GDPR, dan pre

Vladimir Vučinić
Net++ technology

Šta je sutra?

The Drive for Data Privacy

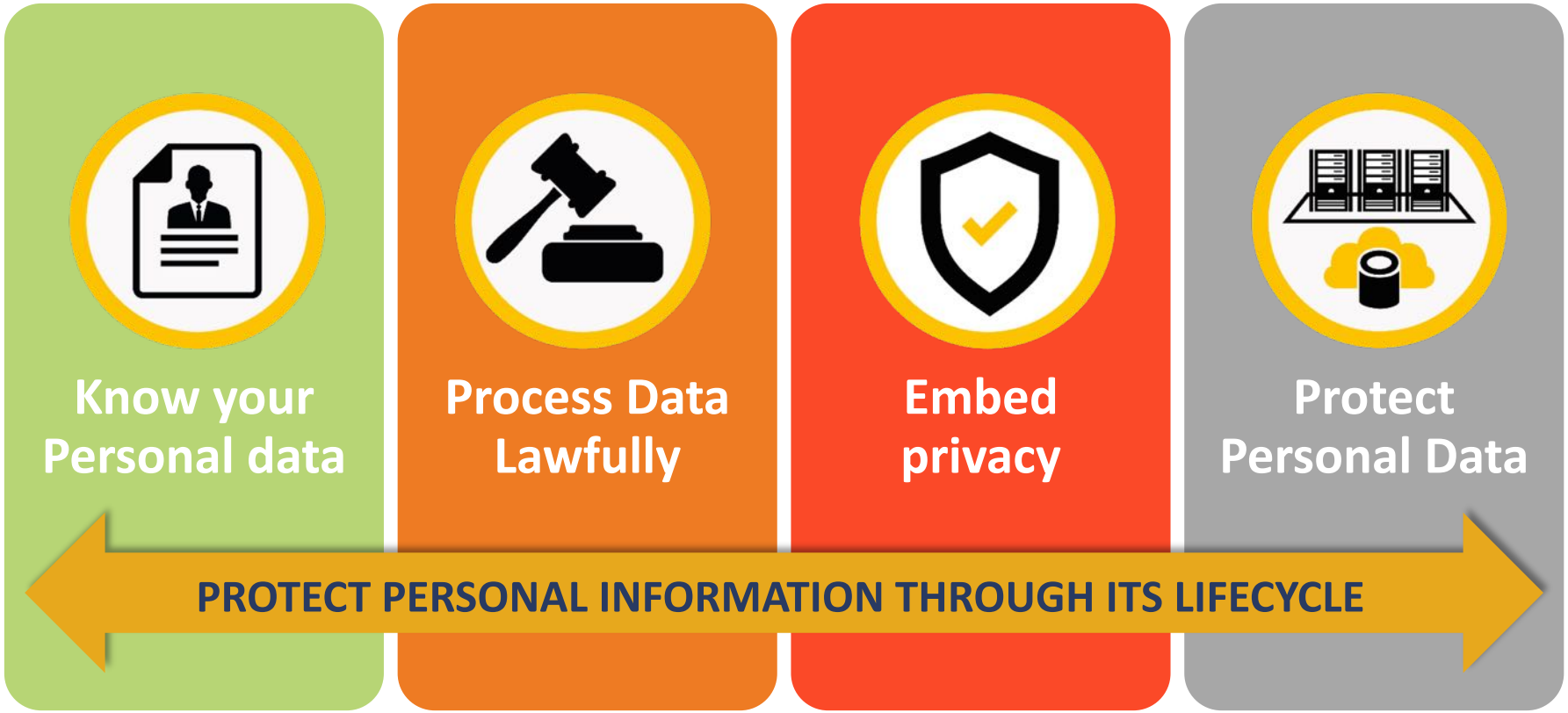
Drivers

- Regulations
- Press Headlines
- Reputation
- Business Opportunity
- Customer Expectations

Inhibitors

- Lack of Business Ownership
- Data Growth
- Evolving Threat landscape
- Lack of Visibility
- Emerging Technology

Technology Considerations for the GDPR



Typical Customer Timeline for the GDPR

96%
Do not fully understand GDPR

9 in 10
Have concerns about ability to become compliant

22%
Consider compliance at top priority in the next two years

Awareness Phase
What is it and does it really impact me?

- Thought Leadership
- Awareness
- Education

Discovery & Planning
What do I need to do and when by?

- Risk Assessments / Gap Analysis
- Advisory Services
- Information Governance Plans
- Budgeting / Hiring Key Staff

Implementation
Making Changes to Prepare

- Policy and Organisational Updates
- Addressing Technology Gaps
- Purchasing of Software and Technology

Privacy & Security

Privacy
The “What” of personal data protection

Strategy

Security
The “How” of personal data protection

Tactics

“You can have security without privacy but you can’t have privacy without security”

Data Governance Framework to Manage Privacy

Symantec

Collect

- Define and Locate Personal Data
- Secure Technology that Collects Personal Data
- Record Consent from Data Subjects
- Pseudonymisation and obfuscation of personal data

Process

- Detect and Block Threats to Data in Use
- Validate Data Processors
- Privacy Impact Assessments
- Secure Transfer and Storage of Collected Data

Retain & Secure

- Restrict Processing of Data YOU have to Retain
- Protect Data at Rest
- Control Access to Data
- Prevent Data Loss, Report Breaches

Manage

- Risk Management of Info Lifecycle
- Validate Data Subjects Invoking Rights
- Educate DPOs on Cyber Risk
- Minimise, Anonymise, Erase Data

Privacy

Security

How Symantec can assist with the GDPR ?

What broad areas do I need to focus on for GDPR?

How do I manage and report on my information risk management practices?

What personal data is out there and ***where*** is it?

Who can access personal data and ***who has*** accessed it?

Can we ***control where*** data resides?

Can we ***control what*** personal data is accessible and ***who*** can access it?

Can we ***encrypt / obfuscate*** personal data?

Can we ***detect*** unauthorised access or breaches of personal data?

Can we quickly and thoroughly ***notify*** in the event of a breach?

Risk Management
CCS
EPM

Information Centric Security

DLP / CASB
VIP
Encryption
CDP

Breach Response
MSS / ATP
Incident Response
Security Analytics

Symantec Supports Across Data Privacy and Security

PREPARE

PROTECT

DETECT

RESPOND

Technology Risk Management

Understand Data Risk

DLP Data Insight

CASB Audit

CCS

EPM

Understand, Report, and Remediate Compliance

Personal Data Protection Everywhere

VIP / MPKI

DLP

Encryption

CASB

Web

CDP

Advanced Breach Detection, Remediation, & Notification

Endpoint

Email

Server

Web / CASB

ATP

Analytics

Cyber Security Services

Unparalleled Threat Intelligence

Endpoint
175M endpoints protected

Email
2Bm emails scanned/day

Physical & Virtual Workloads
64K Datacenters protected

Cloud Security
12,000 cloud applications secured

Web
1.2Bn web requests secured/day

Risk Scenarios

Examples of risks/events in GDPR that Controllers and Processors need to prepare/plan for

Practical Scenario 1: How could I protect against personal data loss?

- **Data In Motion:**
  - Collection on a website: Is the traffic encrypted?
  - Transfer via email: Is the email encrypted?
  - Transfer via a platform: Is the platform secure?
- **Data At Rest:**
  - Storage on servers: Is the data center secured?
  - Storage at end-points: Are the devices protected?
- **Data In Use:**
  - In house: Is access control in place?
  - Outsourced: Are cloud and shadow IT addressed?
  - In management: Is data loss prevention in place?

Website Security

Email Encryption

FileShare Encryption

DCS, DLP, Data Analytics

PGP, SEP, ATP

VIP, mPKI

CASB / CDP

DLP

Practical Scenario 2: How do I mitigate the risk to data subjects?

- **General Risk Assessment**
  - Do I track threats affecting my line of business?
  - Do I track the risk to the kind of data I handle?
  - Do I track the risk posture of the vendors I use?
- **Risk Of Breach Of Sensitive Data, Of Professional Secrecy:**
  - Do I classify information based on sensitiveness?
  - Do I apply specific policies to specific categories?
- **Risk Of Identity Theft Or Fraud:**
  - Do I segregate directly identifiable information?
  - Do I restrict access to re-identification keys?
  - Is my certificate and key management robust?

CSS
Threat Intelligence
CASB

DLP

CDP

VIP

mPKI

Practical Scenario 3: Minimising Risk In Case Of A Breach

- **Pseudonymisation (article 32 paragraph 1(a)):**
  - Have I pseudonymised the data?
  - Can I prevent reversal of pseudonymisation?
- **Encryption (article 33 paragraph 3(a)):**
  - Can I prove that the breached data is encrypted?
  - Can I prove that the encryption is strong enough?
- **Ongoing Testing and Evaluation (Article 32 1(d))**
  - a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing

CDP

PGP

IT Management Suite, Control Compliance Suite

Data Loss Prevention

Answers these critical questions about your information

Data Loss Prevention

Answers these critical questions about your sensitive data

Where does your confidential data live?

DISCOVER

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

Data Loss Prevention

Answers these critical questions about your sensitive data

How is it being used?

MONITOR

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

Data Loss Prevention

Answers these critical questions about your sensitive data

How do you prevent data loss?

