



Protecting the human point.

Changing the security game

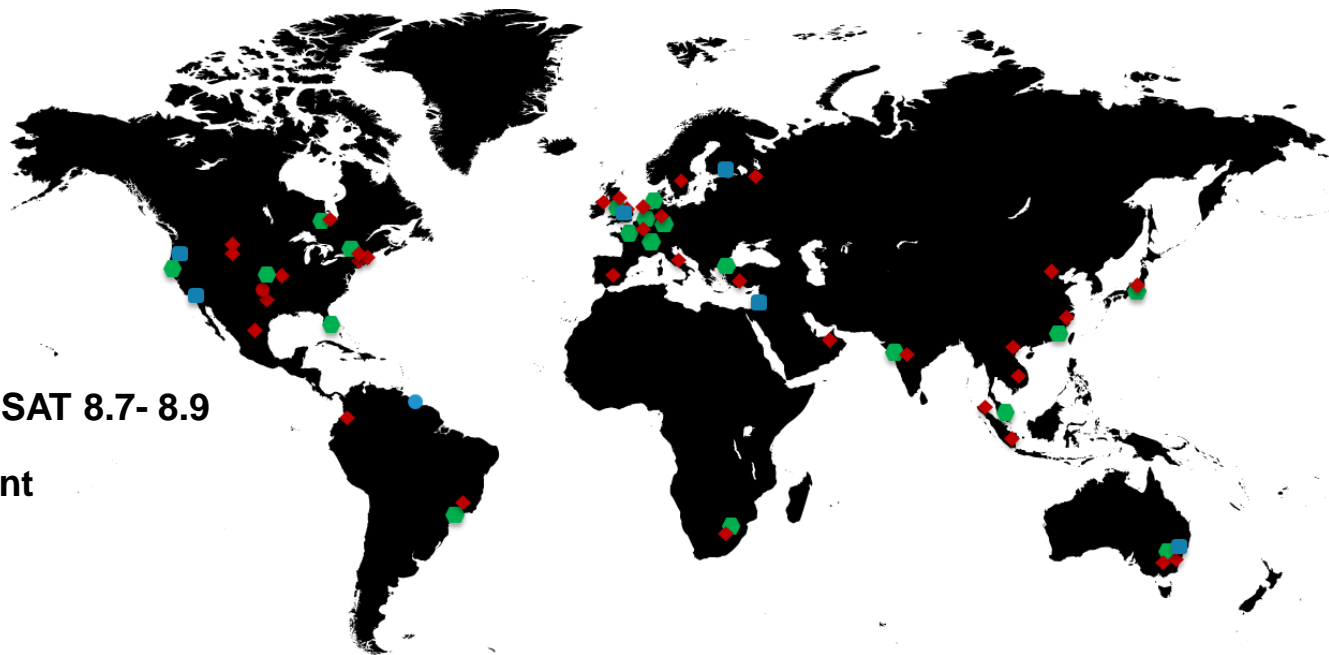
Changing your thinking from “what” to why”

John Enger
Manager, Sales Engineering

STRONG GLOBAL FOOTPRINT

- Headquarters, Austin, TX
- Engineering & Operations
- Cloud Data Center
- ◆ Sales & Support

- ▶ 2,500 Employees
- ▶ 155 Countries
- ▶ 50 Offices
- ▶ 16,000 Partners
- ▶ Average Support CSAT 8.7- 8.9
- ▶ 380 Patents & Patent Applications
- ▶ 27 Data Centers



AMERICAS

EMEA

APAC

RETHINK CYBERSECURITY



Protecting the human point.

LOOKING BEYOND TECHNOLOGY

Technology alone won't create better security outcomes.

\$90b estimated security spend
in 2017

- ▶ Technologies continue to proliferate
- ▶ Breaches remain frequent

< 50%

**of organizations truly agree that
technology will drive increased security**

Understanding behavior is essential, but there's been a gap in the market.

80%

**of companies believe understanding
behavior is important**

< 1/3

**of companies feel they adequately
understand their users' behavior**

PEOPLE ARE THE CONSTANT IN SECURITY



TECHNOLOGIES CHANGE

UNDERSTANDING USER INTENT



ACCIDENTAL INSIDER

Inadvertent Behaviors

Poorly communicated policies and user awareness



Broken Business Process

Data where it shouldn't be, not where it should be



COMPROMISED INSIDER

Malware Infections

Phishing targets, breaches, BYOD contamination



Stolen Credentials

Credential exfiltration, social engineering, device control hygiene



MALICIOUS INSIDER

Rogue Employee

Leaving the company, poor performance review



Criminal Actor Employees

Corporate espionage, national espionage, organized crime



PROTECTING THE HUMAN POINT

**Where critical data and IP are most valuable –
and most vulnerable**

FORCEPOINT

A company with a unique point of view

VISION

To understand the world's cyber behaviors to **STOP THE BAD** and **FREE THE GOOD**.

MISSION

REINVENT cybersecurity by creating uncompromising **SYSTEMS** that understand people's **BEHAVIORS** and **MOTIVATIONS** as they interact with data and **IP EVERYWHERE**.

