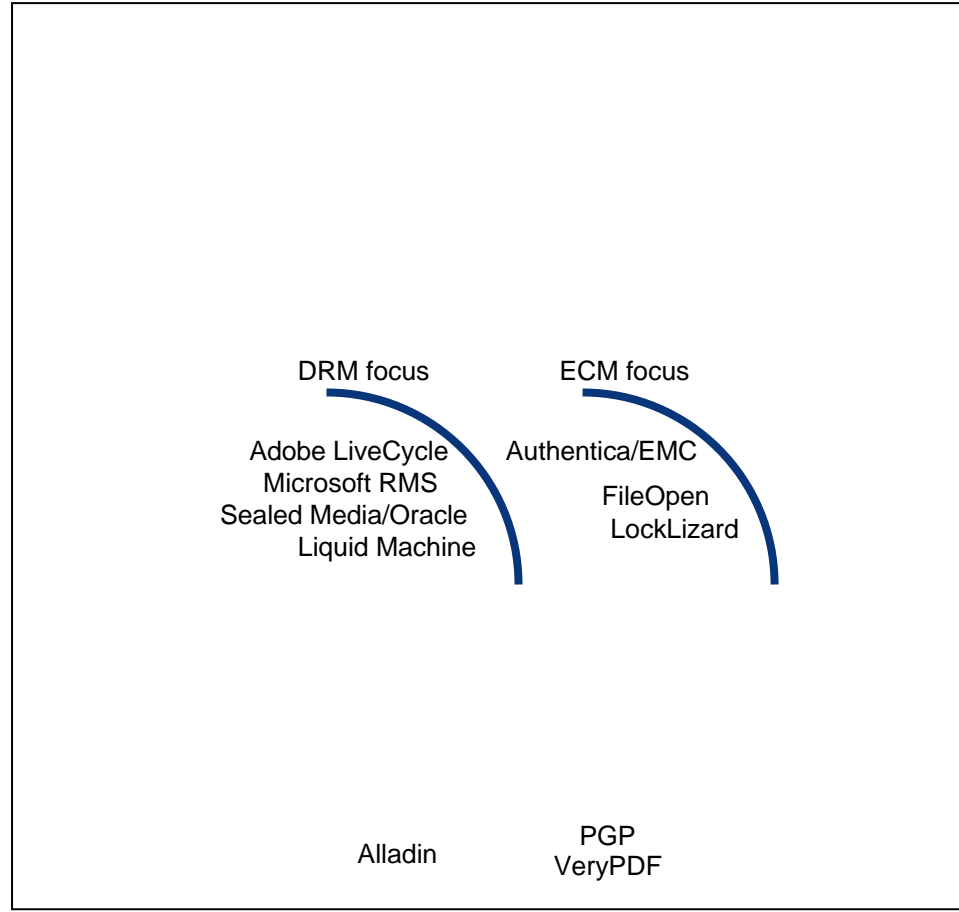
Usage Monitoring

Web Services API

Security Profiles

Encryption

**Restriction**



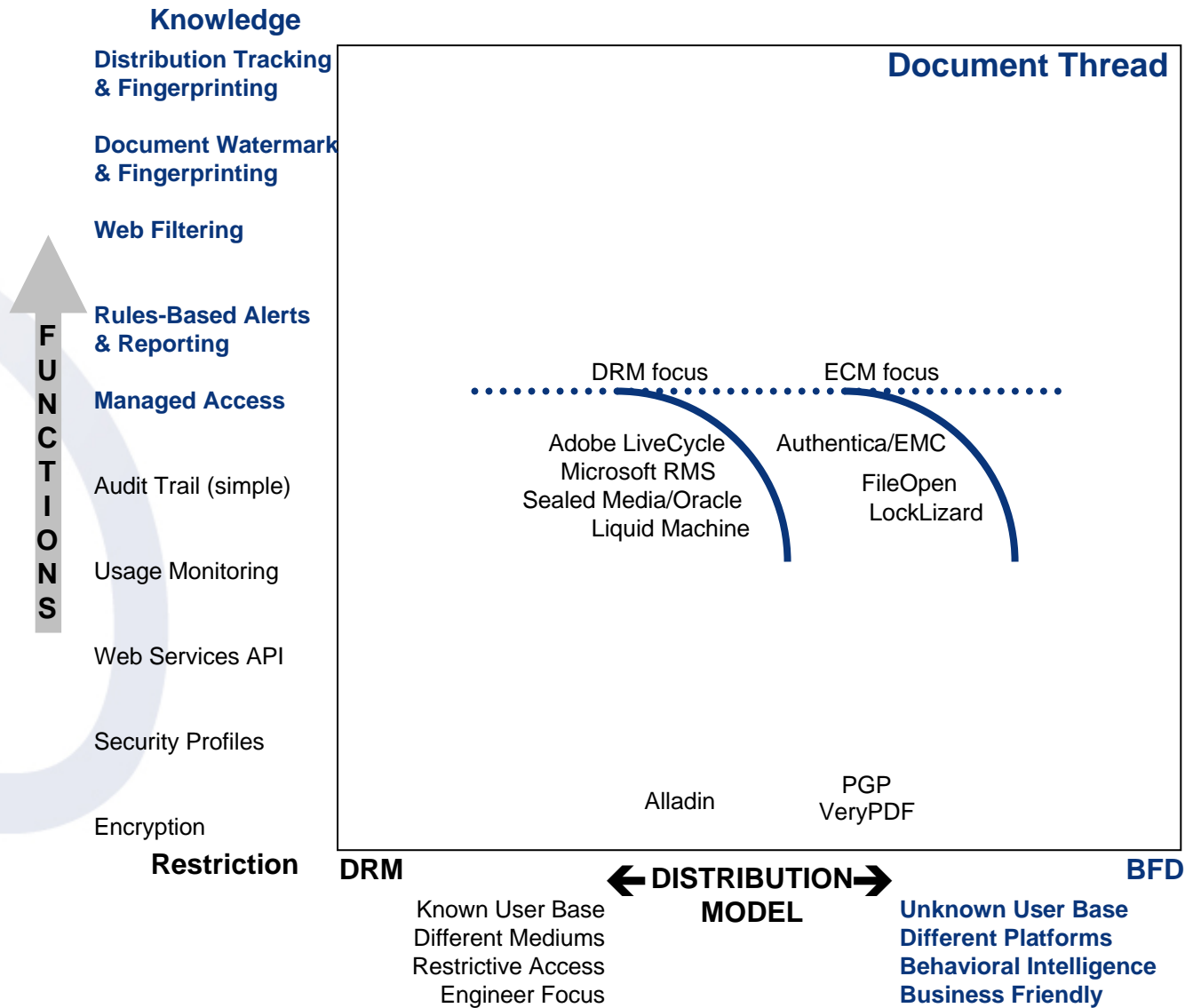
**DRM**

**← DISTRIBUTION MODEL →**

**BFD**

Known User Base  
Different Mediums  
Restrictive Access  
Engineer Focus

Unknown User Base  
Different Platforms  
Behavioral Intelligence  
Business Friendly



**Business Friendly Distribution (BFD)**

BFD is the next generation for document security and tracking for your data in motion both intra and inter enterprise.