PROTECT

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

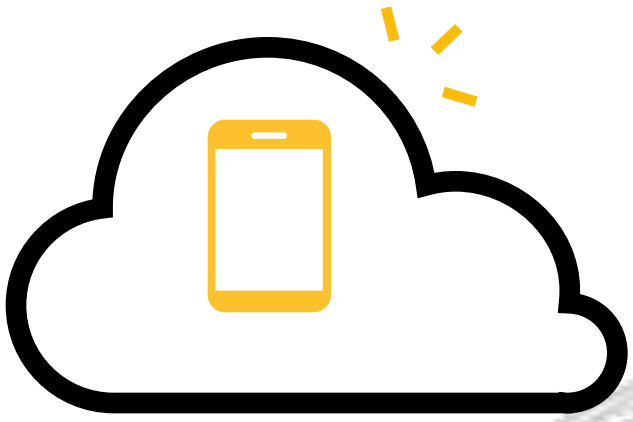
Solution Overview

Symantec™

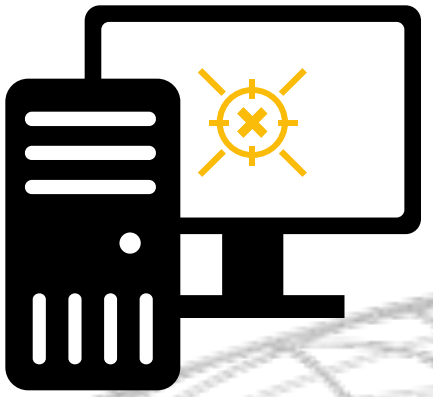
Symantec Data Loss Prevention

Gives you visibility and control of your information everywhere

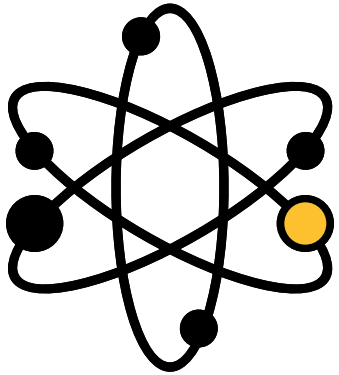
CLOUD



ENDPOINT

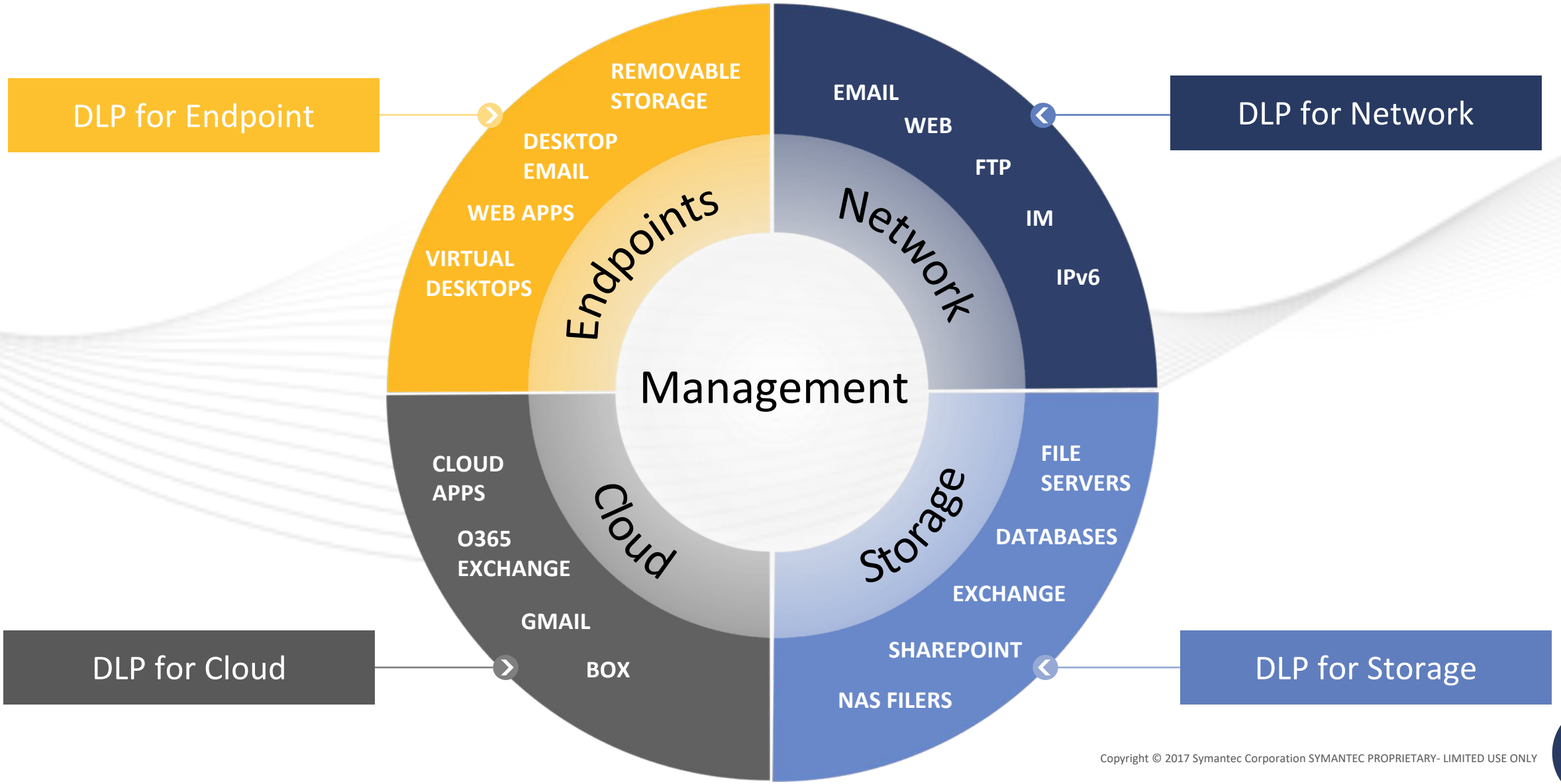


NETWORK



STORAGE

Broadest coverage of data loss channels



Protects any type of data

With the most comprehensive data detection technology

CUSTOMER INFORMATION

- Credit Card Info
- Medical Records
- SSNs and Government IDs
- Financials

COMPANY INFORMATION

- Intellectual Property
- M&A and Strategy
- Internal Auditing
- HR Records

Manage easily

With unified data loss policies across all channels

DETECTION

CONTENT	CONTEXT
Credit Cards	Who?
SSNs	What?
Intellectual Property	Where?

RESPONSE

ACTION	NOTIFICATION
Notify	User
Justify	Manager
Encrypt	Security
Prevent	Escalate

Most comprehensive data detection

Gives you the highest accuracy and minimizes false positives

DESCRIBED CONTENT MATCHING

DESCRIBED DATA

Non-indexable data

EXACT DATA MATCHING

STRUCTURED DATA

Account Numbers, Credit Cards, Government IDs,

INDEXED DOCUMENT MATCHING

UNSTRUCTURED DATA

Financial Reports, Marketing Plans

MACHINE LEARNING

UNSTRUCTURED TEXT

Source Code, Product Designs

FORM RECOGNITION

IMAGES

Scanned or Electronically-Filled Forms

"Symantec offers the most comprehensive sensitive data detection techniques in the market, with advanced functionality that can cover a wide breadth of data loss scenarios."

Magic Quadrant for Data Loss Prevention, Gartner, January 2016

Protect forms and documents

With Symantec DLP Sensitive Image Recognition

1 Collect blank forms and upload to DLP

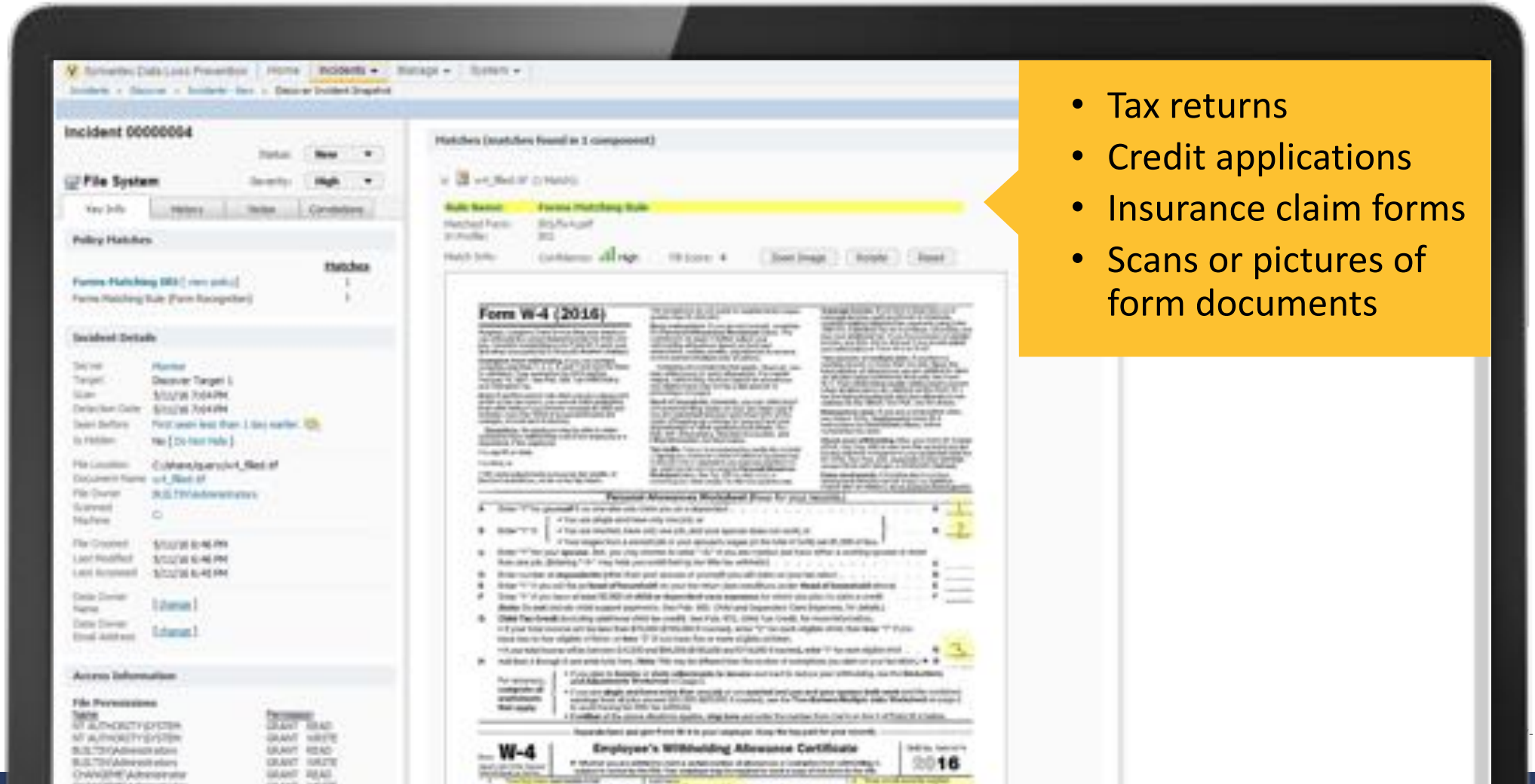
2 DLP indexes the forms and creates a form recognition profile

3 Add the profile to your data loss policy

4 DLP detects data in images of filled-in documents, including handwriting

Protect forms and documents

With Symantec DLP Sensitive Image Recognition

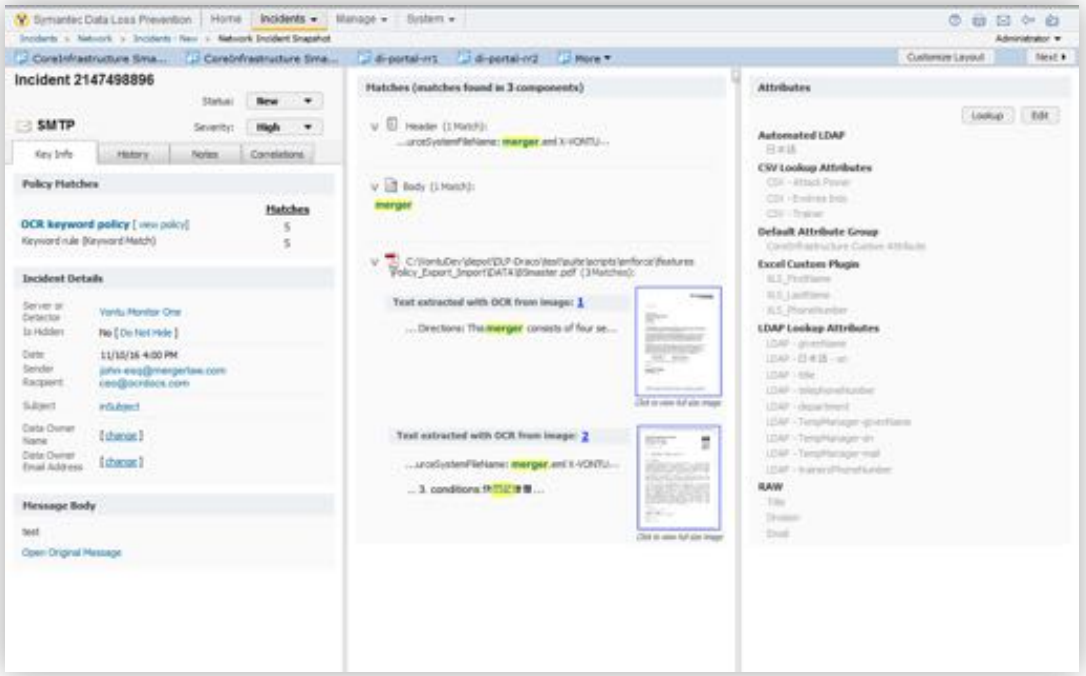


- Tax returns
- Credit applications
- Insurance claim forms
- Scans or pictures of form documents