THE HUMAN POINT IS ABOUT UNDERSTANDING

the rhythm of your people **AND** the flow of your data

BUT HUMANS ARE NOT LOGICAL



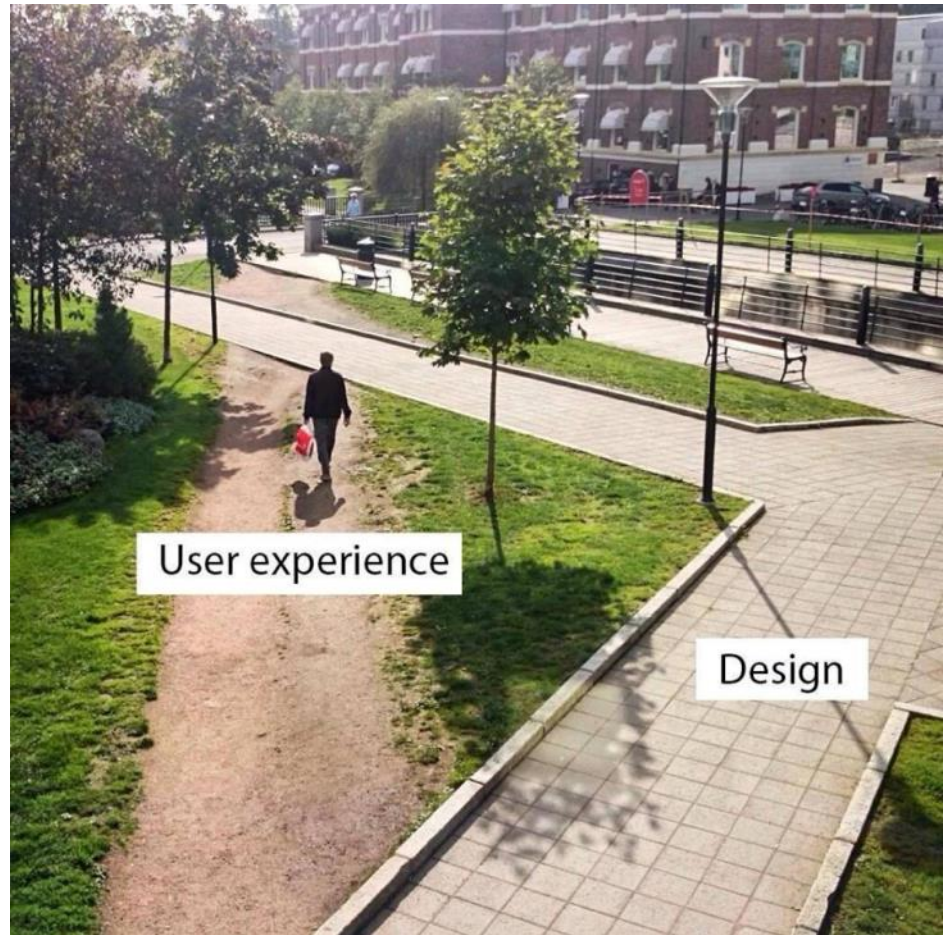
Desire lines

Understand how **Users**
want to use their **Data**
and systems.



Desire lines

Understand how **Users**
want to use their **Data**
and systems.

