

# Is Your Organization Ready for GDPR?



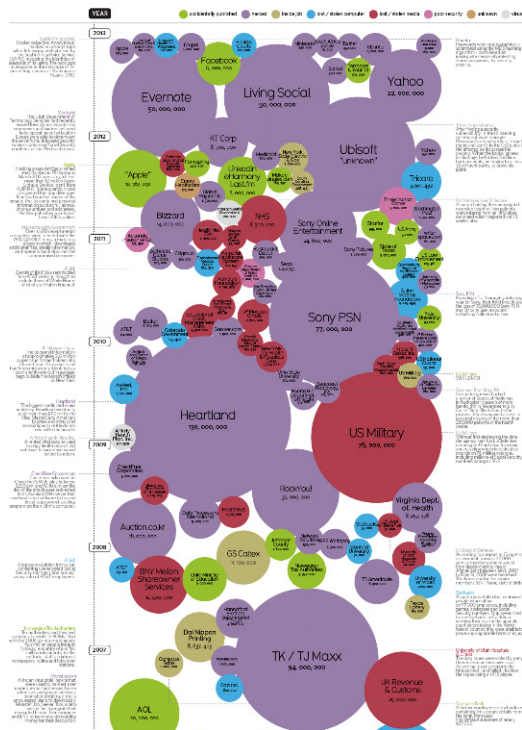
**Presented by:**

*Robin Basham, CEO, Founder,  
EnterpriseGRC Solutions*



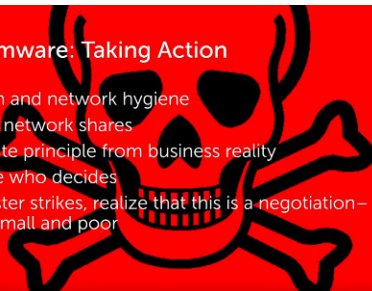
# All that's sure in life is Ransomware, Tax Fraud and lost data

World's Biggest Data Breaches  
Selected losses greater than 30,000 records



## Ransomware: Taking Action

- System and network hygiene
- Watch network shares
- Separate principle from business reality
- Decide who decides
- If disaster strikes, realize that this is a negotiation—Look small and poor



# Designing data strategy is hard



### What is personal data?

- Name
- Address
- Localization
- Online identifier
- Health information
- Income
- Cultural profile
- ... and more

**COLLECT  
STORE  
USE  
DATA?**

You have to abide by the rules.

**Process data** for other companies?  
This is for you too.



Defining the people who will use that data, even harder





## We already see real world data problems (example, laptops banned in international flights).

Companies need to use an Enterprise Digital Rights Management (EDRM) to control access and use of information in stand-alone files and emails (known as 'unstructured' information). This technology (also called Information Right Management or IRM), enables safe data in transit and at rest. Unlike simple encryption, EDRM assigns rights that travel with the data as opposed to simply assigning rights on the system where its stored.

espionage  
data theft



international  
import  
export laws

You're sending me on a business trip and I cannot bring my laptop because...

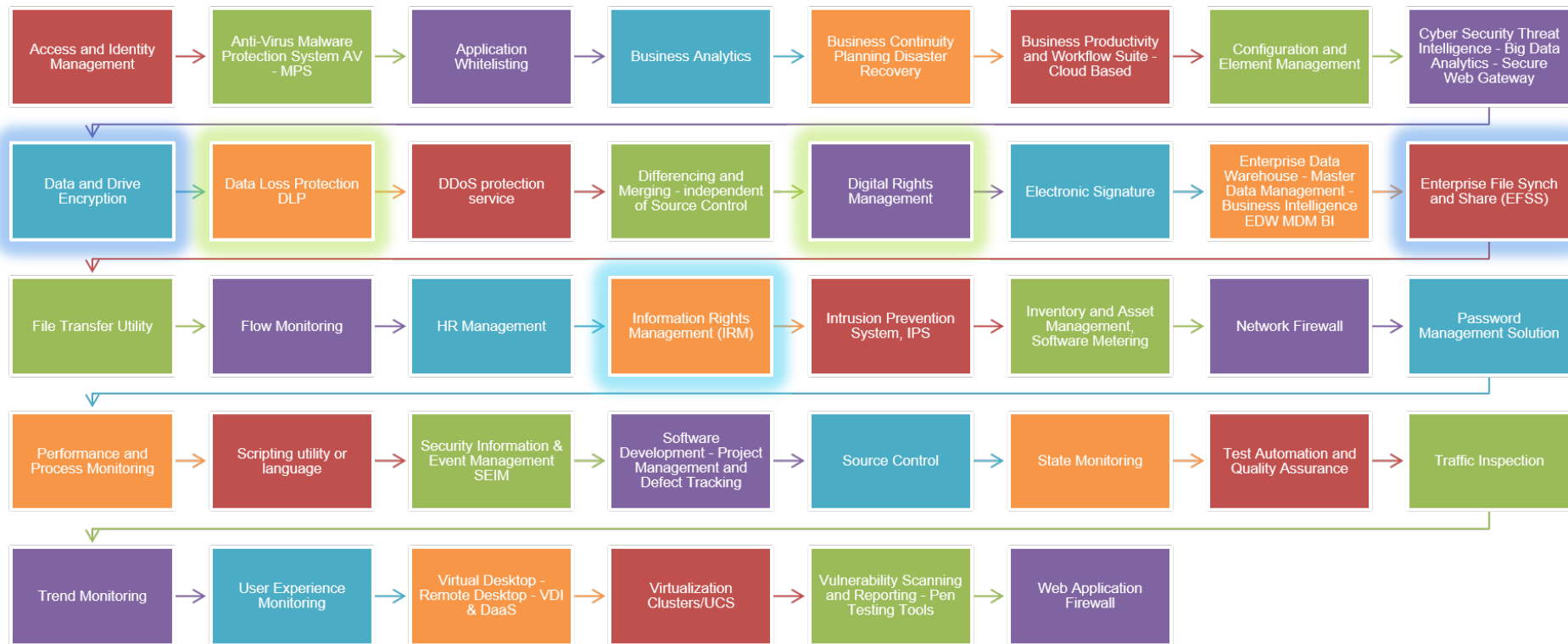
## Ask yourself, “What are the technologies I need?”