Protect sensitive images

With Symantec DLP Sensitive Image Recognition

- Extracts text from images: scanned documents, screenshots, photos
- For use with preexisting policies and rules
  - OCR text treated same as conventionally extracted text
  - Incident snapshot indicates OCR origin
- Support for over 100 languages
- Support for custom dictionaries
  - Hints for challenging words like proper nouns
- Support for all server-side DLP detection channels



Protect sensitive images

With Symantec DLP Sensitive Image Recognition

SCANNED DOCUMENTS

IMAGES

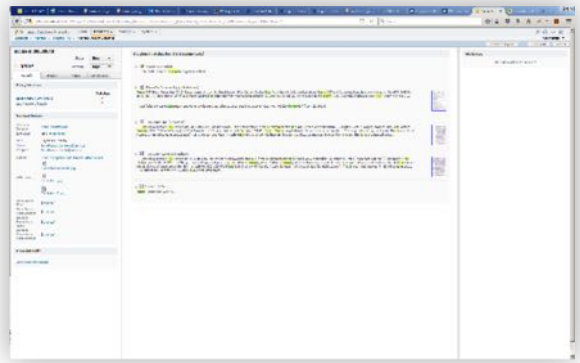
SCREENSHOTS

OCR Engine

EXTRACTED TEXT

Existing DLP policy (DCM, EDM, IDM, and VML)

DLP INCIDENTS

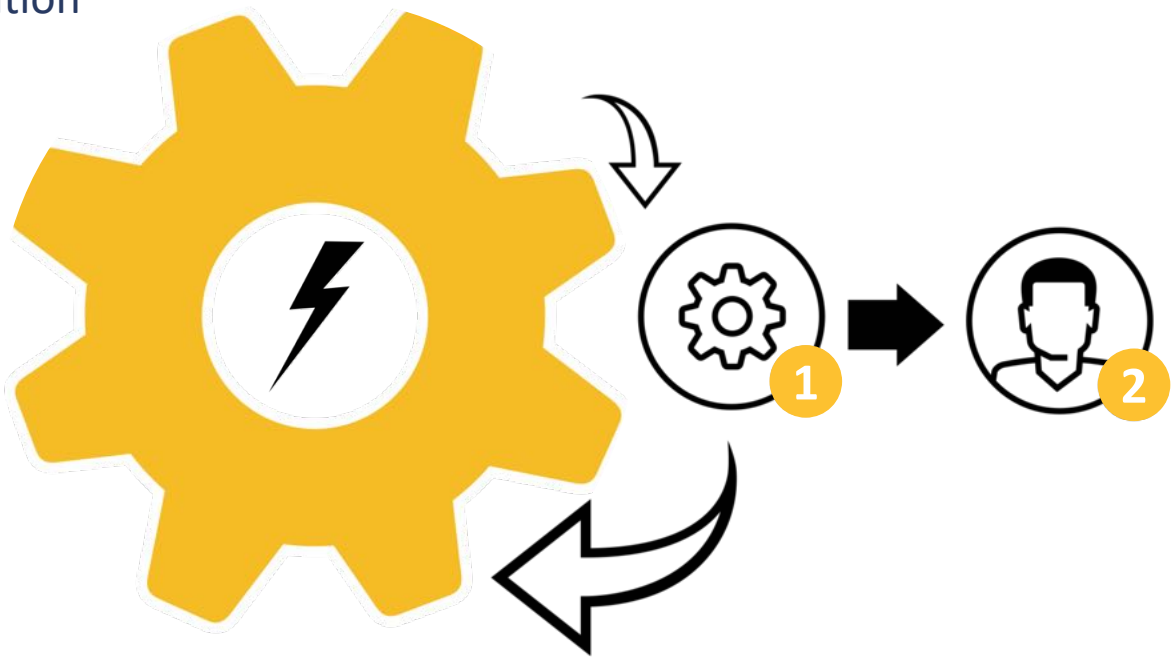


Respond faster

With sophisticated incident remediation workflow

90% of **DLP** is Incident Response

- **Right Automation |** Resolution, Enforcement, Notification
- **Right Person |** Route Incidents to Right Responder
- **Right Order |** High Severity of Incidents First
- **Right Information |** 5-Second Test
- **Right Action |** 1-Click Response
- **Right Metrics |** Prove Results to Execs and Auditors




Protecting your data in the cloud

Protect data in the cloud

With Symantec DLP Cloud Services

DLP Cloud with CloudSOC

FOR CLOUD APPS

DLP Cloud Service for Email

FOR OFFICE 365 EXCHANGE, GMAIL

Protect data in cloud apps

With Symantec DLP and Cloud Access Security Broker

Symantec Data Loss Prevention

The Gold Standard in DLP

+

Symantec CloudSOC

Leading-Edge Cloud Access Security Broker

Extend DLP to capture ALL sensitive data at rest and in motion the cloud

Leverage existing policies and workflows without compromising performance

Gain full cloud access security broker functionality

Extending DLP into the Cloud

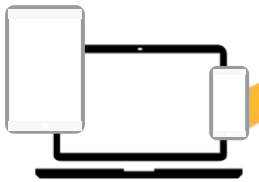
Extend DLP to 60+ Cloud Apps
Apply Fine-Tuned Policies to Cloud
Leverage Workflow Integrations

Gain Full CASB Functionality

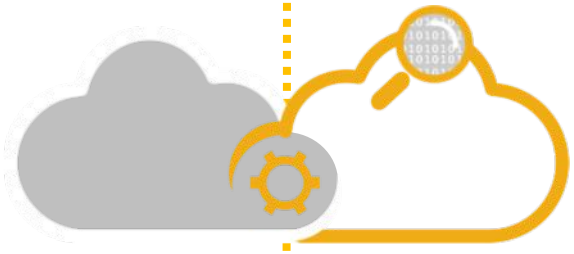
- Shadow IT Analysis
- Granular Visibility and Control
- User Behavior Analytics

Direct to Net

Direct to Net



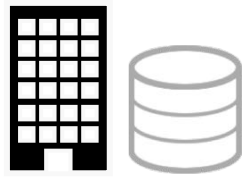
Unmanaged Devices
Extended Perimeter



Symantec CASB

Symantec DLP Cloud

Managed Devices w/ Symantec DLP
Endpoint Agent



Corporate Datacenter

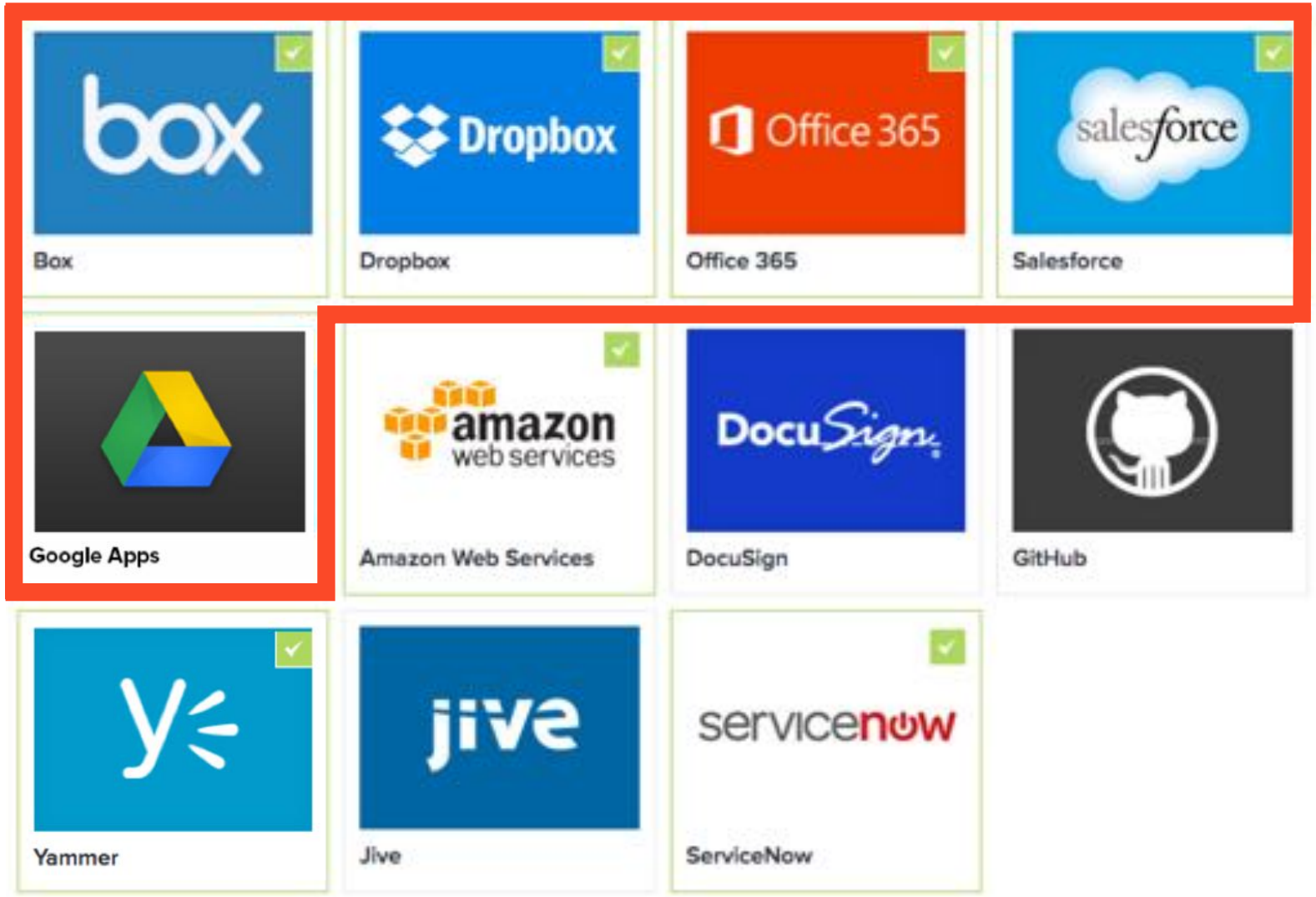
Symantec DLP
Management Console

Coverage for sanctioned apps

API Coverage for Cloud Apps:

11 Total

5 With DLP



Coverage for unsanctioned apps

Gateway Coverage for Cloud Apps:

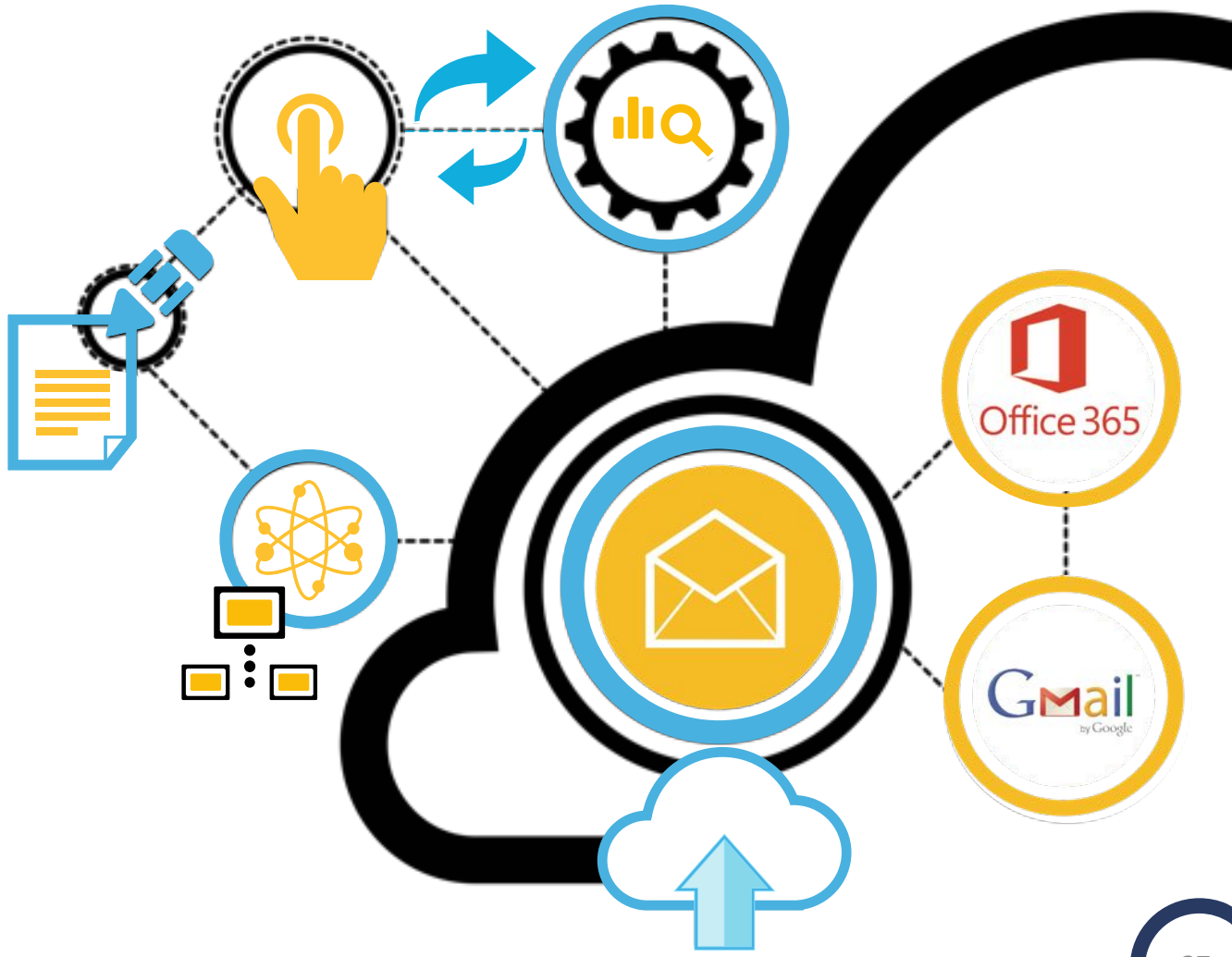
100+ **86**

Total With DLP

Complete Email Security for Office 365 and Gmail

With DLP Cloud Service for Email with Cloud Console

- Protects sensitive emails sent from Microsoft Exchange Server, Office 365 Exchange Online and Gmail for Work
- Adds a powerful layer of data protection to strengthen outbound email security
- Leverages Symantec Email Security.cloud with inbound protection against malware, spam and bulk email
- 100% cloud-based solution makes it easy to deploy and manage



Superior Cloud Email Protection

With industry-leading email security and data loss prevention

COMPLETE CLOUD EMAIL SECURITY

- Superior inbound and outbound email protection for Office 365 and Gmail
- 100% cloud-based solution deploys easily – no software or hardware!

EMAIL PROTECTION

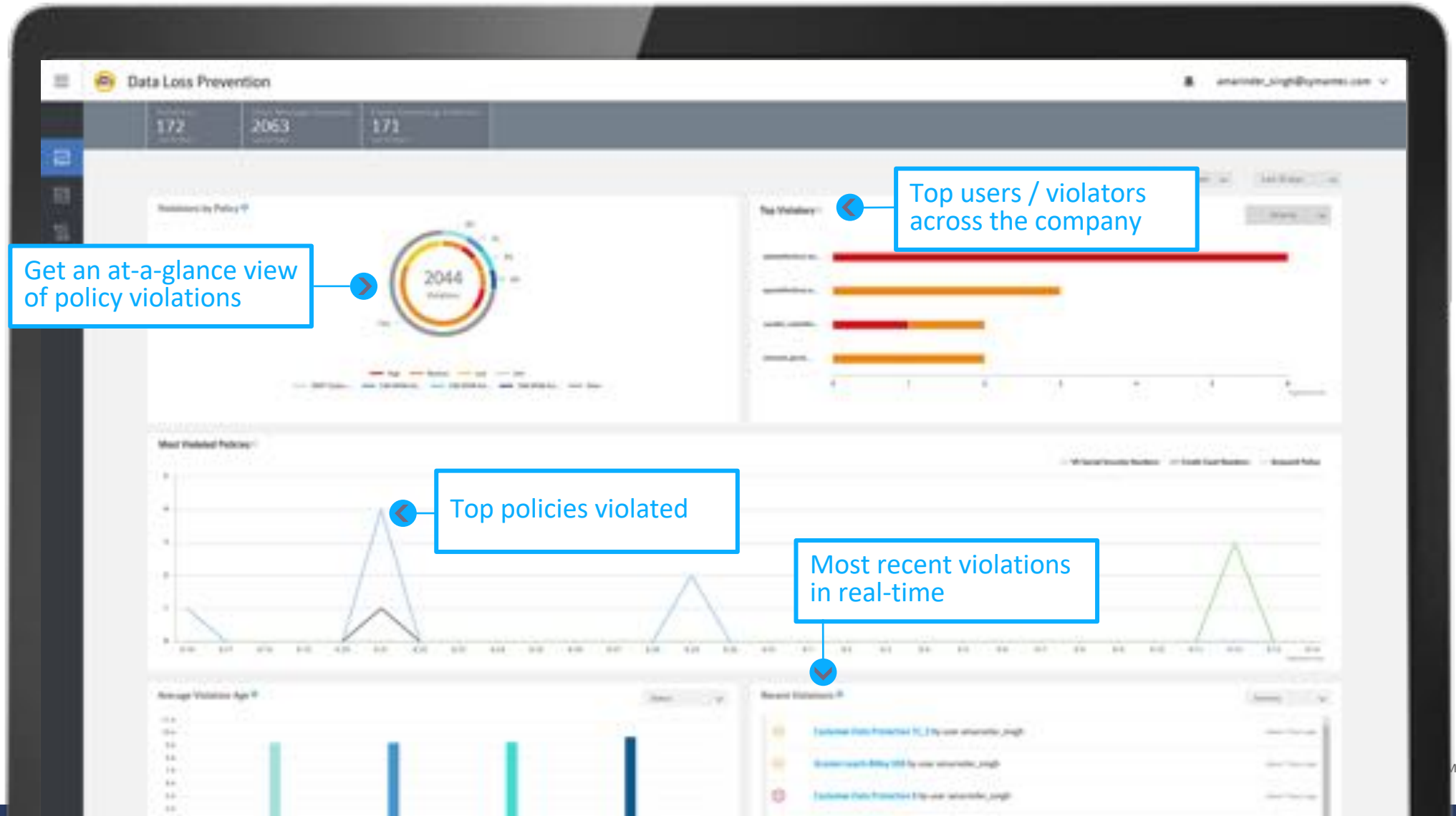
- Safeguards users from inbound email threats such as phishing, malware, spam
- Stops ransomware and business email compromise with multi-layered detection

SENSITIVE DATA PROTECTION

- Catches data loss other solutions miss with powerful, cloud-based content detection
- A sleek cloud console makes it easy to manage polices and violations
- Dozens of built-in policy templates get you up and running quickly