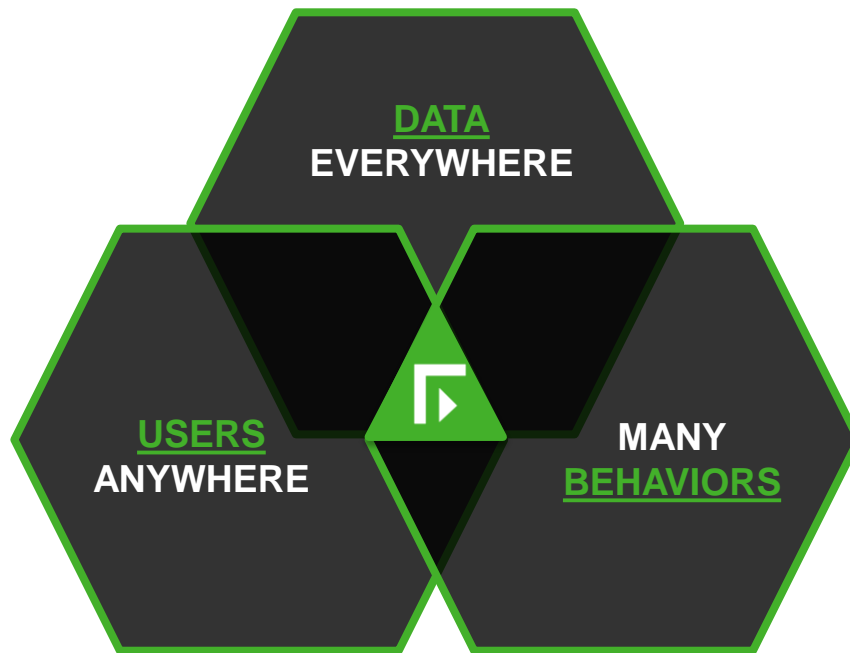


Desire lines

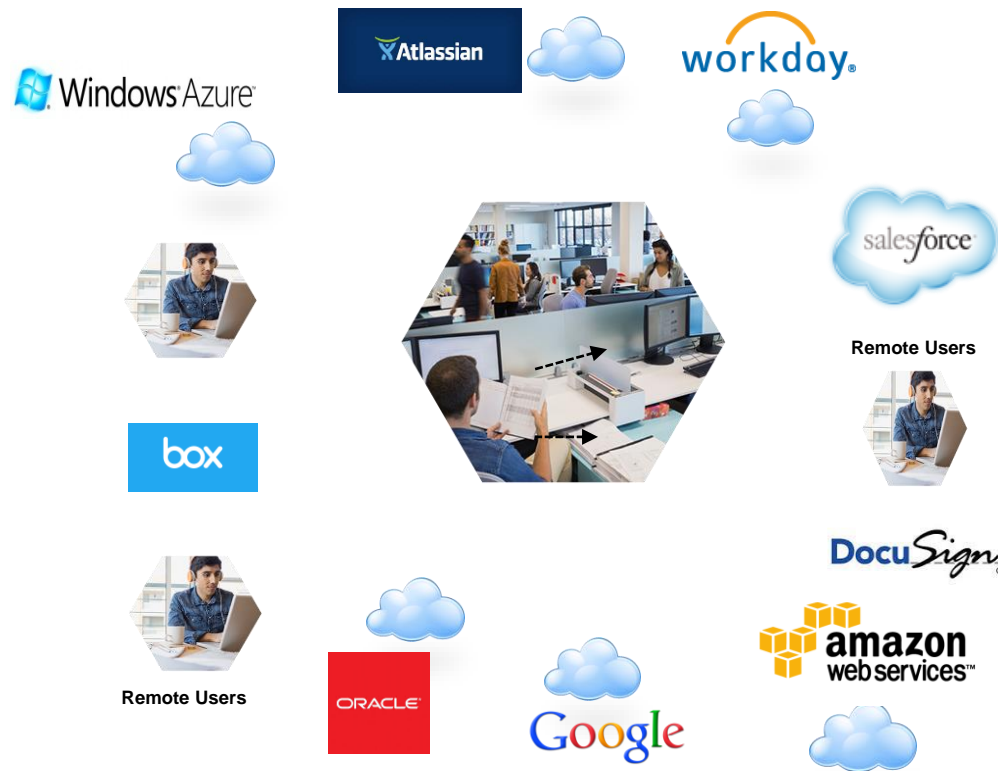
Understand how **Users**
want to use their **Data**
and systems.



FORCEPOINT'S APPROACH TO SECURITY



TODAY'S REALITY: THE ZERO-PERIMETER WORLD



- 1. Significantly increased attack surface**
- 2. Lack of Visibility**
You cannot secure what you cannot see
- 3. Disjointed Security Policy**
From one perimeter to defend to many
- 4. Silo'd Intelligence & limited visibility to risk**
Unable to make informed decisions for the entire business
- 5. Ineffective Enforcement**
Unable to make informed decisions for the entire business
- 6. Compliance**
Things just got a lot more complicated

THE HUMAN POINT IS ABOUT UNDERSTANDING

the rhythm of your people **AND** the flow of your data

BENEFIT FROM THE HUMAN POINT



Visibility

Identify your data and users everywhere your people work

Control

One policy to manage data movement & access across ALL distributed systems

Risk

Consolidated view of risk that considers user actions & value of the data in addition to machine logs

Enforcement

Risk adaptive protection to act on change in human risk to critical data in real time

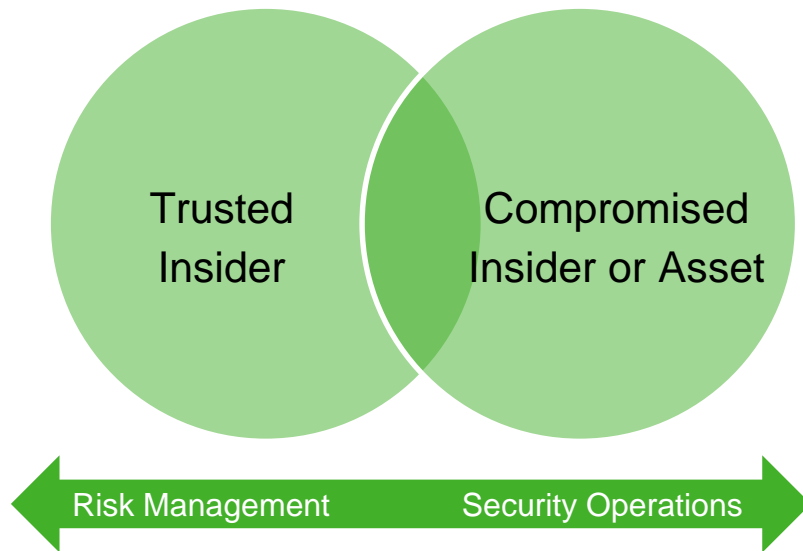
Compliance

Effectively enforce compliance no matter where your data resides

TRUSTED INSIDERS VS. COMPROMISED USERS & ASSETS

Customer challenge:

- ▶ Centralized, correlated visibility to user activity
 - ▶ Cloud apps
 - ▶ Devices
 - ▶ User communications
 - ▶ HR data



Customer challenge:

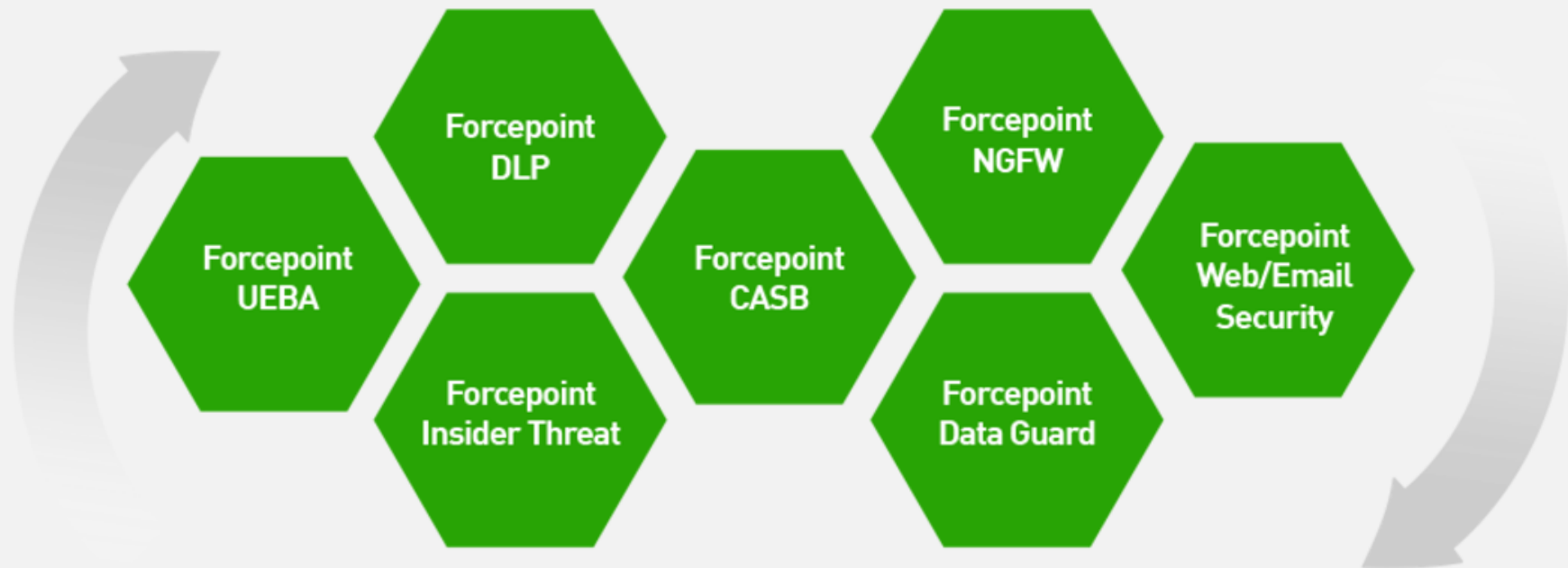
- ▶ Cyber threats target the people & authorized users who access data & critical systems
 - ▶ Mean time to detection: ~150 days

