



Bytes GDPR Breakfast Briefing

Mapping Forcepoint Technology to the EU GDPR

September 2017



DATA
EVERYWHERE

USERS
ANYWHERE

MANY
BEHAVIORS

TECNOLOGIES CHANGE



ACCIDENTAL INSIDER



MALICIOUS INSIDER



COMPROMIZED INSIDER





MAPPING TECHNOLOGY TO GDPR

GDPR STRATEGY



Preparation

- Appoint a Data Protection Officer (DPO)
- Review controller/processor responsibilities
- PII Data Discovery



<12 Months

- Data Flow Mapping (Internal/External processing)
- Contract Review
- Data Protection Impact Assessments



<25th May 2018

- Updated Technical & Organisational controls
- Data Breach Notification Readiness (<72hrs)
- Right to Erasure, Portability, SAR, Consent etc

WHAT TECHNOLOGIES WILL ORGANIZATIONS LOOKS TO INVEST IN?

WHITE PAPER

GDPR Compliance and Its Impact on Security and Data Protection Programs

An Osterman Research White Paper
Published January 2017

actiance®

CipherCloud®
Trust in the Cloud™

FORCEPOINT
POWERED BY RAYTHEON

Hewlett Packard
Enterprise

janusNET
security starts with you

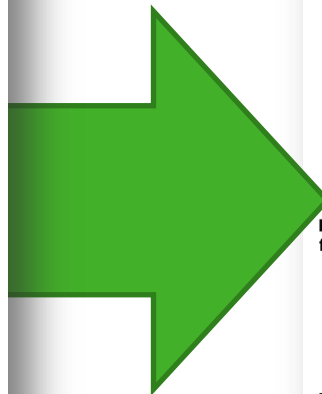
mimecast®

sonian

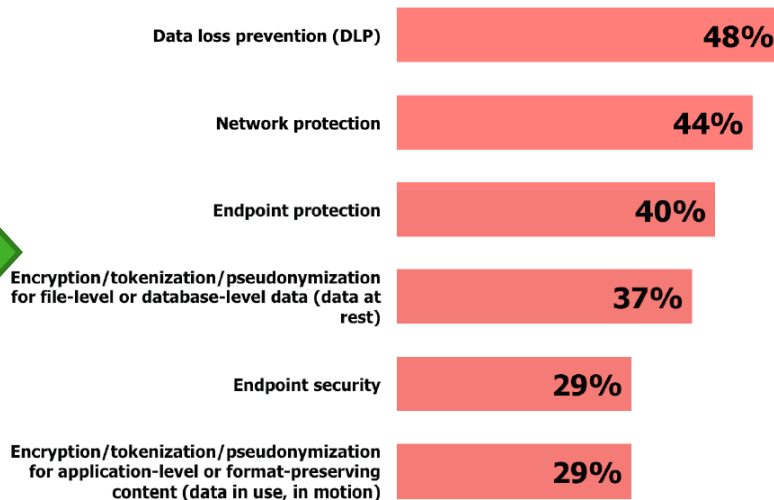
WATERFORD
TECHNOLOGIES



Osterman Research, Inc.
P.O. Box 1058 • Black Diamond, Washington • 98010-1058 • USA
Tel: +1 253 630 5683 • info@ostermanresearch.com
www.ostermanresearch.com • @osterman



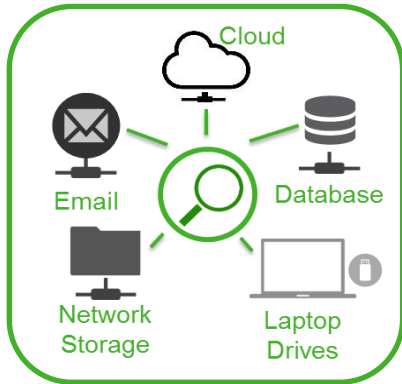
Data Protection Technologies That Organizations Will Spend More On During the Next 12-18 Months to Specifically Address the GDPR



Source: Osterman Research, Inc.

HOW DLP CAN HELP

INVENTORY PERSONAL DATA



DLP: Discover,
Cloud, Endpoint

MAP, MANAGE & CONTROL PERSONAL DATA FLOWS

Who	What	Where	How	Action
Human Resources	Source Code	Evernote	File Transfer	Confirm
Customer Service	Credit Card Data	Dropbox	Web	Block
Marketing	Personal Data	Business Partner	Instant Messaging	Notify
Finance	M&A Plans	Facebook	Peer-to-Peer	Remove
Accounting	Employee Salary	OneDrive	Email	Encrypt
Sales / Marketing	Financial Report	Malicious Server	Print	Quarantine
Legal	Customer Records	Removable Media	File Copy	Confirm
Technical Support	Manufacturing Docs	Competitor	Print Screen	Audit
Engineering	Research	Customer	Copy/Paste	Notify



DLP: Network, Endpoint
Web & Email Security modules

PREPARE TO RESPOND IN A TIMELY MANNER



Security Manager & Insider
Threat Command Center

The Need to Inventory Personal Data

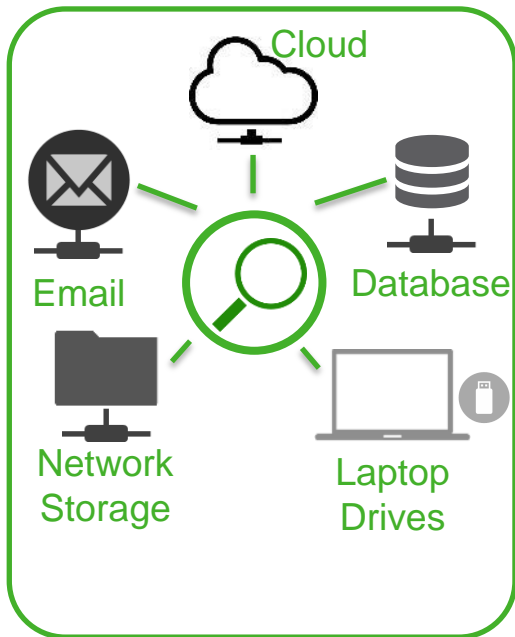
Understand an organization's exposure to GDPR

