Data-Centric Security for the Cloud Generation

Gregory Martin, CISSP

DLP Architect, Symantec Corporation

Breakout Session Agenda

1. DLP Program Basics
2. Extending DLP Programs to the Cloud
3. Complementary tools for the Cloud (DRM and UEBA)

Data Loss Prevention Program Basics

Answers these critical questions about your information

DISCOVER

Locate where your sensitive information resides across your cloud, mobile, network, endpoint and storage systems

Where does your confidential data live?

MONITOR

Understand how your sensitive information is being used, including what data is being handled and by whom

How is it being used?

PROTECT

Stop sensitive information from being leaked or stolen by enforcing data loss policies and educating employees

How do you prevent data loss?

Define what is “Sensitive” to your Organization

Prioritize by the impact of data disclosure

CUSTOMER INFORMATION

- Credit Card Info
- Social Security Info

COMPANY INFORMATION

- Intellectual Property
- M&A and Strategy

NATIONAL SECURITY INFORMATION

- Military Intelligence Data
- Security Clearance Data

Data Comes in Different Forms

Described, Structured and Unstructured Data, Images

TEXT AND MARKUP

TXT
HTML
XML
Visio
RTF
Oasis

WORD-PROCESSING

PAGES
Corel
Folio
Lotus
Word Files
OneNote

PRESENTATION FORMATS

Keynote
Corel
Lotus
Flash
PowerPoint
Impress

SPREADSHEET FORMATS

NUMBERS
XLS
CSV
Corel
Lotus
DIF

EMAIL FORMATS

DXL
EMC ONM
MSG
EML
Encapsulation
Various

CAD FILES

AutoCAD (DWG, DFX)
Visio
Microstation

GRAPHICS FORMATS

JPEG
PNG
BMP
Lotus PIC
TIFF
WMF

ENCAPSULATION FORMATS

ZIP (PKZIP, WinZip…)
RAR
TAR
UNIX Compress

PROPRIETARY and OTHERS

PDF
Databases
iCalendar
MP3
PFILE
Virtual Card File
Encrypted

Data Detection Technologies

Choose the optimal technology for highest accuracy and minimizes false positives

DESCRIBED CONTENT MATCHING

Non-indexable data

DESCRIBED DATA

EXACT DATA MATCHING

PII, Credit Cards, Government IDs

STRUCTURED DATA

INDEXED DOCUMENT MATCHING

Financial Reports, Marketing Plans

UNSTRUCTURED DATA

VECTOR MACHINE LEARNING

Source Code, Product Designs

UNSTRUCTURED TEXT

SENSITIVE IMAGE RECOGNITION

OCR, Form Images, Scanned Documents, Screenshots

IMAGES

The Need for Data Classification (Tagging)