Pinpoint threats

Reduce signal to noise ratio

THE HUMAN POINT SYSTEM

The human point is the intersection of users, data & networks.



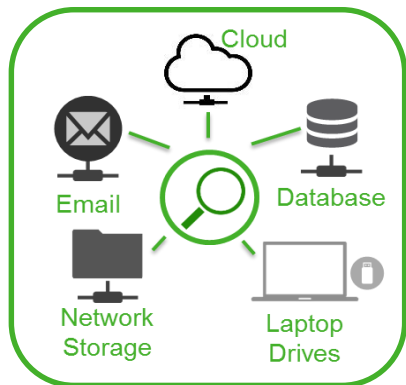
ANALYTICS | MANAGEMENT | ORCHESTRATION

GDPR:

EU General Data Protection Regulations

GENERAL DATA PROTECTION REGULATION: HOW FORCEPOINT 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: Gateway, Endpoint
Web & Email Security modules

PREPARE TO RESPOND IN A TIMELY MANNER

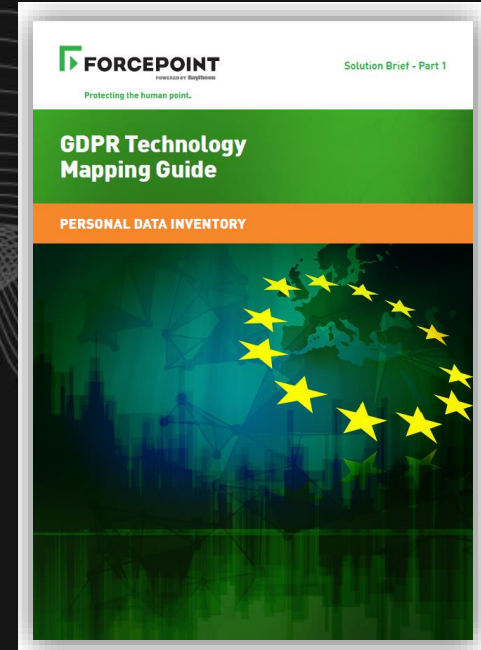


Management Consoles &
Dashboards

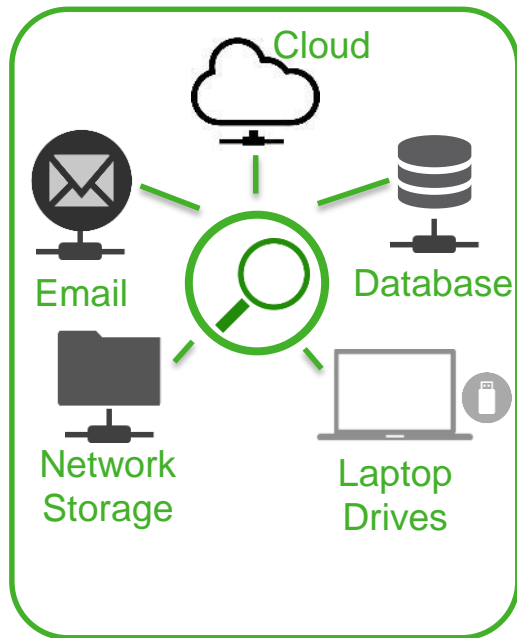
The Need to Inventory Personal Data

GDPR Relevance:

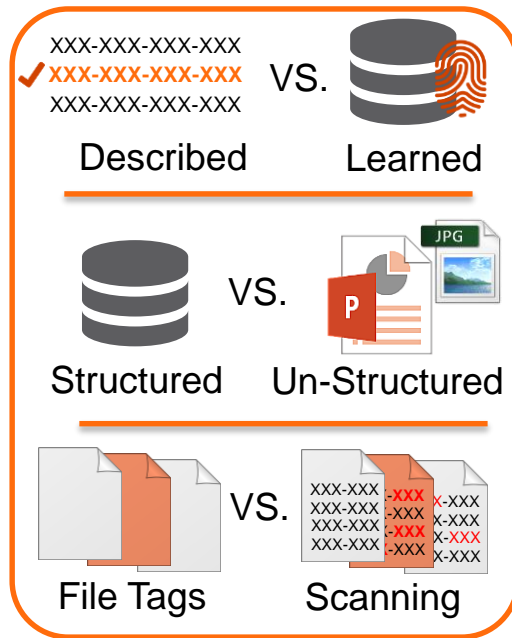
- ▶ Chapter 2 (Principles), section 3 (Rectification & Erasure)
- ▶ Chapter 4 (Controller & Processor), section 1 (General Obligations)
- ▶ Chapter 5 (Transfers of personal data to third countries or international organisations)