Understand an organization's 'Attack Surface'

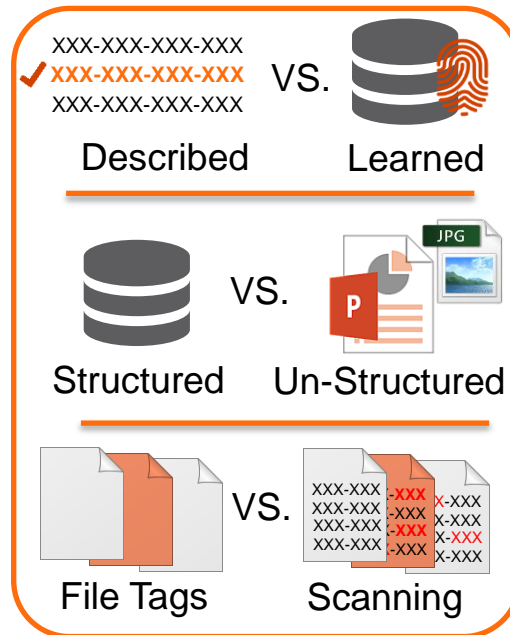
ARTICLES OF THE GDPR – RELEVANT TO DATA INVENTORY

- Chapter 2 (Principles), section 3 (Rectification & Erasure):
 - Article 17 (Right to erasure / 'right to be forgotten'): *'The data subject shall have the right to obtain from the controller the **erasure of personal data** concerning him or her without undue delay'*
 - Article 20 (Right to data portability): *'The data subject shall have the right to **receive the personal data** concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format'*
- Chapter 4 (Controller & Processor), section 1 (General Obligations):
 - Article 24 (Responsibility of the Controller): (1) *'The controller shall **implement appropriate technical and organisational measures** to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation'.*
- Chapter 5 (Transfers of personal data to third countries or international organisations):
 - Articles 44 – 50 This chapter explains the conditions of when personal data can be transferred or processed outside of the EU, including Article 46: (Transfers subject to appropriate safeguards)
 - including Article 46: (Transfers subject to appropriate safeguards)

PERSONAL DATA DISCOVERY



DATA IS
EVERYWHERE



DATA IS NOT ALWAYS
EASY TO FIND

FORCEPOINT PRODUCTS: DLP DISCOVER & DLP ENDPOINT

PRE-DEFINED POLICIES ARE A DIFFERENTIATOR

FORCEPOINT TRITON® APX User name: admin Log Off

Web Data Email Mobile

Appliances TRITON Settings Help

Role: Super Administrator Deploy

Main Manage Policies > Policy Library

View

116 Policies: Search for:

PII policies

Policy: Netherlands Personal Data Protection Act

Description: Policy to promote compliance with the Dutch Personal Data Protection Act, which implements the EU Directive 95 on privacy. The policy contains rules to detect combinations of Netherlands sofnummer and sensitive private information like account number, driver license number, passport number, ethnicity and health conditions.

Rules (enabled: 6, total: 9)

- 1. DUTCH PDP: Sofi and Ethnicities (1277590)**
Rule for detecting a Netherlands sofnummer when appearing together with the name of a race or ethnicity, in English or Dutch.
- 2. DUTCH PDP: Sofi and Account with Password (1277590)**
Rule for detecting a Netherlands sofnummer when appearing together with a 5-10 digit account number, in proximity to a password having a password related term next to it. Monitors Data in Motion channels, excluding HTTP.
- 3. DUTCH PDP: Sofi and CCN (1277590)**
Rule for detecting a Netherlands sofnummer when appearing together with a valid credit card number prevalent in Europe, employing various heuristics involving credit card related terms and use of delimiters.
- 4. DUTCH PDP: Sofi and Crime (1277590)**
Rule for detecting a Netherlands sofnummer when appearing together with the name of a crime, in English or Dutch.
- 5. DUTCH PDP: Sofi and Diseases (1277590)**
Rule for detecting a Netherlands sofnummer when appearing together with the name of a sensitive health condition, in English or Dutch.
- 6. Dutch PDP: Dutch Bank Accounts with proximity (1277590)**
PreciseID NLP rule for detecting Eliproef validated Dutch Bank Account numbers, when found in proximity to Bank Account related terms, such as "giropas".
- 7. Dutch PDP: Dutch Bank Accounts (1277590) - Disabled**
PreciseID NLP rule for detecting Eliproef validated Dutch Bank Account numbers. This rule may cause false positives, and is not selected by default.
- 8. Dutch PDP: Driver License Numbers (1277590) - Disabled**
Rule for detection of at least 3 Driver's License Numbers of the Netherlands, when appear in proximity to support terms. This rule is not selected by default.
- 9. Dutch PDP: Passport Numbers (1277590) - Disabled**
Rule for detection of at least 3 Passport Numbers of the Netherlands, when appear in proximity to support terms. This rule is not selected by default.

NOTE: For a rule to take effect, you must enable it.
To enable a rule, highlight it in the Policy Management tree view, select Edit, and click Enabled.

