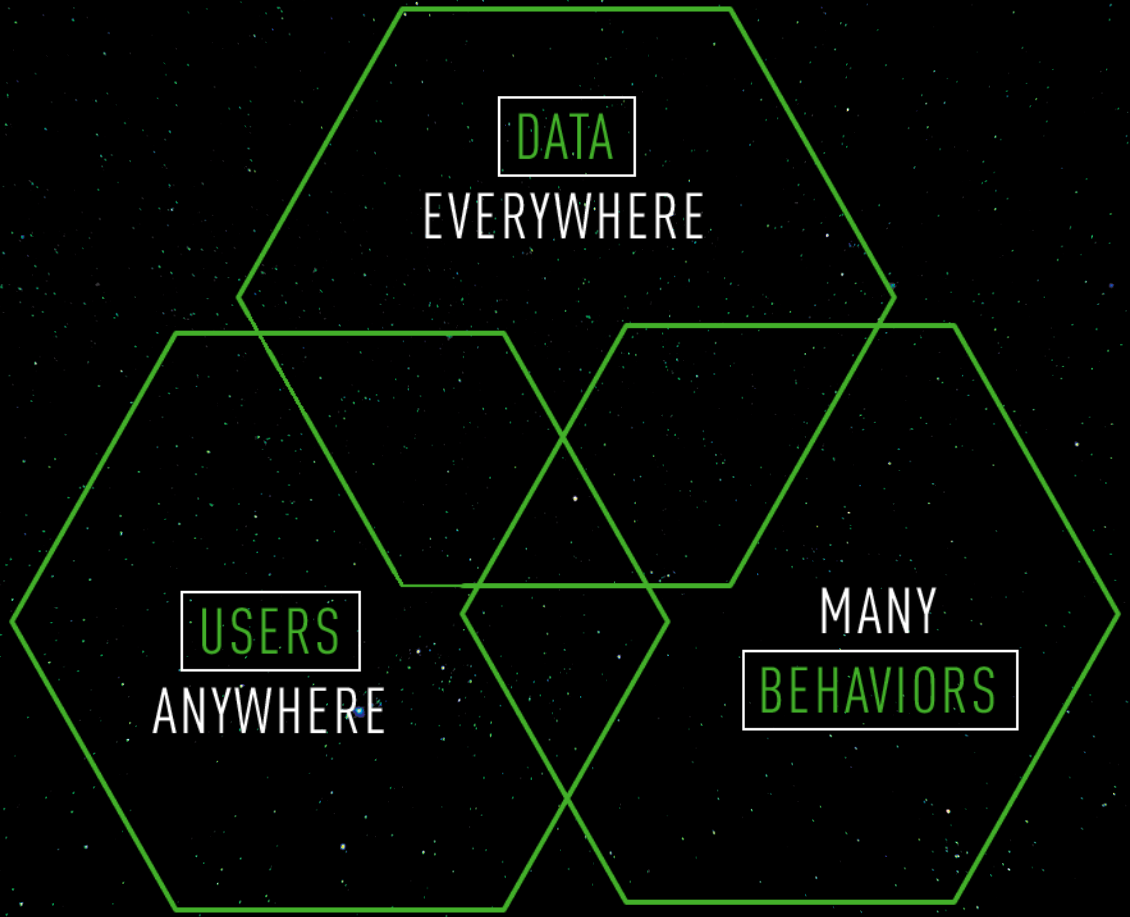
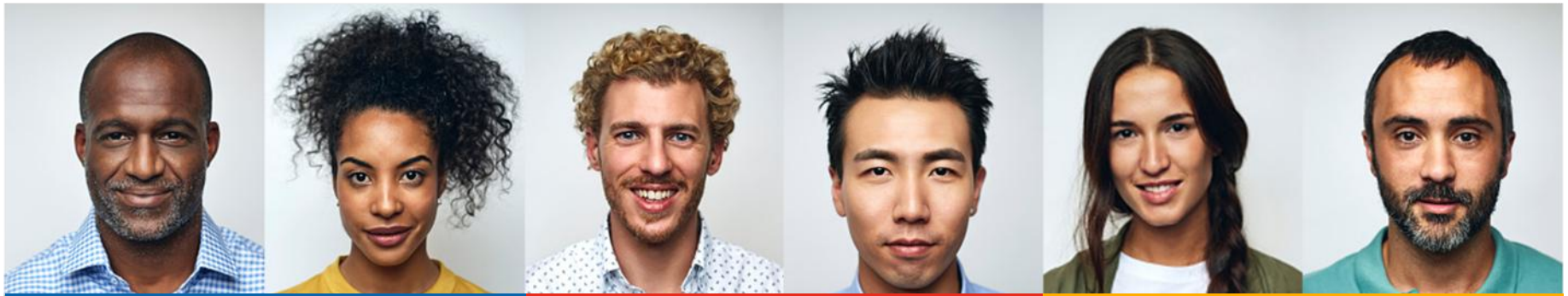
Bytes GDPR Breakfast Briefing

Mapping Forcepoint Technology to the EU GDPR

September 2017


DATA
EVERYWHERE
USERS
ANYWHERE
MANY
BEHAVIORS

TECNOLOGIES CHANGE



ACCIDENTAL INSIDER	MALICIOUS INSIDER	COMPROMIZED INSIDER
68%	22%	10%

MAPPING TECHNOLOGY TO GDPR

GDPR STRATEGY

Preparation

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

<12 Months

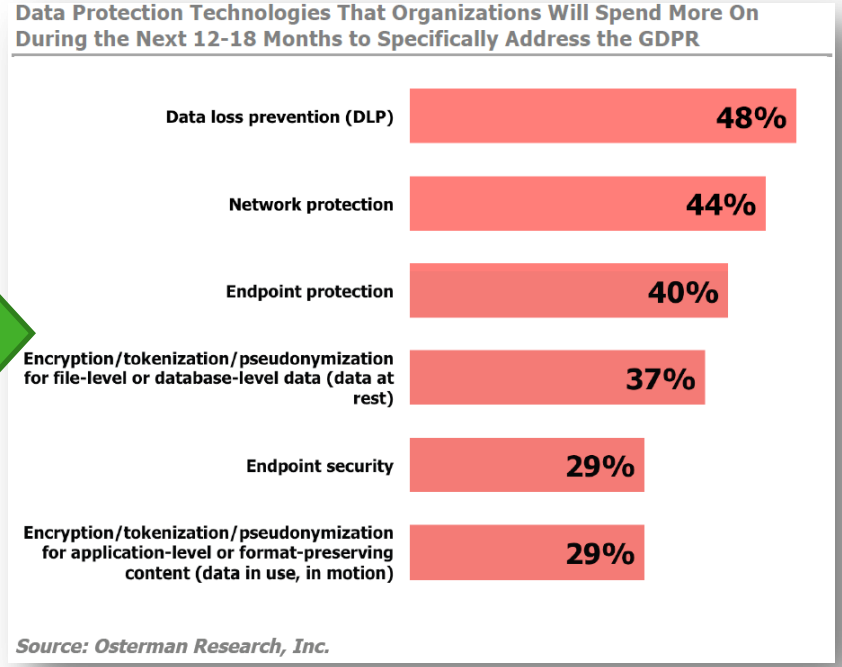
- Data Flow Mapping (Internal/External processing)
- Contract Review
- Data Protection Impact Assessments