I need to protect regulated data and intellectual property from loss and theft

Automatic detection technologies cover most of the scenarios

Account Numbers, Credit Cards, Government IDs,

Financial Reports, Marketing Plans

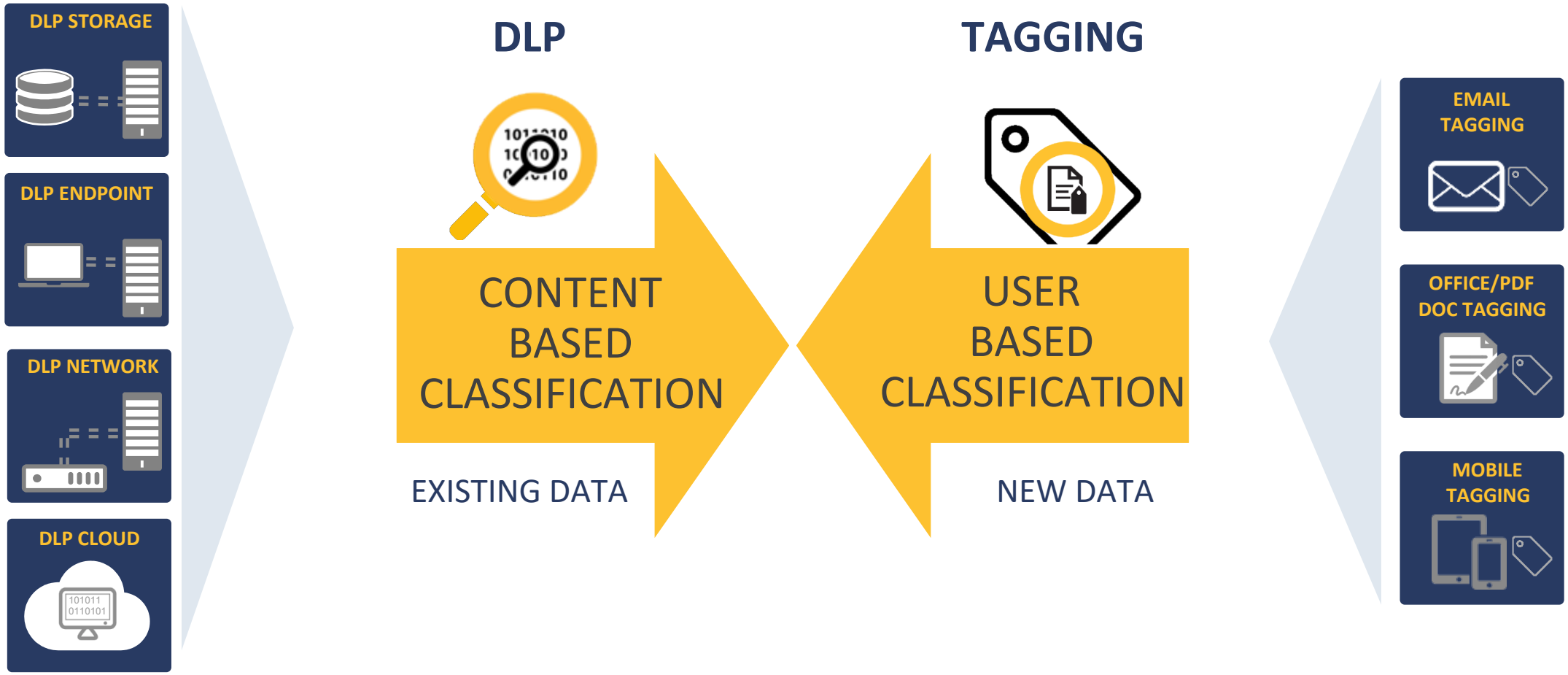
Source Code, Product Designs

Tax returns, insurance claim forms