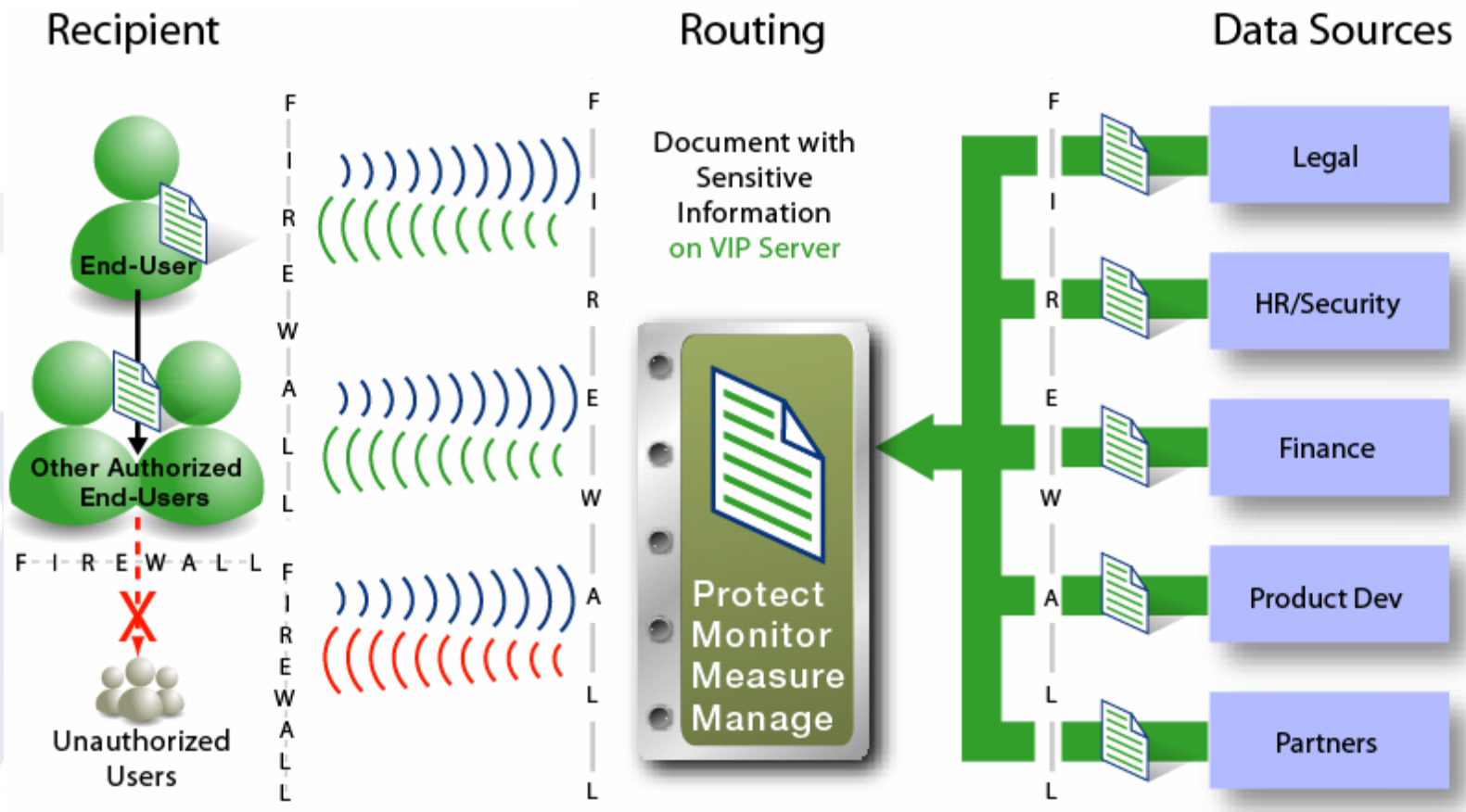
BFD enables the encrypted distribution of data in motion based on the appropriate security level.

BFD enables the content owner to gather behavioral intelligence as the content is distributed, viewed and, in many cases, re-distributed by the initial recipient, aka the Document Thread.

BFD enables the ability to disable access to the document by any particular machine or user, taking that “document thread” of the digital content out of circulation.

BFD leverages your security infrastructure for your data in motion and strengthens your data loss prevention capabilities inside and beyond your firewall.

- Protect
  - encryption and watermarking to deter inappropriate use
  - hashed fingerprint of source and PDF document
- Monitor
  - hashed desktop to establish the ***Document Thread***
  - non-repudiation of eDiscovery and forensic audits
- Measure
  - metrics are managed in a central repository and mined
  - reporting supports management, compliance & audit needs
- Manage
  - self-administrating for recipient of document (security policy)
  - behavioral driven response, i.e. disable document or recipients
  - detection is the key, i.e. tampering, breach
  - address “data leakage” from your documents



**Manage Document**  
i.e. disable/enable

**Business Friendly Distribution**

(Note: the process did not change!)

VINCERA® Intelligent Protection™

*Deter*

*Detect*

*Disable*

**VIP**

**Document Security**

**Thank You!**

**Kevin Schick**

[www.vincera.com](http://www.vincera.com)

[kevin.schick@vincera.com](mailto:kevin.schick@vincera.com)

**480-767-9041**