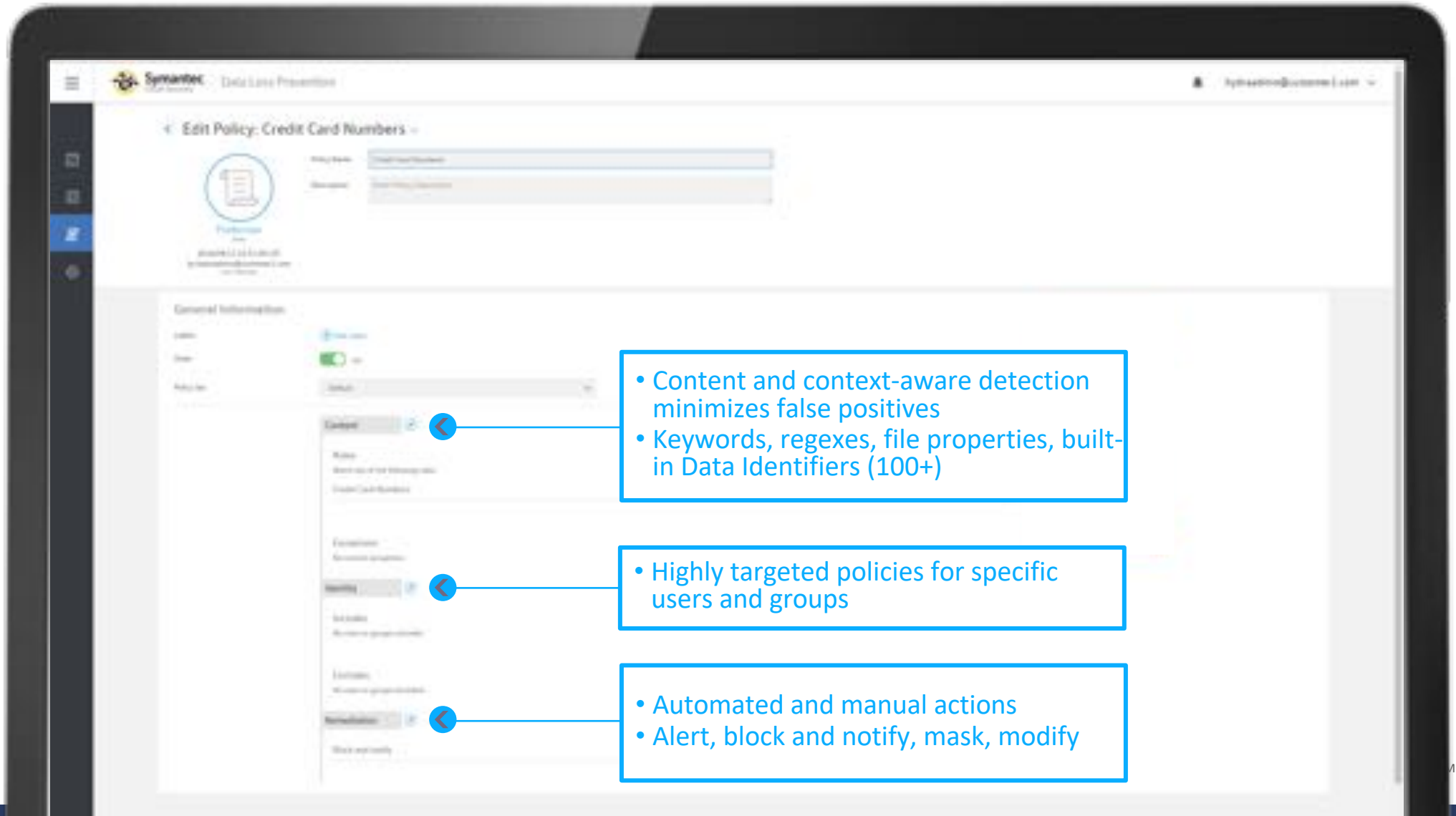
DLP Cloud Console

Dashboard View



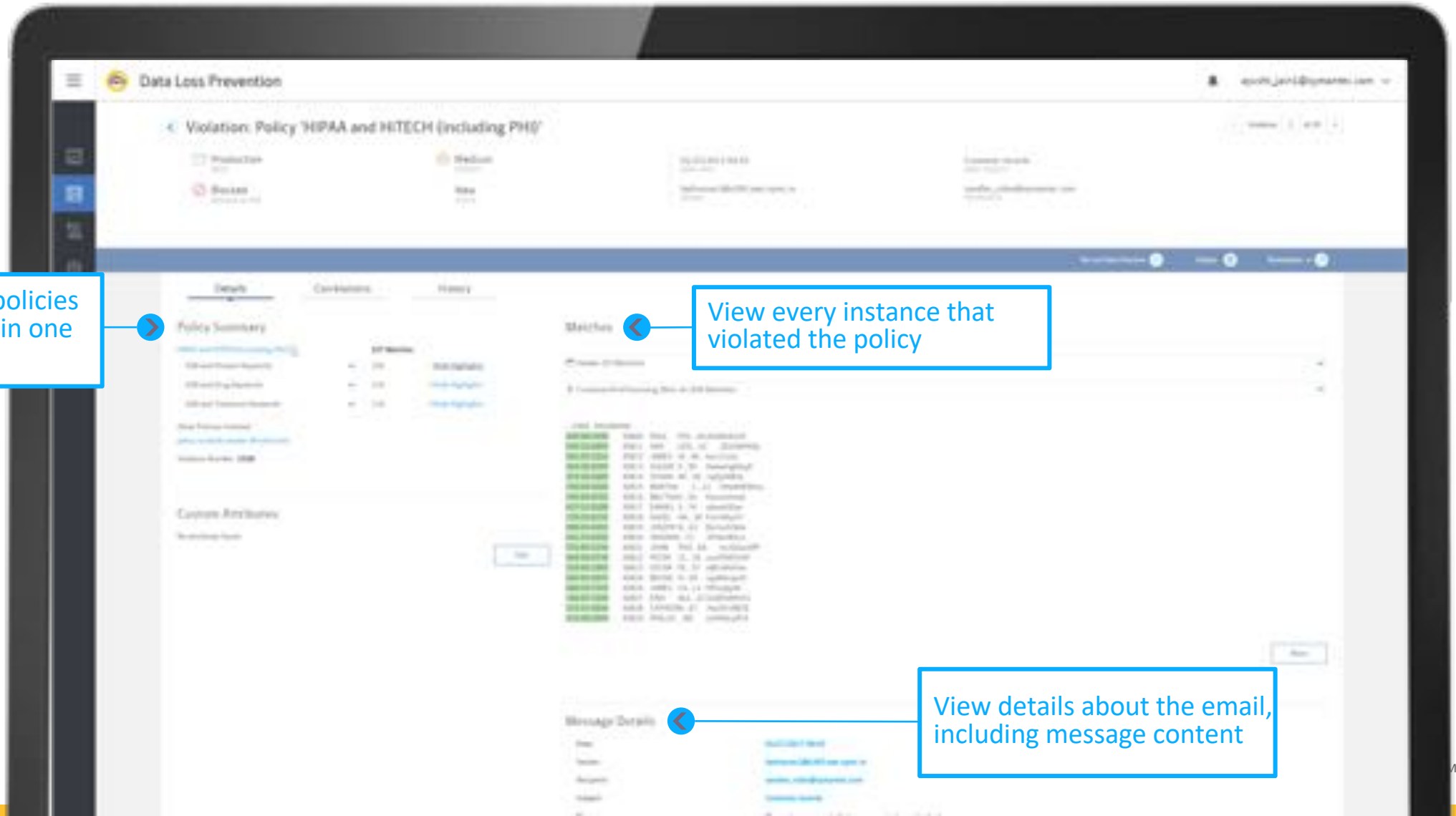
DLP Cloud Console

Policy Authoring



DLP Cloud Console

Violation Remediation



View violated policies and drill down in one click

View every instance that violated the policy

View details about the email, including message content

Information Centric Security

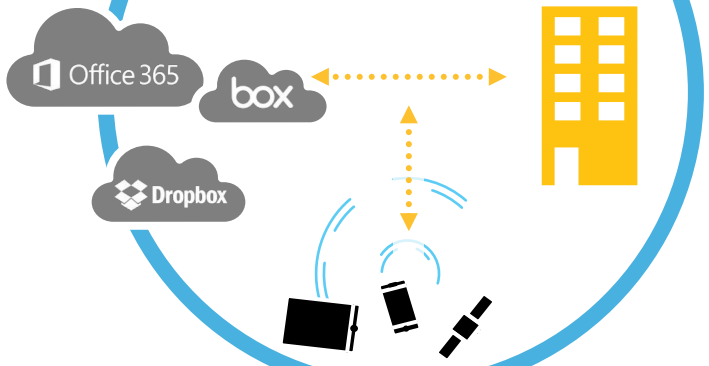
Symantec™

New trends in data protection

Symantec

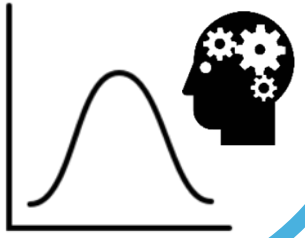
Trends in Data Protection

Data going everywhere



Privacy & data regulations

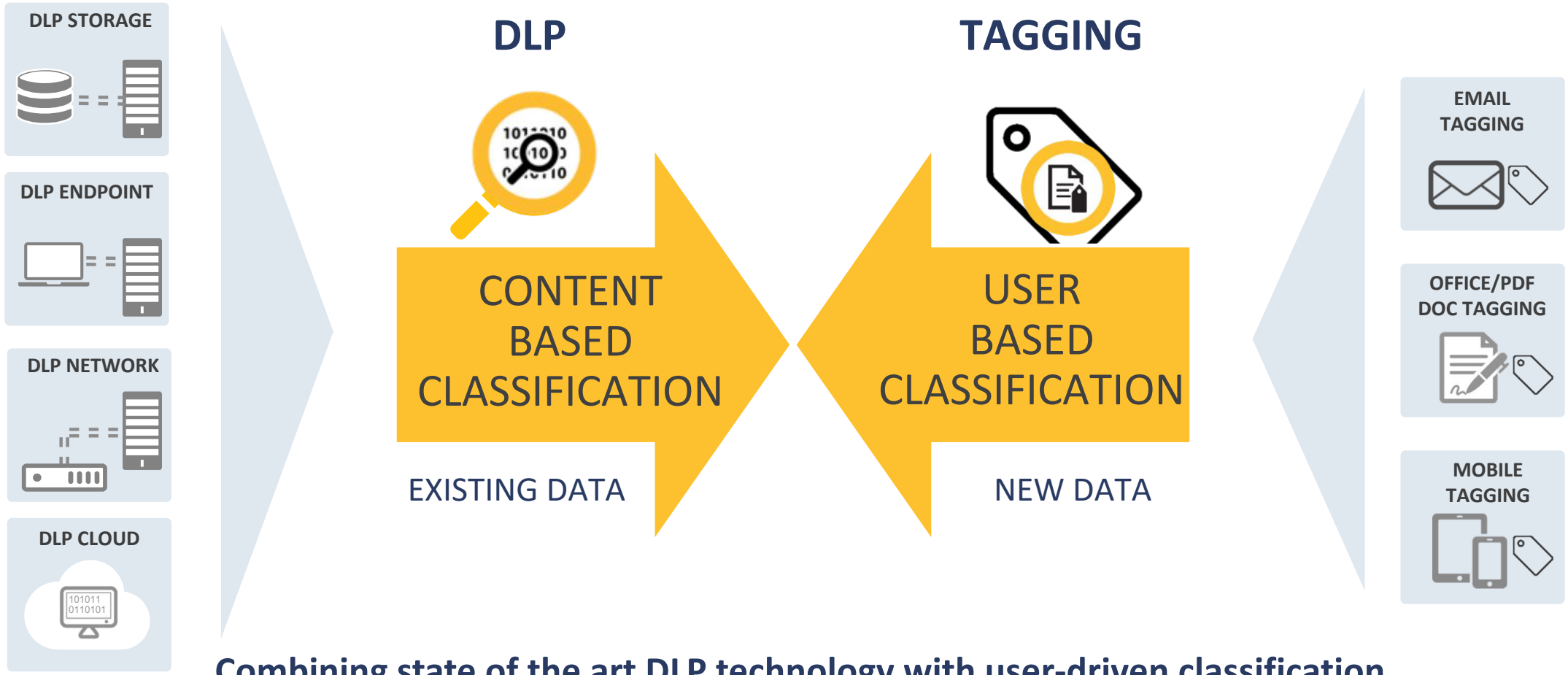
Insider risk & behavior analysis



Machine learning

Augment DLP with Data Classification

DLP with Symantec Information Centric Tagging (ICT)



Combining state of the art DLP technology with user-driven classification to identify and protect sensitive data

Protect sensitive data when it leaves the managed channels

DLP with Information Centric Encryption (ICE)

DLP/Tags identify confidential data to automatically **ENCRYPT**	**ENCRYPTION** "travels" to protect data everywhere (**DRM**)
ICE Principles	
IDENTITY drives decryption, providing **visibility & control**	

Protects your organization's sensitive data across its lifecycle. Integrates CASB, DLP, Encryption and Identity

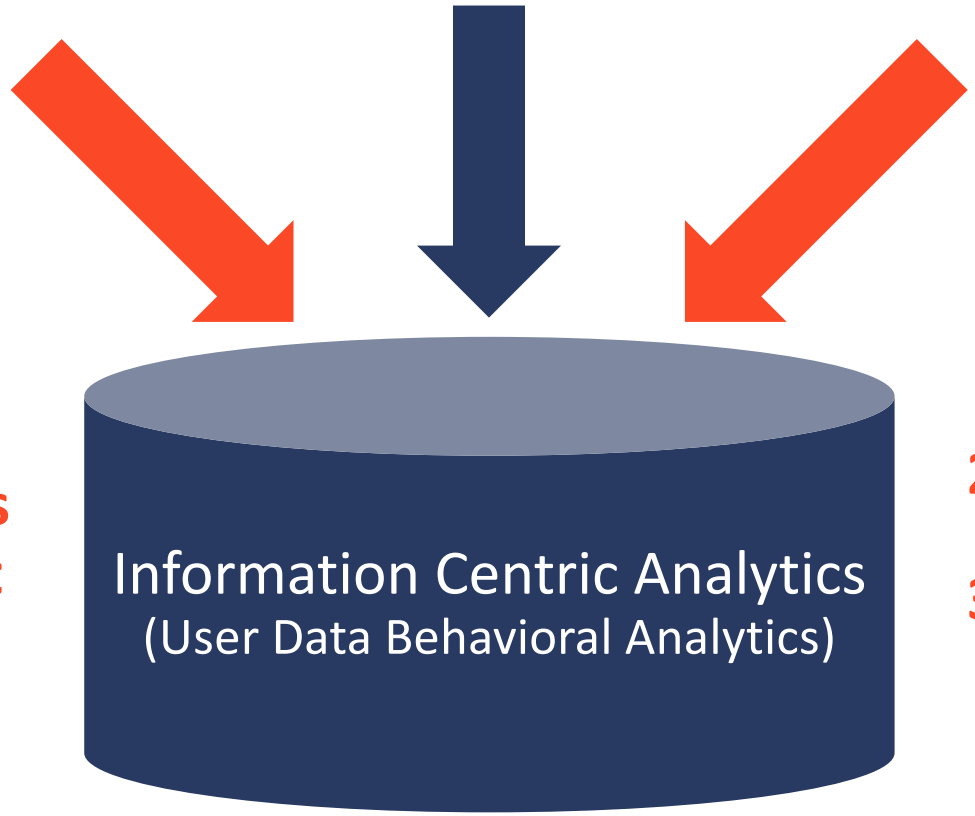
Analytics: towards ML-based DLP

DLP with Information Centric Analytics (ICA)