But some types of sensitive data are best classified by the users who create it

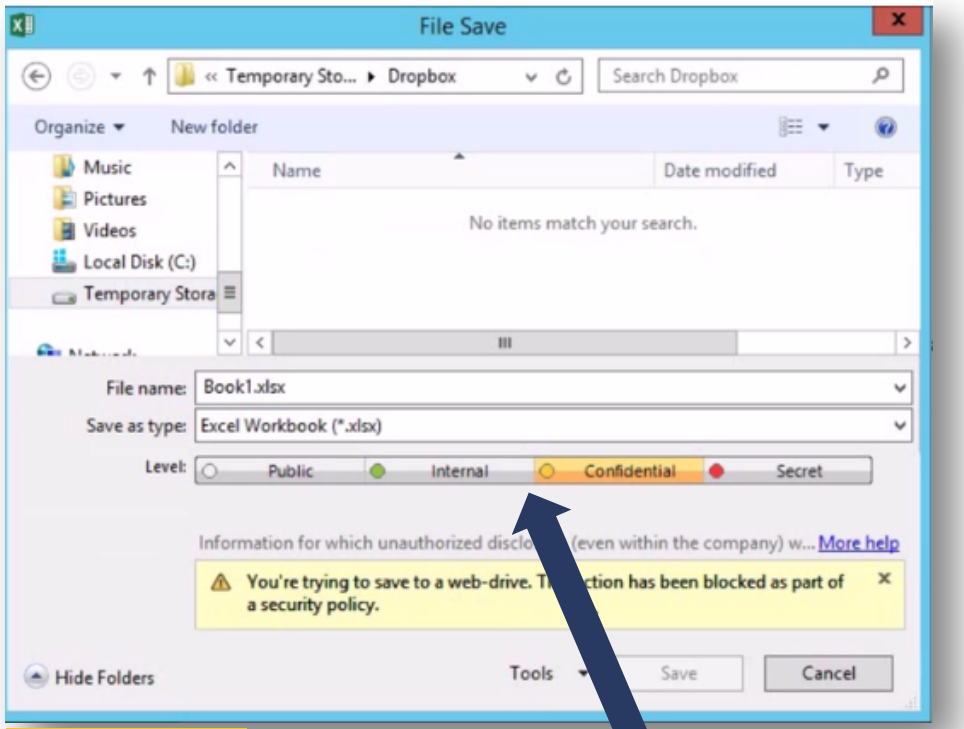
Data Classification Augments DLP

Policy Driven + User Driven



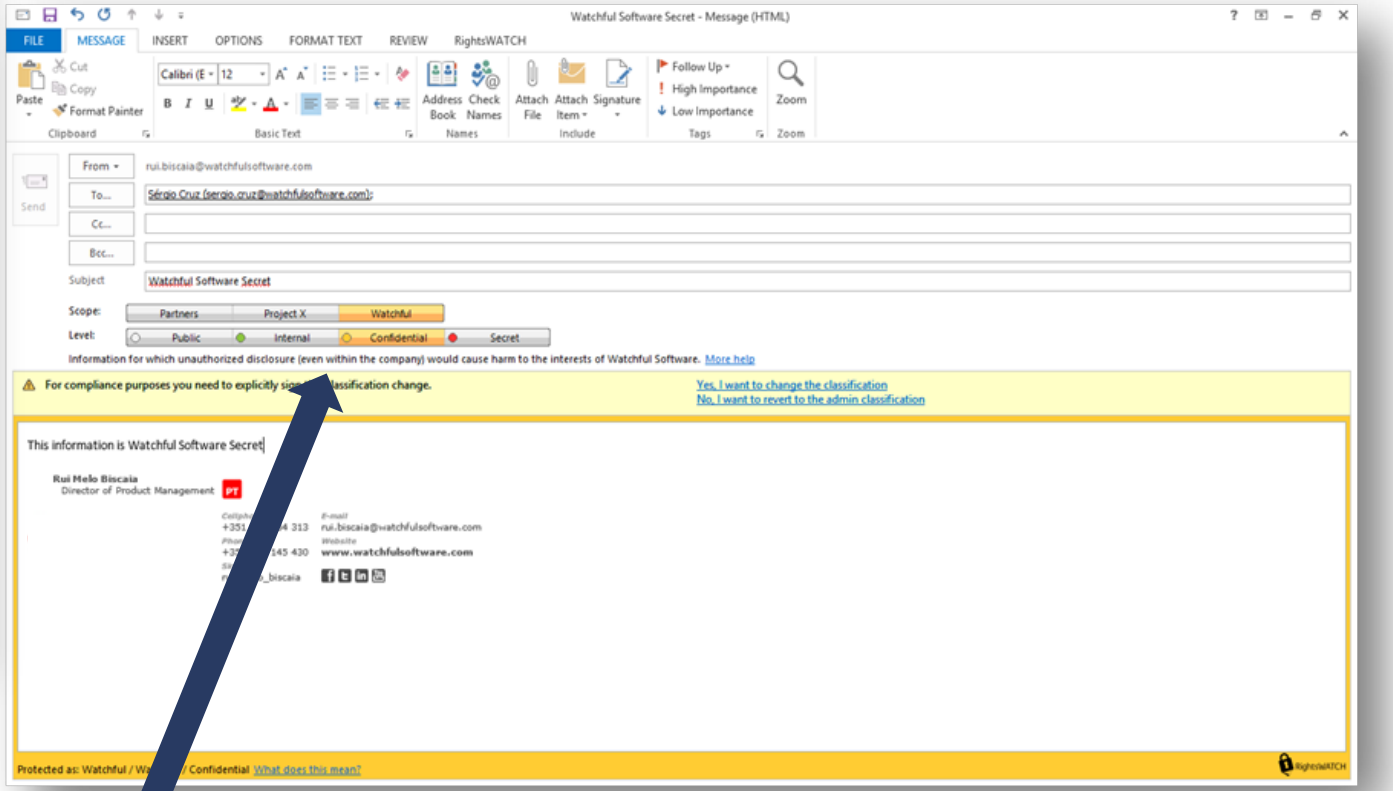
Intuitive Data Classification User Experience

Information Centric Tagging (ICT)



Files

Emails



Classify data upon creation

Personas of Who is Leaking Data?