The truth about our private information is we need control over its perpetual use. The companies receiving our data may not have the knowledge, incentive, or bandwidth to implement security for our needs. Technology must empower the citizen to engage in fearless communication, unencumbered by the clunky mechanics of encryption.

We need to tag our assets, restrict them, call them back, and even delete them from locations where they have been stolen or simply wrongly maintained.



# Data Centric Security Products Enable Privacy (GDPR, SOC2, NIST 800-53r4 App J, NIST 800-171, CIS CSF, HIPAA, FISMA)



# What is the General Data Protection Regulation – GDPR?

The new [General Data Protection Regulation 2016/679](#) ("GDPR" or the "Regulation") is about protecting **people and their privacy**.

The law is applicable to all citizens under the European Convention, however, it is equally relevant to any US or other foreign nation who wishes *to do business with* most of Europe and Australia.



## The Seven Principles of GDPR

1. Privacy by Design
2. Data Protection Officer
3. Opt-In for data collection
4. Right to be forgotten
5. Breach notification
6. One-stop shop
7. Fines and Enforcement:  
Violations result in 20 Million Euros or **4% of Global Turnover**



# EU General Data Protection Regulation 2016/679 “GDPR”



What is the  
relationship of  
security to privacy?

What the  
relationship of  
privacy to business?

Effective May of 2018, GDPR Compliance requires system capabilities to manage citizen privacy; to understand how “sensitive” information comes in, moves around, leaks out. Without enhanced privacy technology integration most businesses won’t be able to “transfer” personal data to:

Austria	Italy	Belgium	Latvia	Bulgaria	Lithuania	Croatia
Luxembourg	Cyprus	Malta	Czech Republic	Netherlands	Denmark	Poland
Estonia	Portugal	Finland	Romania	France	Slovakia	Germany
Slovenia	Greece	Spain	Hungary	Sweden	Ireland	United Kingdom

## People don't trust businesses with their private data



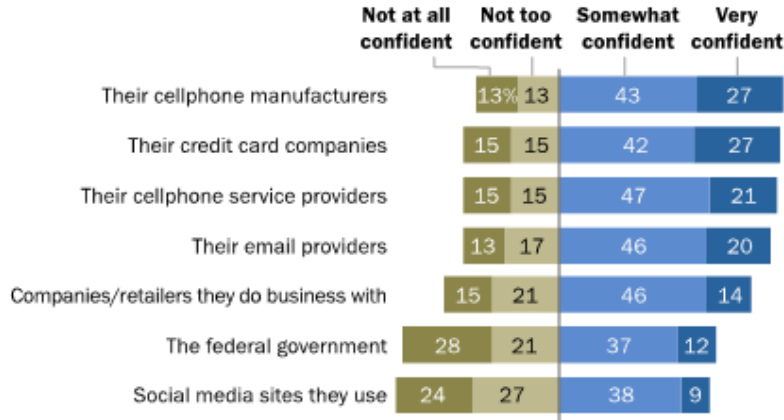
While 15% of EU citizens report not trusting businesses with their information, they also lack the tools to securely manage their own private information.

15% of EU citizens don't trust companies with their personal information

# The data problem is enormous

## Roughly half of Americans do not trust the federal government or social media sites to protect their data

% of U.S. adults/tech users (see note below) who are \_\_\_ in the ability of the following institutions to protect their data



Note: Data on cellphone manufacturers and service providers based on cellphone owners; data on email providers based on internet users; data on social media sites based on social media users. Data for credit card companies recalculated to exclude "does not apply" responses. Otherwise, refusals and "does not apply" responses not included in this chart.  
Source: Survey conducted March 30-May 3, 2016.

"Americans and Cybersecurity"

PEW RESEARCH CENTER

Issues: Data expiration, Duplicate documents, Documents that no longer serve a business purpose. Most documents exist beyond their legal retention and in many cases no one knows who owns them.



# A breach is a breach – (Common and Not Common Principles)

## General Data Protection Regulation (EU) 2016/679

Article 33 (of 99): “Notification of a personal data breach to the supervisory authority - In the case of a personal data breach, the controller shall without undue delay and, where feasible, **not later than 72 hours after having become aware of it**, notify the personal data breach to the supervisory authority competent in accordance with Article 55, ***unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons***. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay...”



Aren't most of us already covered with SOC2 or PCI?

For example, Trust Services Principles and Criteria P6.7 The entity provides notification of breaches and incidents to affected data subjects, regulators, and others consistent with the entity's privacy commitments and system requirements.

For example, PCI DSS V3.2 12.10 Implement an incident response plan... responding immediately to a system breach.

For example, 47 out of 50 States (US) have Breach Notification laws

Right to Access

Breach Notification

Right to be Forgotten

Data Portability

Privacy by Design

Consent

# Even if security within the Enterprise is Perfect – 3<sup>rd</sup> Party is not

- 41% to 63% of breaches involved third parties
- 71% of companies failed to adequately manage risk of third parties
- 92% of companies planned to expand their use of vendors
- 90% of anti-corruption actions by DOJ involved 3<sup>rd</sup> parties

## Data Risk in the Third-Party Ecosystem

Ponemon Institute, March 2016





# Global Data Protection Regulation proposes solving privacy problems with 8 Data Principles

Fair and Lawful  
Processing

Minimal  
Storage Term

Data Quality

Special  
Categories of  
Data

Purpose  
Limitation and  
Specification

Transparency

Security

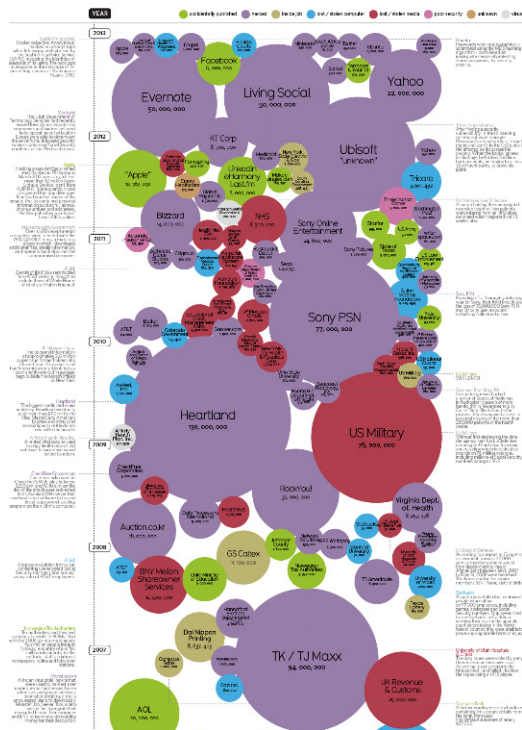
Data  
Minimization



What if customer information leaks and there's no way to track the location of the lost data?