Use Policies Cancel

DATA DISCOVERY RESULTS

FORCEPOINT TRITON® APX

User name: admin [Log Off](#)

Web Data Email Mobile

Appliances TRITON Settings Help

Role: Super Administrator [Deploy](#)

Main

Status

Reporting

Policy Management

Logs

Settings

General

Authorization

Deployment

DLP Demo Discovery Incidents Report

Workflow Remediate Escalate

Report: DLP Demo Discovery Incidents Report Date Range: Last 80 Days

Manage Report

Incident Tag	Discovery Task	ID	Policies	File Name	Ma...	File Size	Severity	Folder	Incident Time	Detected by	Discovery Type
2.5.1	Windows Endpoint ...	3644219	Suspected Malicio...	8bpjUBP1.txt		N/A 21.88 KB	Medium	\\GUYDEMO2016.QAE...	2016-11-13 20:41:28	Endpoint Agent	Endpoint
2.5.2	Windows Endpoint ...	3643572	Deep Web URLs for...	tor-links.docx		225 24.13 KB	High	\\GUYDEMO2016.QAE...	2016-11-13 20:41:25	Endpoint Agent	Endpoint
2.4.2	Mac Endpoint Disc...	5722651	MSA Documents	dip-B667E44E...		1 76.87 KB	Medium	\\Library\\Applicat...	2016-11-13 18:39:46	Endpoint Agent	Endpoint
2.4.1	Shared Storage DB...	3641618	Croatian Candida...	Mojj kandida...		16 456 B	Medium	\\qstorage.webse...	2016-11-10 16:22:06	Crawler E...	File System
2.1.1	Box Discovery Task	3384283	Japan Private Inf...	箱2 様式第1号 小児...		5 62.87 KB	High	\\Box3@websense.c...	2016-11-10 12:08:25	Crawler E...	Box Cloud
2.2.2	Box Discovery Task	3383493	Fingerprinted Des...	2020_1.rar		1 125.63 KB	Medium	\\Box3@websense.c...	2016-11-10 12:08:15	Crawler E...	Box Cloud
2.3.2	Shared Storage Di...	3383585	US PHI For Discovery	bariatric fo...		1 200.77 KB	High	\\qstorage.webse...	2016-11-09 16:15:13	Crawler E...	File System
2.3.1	Sharepoint Online	3384047	Software Source C...	PhishingDete...		N/A 13.95 KB	Low	https://websense3...	2016-11-08 16:56:04	Crawler E...	SharePoint Online

Incident: 3641618 Severity: Medium Channel: Discovery Discovery Type: File System

Display: Violation triggers

Rule: Croatian Candidates information

DB Fingerprint PII (PreciseID Fingerprinting - Database Records) 16

Gondi, Stepan, 87269108171, Kezelj, Tara, 24517049889, 37452260107, 62584481930, Vurnek, Matjja,

Properties History

File Details

File path: \\qstorage.websense.com\\Volume_1\\Users\\Public\\Documents\\Mojj kandidati.txt

Hostname: qstorage.websense.com

File Size: 456 B

Date Created: 06 Nov. 2016, 04:48:10 PM GMT+0000

Date Modified: 10 Nov. 2016, 04:15:23 PM GMT+0000

Date Accessed: 10 Nov. 2016, 04:15:23 PM GMT+0000

Checksum: bbd06a738d439cfbaf072e2ecbe11c1f

Folder Owner: Unix User\$01

File Owner: Unix User\$01

File Permissions

Unix Group\\fp_145 [RW]

Everyone [RW]

Unix User\$01 [RW]

Incident Details

Severity: Medium

Status: New

Channel: Discovery

Analyzed by: Policy Engine EIPMANAGER.tegdom.com

Detected by: Crawler EIPMANAGER.tegdom.com

Event time: 2016-11-10 16:22:06

Incident time: 2016-11-10 16:22:06

Assigned to: Unassigned

Incident tag: 2.4.1

Discovery Task

Task name: Shared Storage DB PII discovery

Access Control

Location

Type

File Properties

Close

The Need to Monitor, Manage & Control Personal Data Flows

Ensure Personal data is processed in accordance with
Data Protection Policies.

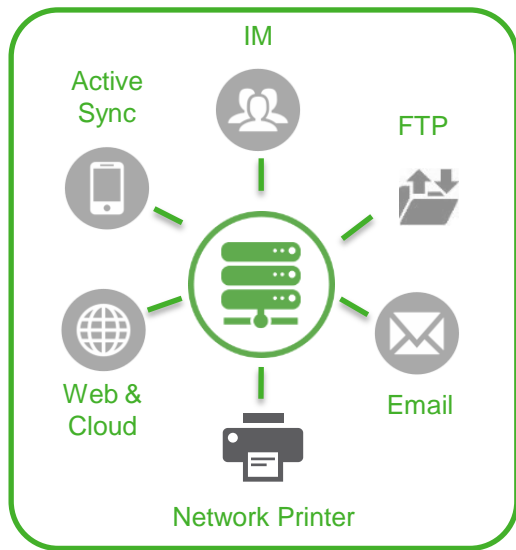
Manage the flow of personal data to approved suppliers
and third countries

ARTICLES OF THE GDPR – RELEVANT TO MAPPING DATA FLOWS

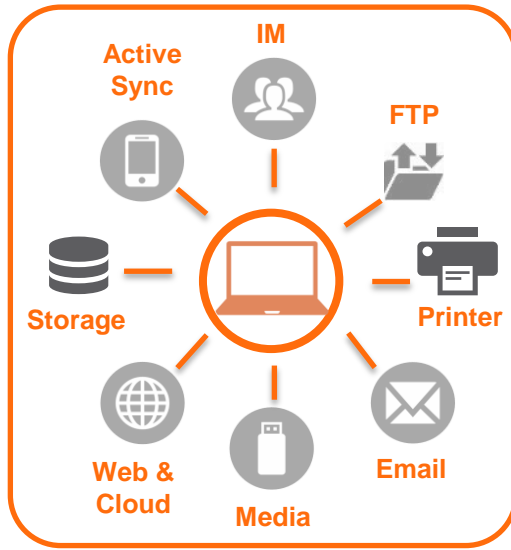
Chapter 4 (Controller & Processor), section 1 (General Obligations):

- Article 24 (Responsibility of the Controller): (1) ‘The controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation’.
- Article 25 (Data protection by design and by default): ‘The controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects’.