- Well-meaning Insiders
  - Email
  - Contractors/Business Partners
  - Cloud Storage/Apps
  - Lost laptop/hard drive
  - Lack of business controls
- Malicious Insiders-any way possible
  - Email
  - USB devices/DVD
  - Print
  - Cloud Storage/Apps
  - Encrypted traffic (email/web/FTP)
- Outsiders/Malicious Code-any way possible
  - Email
  - Cloud Storage/Apps
  - Encrypted traffic (web, FTP)

Why Channel Coverage Must be Comprehensive

Data Egress Points: Endpoint, Storage, Network, Email, Cloud

Removable media

Printer/FAX

Email

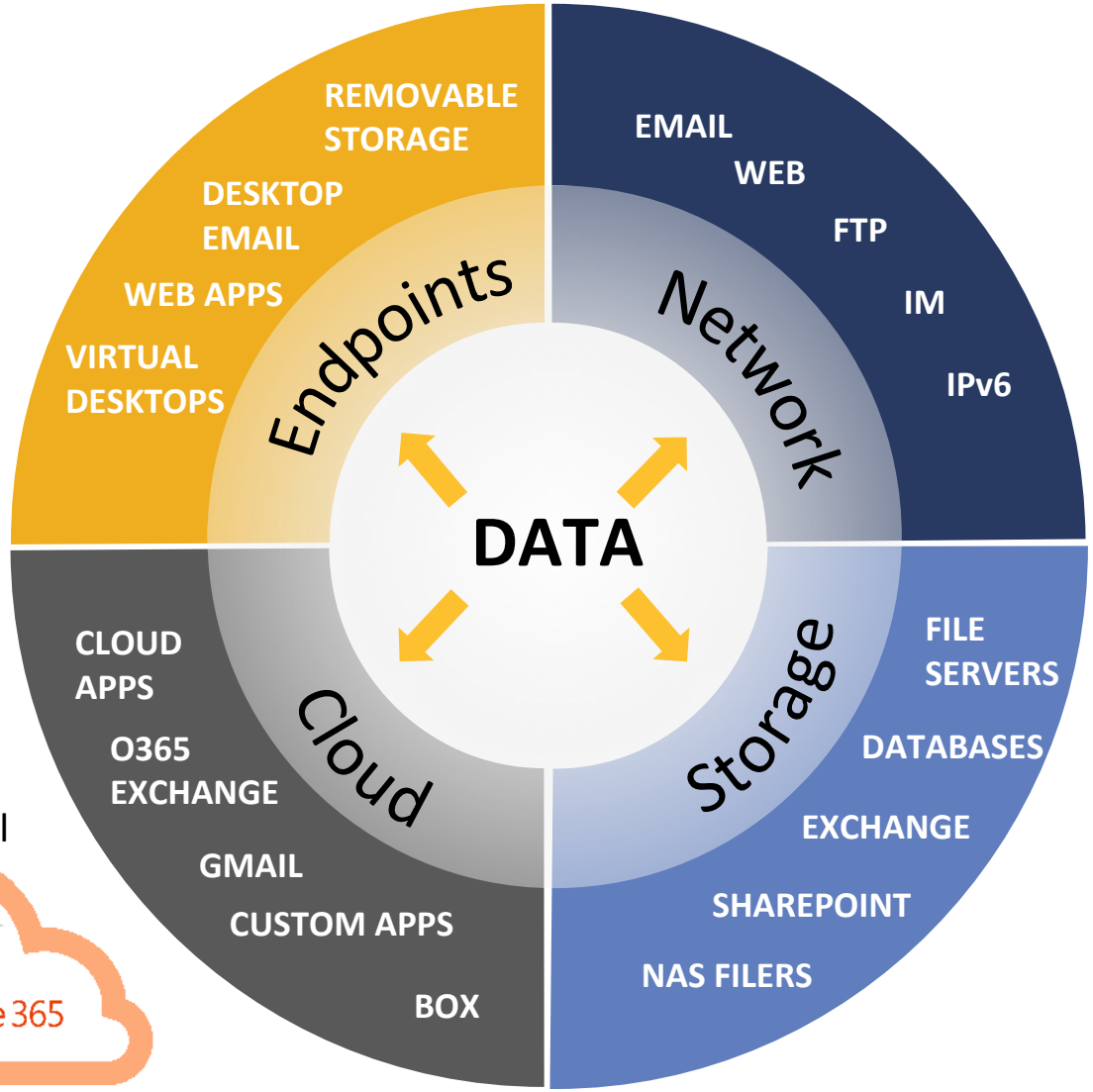
Browser

Copy/paste

Cloud apps

CD/DVD

File Shares



SMTP …

HTTP, Ftp, SSLV,…

HTTPS, …

SharePoint

File servers

NAS

Corporate Web sites

Databases

box
OneDrive
Dropbox
salesforce
SharePoint Online

Cloud apps

Cloud email

Gmail
Office 365

Extending DLP to the Cloud

Sensitive Data Moves to The Cloud

SaaS and Cloud Email Support Availability of Data and Services

Office 365

Gartner estimates that by 2021, more than **70%** of businesses will be substantially provisioned with cloud office capabilities.