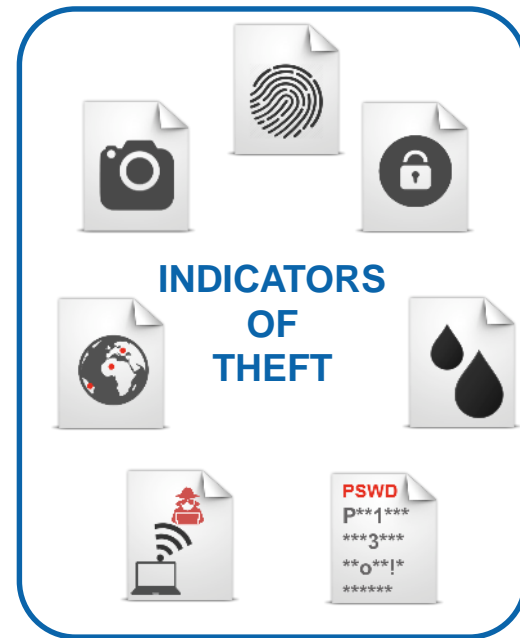
PERSONAL DATA DISCOVERY



DATA IS
EVERYWHERE



DATA IS NOT ALWAYS
EASY TO FIND



DATA ISN'T JUST LOST, IT
CAN BE STOLEN TOO

PRODUCTS: DISCOVER DLP & ENDPOINT DLP

PRE-DEFINED POLICIES ENABLE FASTER TIME TO DEPLOY

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)

- 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.
- 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.
- 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.
- 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.
- 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.
- 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".
- 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.
- 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.
- 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

https://www.websense.com/content/support/library/data/v83/policy_classifier/data%20usage%20policies.aspx

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...	第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, Stjepan, 87269108171, Kezelj, Tara, 24517049889, 37452260107, 62584481930, Vurnek, Matij...

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

Location

Type

File Properties

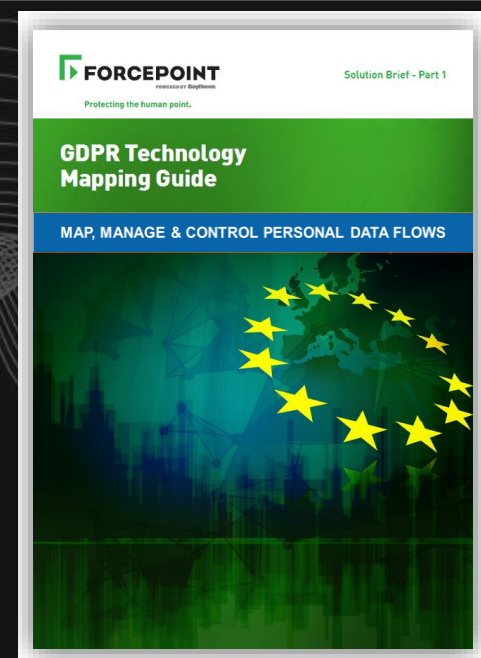
Access Control

Close

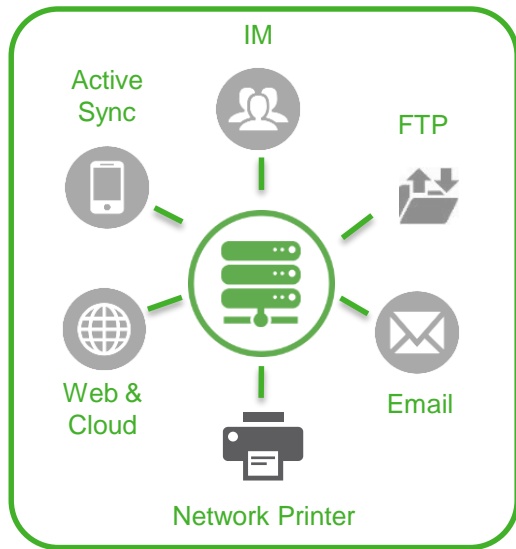
The Need to Monitor, Manage & Control Personal Data Flows

GDPR Relevance:

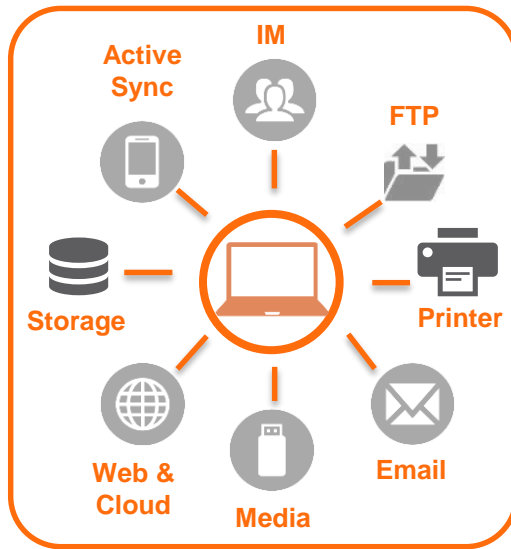
- ▶ Chapter 2 (Principles), section 3 (Rectification & Erasure)
- ▶ Chapter 4 (Controller & Processor), section 1 (General Obligations), section 2 (Security of personal data)
- ▶ Chapter 5 (Transfers of personal data to third countries or international organisations)