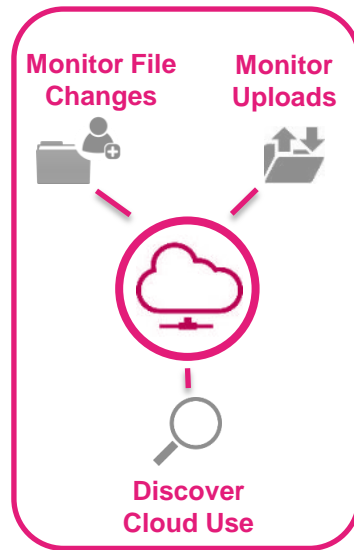
CONSIDERATIONS FOR MONITORING DATA FLOWS



NETWORK
Data in Motion



ENDPOINT
Data in Use
& in Motion



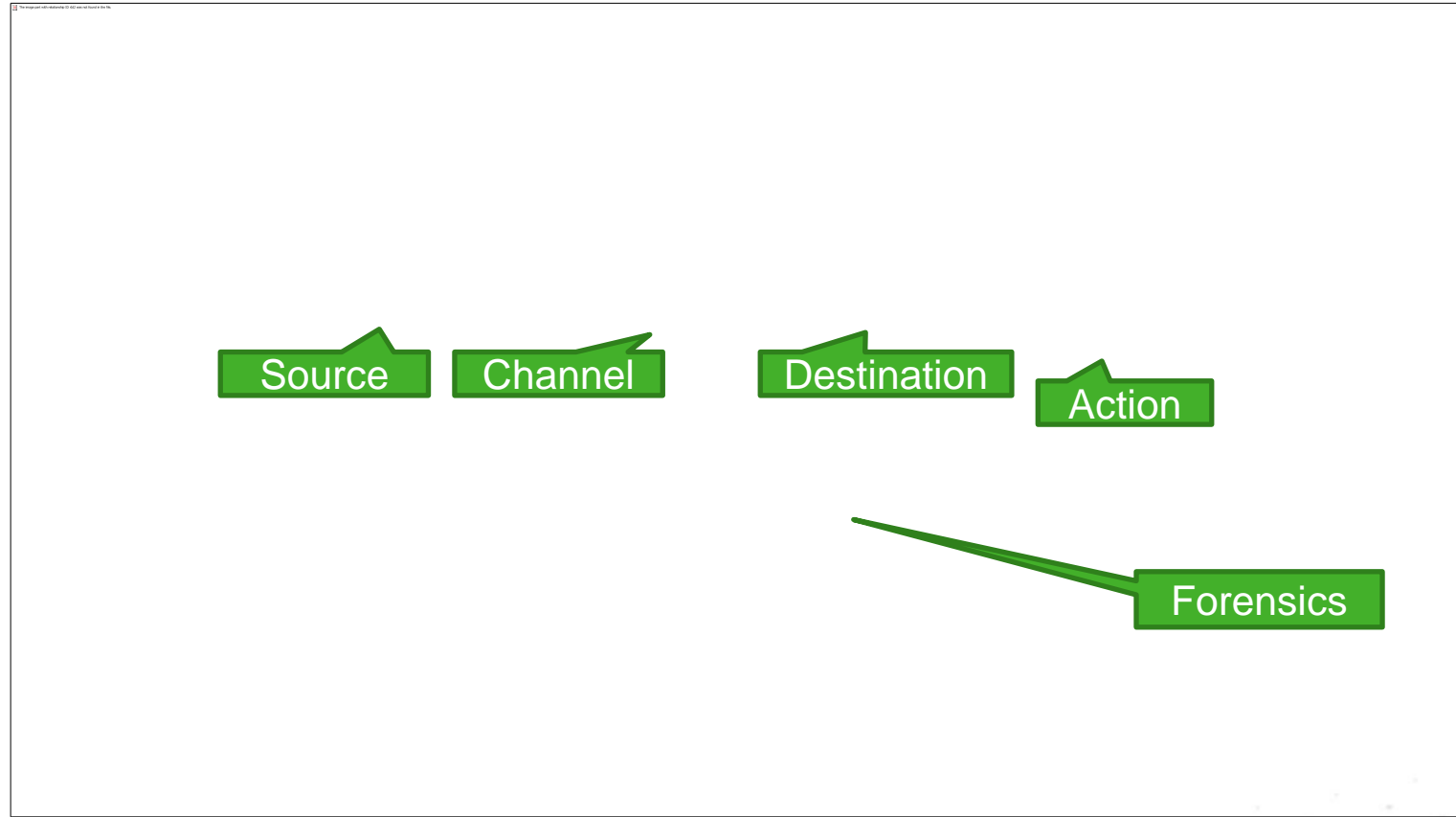
CLOUD
Data In Use
& in Motion

**FORCEPOINT PRODUCTS: DLP NETWORK, DLP ENDPOINT & DLP CLOUD,
WEB SECURITY + CASB, EMAIL SECURITY + ENCRYPTION**

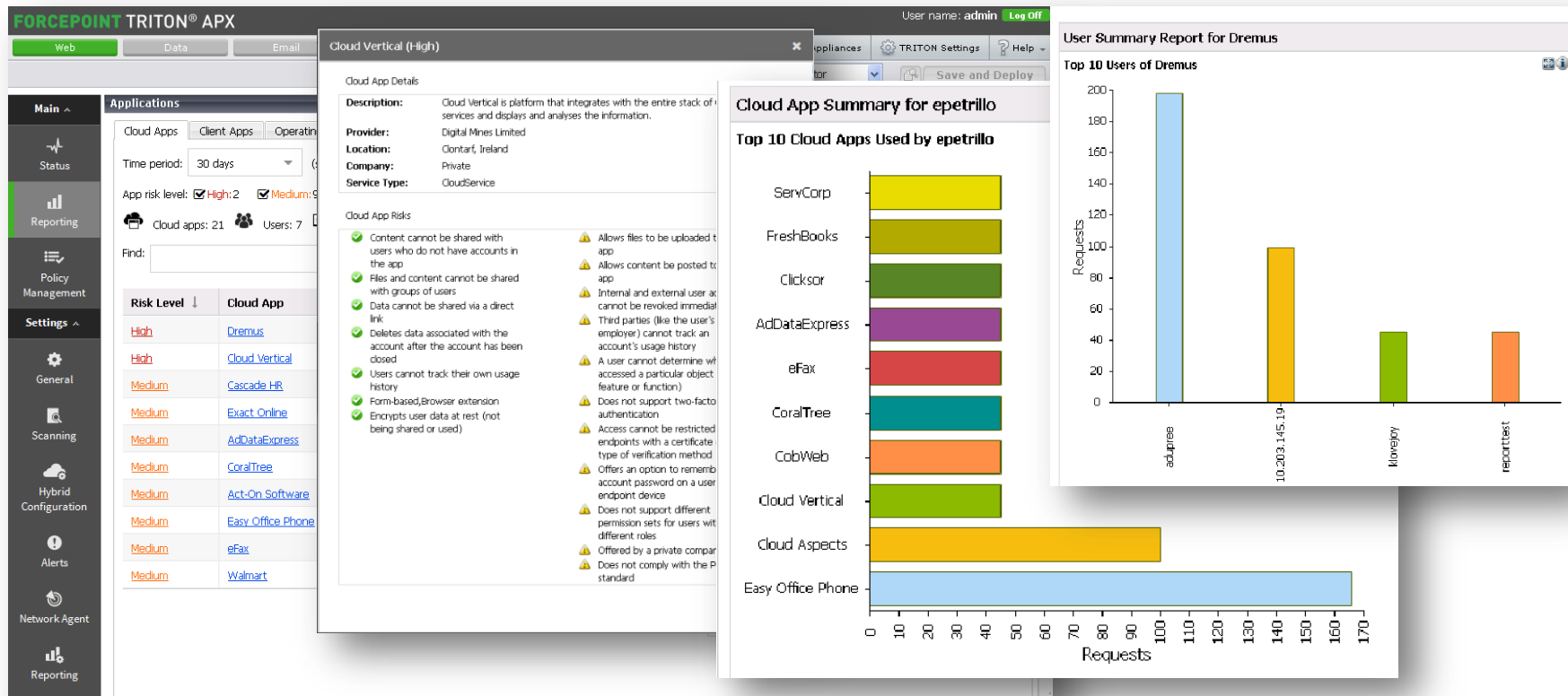
DATA IN USE & IN MOTION

Who	What	Where	How	Action
Human Resources	Source Code	Evernote	File Transfer	Confirm
Customer Service	Credit Card Data	Dropbox		Block
Marketing	Personal Data	Business Partner	Instant Messaging	Notify
Finance	M&A Plans	Facebook	Peer-to-Peer	Remove
Accounting	Employee Salary	OneDrive	Email	Encrypt
Sales / Marketing	Financial Report	Malicious Server	Print	Quarantine
Legal	Customer Records	Removable Media	File Copy	Confirm
Technical Support	Manufacturing Docs	Competitor	Print Screen	Audit
Engineering	Research	Customer	Copy/Paste	Notify

MAPPING DATA FLOWS



VISIBILITY OF UNSANCTIONED CLOUD APPLICATION USAGE



Identifies usage of cloud apps that can represent risk to an enterprise