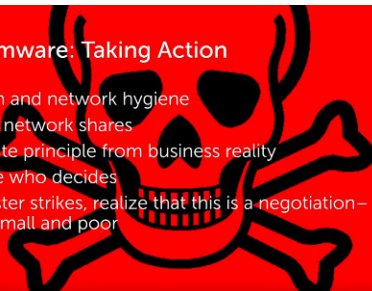
# All that's sure in life is Ransomware, Tax Fraud and lost data

World's Biggest Data Breaches  
Selected losses greater than 30,000 records



## Ransomware: Taking Action

- System and network hygiene
- Watch network shares
- Separate principle from business reality
- Decide who decides
- If disaster strikes, realize that this is a negotiation—Look small and poor



# Security is One Big business Problem:

"Why can't I keep a copy on my home PC?"

Hey team, got a snag. Laptop stolen somewhere between Greece and arriving in Seattle. Need someone to resend the board presentation to hotel lobby. Also, which country gets theft report?"

Mr. Chen says he'd give it to you but we sent our finance statement to the wrong *Peter Chen*, again.

"No worries, I got the report. I just asked my husband to print it out and fax from home."

"Hi, I'm your new Data Protection Officer. I can't wait to get started."



# General Data Protection requires security CIA triad

- Aim for the CIA triad: customer information **c**onfidentiality, **i**ntegrity, **a**vailability, preventing wrongful disclosure, manipulation, denial of service
- Strong security lowers cyber insurance cost.
- Improved cybersecurity earn higher service price and faster service adoption.
- Strong cybersecurity gains the approval of major assessors and regulators like FTC, FCC, FDIC, PCI, AICPA, DOJ, ISO and EU




# Data centric security tools reduce security problems

- Risk: *Stolen (lost) laptop*
- Actual Risk: ***Premature breach notification***
- “Absence of evidence” = no evidence to defend a data breach
- Default access to information is set to private, enforcing privacy by design
- Log and audit functions exist to prove compliance and even to enforce remediation to violations of access
- Response: Early detection of irregular distribution of files leads to better incident identification and response

*...unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons*

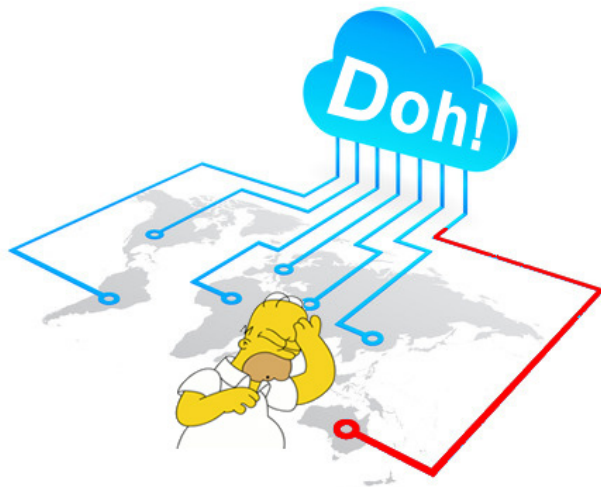




GDPR requires that people give their **consent** to how their data is used 

Over time, if the customer or employee disagrees with how the data is being used or with the accuracy of the data, then what?

How do we modify protection on a document once it has left our perimeter?



## Data Centric Security Supports *Fair and Lawful Processing*

Protection persistence travels beyond the perimeter and is tied to the customer's data.

Based on our understanding, the permissions we grant will change



Companies must honor all reasonable requests to stop processing or ENABLING USE of citizen private information

Audits and Activity Logging create a capacity to *perform web-based audits and easily examine a trail of all activities performed on all files for all use.*



# Right to Erasure (“Right To Be Forgotten”)



Right to  
Access

Breach  
Notification

Right to be  
Forgotten

Data  
Portability

Privacy by  
Design

Consent

Individuals have the right to require a company to delete their personal data if the continued processing of data is not justified (especially where the data is inaccurate or incomplete).

Once the business has built operational dependencies on shared information, getting that data back involves a number of business impacts.

Enterprise Data Rights Management (EDRM) and Electronic File Synch and Storage (EFSS) make it possible to remove visibility to that information no matter where it is in the world.

# One Stop Shop – Centralized Consistent Privacy

**European** Data Protection Board (**EDPB**) is far less likely to find fault with an organization taking active protection measures involving data-centric privacy. With data centric security there's evidence of consistent rules applied at the moment information is taken into business custody and throughout the data lifecycle.



## Avoids over dependence on file encryption

If your answer to protecting data is encryption, consider that encryption on its own can be hacked and the greatest barrier to its success is that people simply don't use it.

File encryption alone *isn't persistent*, doesn't protect a file while it is open, does not support revoking access after distribution, and doesn't provide tracking of what is happening with the file.





# A data centric product and program approach

- Know your data flow
- Identify EU citizen personal data
- Flag systems needing opt-in, EU data access, correction and deletion requests, and age-gating requirements
- Shore up your ISMS



- Things to get right:
  - encryption or pseudonymisation of personal data
  - processes and capabilities to handle personal data access, correction, deletion and
  - portability requests
  - a Data Protection Impact Assessment process
  - a data breach response plan

# Some Technologies are more important - DRM plus EFSS

## Digital or Information Rights Management (DRM):

A set of technologies that provides control over how a given piece of protected content can be used including what the recipient can do with the file, for how long and from which device/IP location. Rights Management also provides rich tracking wherever the file goes and provides modification of usage controls or revocation of usage.

## Enterprise file sync-and-share (EFSS):

Enterprise file sync-and-share is a service that allows users to save files in cloud or on-premises storage and then access them on other desktop and mobile computing devices. This is a baseline product expectation to any modern enterprise, and soon, we'll find that all persons are using file storage as opposed to local storage. We'll see less thumb drives and more digital storage.