<25th May 2018

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

FORCEPOINT
POWERED BY Raytheon

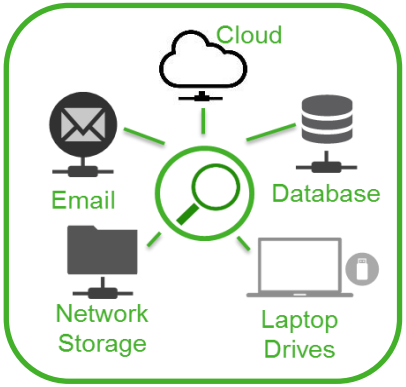
WHAT TECHNOLOGIES WILL ORGANIZATIONS LOOKS TO INVEST IN?



FORCEPOINT
POWERED BY Raytheon

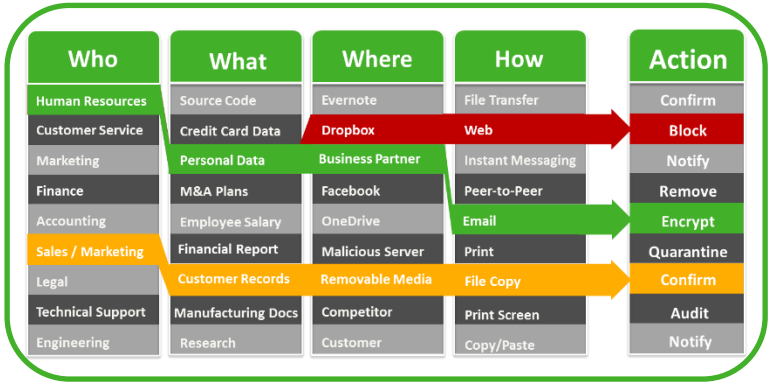
HOW DLP CAN HELP

INVENTORY PERSONAL DATA



DLP: Discover, Cloud, Endpoint

MAP, MANAGE & CONTROL PERSONAL DATA FLOWS



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'

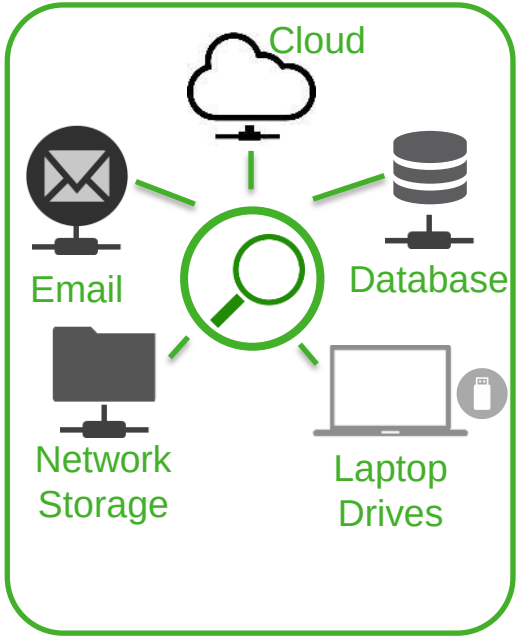
FORCEPOINT
POWERED BY Raytheon

ARTICLES OF THE GDPR – RELEVANT TO DATA INVENTORY

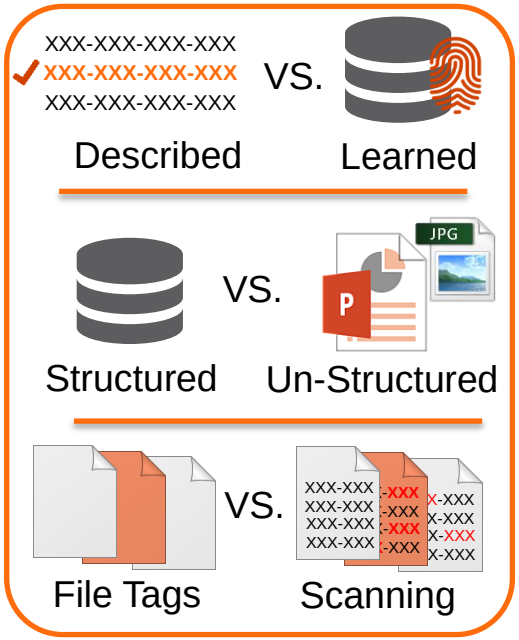
- Chapter 2 (Principles), section 3 (Rectification & Erasure):
  - Article 17 (Right to erasure / 'right to be forgotten'): '*The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay*'
  - Article 20 (Right to data portability): '*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)