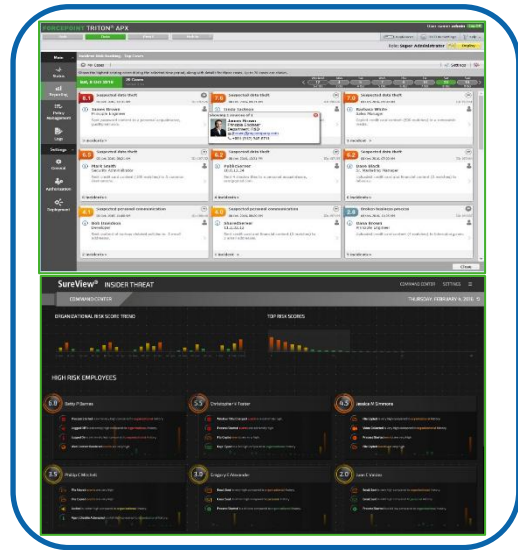
The Need to Be Prepared to Report a Data Incident

Understand an organization's exposure to GDPR

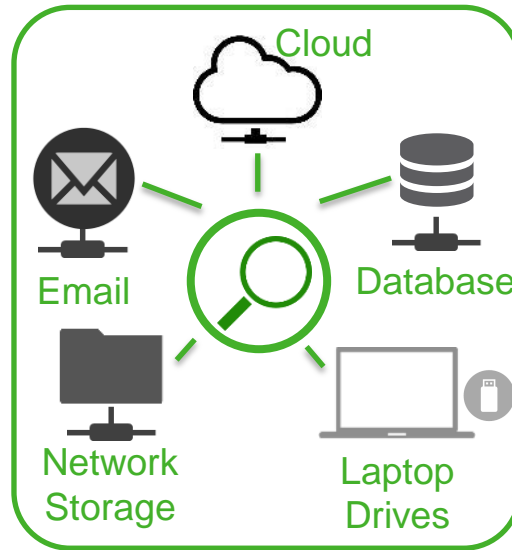
ARTICLES OF THE GDPR – RELEVANT TO RESPONDING TO A DATA BREACH

- Chapter 4 (Controller & Processor), section 2 (Security of personal data):
 - Article 33 – (Notification of a personal data breach to the supervisory authority): (1) *‘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’.*
 - Article 34 – (Communication of a personal data breach to the data subject): (1) *‘When the personal data breach is likely to result in a **high risk** to the rights and freedoms of natural persons, the controller shall **communicate the personal data breach to the data subject** without undue delay’.*
 - (2) ‘The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:
 - (a) The controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
 - (b) The controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;
 - (c) It would involve disproportionate effort. In such a case, there shall instead be’