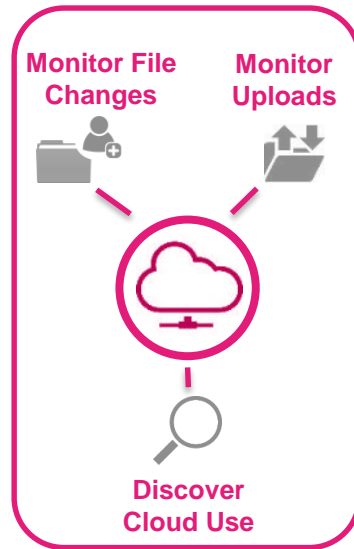
CONSIDERATIONS FOR MONITORING DATA FLOWS



NETWORK
Data in Motion



ENDPOINT
Data in Use
& in Motion



CLOUD
Data In Use
& in Motion

PRODUCTS: GATEWAY DLP + ENCRYPTION, NETWORK DLP, ENDPOINT DLP, CLOUD DLP & CASB

DLP SECURES SENSITIVE DATA IN USE & IN MOTION

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

USE PLAIN LANGUAGE

Do not allow professors to send research data
to...↓

(Action)

Rule Properties |

Severity: (High)

Action Plan: (Block_All)



(Who: From)

Rule Properties | Source |

Edit: Directory Entries



(How)

Rule Properties | Destinations |

✓ Email

✓ Web

✓ HTTP/HTTPS

✓ Chat



(What)

Rule Properties | Condition |

Add: PrecisID FP – DB Records



(Who: To)

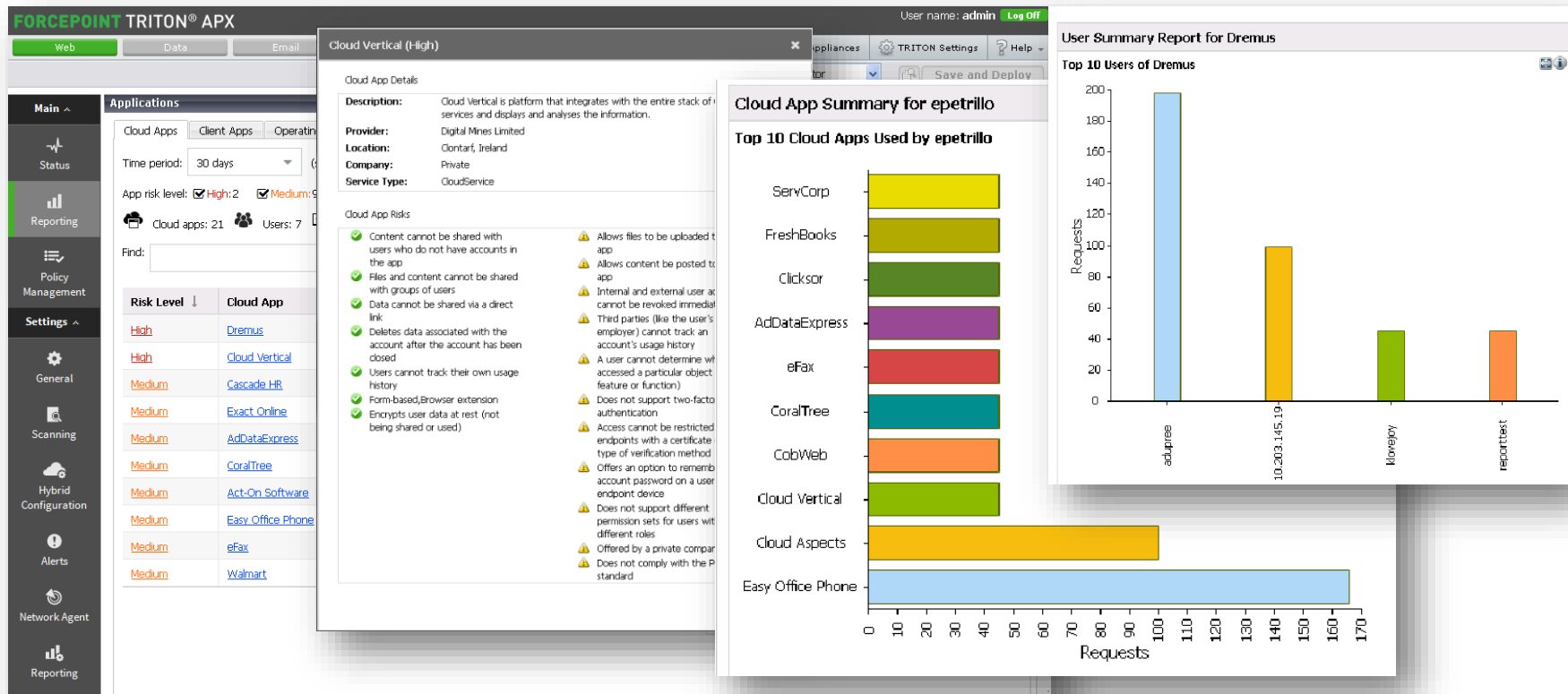
Rule Properties | Destinations |

✓ Email: All

✓ Web: All



VISIBILITY OF UNSANCTIONED CLOUD APPLICATION USAGE



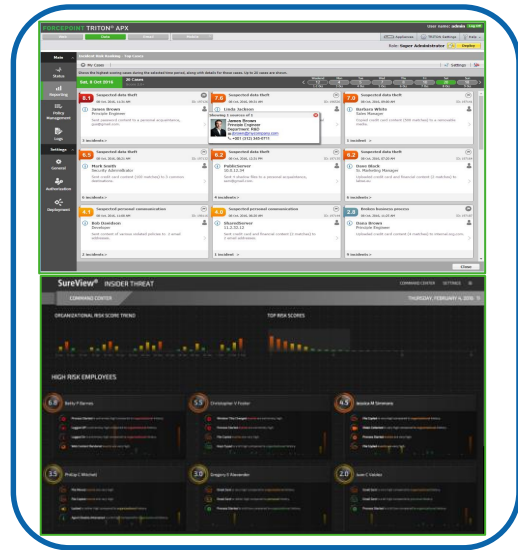
CASB: Identifies usage of cloud apps that can represent risk to an enterprise