FORCEPOINT
POWERED BY Raytheon

PERSONAL DATA DISCOVERY



DATA IS EVERYWHERE

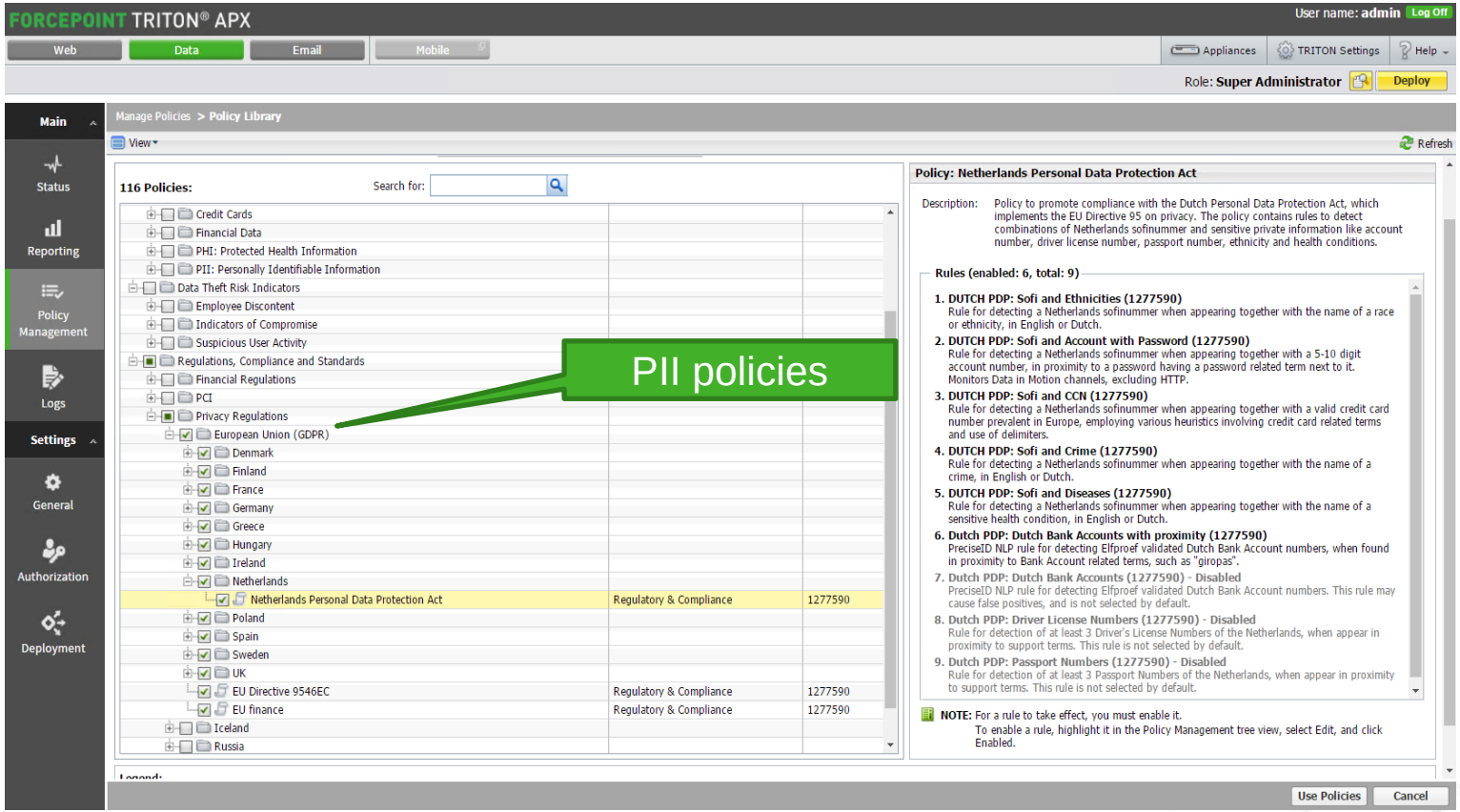


DATA IS NOT ALWAYS EASY TO FIND

FORCEPOINT PRODUCTS: DLP DISCOVER & DLP ENDPOINT

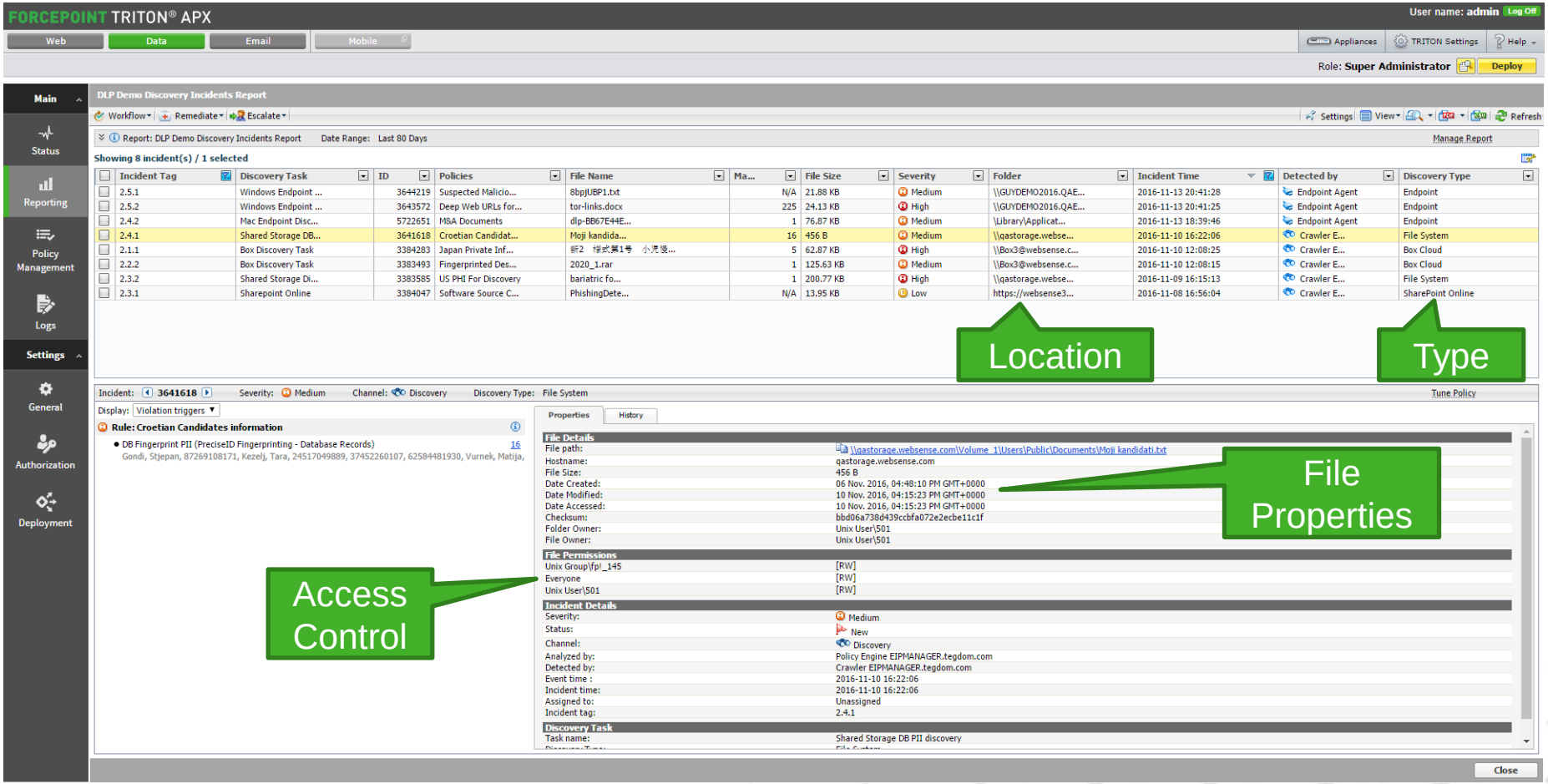
FORCEPOINT
POWERED BY Raytheon

PRE-DEFINED POLICIES ARE A DIFFERENTIATOR



FORCEPOINT
POWERED BY Raytheon

DATA DISCOVERY RESULTS



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

FORCEPOINT
POWERED BY Raytheon

ARTICLES OF THE GDPR – RELEVANT TO MAPPING DATA FLOWS