INVESTIGATING A DATA BREACH



MAKE USE OF SECURITY
ANALYTICS AND RISK
RANKING TO PRIORITIZATION
RESPONSE PROCESS



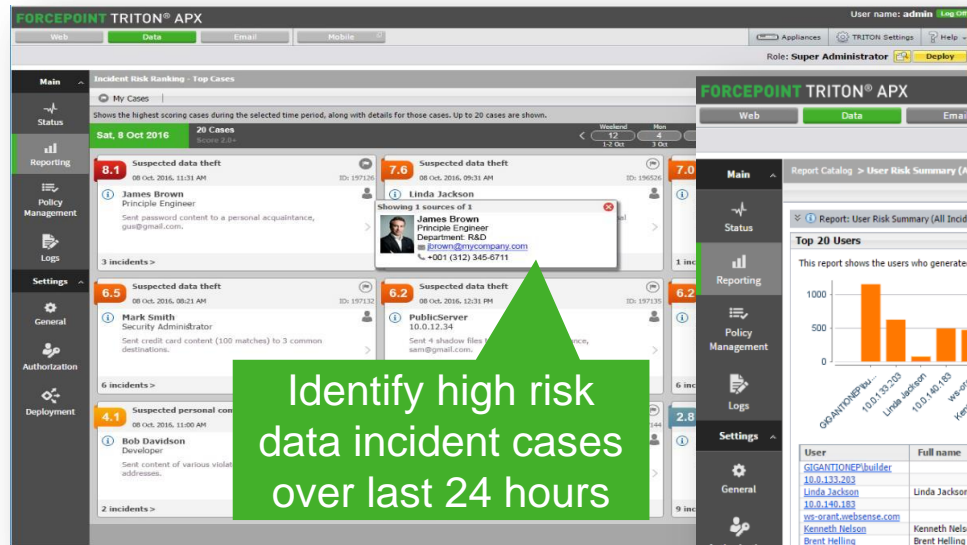
REVIEW RESULTS TO
HISTORICAL
PERSONAL DATA
INVENTORIES

Who	What	Where	How	Action
Human Resources	Source Code	Evernote	File Transfer	Confirm
Customer Service	Credit Card Data	Dropbox	Web	Block
Marketing	Personal Data	Business Partner	Instant Messaging	Notify
Finance	M&A Plans	Facebook	Peer-to-Peer	Remove
Accounting	Employee Salary	OneDrive	Email	Encrypt
Sales / Marketing	Financial Report	Malicious Server	Print	Quarantine
Legal	Customer Records	Removable Media	File Copy	Confirm
Technical Support	Manufacturing Docs	Competitor	Print Screen	Audit
Engineering	Research	Customer	Copy/Paste	Notify

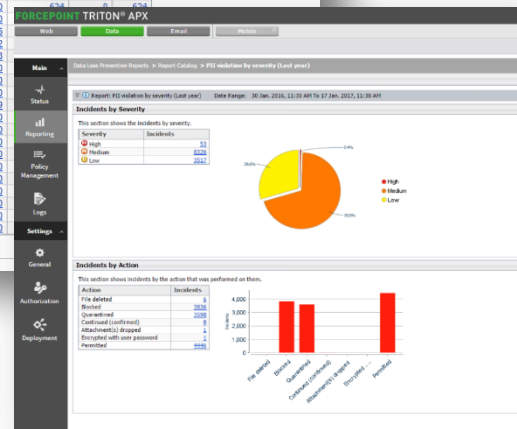
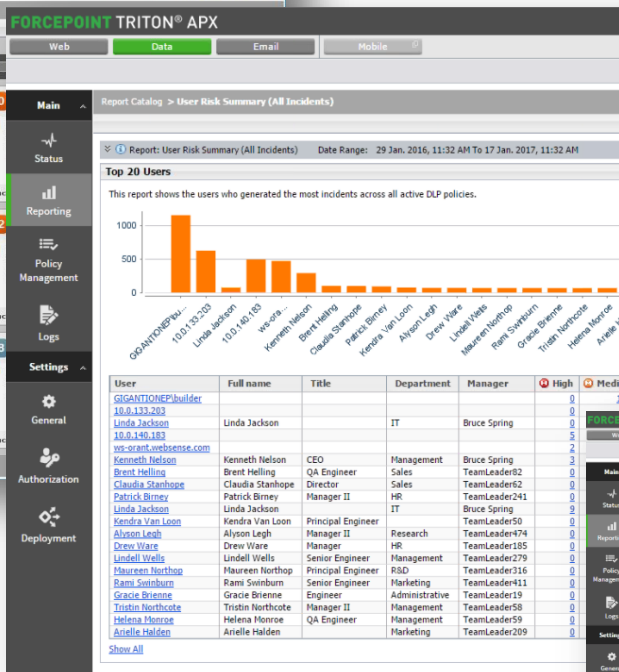
REVIEW INCIDENTS
TO PAST DATA FLOW
POLICY VIOLATIONS