DLP "EVERYWHERE" INCIDENTS
(on-prem (DLP) , SaaS (CASB), mobile (ICE))

ICE
(confidential data access)

TAGGING
(file access recorder (FDR))



1. DLP incidents management

2. Malicious Insider

3. Malicious Outsider

DLP for GDPR

- DLP core to GDP: DAR, DIM, DIU
- Prebuilt GDPR policies
- GDPR specific reports
- DLP Risk assessment for GDPR
- Proactive tools: Information Centric Security (data classification, analytics, and encryption service)
- Extend protection to PII in scanned forms, pictures and images (driver's license, passports, checks…)
- GDPR breach detection & response: analysis to respond to data breach via Information Centric Analytics

Symantec

GENERAL DATA PROTECTION REGULATION

- Banking and Finance
- Digital Identity
- Government Identification
- Travel
- Personal Profile
- Healthcare and Insurance

INTERNATIONAL REGULATORY ENFORCEMENT

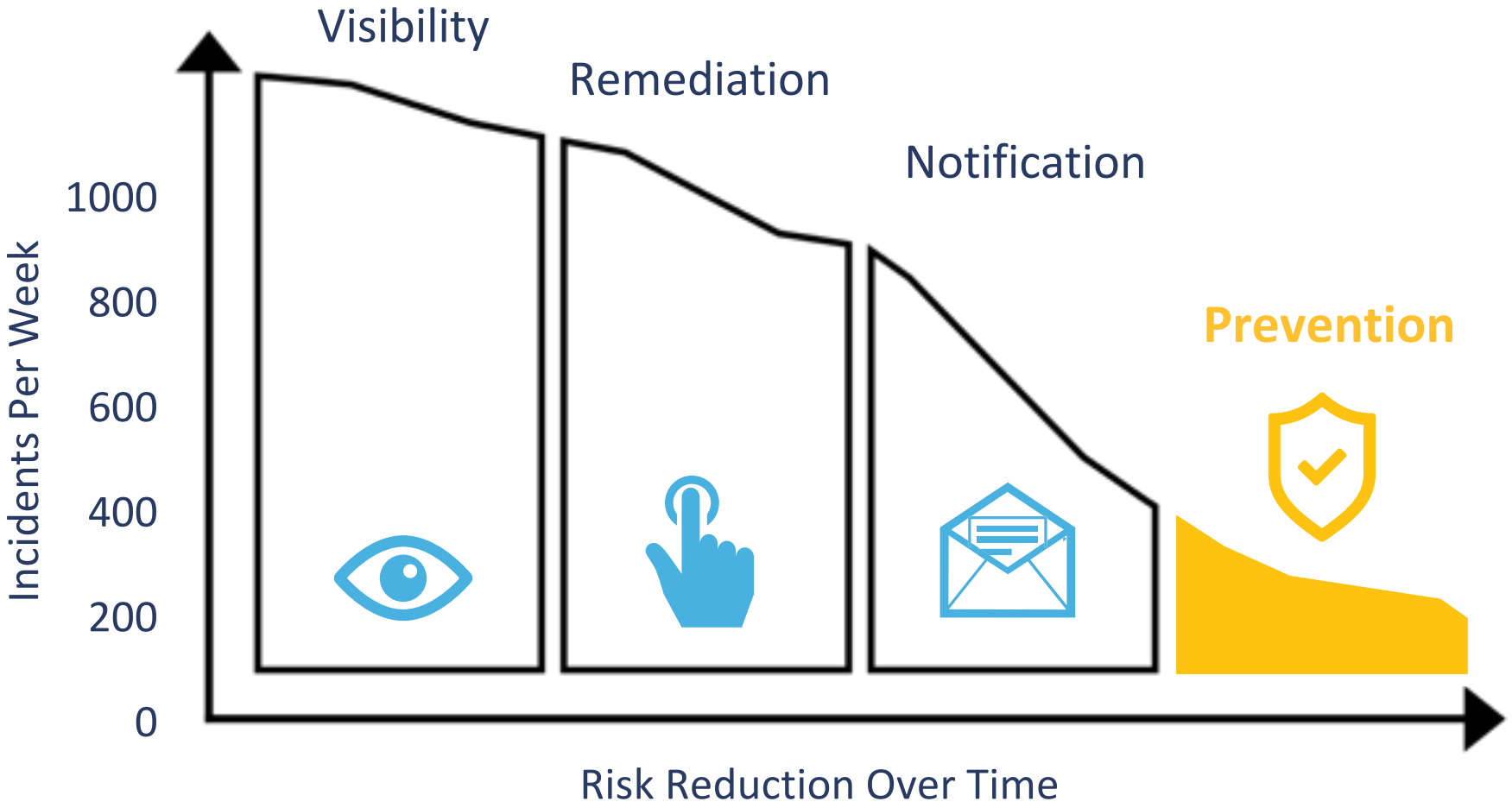
- Caldicott Report
- PIPEDA
- Data Protection Act 1998
- Human Rights Act 1998
- EU Data Protection Directives

Deploying Data Loss Prevention

Symantec™

Proven deployment methodology

To measurably reduce your data loss risk



Title

Symantec Information Centric Tagging (ICT)

Protect the Data You Value

Presenter

Date

The Need for User Driven Classification

Section
01

The Need for Data Classification

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 may be best identified and classified by the users who create it

User Stories

User driven classification

"I need to enable my employees to classify sensitive documents and email at the time of creation"

Augment DLP driven classification

"I want to extend protection to sensitive data that may not yet be covered by DLP policies"

Information Centric Tagging

Protect documents everywhere (w/Integrations)

"I need to protect sensitive documents with encryption or digital rights"

Introducing Information Centric Tagging (ICT)

Section
02

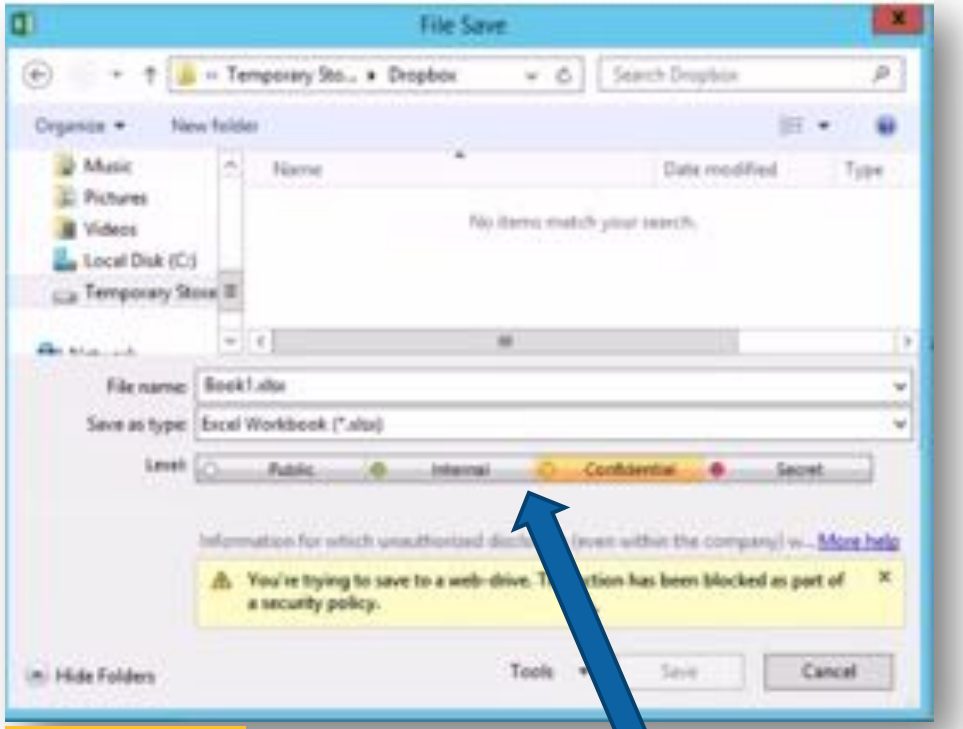
Information Centric Tagging (ICT)

User-based classification that expands DLP detection:

enables employees to identify sensitive data as they create it and apply classification levels