The Need to Be Prepared to Report a Data Incident

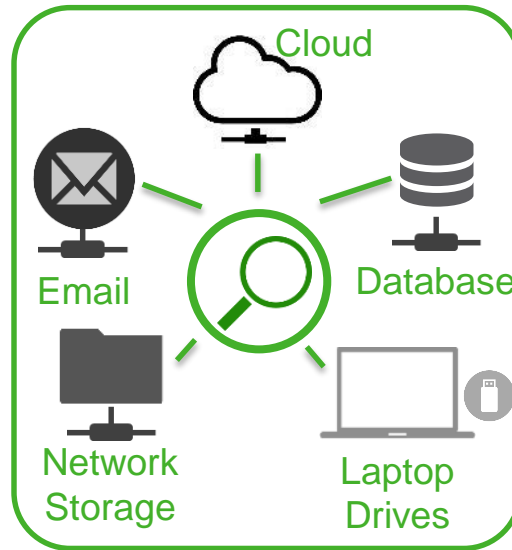
GDPR Relevance:

- ▶ Chapter 4 (Controller & Processor), section 2 (Security of personal data):
 - ▶ Article 33 – (Notification of a personal data breach to the supervisory authority)
 - ▶ Article 34 – (Communication of a personal data breach to the data subject)

INVESTIGATING A DATA BREACH



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



REVIEW RESULTS TO
HISTORICAL
PERSONAL DATA
INVENTORIES

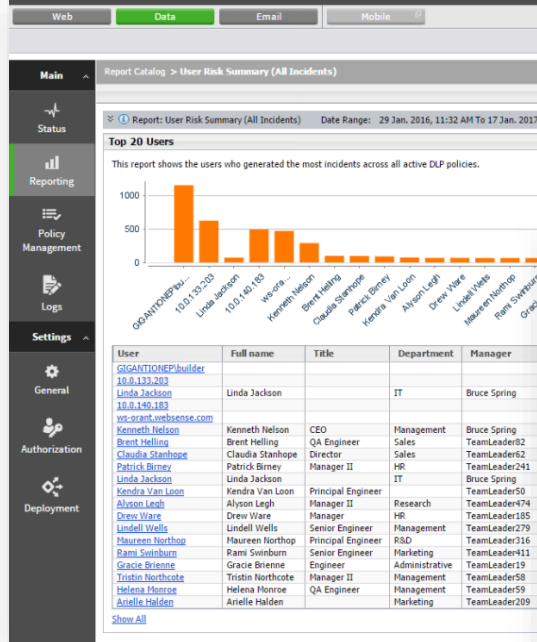
Who	What	Where	How	Action
Human Resources	Source Code	Evernote	File Transfer	Confirm
Customer Service	Credit Card Data	Dropbox	Web	Block
Marketing	Personal Data	Business Partner	Instant Messaging	Notify
Finance	M&A Plans	Facebook	Peer-to-Peer	Remove
Accounting	Employee Salary	OneDrive	Email	Encrypt
Sales / 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