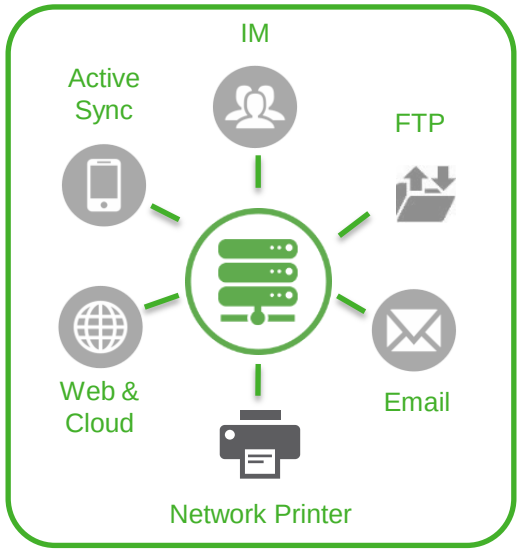
Chapter 4 (Controller & Processor), section 1 (General Obligations):

- 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'.

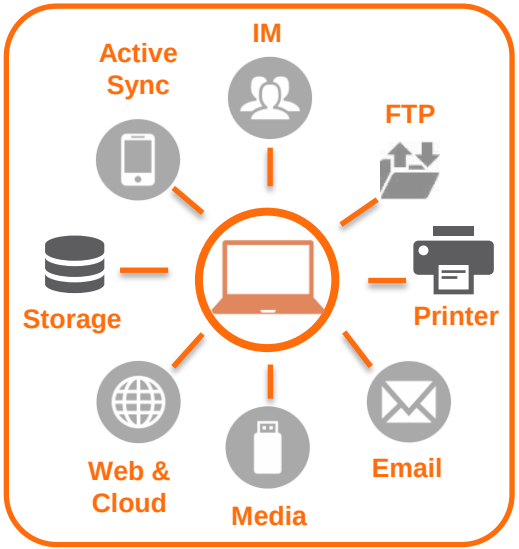
- Article 25 (Data protection by design and by default): 'The controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement 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'.

FORCEPOINT
POWERED BY Raytheon

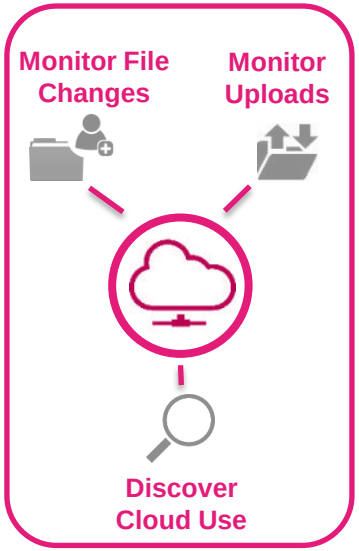
CONSIDERATIONS FOR MONITORING DATA FLOWS