### **"Strategic Planning Assumption**

By 2020, information-centric capabilities, especially enterprise digital rights management (EDRM) encryption, will be the only durable, granular, file-level mobile data protection."

**Gartner Security & Risk Management Summit, 12 –15 June 2017 / National Harbor, MD**

# DLP plus Data Classification

## Data Loss Protection (DLP)<sup>2</sup>

is a comprehensive approach (covering people, processes, and systems) of implementing policies and controls designed specifically to discover, monitor, and protect confidential data wherever it is stored, used, or in transit over the network and at the perimeter. However, while sensitive information can be detected, DLP does nothing to secure information that must be exchanged to complete business processes.

## Data classification program:

is a program that categorizes data to convey required safeguards for information confidentiality, integrity, and availability; establishes controls required based on value and level of sensitivity. The challenge is that just because a document is classified, that does nothing to protect the information in transit, at work, or at rest. (Source: Derived from SANS Institute InfoSec Reading Room).

### **“Strategic Planning Assumption**

By 2020, information-centric capabilities, especially enterprise digital rights management (EDRM) encryption, will be the only durable, granular, file-level mobile data protection.”

**Gartner Security & Risk Management Summit, 12 –15 June 2017 / National Harbor, MD**

# How do we start a conversation about Global Data Protection? Ask!

Where is the sensitive data and who owns it?

How do you know who is accessing it?

Where is it flowing and how is it shared-  
including 3rd parties and vendor access?

What is the quantifiable value and risk?

How would you like to automate the access  
control process? What do you most want to  
accomplish through automation?





# REGULATORY USE CASES





# Regulatory Requirements v. Guidance and Frameworks

- U.S. - sector specific:
  - Federal Trade Commission Act – Section 5 Unfair and Deceptive Acts - 1914
  - The Fair Credit Reporting Act 1970
  - Federal Privacy Act of 1974
  - Family Educational Rights and Privacy Act of 1974 (FERPA)
  - Telephone Consumer Protection Act of 1991
  - HIPAA/HITECH 1996/2009
  - Children's Online Privacy Protection Act (COPPA) of 1998
  - Gramm-Leach Bliley (Financial Services Modernization Act of 1999)
- EU Data Protection Directive of 1995 (being replaced by General Data Protection Regulation, effective, May 2018). Privacy Shield U.S. – Europe replacing Safe Harbor.



The screenshot displays the EnterpriseGRC Assessment Universe interface. The top navigation bar includes links for Home, Corporate Governance GRC, ISMS Program, Services, and Training & Development. The main header reads "Assessment Universe". On the left, a sidebar menu lists various categories: Home, Notebook, Process Asset Library PAL, Audit Plan, Audit Types, Audit Phases, Audit Stage, Assessment Domains, Assessment Universe, Assessment Testing, RACI, Information Assets and Approvers, OSI Layer, Tool Type, Rules Mapping, Strategic Goals, Vendor and Stakeholder Info, GRC Tasks, Calendar, CSF Illustrative References, Recent, Drop Off Library, Deliverables, Issues, Risks, Risk Asset Class Rating, Cloud Audit Detail Control and Testing, Pages, and EU Data Privacy Legacy. The main content area features a "new item" button, a search bar, and a table of assessment items. The table has columns for Control ID, Control Objective, Test ID, Control Objective Description, Testing Procedure, Domain ID, and Risk. It shows a count of 144 items and lists several assessment frameworks, including Center for Internet Security Critical Security Controls Version 6.1 (5), NIST 800-171 (3), and PCI DSS V3.2 Copyright © 2016 VISA (6).

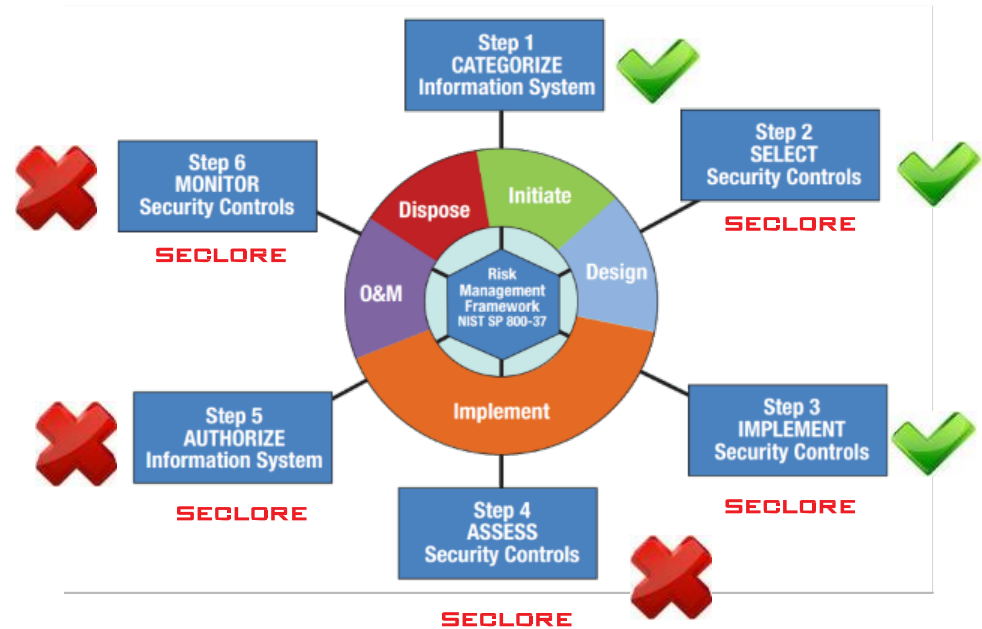
# Data Centric Cybersecurity Risk Management

**Aids Market Entry** = solid cybersecurity and a functioning risk management program.

**Answers Customers demand** cyber insurance

**Assesses Security Controls** is the most critical step of a risk management program.

**Missing the tools and expertise to manage data centric security** = missing the business boat.



RISK MANAGEMENT FRAMEWORK  
NIST SP800-37

Most Businesses are a combination of geographies and industries leveraging multiple regulations and standards.

Multiple standards support same technical functions.