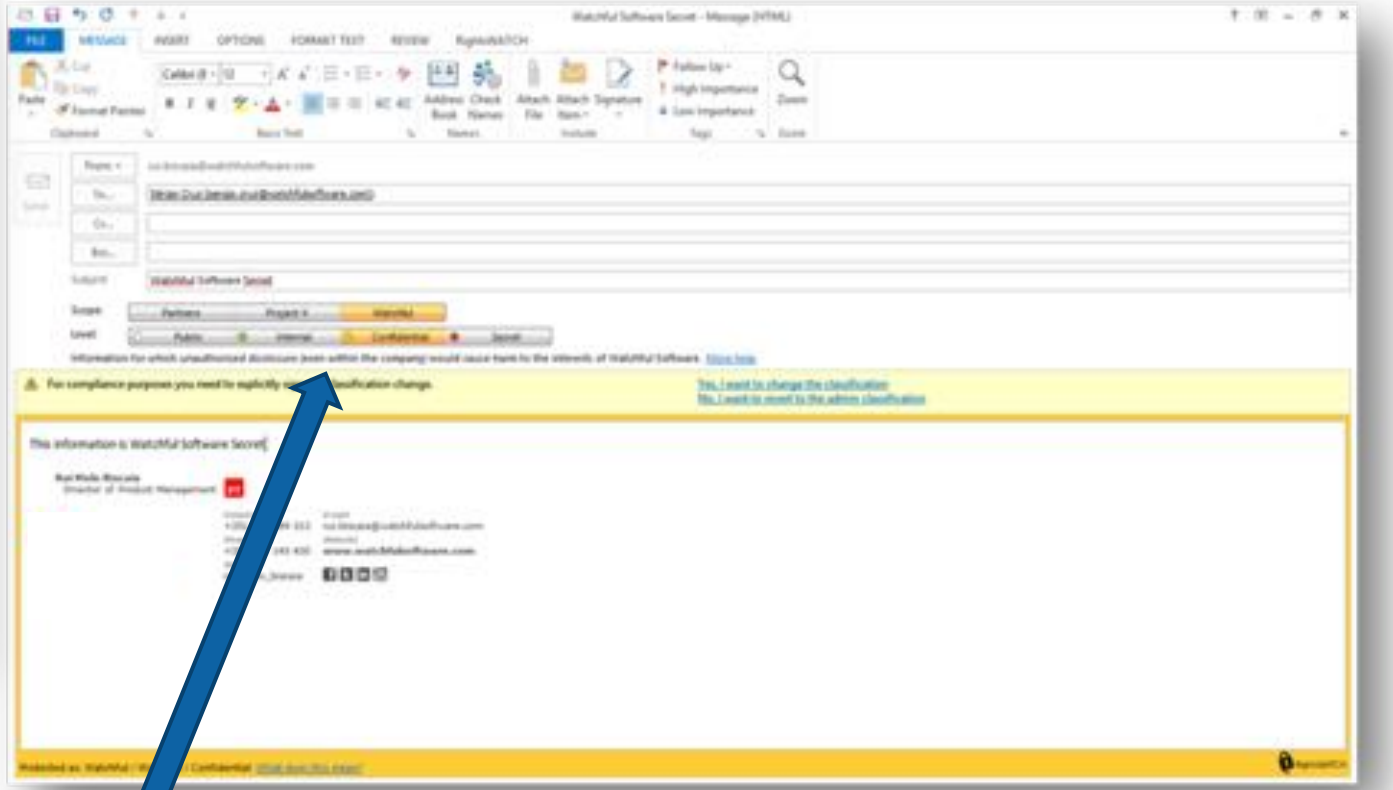
- Software agent based
- Add-on to DLP

Classification with ICT



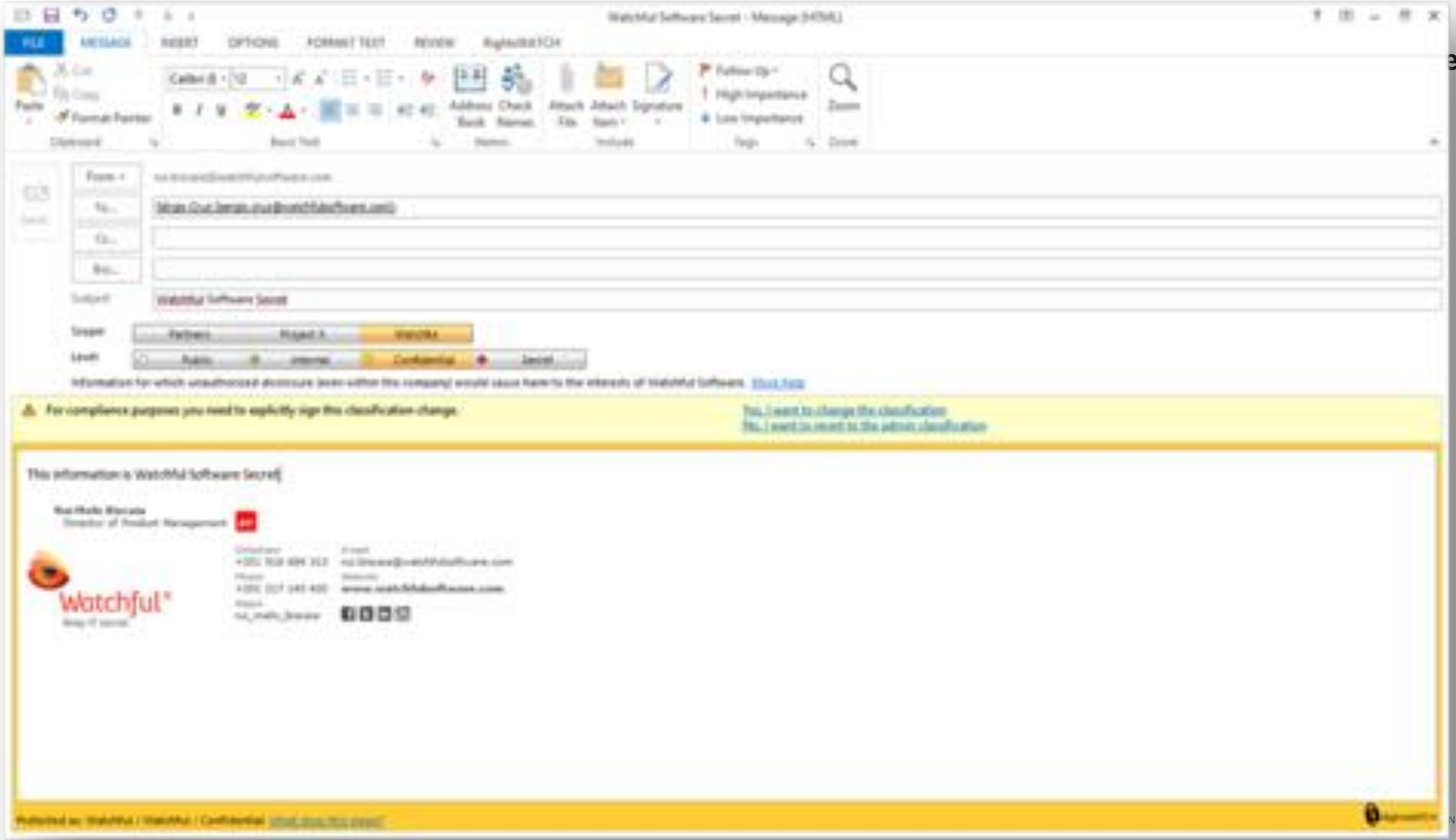
Files

Emails

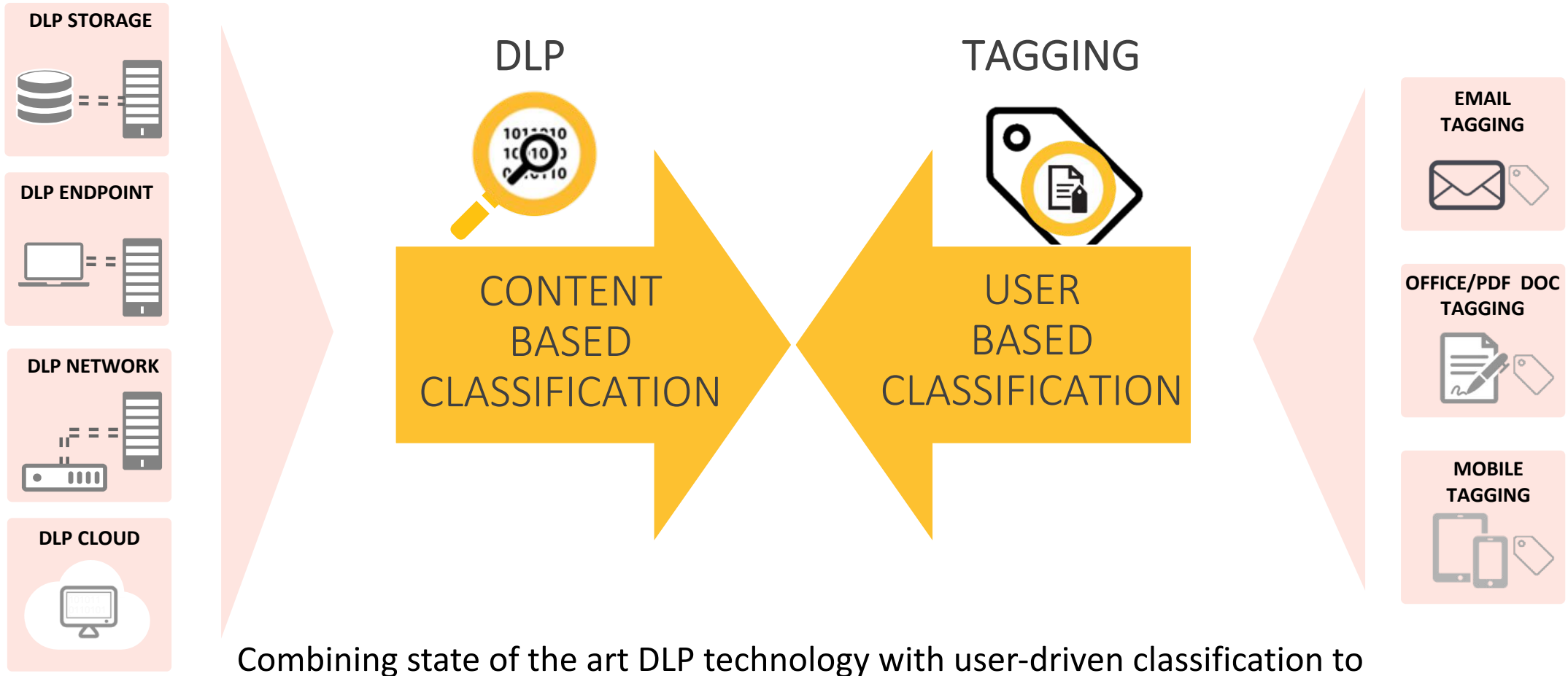


Classify data upon creation

Symantec.


Watchful Software Secret - Message (HTML)
FILE
MESSAGE
INSERT
OPTIONS
FORMAT TEXT
REVIEW
Paste
Cut
Copy
Format Painter
Address Book
Check Names
Attach File
Attach Item
Signature
Follow Up
High Importance
Low Importance
Zoom
Send
From
To...
Cc...
Bcc...
Subject
Watchful Software Secret
Scope
Partners
Project X
WWDRA
Level
Public
Internal
Confidential
Secret
Information for which unauthorized disclosure (even within the company) would cause harm to the interests of Watchful Software.
For compliance purposes you need to explicitly sign this classification change.
No, I want to change the classification
No, I want to revert to the above classification
This information is Watchful Software Secret
Director of Product Management
Watchful
Keep IT secret
Protected by: Watchful / Watchful / Confidential

User Classification augment DLP



Combining state of the art DLP technology with user-driven classification to identify and protect sensitive data

ICT Functionalities

Section
03

Classification&Tagging in a Nutshell

Data Classification & Labeling

Enables enterprises to classify newly created content, existing files, and emails in a DLP policy-driven or user-driven manner

Enterprise-Ready Architecture

Highly scalable architecture with centralized management that integrates with DLP, Microsoft RMS, and Active Directory

Role-Based Taxonomies & Policy

Policy engine allows enterprises to set up different classification taxonomies and policies to be applied to designated users

Comprehensive Audit Trails

Rich audit trails provide visibility into user and administrator actions enabling regulatory compliance and forensic mandates

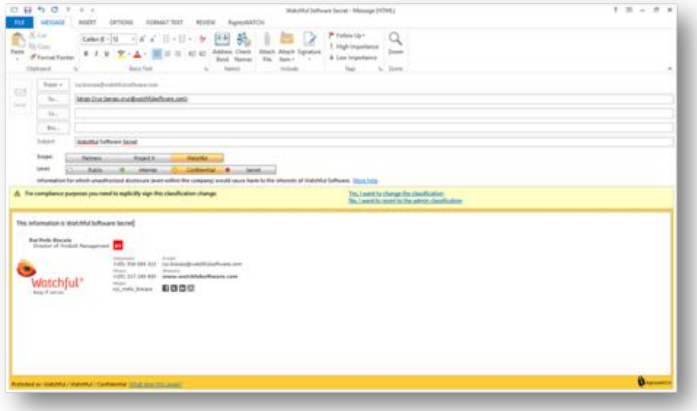
Dynamic Watermarking & Tagging

Automatic tagging and watermarking all unstructured data, including emails, documents, and images according to enterprise policy

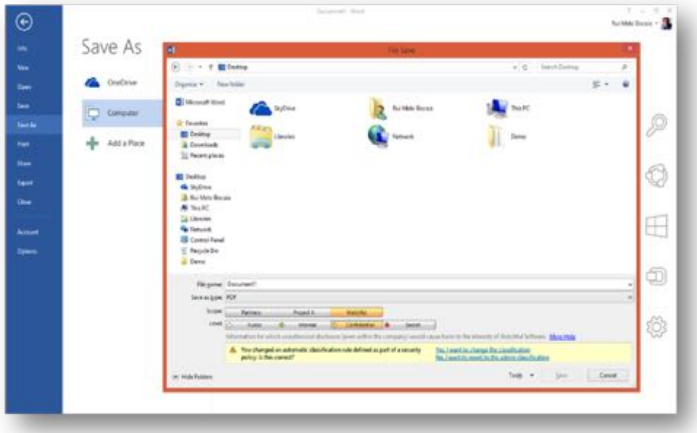
Ease of Use

Intuitive and seamless user experience ensures a smooth roll-out of classification and tagging