NETWORK
Data in Motion



ENDPOINT
Data in Use & in Motion

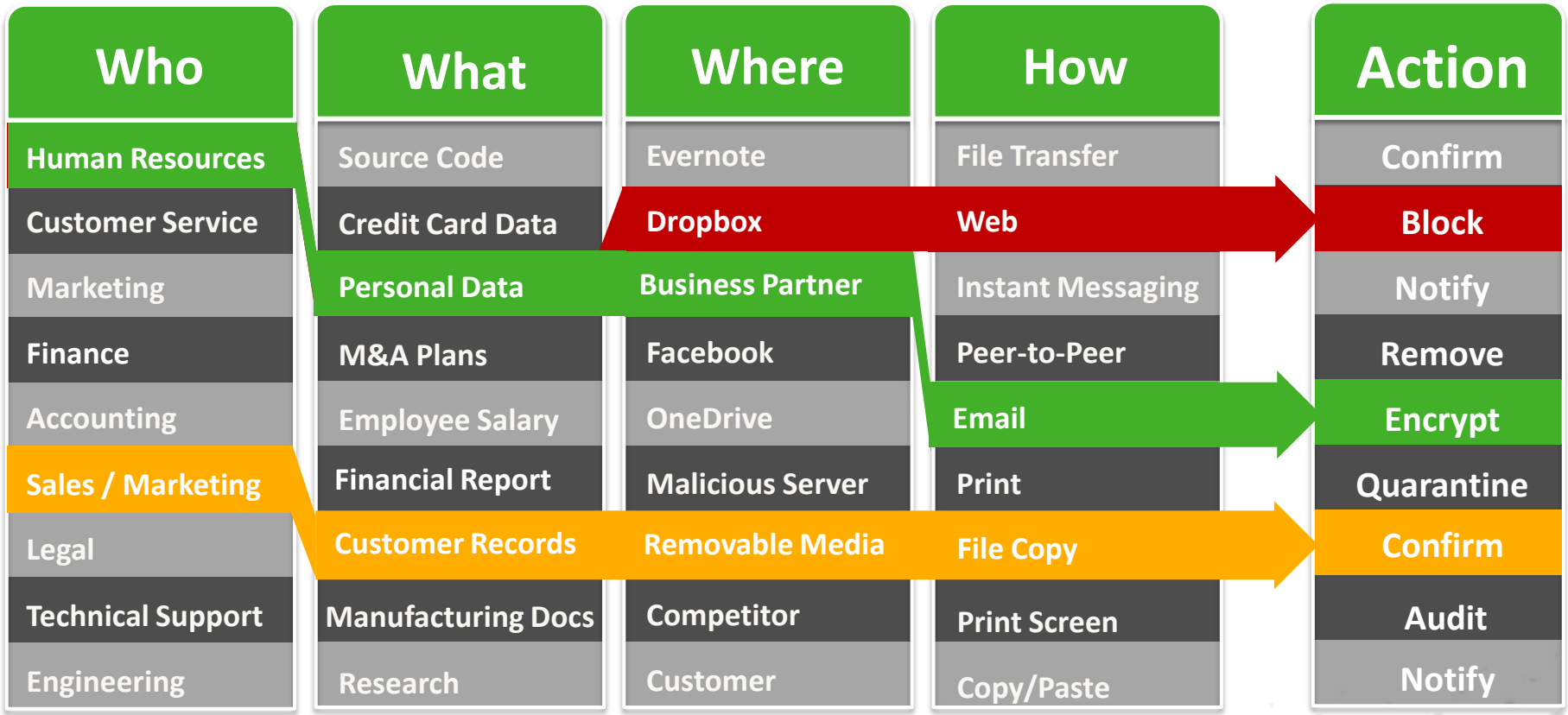


CLOUD
Data In Use & in Motion

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

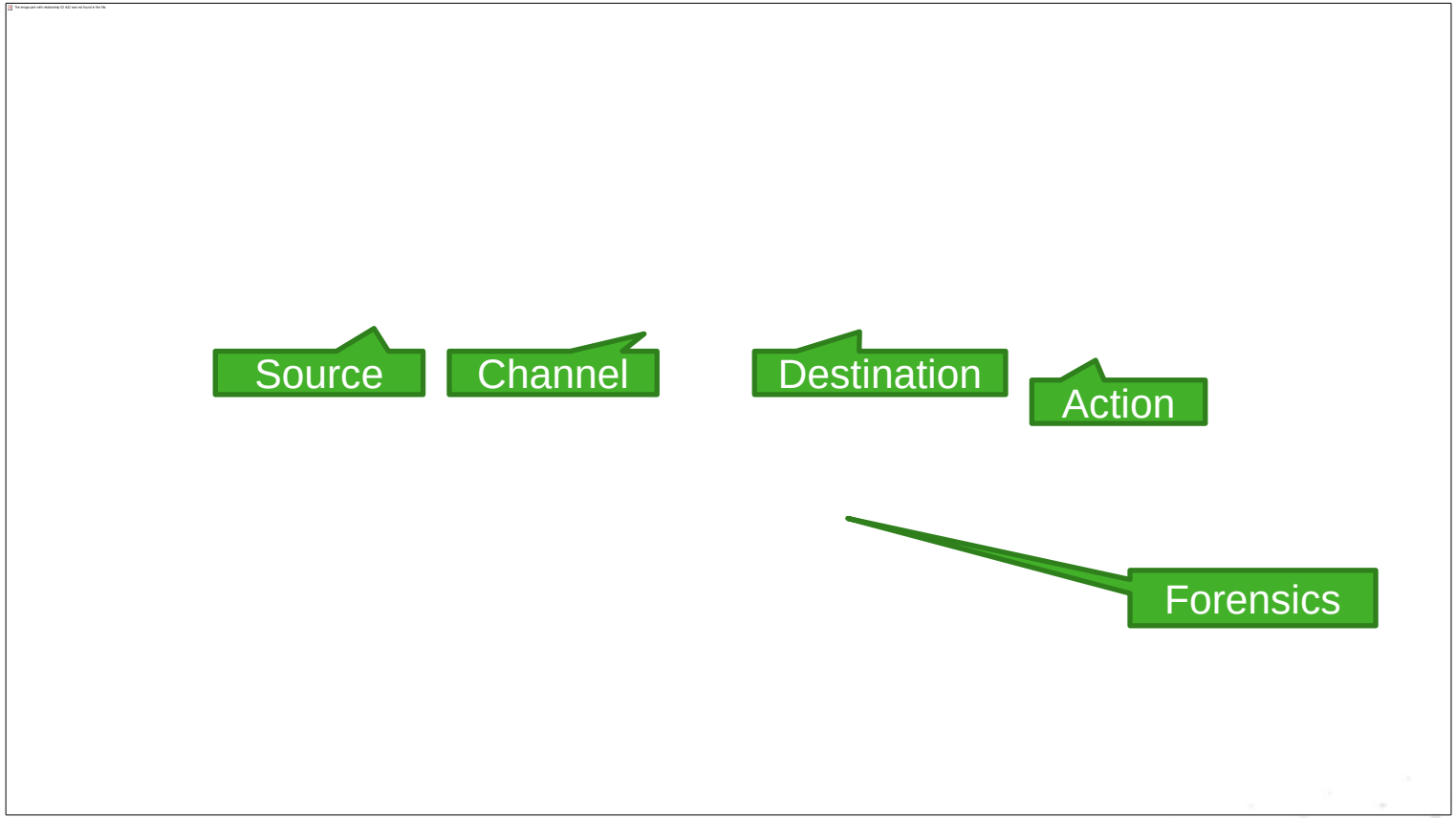
FORCEPOINT
POWERED BY Raytheon

DATA IN USE & IN MOTION



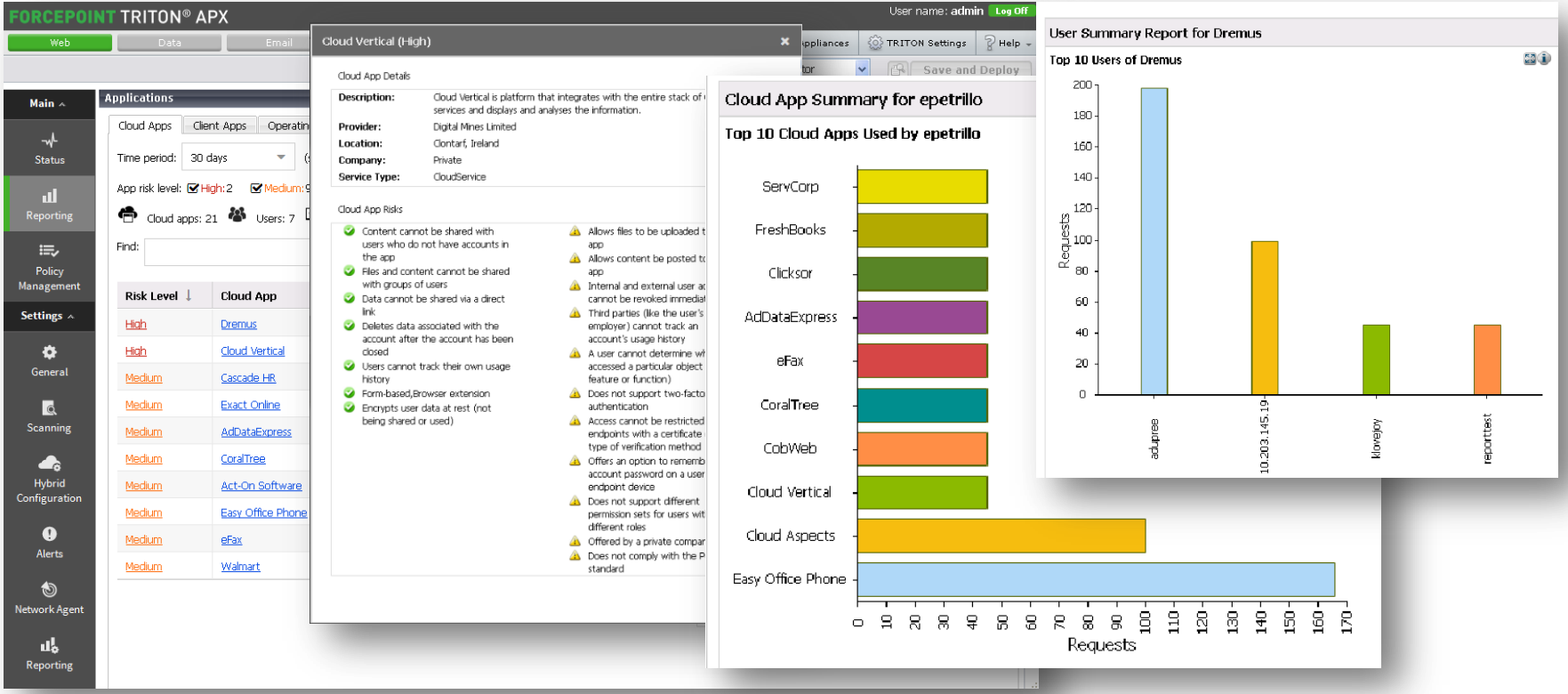
FORCEPOINT
POWERED BY Raytheon

MAPPING DATA FLOWS



FORCEPOINT
POWERED BY Raytheon

VISIBILITY OF UNSANCTIONED CLOUD APPLICATION USAGE



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

FORCEPOINT
POWERED BY Raytheon