box

G Suite

Dropbox

Problem: Increased Exposure of Sensitive Data

Reduced visibility and protection

Low Visibility

Data not visible and more exposed
when shared across public cloud apps & cloud email

Data Detection

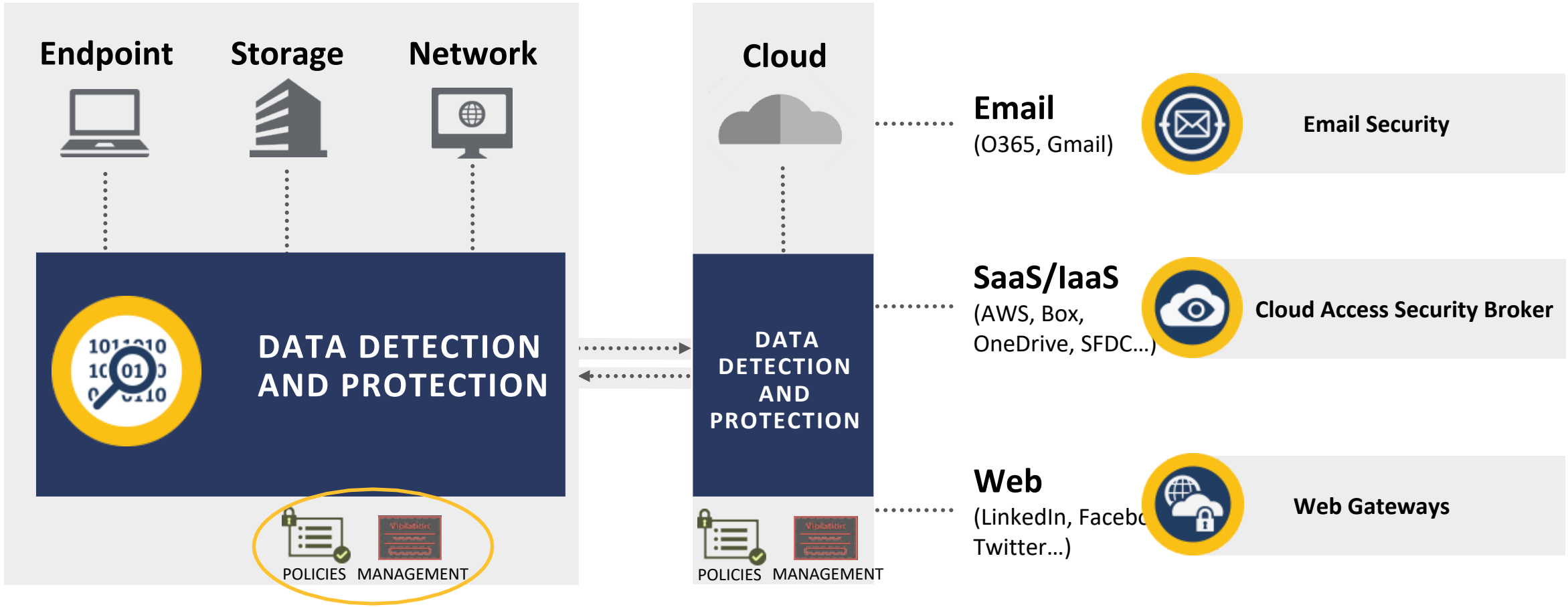
“Good-enough” detection in a point product is unreliable
because it misses critical PII and Intellectual Property and causes too many false positives

Management Complexity

Disjointed policies and management
between on-prem and cloud result in complex incident triage and increased security spend