System based controls are more reliable than manual controls

Example “Access Limitation” is a requirement in NIST 800-171, NIST 800-53r4, PCI DSS 3.2, ISO/IEC 27002:2013 and SOC 2 TSP

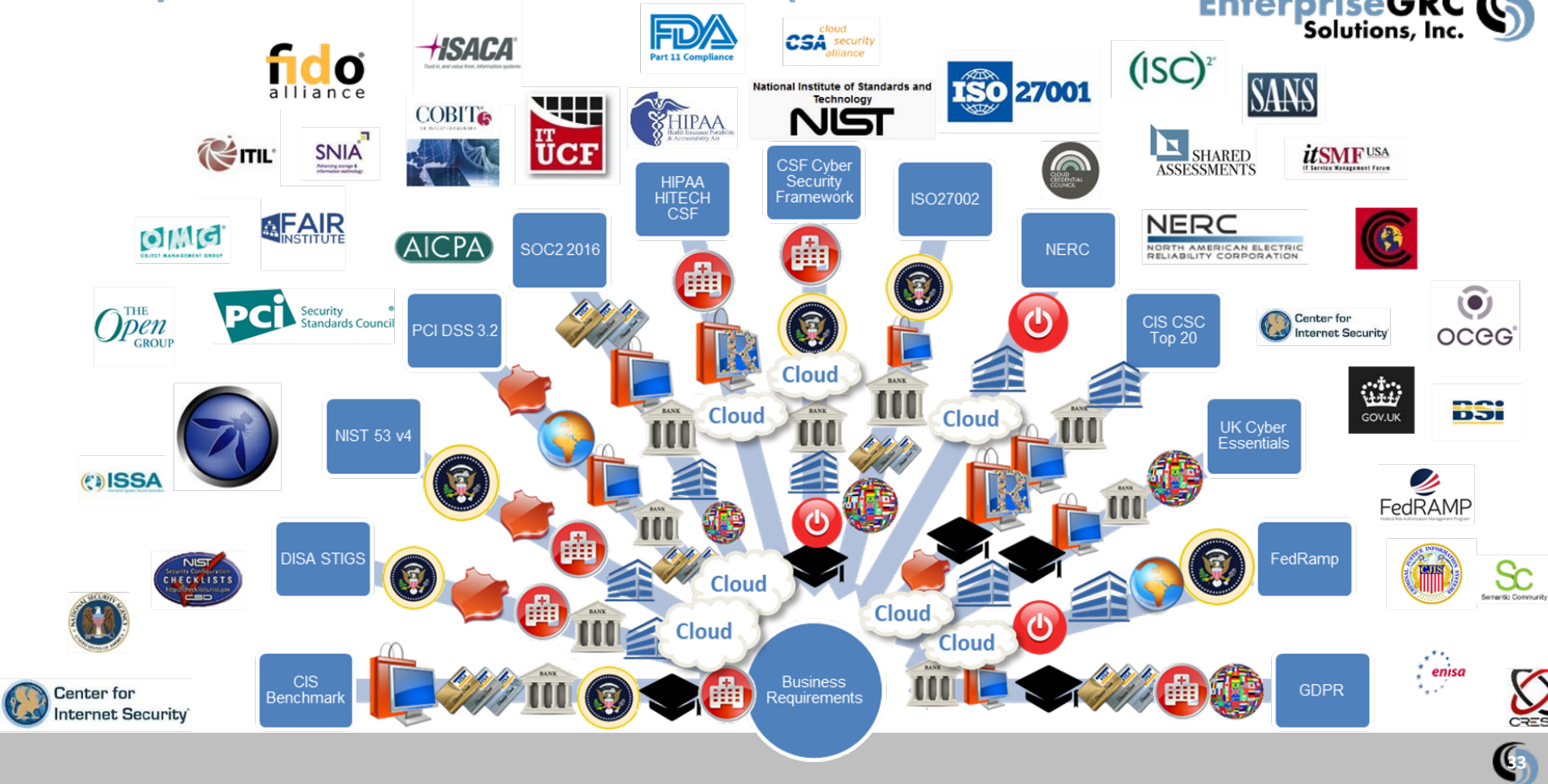
In each case, limits on access could be satisfied through use and monitoring of the functions found in an EDRM product like SECLORE.

Images show controls where EDRM can be used to automate a necessary access control function.

Center for Internet Security Critical Security Controls Version 6.1 (4)
CobiT Fourth Edition © ISACA (3)
Criminal Justice Information Services (CJIS) Security Policy (6)
CSF Framework for Improving Critical Infrastructure Cybersecurity (2)
General Data Protection Regulation (EU) 2016/679 (9)
HIPAA - HITECH Title 45 C.F.R. § 164 (1)
HITRUST CSF 2015 (2)

Center for Internet Security Critical Security Controls Version 6.1 (3)
ISO/IEC 27002:2013 € (4)
NIST 800-171 r1 (4)
NIST 800-53 r4 (1)
PCI DSS V3.2 Copyright © 2016 VISA (2)
Trust Services Principles and Criteria © 2016 AICPA (1)

# Industry Drives Risk Mandates. Frameworks help to meet them.



# Data Centric emphasis in meeting GDPR

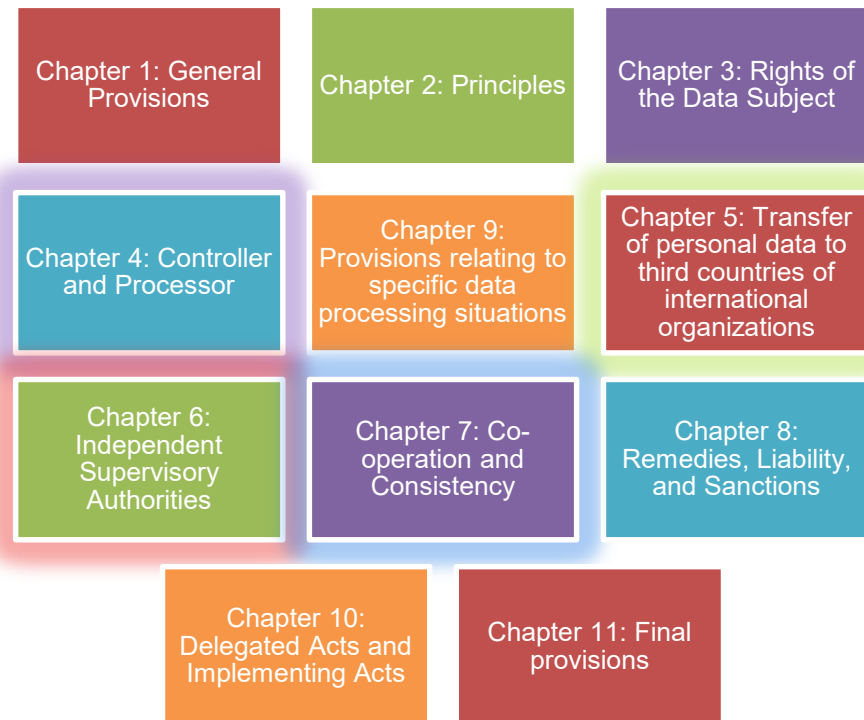
Data centric security products (like SECLORE) can have impact to enabling, tracking or verifying control objectives across multiple control framework domains. The majority of articles with applicability from GDPR are identified within the domains of:

**Controller and Processor**

**Transfer of personal data to third countries of international organizations**

**Independent Supervisory Authorities**

**Co-operation and Consistency**





# Security Risk Assessment Frameworks include data centric control requirements

We found 144 Control Assertions or objectives that could be better enabled through implementation of SECLORE application features.

To accomplish this, you need to implement that.

Center for Internet Security Critical Security Controls Version 6.1 (5)

CobIT Fourth Edition © ISACA (4)

Criminal Justice Information Services (CJIS) Security Policy (8)

CSF Framework for Improving Critical Infrastructure Cybersecurity (4)

Cybersecurity Risk MGT Program - Description Criteria © AICPA 2017 (1)

General Data Protection Regulation (EU) 2016/679 (14)

HIPAA - HITECH Title 45 C.F.R. § 164 (1)

HITRUST CSF 2015 (2)

ISO/IEC 27002:2013 € (17)

NCSC NATIONAL CYBER SECURITY STRATEGY 2016-2021 (5)

NERC CIP (9)

NIST 800-171 r1 (8)

NIST 800-53 r4 (42)

PCI DSS V3.2 Copyright © 2016 VISA (6)

Trust Services Principles and Criteria © 2016 AICPA (6)

## Capabilities

### Breadth and Depth of Security & Usage Controls

- Ability to restrict file access and usage to specific users
- Ability to restrict file access and usage to specific user groups
- Ability to restrict file access to a specific computer
- Ability to restrict file access to a specific mobile device
- Ability to restrict file access on any mobile device
- Support for watermarked viewing of files
- Ability to restrict editing of files
- Ability to restrict printing of files
- Support for watermarked printing of files'
- Ability to restrict copying content from a file to an external location
- Ability to restrict screen grabbing via the Prnt Scrn key

\* Also known as Information Rights Management (IRM) / \* Upon integration with DLP systems.

## Capabilities

### Breadth and Depth of Security & Usage Controls

- Ability to restrict screen grabbing via third-party screen capturing tools (e.g. Camtasia, Snagit, etc.)
- Ability to restrict screen sharing via conferencing tools (e.g. Webex, GotoMeeting etc.)
- Ability to restrict a user to cut and paste content from a protected document to a non-protected document
- Ability to restrict file access via remote connections (e.g. Windows Remote Desktop, Citrix, etc.)
- Ability to restrict file access on virtual environments (e.g. VDI, Citrix environments, virtual machines)
- Ability to restrict file access and usage based on date and time
- Ability to restrict file access and usage based on time period (no. of days)
- Ability to expire all copies of a file remotely at any time
- Ability to protect files with built-in automatic expiry
- Ability to restrict file access while offline

Government Sector  
DOJ  
Federally Funded



- CIS CSC top 20 6.1
- Criminal Justice Information Services (CJIS)
- CSF Framework for Improving Critical Infrastructure Cybersecurity
- Cybersecurity Risk MGT Program - Description Criteria © AICPA 2017
- FFIEC
- FedRamp
- General Data Protection Regulation (EU)
- ISO/IEC 27002:2013 €
- NCSC NATIONAL CYBER SECURITY STRATEGY
- NIST 800-53 r4
- PCI DSS V3.2
- SOC2 Trust Services-AICPA

## SECLORE

- Persistent, granular usage controls
- Remote management of usage controls
- Compliant file-sharing
- real-time risk scoring
- continuous compliance reporting
- remediation steps
- improved enterprise security posture
- reduced attack surface

- **Persistent, granular usage controls** making it easy to ensure sensitive IP (e.g., drawings, assemblies, parts) remains secure wherever it travels and is stored.
- **Remote management of usage controls** allow the file owner to dynamically modify or revoke usage policies to previously shared files no matter where the file is located.
- **Compliant file-sharing** maximizes business agility as files have security mechanisms wherever they go and however they travel. File sharing, cloud services, mobile devices and external partnerships can be embraced with confidence.
- **End-to-end auditing and regulatory compliance** makes it possible to automatically collect authorized usage actions as well as unauthorized usage attempts. Alerts, dashboards, and detailed reports provide rapid, real-time visibility into document usage.