The Need to Be Prepared to Report a Data Incident

Understand an organization’s exposure to GDPR

FORCEPOINT
POWERED BY Raytheon

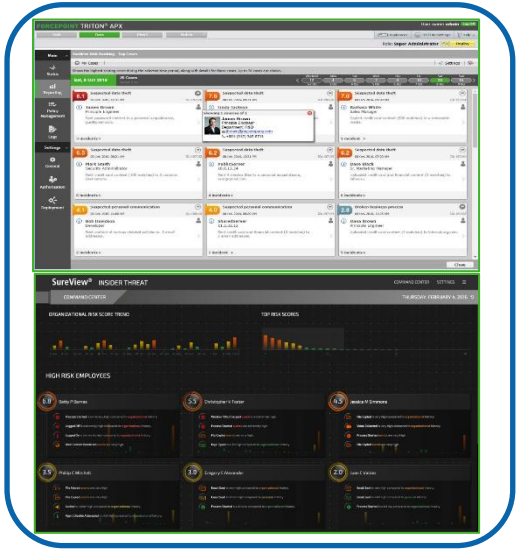
ARTICLES OF THE GDPR – RELEVANT TO RESPONDING TO A DATA BREACH

- 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*'.

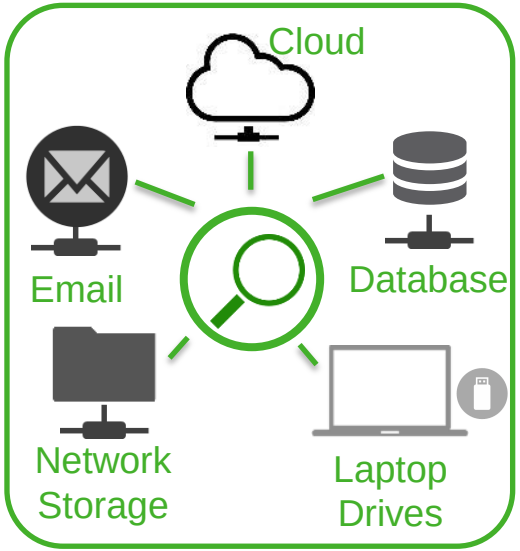
  - Article 34 – (Communication of a personal data breach to the data subject): (1) '*When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay*'.
    - (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'