FORCEPOINT PRODUCTS:
SECURITY MANAGER, INSIDER THREAT COMMAND CENTER

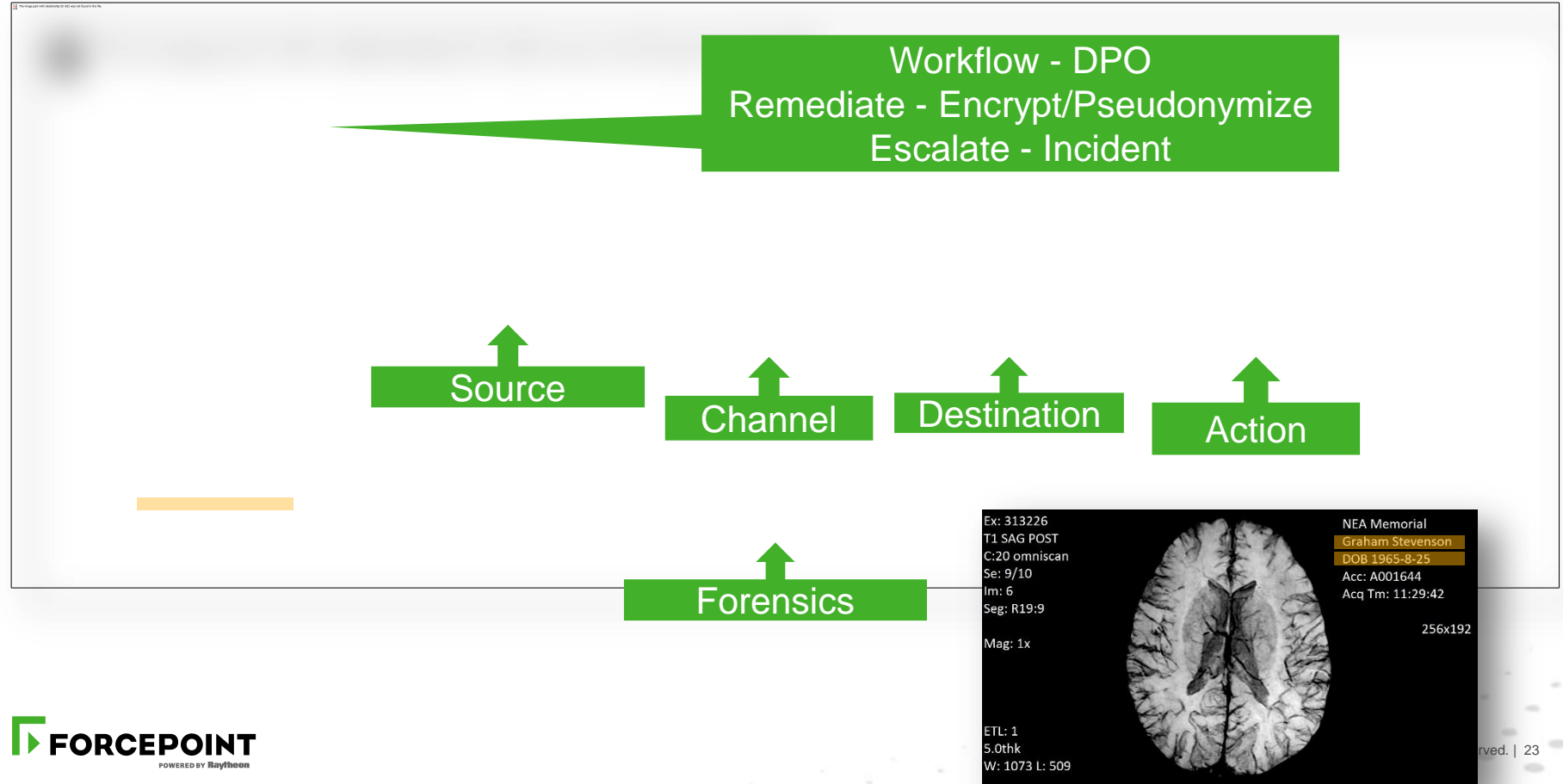
EXAMPLES OF REPORTS TO ASSIST WITH BREACH INVESTIGATION



IRR Utilizes Machine Learning and Security Analytics to cluster incidents into cases



INVESTIGATING A DATA INCIDENT



INTEGRATED WORKFLOW

Remediation actions might include:

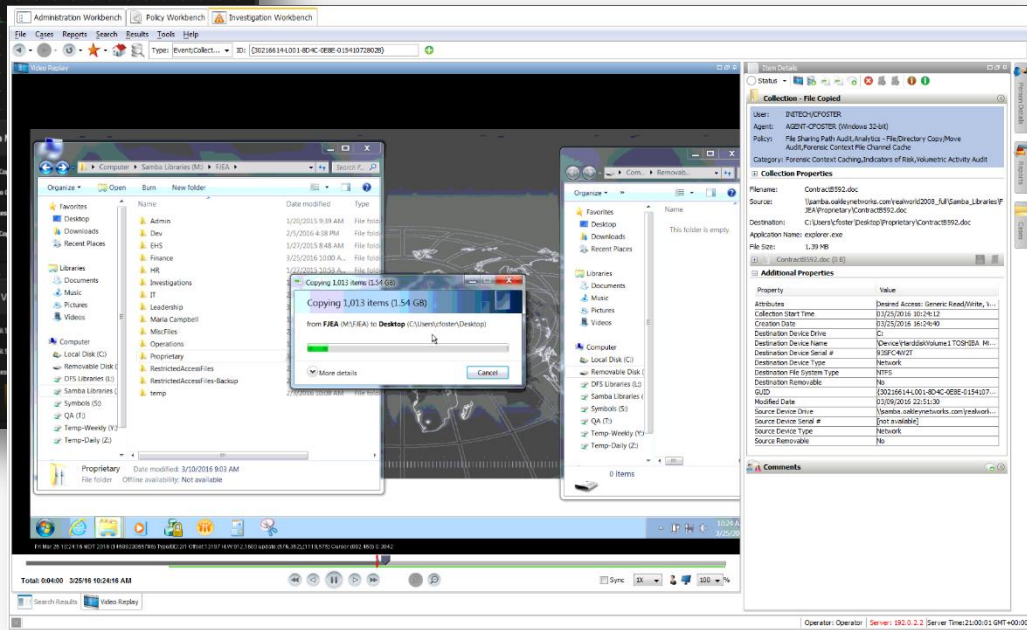
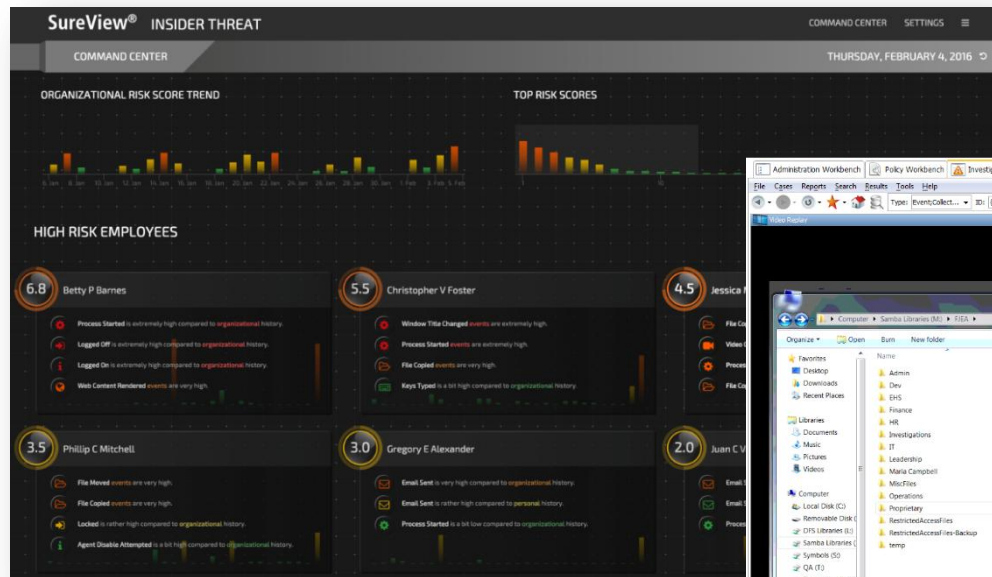
- Move
- Delete
- Encrypt
- Apply DRM
- Apply Masking
- Apply Categorisation
- Apply Pseudonymisation

The screenshot displays the Forcepoint Triton APX web interface. The top navigation bar includes tabs for Web, Data (highlighted), Email, and Mobile. A left sidebar contains navigation links: Main, Status, Reporting, Policy Management, Logs, and Settings. The main content area is titled 'Incidents (last 7 days)' and features a 'Remediate' dropdown menu. The menu options include Assign..., Change Status (highlighted), Change Severity, Ignore Incident, Tag Incident..., Add Comments..., Download Incident..., and Delete. A secondary menu for 'Change Status' is open, showing options like Critical, New, In Process, Closed, False positive, Escalated, and Edit Status... Below the menu, a table lists incidents with columns for Incident ID, Date/Time, User, and Action. The bottom of the interface shows a detailed view of a specific incident (ID: 7667863) with fields for Severity (Medium), Action (Denied (confirmed)), and Display (Violation triggers).

Incident ID	Date/Time	User	Action
7667482	2016-12-22 16:50:46	Barbara White	Information
7373044	2016-12-13 04:35:07	Linda Jackson	SEC
7372894	2016-12-13 04:20:50	Linda Jackson	SEC
7372774	2016-12-07 05:33:23	ws-orant.websense.com	Suspected M
7373227	2016-12-07 05:21:42	ws-orant.websense.com	Encrypted M

Incident: 7667863 | Severity: Medium | Action: Denied (confirmed) | Display: Violation triggers

DATA BREACH NOTIFICATION – USER BEHAVIOR RISK SCORING & INVESTIGATION WITH **FORCEPOINT INSIDER THREAT**



GDPR PRACTICAL ADVICE

- Assess current data protection practices
- Create a data protection governance structure
- Maintain a personal data inventory
- Create information notices
- Maintain consent mechanisms
- Apply technical and organisational controls
- Perform Data Protection Impact Assessments (DPIA)
- Report personal data breaches to Supervisory Authority (SA)



GDPR RESOURCE PACK: WWW.FORCEPOINT.COM/GDPR

The screenshot shows the Forcepoint website's landing page for the GDPR Resource Pack. The page has a green header with the Forcepoint logo and navigation links. The main content area features a large title 'EU General Data Protection Regulation (GDPR)' and a subtitle 'Supporting Your GDPR Compliance Program'. Below this, a section titled 'The Forcepoint GDPR Resource Pack' states 'Helping your organization prepare for compliance with the new regulation.' and includes a 'FIND OUT MORE' button. Three featured resources are displayed: 'GDPR Overview - A legislative milestone for a digital age' with a map of Europe, 'GDPR - A guide to key articles for security & privacy professionals' by Hunton & Williams, and '(ISC)2 Security Briefings: GDPR: Countdown to Day 0' featuring a webcast. A green footer bar contains the text 'Access The GDPR Resource Pack' and a 'DOWNLOAD NOW' button.

Secure | <https://www.forcepoint.com/solutions/need/eu-general-data-protection-regulation-gdpr>

English Support Partners Blogs

FORCEPOINT
POWERED BY Raytheon

Solutions Products Services Case Studies Resources Company

EU General Data Protection Regulation (GDPR)

Supporting Your GDPR Compliance Program

The Forcepoint GDPR Resource Pack
Helping your organization prepare for compliance with the new regulation.

FIND OUT MORE

GDPR Overview – A legislative milestone for a digital age

HUNTON & WILLIAMS
GDPR – A guide to key articles for security & privacy professionals

(ISC)2 Security Briefings
GDPR: Countdown to Day 0
(ISC)2 webcast - GDPR: Countdown to Day 0

Access The GDPR Resource Pack

DOWNLOAD NOW



QUESTIONS