# *Make Data the New Perimeter*

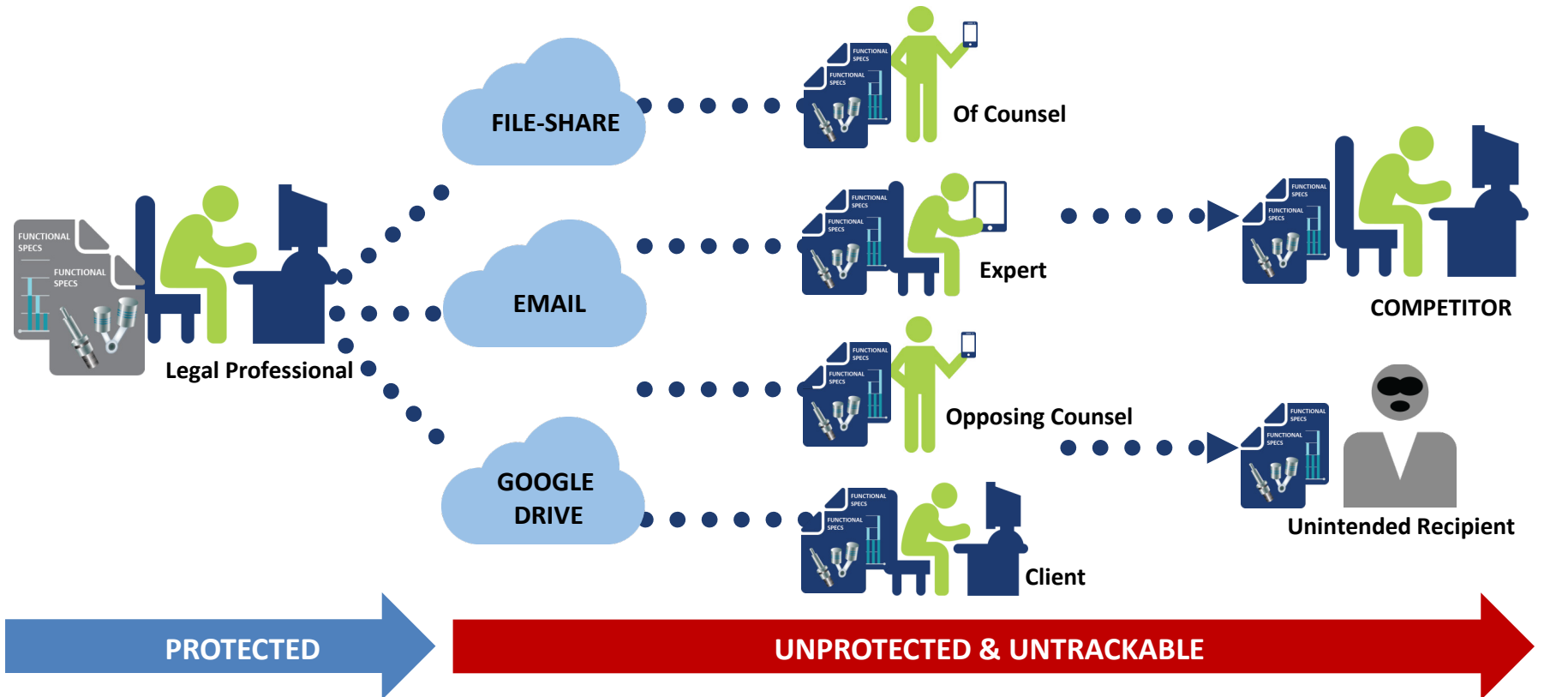


# Seclore Document Rights Management: Addresses a Huge Security Gap



**Sensitive information is flowing outside of organizations at an unprecedented rate**

# What and Where is the Problem?





# Control Is Important



# Persistent, Granular Usage Controls



## WHO can access the file?

*Specific Users/groups within and outside the organization*



## WHAT rights do they have?

*View, edit, print, copy content, take screen grabs, work offline*



## WHEN can they do it?

*Automatic file expiry, date and time ranges, number of days from first access*



## WHERE can they do it?

*Specific computers, devices, IP addresses*

- **Permanence:**  
*Protection persists with the file forever*
- **Remote Control:**  
*File rights can be changed from anywhere in the world*
- **Audit Trail:**  
*All activities are tracked*

# Automatically Audits Usage of Information

## List File Activities

### List File Activities

Criteria : 'file id' equals '24'

Total : 25

Activity Id	File Id	File Name	User	Activity	Date	Authorized?	Mode
<u>131</u>	<u>24</u>	Invoice0387.docx	John Doe	Access on Virtual Machine	10 Apr 2014 01:13:48 PM	Y	Online
<u>130</u>	<u>24</u>	Invoice0387.docx	Rich Roe	View	10 Apr 2014 01:13:11 PM	N	Online
<u>129</u>	<u>24</u>	Invoice0387.docx	Rich Roe	Unprotect	10 Apr 2014 01:10:02 PM	N	Online
<u>128</u>	<u>24</u>	Invoice0387.docx	John Doe	Protect	10 Apr 2014 01:08:32 PM	Y	Online
<u>127</u>	<u>24</u>	Invoice0387.docx	John Doe	View	10 Apr 2014 01:08:32 PM	Y	Online
<u>126</u>	<u>24</u>	Invoice0387.docx	John Doe	Edit	10 Apr 2014 01:08:32 PM	Y	Online

*Automatically captures and consolidates file usage data from distributed environments:*

**WHO** *accessed the file,*

**WHAT** *the user did with the file,*

**WHEN** *and from*  
**WHERE**

# Usage Policy Attributes



## Permanence

Protection *will always persist* with the file



## Remote-Control

Change your usage policies  
for information sitting *anywhere in the world*



## Audit Trail

All *activities on information tracked*:  
Users, activity type, date/time, location

# Easily Access Protected Documents

- *Browser-based access*
- *Lite-weight agents*
- *iPhone, iPads, Android, Windows*