FORCEPOINT
POWERED BY Raytheon

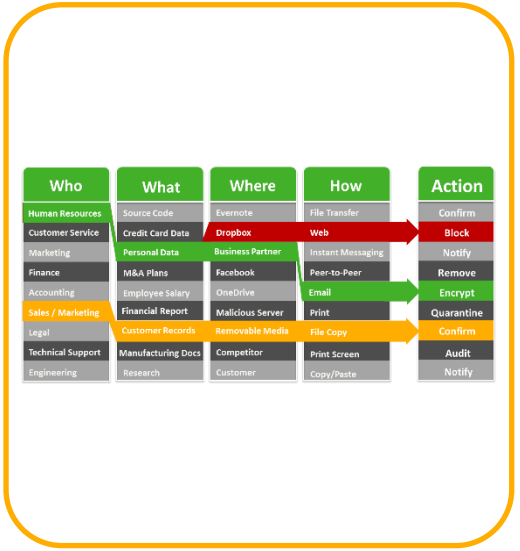
INVESTIGATING A DATA BREACH



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



REVIEW RESULTS TO HISTORICAL PERSONAL DATA INVENTORIES

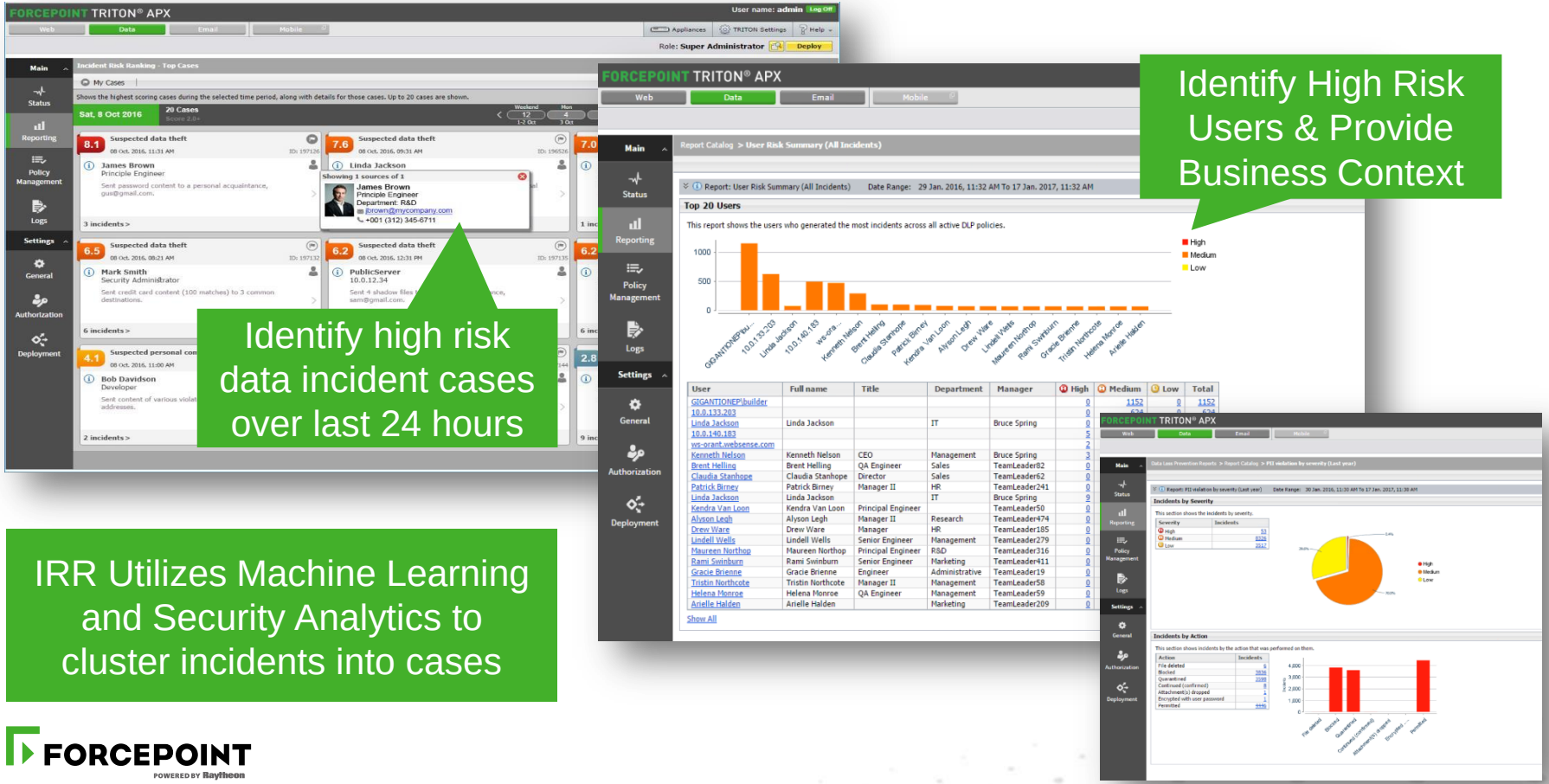


REVIEW INCIDENTS TO PAST DATA FLOW POLICY VIOLATIONS

FORCEPOINT PRODUCTS:
SECURITY MANAGER, INSIDER THREAT COMMAND CENTER

FORCEPOINT
POWERED BY Raytheon

EXAMPLES OF REPORTS TO ASSIST WITH BREACH INVESTIGATION



FORCEPOINT
POWERED BY Raytheon

INVESTIGATING A DATA INCIDENT

Workflow - DPO
Remediate - Encrypt/Pseudonymize
Escalate - Incident

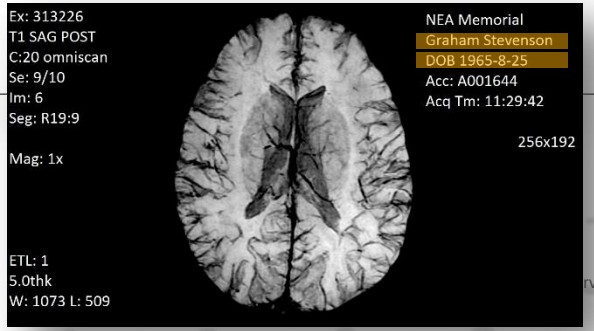
Source

Channel

Destination

Action

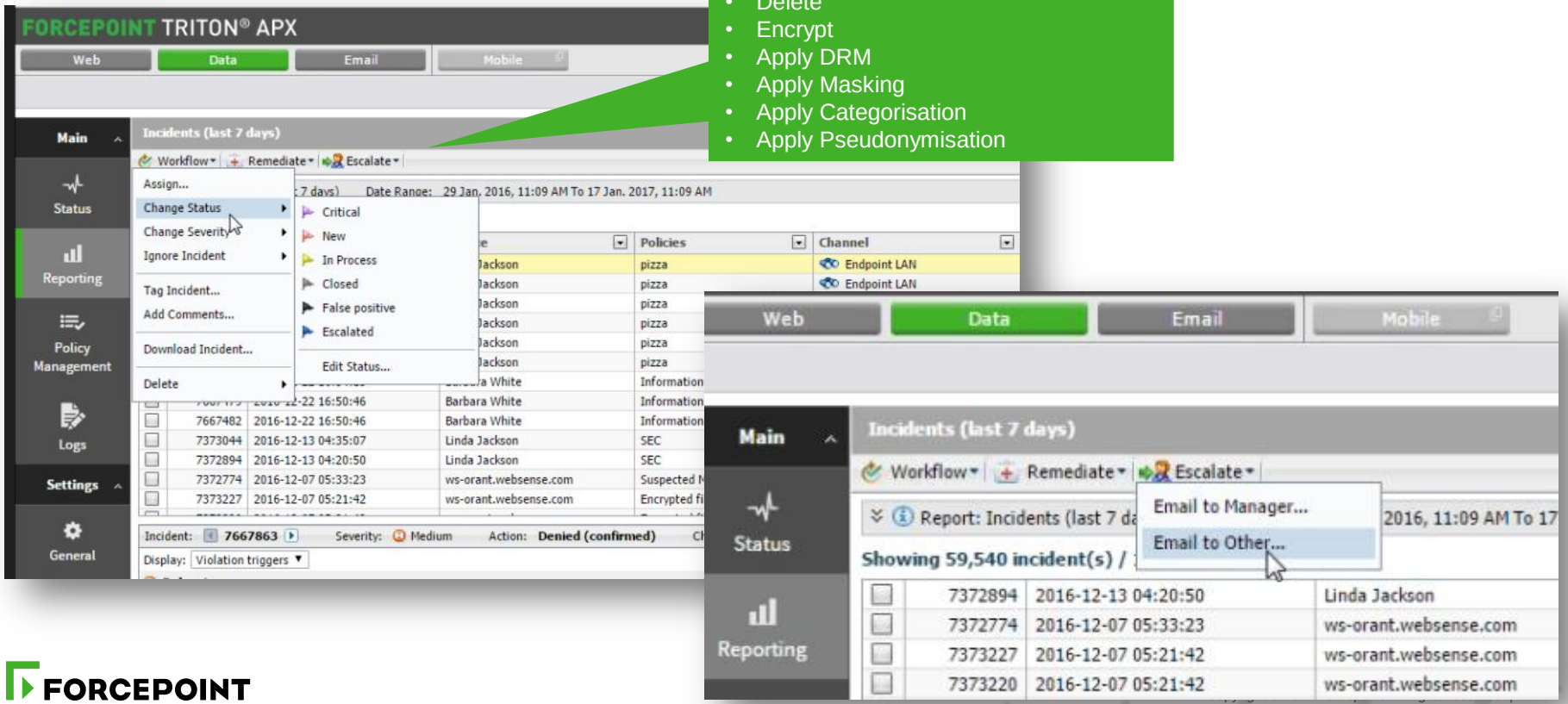
Forensics



INTEGRATED WORKFLOW

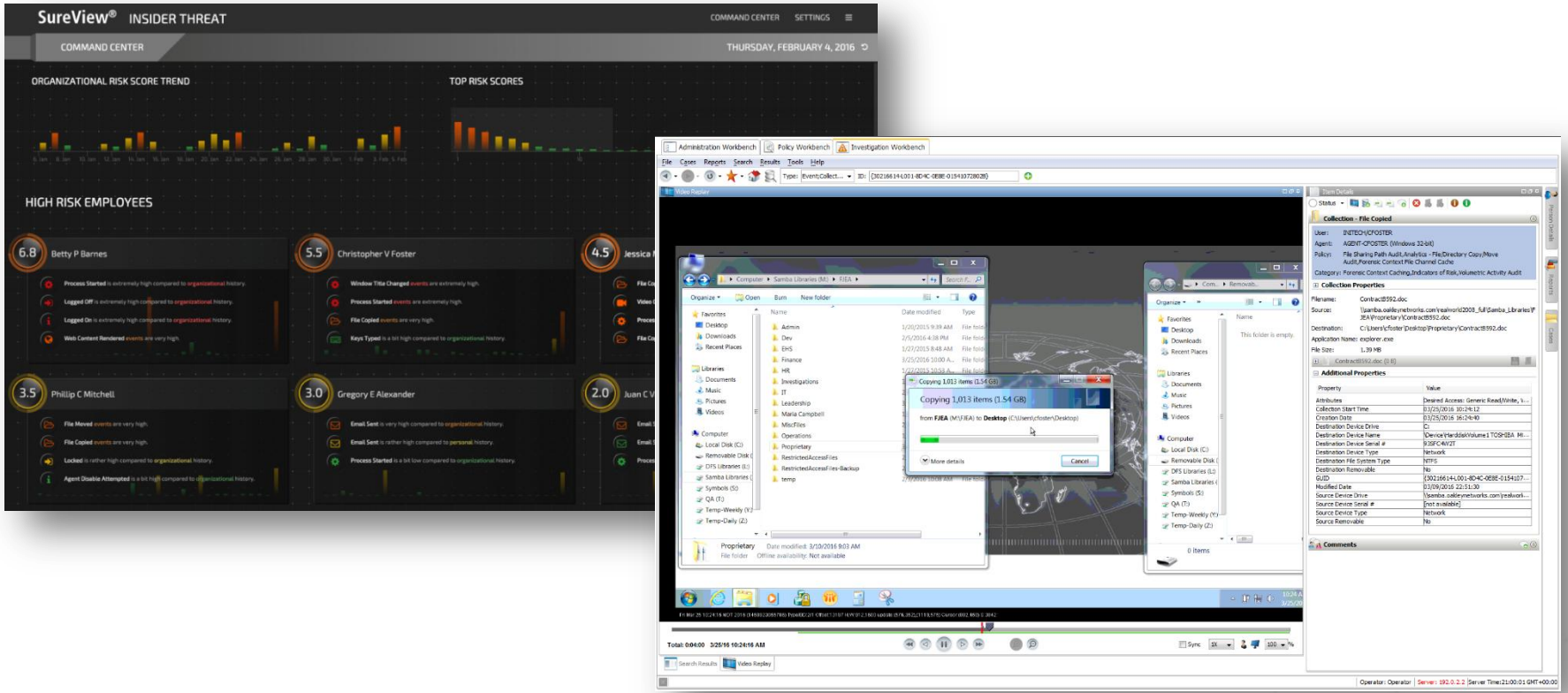
Remediation actions might include:

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



FORCEPOINT
POWERED BY Raytheon

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



FORCEPOINT
POWERED BY Raytheon

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)

FORCEPOINT
POWERED BY Raytheon

GDPR – A legislative milestone for a digital age

BY NEIL THACKER, INFORMATION SECURITY & STRATEGY OFFICER, EMEA FORCEPOINT™

The clock is officially ticking for organisations to get their data protection policies in order now that the General Data Protection Regulation (GDPR) has been approved and is set to replace the previous EU Data Protection Directive.

The new regulation will come into effect in May 2018 and will require organisations to put a much stricter focus on data protection. The headline items for organisations that collect or process EU citizen records are:

- They must notify their supervisory authority of a data breach within 72 hours.
- The subject will have the right to retract consent, request data erasure or data portability.
- They may face fines of up to 4% of their worldwide turnover, or €20 million for intentional or negligent violations.

These increased sanctions mean it is vital that this new law be fully understood by a number of key stakeholders within the organisation, and that organisations start preparing to comply with the new regulations as soon as possible.

There are five key steps to help organisations perform a basic assessment of their current data protection strategy and to identify any potential gaps that need filling prior to a more comprehensive view of the GDPR.

1. IDENTIFY OBLIGATIONS