Seamlessly Integrated Classification



Microsoft Outlook



Microsoft Office

Mobile

Other classification integrations:
Global Protector (Windows Explorer, CLI)
Outlook Web Access

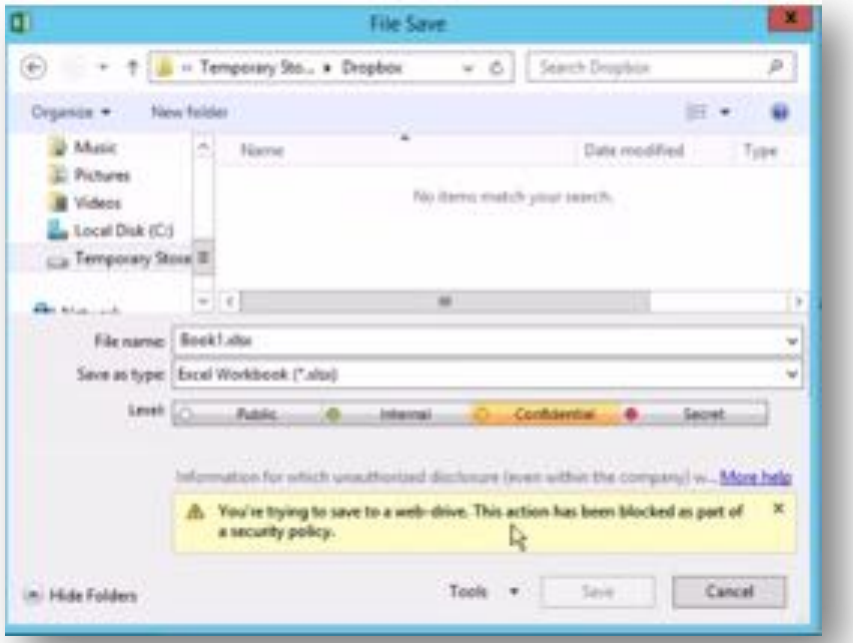
Document and Message Watermarking

Applying Visual Indication of Classification Level

Use classification tags to apply watermarks to documents and email messages

Supports Office documents, spreadsheets, presentations, PDF files, and email messages

Classification & Tagging Engine



Warn Rule

Guide or educate the user when performing a classification action during content creation

Block Rule

Prevent the user from transmitting incorrectly classifying content

Tag

Tag the content at the metadata layer to enhance the efficiency and effectiveness of the DLP policies

A new approach:
Information Centric Security

Section
04

Symantec Information Centric Security Components

- **Data Loss Prevention (DLP)**

Discovers sensitive data across all channels with central policy controls

- **CloudSOC (CASB)**

Extends existing DLP policies, workflows, and detection to Cloud Apps

- **Validation and ID Protection Service (VIP)**

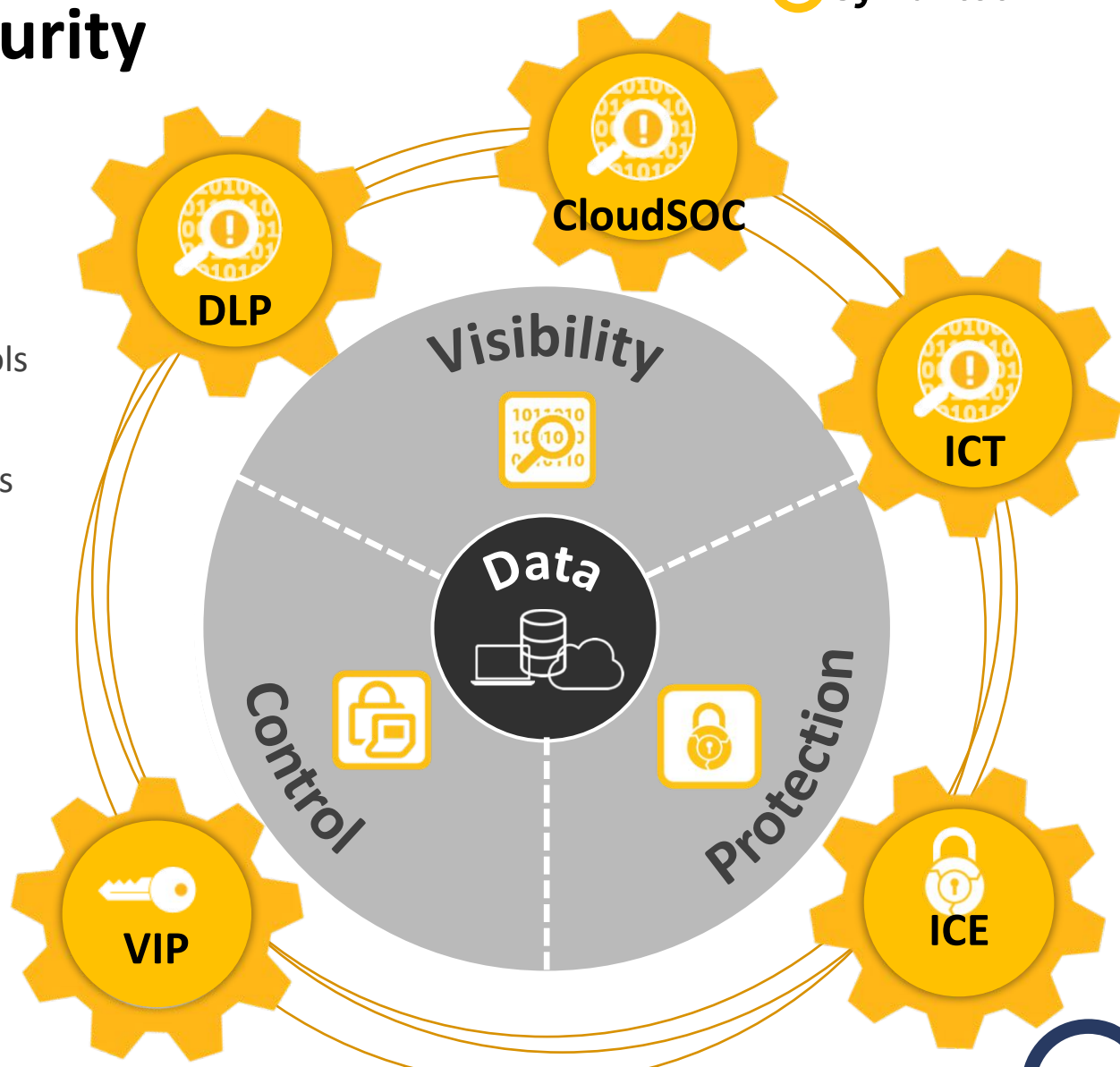
Secures access to critical data with Multi-Factor Authentication

- **NEW Information Centric Encryption (ICE)**

Integrated policy driven encryption and identity access

- **NEW Information Centric Tagging (ICT)**

Increases DLP efficiency with User driving DLP tagging



Why Symantec

Symantec™

Why Symantec

Innovation and market leadership

10 Consecutive Years of Technology Leadership

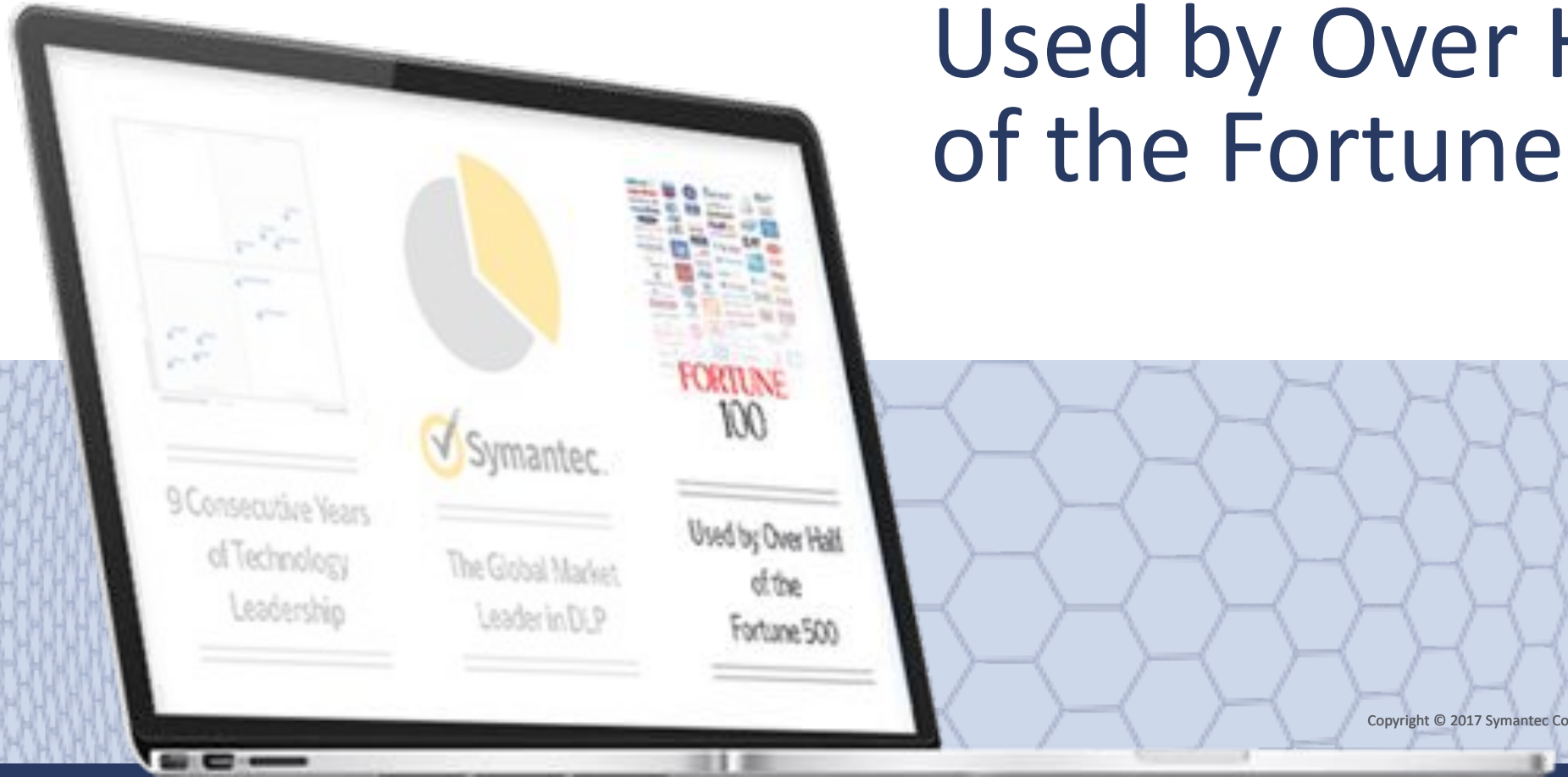
Why Symantec

Innovation and market leadership

The Global Market Leader in DLP

Why Symantec

Innovation and market leadership



Used by Over Half of the Fortune 500

Net++ TECHNOLOGY

HVALA

?

Symantec™