Data Detection and Protection in The Cloud

Data protection must be consistent across all channels



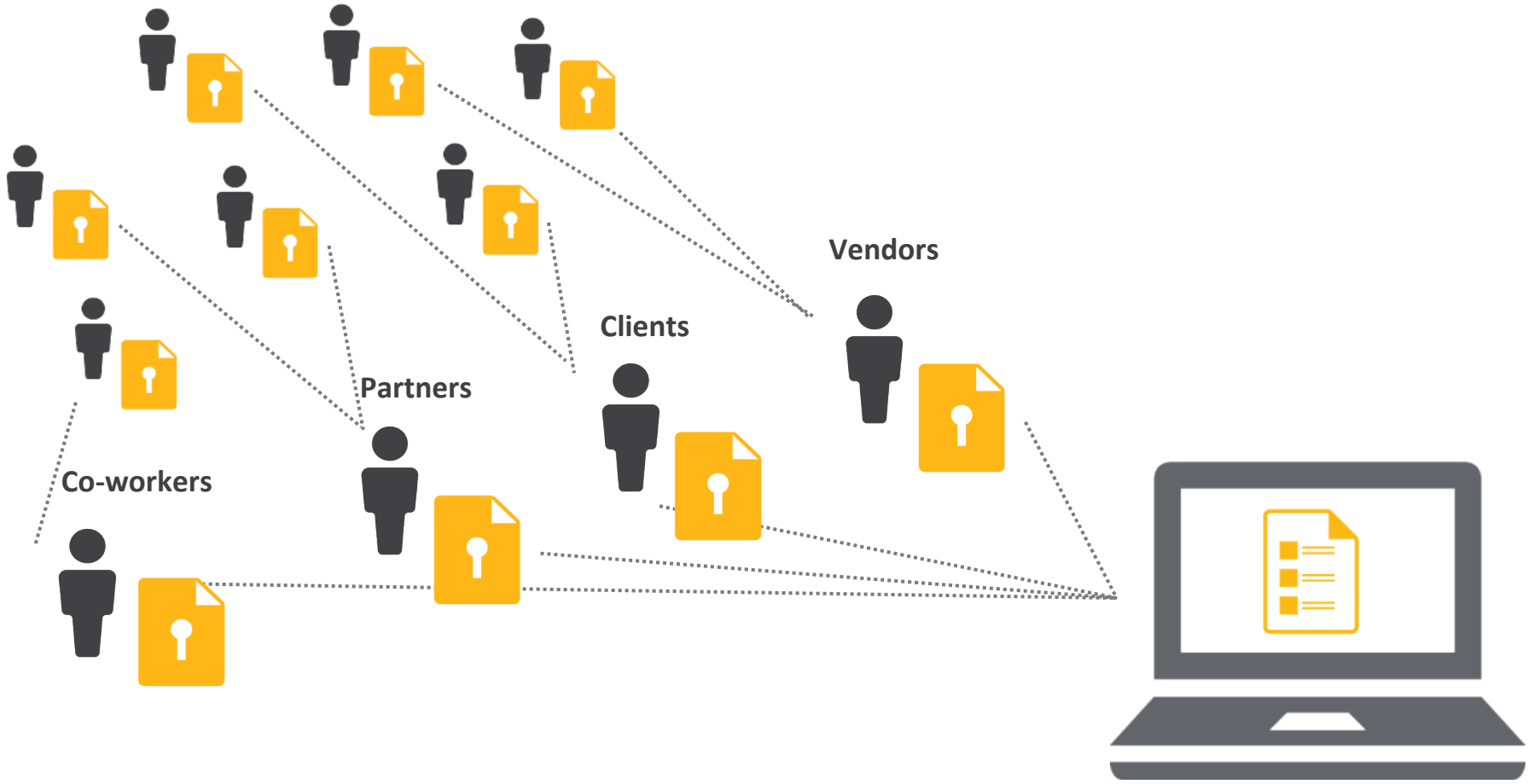
- Detection in the cloud
- Utilize Cloud Elasticity
- Consistent User Experience
- Consistent Incident Response

Digital Rights Management

Information Centric Encryption

Increased Need for Collaboration with 3rd Parties

Sensitive data is shared with partners, vendors and contractors



Data Vulnerable When Shared with 3rd Parties

Data protection perimeter is gone and visibility is lost

Lost Visibility

Data must be shared with partners
But tracking of data distribution is challenging after data is shared with external users

Vanished Protection

Data protection fades with decryption
Encryption doesn’t persist after key is provided, and sensitive data must be retrieved after partnership ends