The first task for any organisation must be to identify whether they are considered a data controller or processor. They must review the relevant obligations these carry, such as issuing notice to citizens and maintaining relevant consent from the data subject.

Organisations should make it common practice to regularly review existing and new business processes to identify personal identifiable information (PII). They should identify where this data resides – whether it's at-rest, in-motion and/or in-use and maintain a record of processing activities and understand how this data is protected.

2. PROTECT PII

Once PII has been identified, organisations must then ensure that they adequately protect this data. Encryption and access control are common control standards, but managing encrypted data across multiple business processes is a hugely difficult task.

Data sovereignty and data lifecycle management are key to helping organisations ensure that EU citizen data is processed and stored appropriately. In addition to these responsibilities, they also need to manage data flows to approved third party processors, monitor for accidental data leakage from negligent or malicious employees and protect against data theft from external attackers.

3. DETECT BREACHES AND THEFT

If an organisation does suffer a loss of data then it is vital to detect the breach and identify if PII records were lost or stolen. If they have, the organisation will be required to notify the necessary authorities within 72 hours of the discovery to initiate a full investigation.

The investigation will focus on identifying the source and destination of the breach through event and incident information from Data Leakage Prevention (DLP) and Data Theft Prevention (DTP) tools. Data forensics will then help to pinpoint the stolen data, at which time the organisation will be required to issue notice to any affected data subjects.

"There are increased obligations on controllers and processors. Individuals are put in a stronger position, and critically for business, increased enforcement powers, fines, and rights of individuals to take action."

— ROSEMARY JAY, SENIOR CONSULTANT ATTORNEY, HUNTON & WILLIAMS

www.forcepoint.com

1

FORCEPOINT
POWERED BY Raytheon

Source: https://www.forcepoint.com/solutions/need/eu-general-data-protection-regulation-gdpr
GDPR: http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

GDPR RESOURCE PACK: WWW.FORCEPOINT.COM/GDPR

FORCEPOINT
POWERED BY Raytheon

QUESTIONS