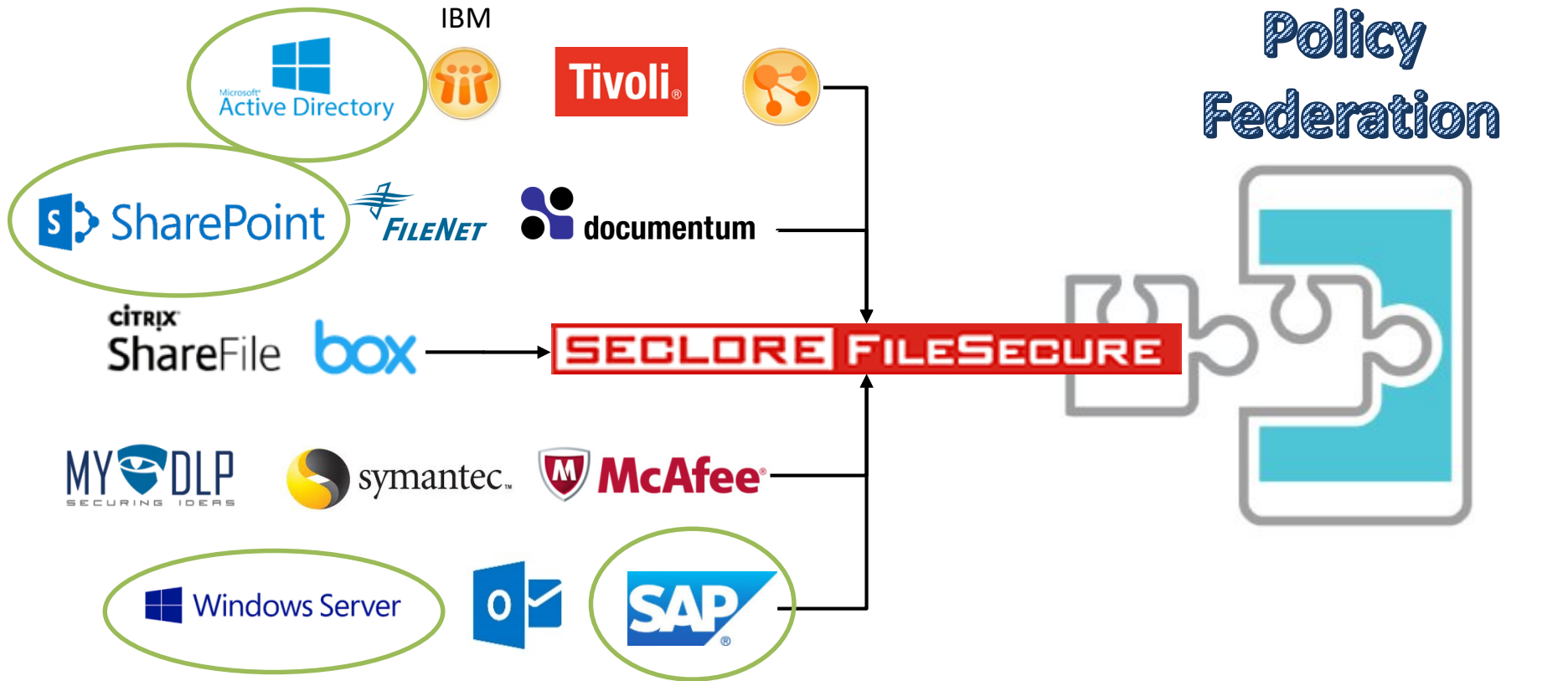




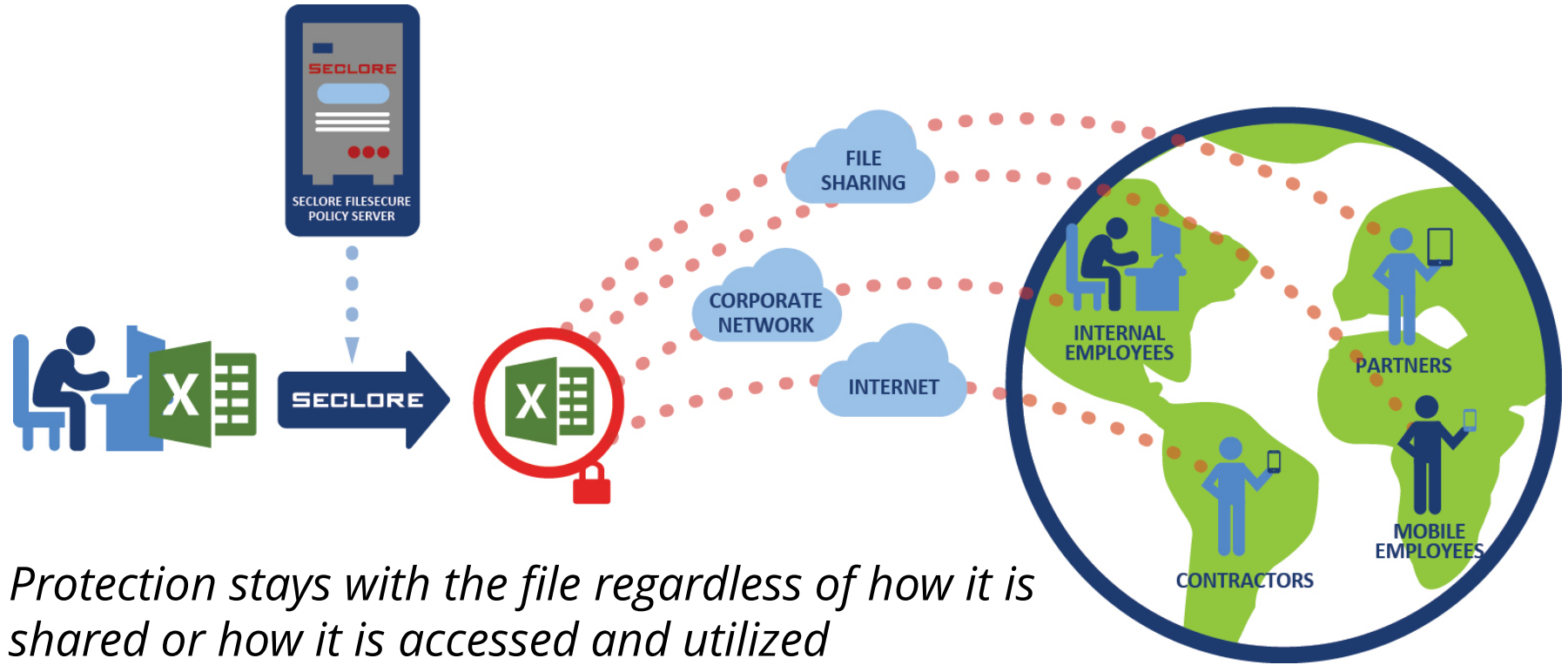
# *Automated Usage Policies Applied to Files*



# Automate File Protection with Pre-Built Connectors



# Utilize Any File-Sharing Method Without Risk



*Protection stays with the file regardless of how it is shared or how it is accessed and utilized*

# Q & A

Robin Basham, CEO, Founder,  
EnterpriseGRC Solutions  
[robin@enterprisegr.com](mailto:robin@enterprisegr.com)  
[@EntGRCSolutions](#)

Bob Metzger, Shareholder, RJO  
[RMetzger@rjo.com](mailto:RMetzger@rjo.com)  
<https://linkedin.com/in/robertmetzger>  
[@RobertMetzger2](#)

Lisa Harchuck Popadic, Director of Legal  
Business Development, Seclore  
[lisa.popadic@seclore.com](mailto:lisa.popadic@seclore.com)  
[@secloretch](#)

# Thank You!

[www.seclore.com](http://www.seclore.com) | [info@seclore.com](mailto:info@seclore.com) | <http://blog.seclore.com>