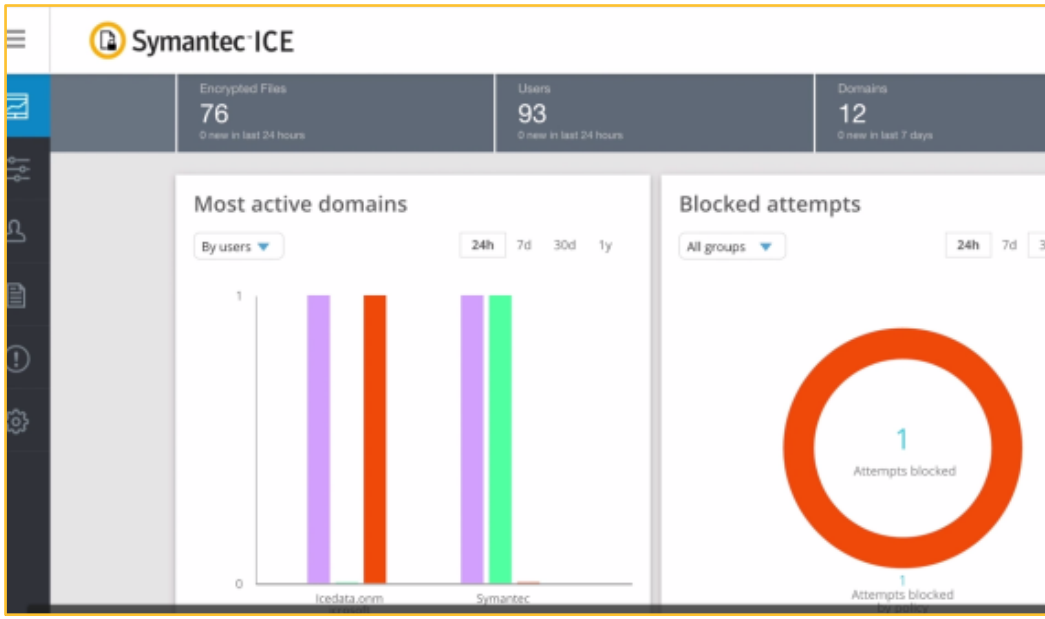
Non-Compliance Risk

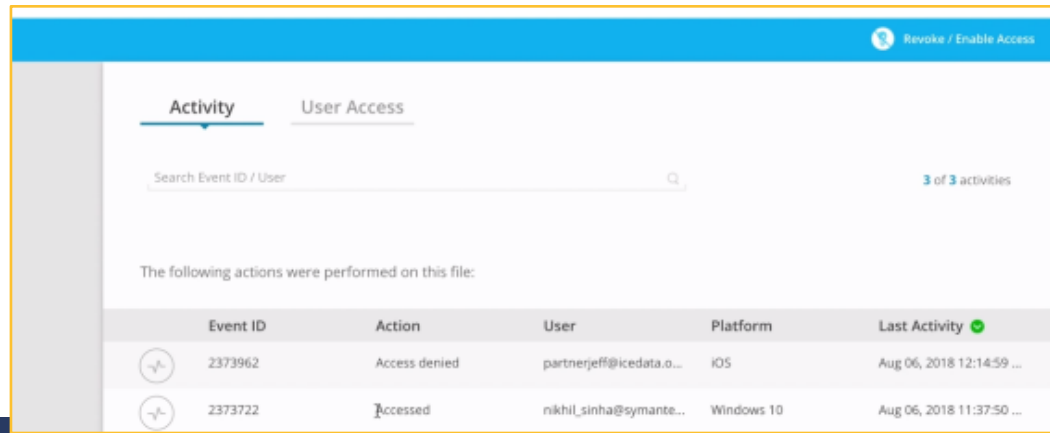
Unsecured devices access data
Security postures and malicious behavior are uncontrollable for external unmanaged devices

Digital Rights Management

Using Symantec Information Centric Encryption (ICE)

- **Protection that follows data everywhere**
  - For endpoint, storage, cloud apps and email
  - Cloud based to track data distribution
  - On-prem or cloud keystores
- **Identity-based data access and digital rights**
  - Ensure access only to authorized users
  - Limit permissions: view, edit, save, print, etc.
  - Agentless viewing via web isolation technology
- **Access revoking**
  - Revoke access as business needs change





User and Entity Behavior Analytics

Information Centric Analytics

Data Security Challenges

- **Manage incident volume**
  - *Prioritize critical alerts first*
  - *Tune DLP policies (fewer pattern based policies, more exact data based policies)*
- **Insider threat disguised**
  - *Need to correlate risky behavior across many threat vectors*
  - *Low threat incidents spread out over time*
- **Persistent threats undetectable**
  - *Cross platform blind spots still thwart breach detection*
  - *Data security monitoring analyzed by separated teams*

User and Entity Behavior Analytics (UEBA)

Using Symantec Information Centric Analytics (ICA)

- **Simplify DLP incident management**
- **Identify risky users and behavior**

Information Protection

On Prem DLP Policy Violations

Cloud DLP Policy Violations

Tagging Activity

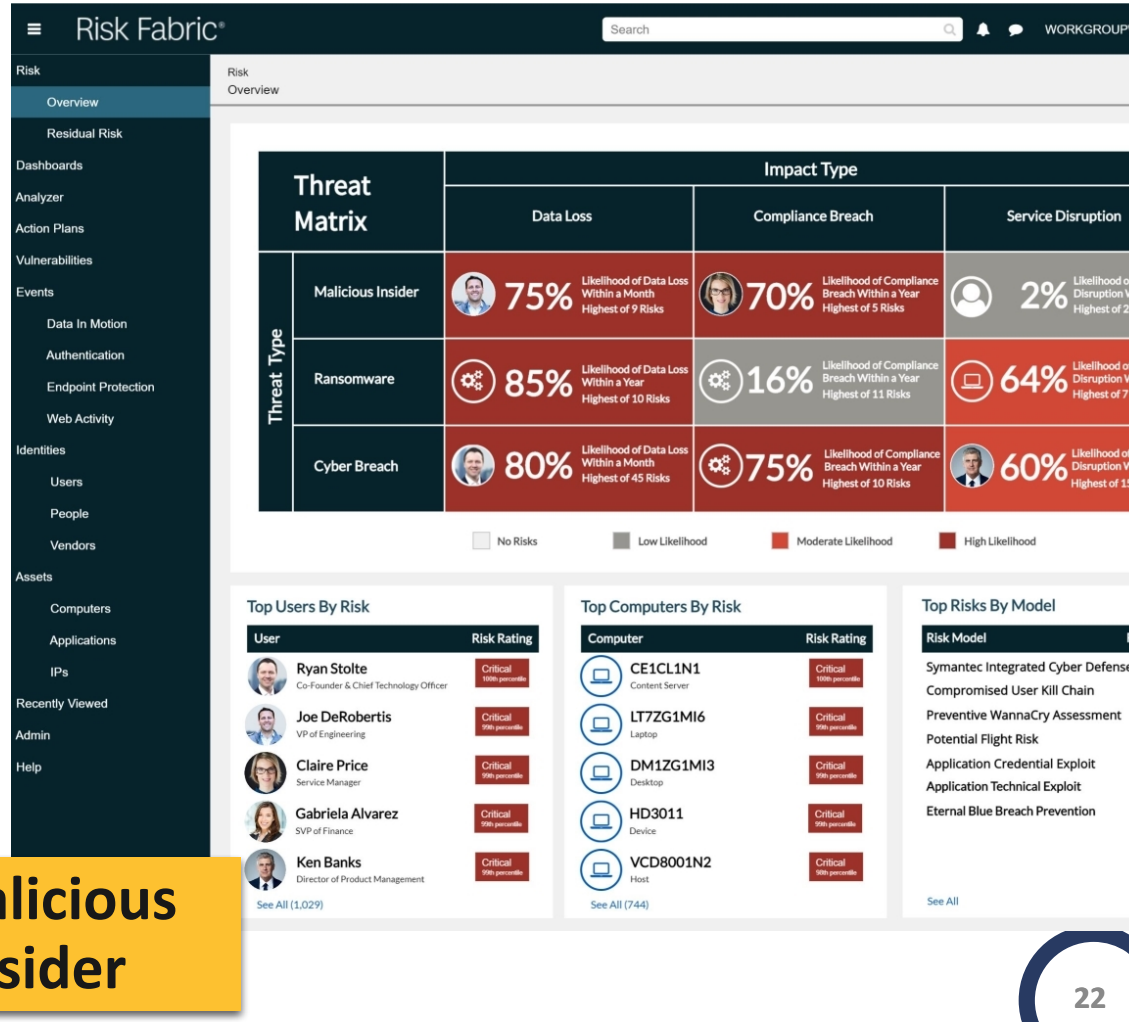
Encrypted File Access Activity

Information Centric Analytics

(User and Entity Behavior Analytics)

1. Prioritize Incidents

2. Identify Malicious Insider/Outsider



Integrated Data Security Platform

Symantec Information Protection Suite

From DLP to an Integrated Data Security Platform

Key products

Data Loss Prevention
Endpoint, Storage, Network, Cloud

- Cloud Access Security Broker (CASB)
- Data Classification (ICT)
- Digital Rights Management (ICE)
- Endpoint Security (SEP)
- User and Entity Behavior Analytics (ICA)
- Identity and Access Management (VIP)
- Web Gateways (ProxySG, WSS, Mobile)
- Email Security, Encryption, SSLV, SEP, CCS…

Information Centric Security Demo

Q&A

Gregory Martin, CISSP
DLP Architect, Symantec Corporation
Gregory_Martin@Symantec.com