PRODUCTS: MANAGEMENT INFORMATION & REPORTING & RESPONSE TOOLS

EXAMPLES OF REPORTS TO ASSIST WITH BREACH INVESTIGATION

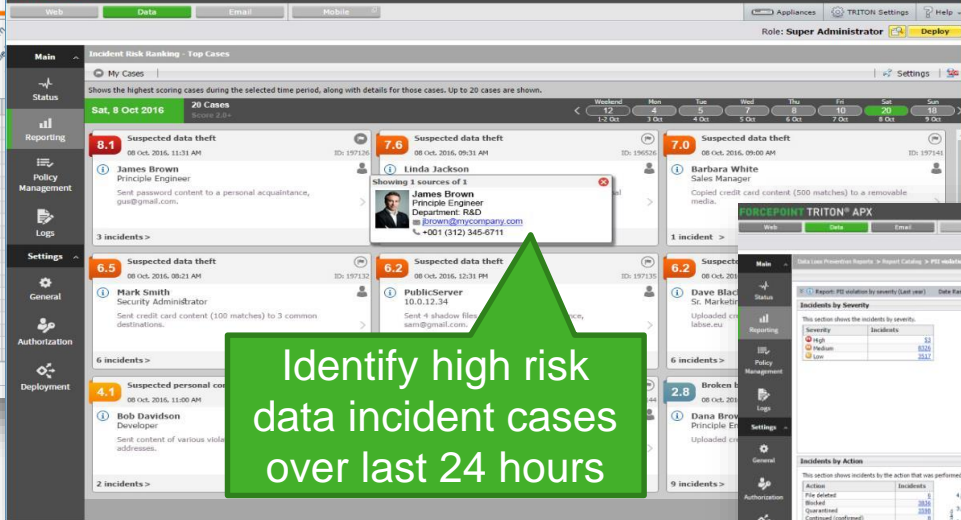
FORCEPOINT TRITON® APX



Identify High Risk Users & Provide Business Context

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

FORCEPOINT TRITON® APX



INVESTIGATING A DATA INCIDENT IN FORCEPOINT MANAGER

FORCEPOINT TRITON® APX

User name: admin Log Off

Web Data Email Mobile

Appliances TRITON Settings Help

Role: Super Administrator Deploy

Settings View Refresh

Manage Report

Main

DLP Demo Incidents Report

Workflow Remediate Escalate

Report: DLP Demo Incidents Report Date Range: Last 60 Days

Showing 10 incident(s) / 1 selected

Incident	ID	Incident Time	Source	Policies	Channel	Destination	Severity	Action	Transaction Size	Status
3.1	5859195	2016-11-14 20:44:26	Nathalie Derby	PCI; Peoples Repu...	Network email	barackadama@yahoo...	High	Permitted	17.5 KB	New
3.2.1	7005210	2016-11-17 12:37:02	Barbara White	Email to Competit...	Network email	adassler@adidas-g...	High	Quarantined	330.68 KB	New
3.2.2	3440707	2016-11-09 18:45:42	Linda Jackson	Suspected Mail to P...	Network email	linda.jackson1976...	Medium	Quarantined	34.95 KB	New
3.4	5846287	2016-11-14 11:36:44	10.0.140.183	Web DLP Policy; P...	HTTP	www.filedropper.com	High	Blocked	1.15 KB	New
3.5	3693321	2016-11-13 17:01:02	10.0.140.183	3M Product Numbers	HTTPS	safebrowsing.goog...	Medium	Permitted	23.97 KB	New
3.6	3670239	2016-11-10 16:56:21	10.0.140.183	Galaxy Note 7 doc...	FTP	10.11.2.67	Medium	Permitted	8.47 MB	New
3.7	7088314	2016-11-18 12:16:28	10.0.151.51	Password files	HTTP	10.11.2.72	High	Permitted	1.13 KB	New
5.2	7667629	2016-12-22 16:54:15	Barbara White	Information Gover...	Network email	knelson@qaexch201...	Medium	Permitted	283.94 KB	New
OneDrive	3276851	2016-11-06 11:32:56	cloud:forcecloud...	PCI; Credit Cards	File Sync and Sharing	forcecloud-my.sha...	High	File deleted	468 B	New
RMS	3211353	2016-11-03 16:12:34	Q...	PCI; Credit Cards...	Endpoint LAN	\\10.0.20.80\VOLUME_1	High	Blocked	54.5 KB	New

Incident: 7667629 Severity: Medium Action: Permitted Channel: Network email

Display: Violation triggers

Rule: IG Toolkit: DOB and Name

- Date Of Birth near UK Names
- Graham Stevenson, 1965-8-25

Forensics Properties History

From: Barbara White

To: knelson@qaexch2010.wbwn

Subject: Automatic Email Subject with <keyword>

Attachments: optima_mr450w_with_gem_suite_mr450wswn_ex433_clinical.jpg(282.88 KB)

Message Body

Sent: 20 Jan. 2017, 1:02:40 AM

Ex: 313226

T1 SAG POST

C:20 omniscan

Se: 9/10

Im: 6

Seg: R19:9

Mag: 1x

ETL: 1

5.0thk

W: 1073 L: 509

NEA Memorial

Graham Stevenson

DOB 1965-8-25

Acc: A001644

Acq Tm: 11:29:42

256x192

Workflow - DPO

Remediate - Encrypt/Pseudonymize

Escalate - Incident

Source

Channel

Destination

Action

Forensics

Forcepoint

POWERED BY Raytheon

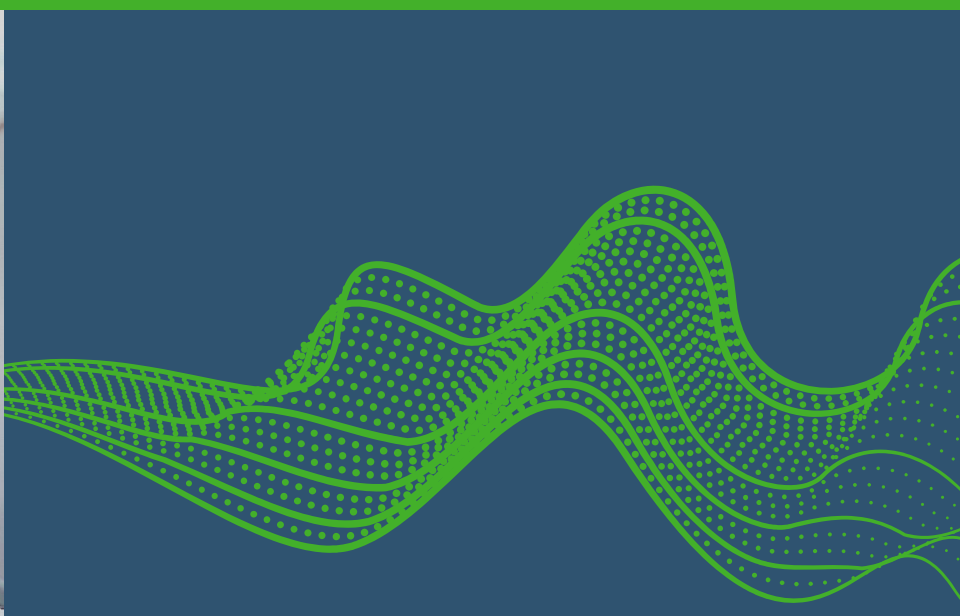
erved. | 34



GDPR:

Forcepoint Can Help

PROTECT THE HUMAN POINT BY UNDERSTANDING



the rhythm of your people

AND

the flow of your data



VISIBILITY

Know where your critical IP is & who is interacting with it everywhere



POLICY

One policy to manage data movement & access across ALL distributed systems



ENFORCEMENT

Risk adaptive protection to act on change in human risk to critical IP in real time



COMPLIANCE


Effectively adhere to compliance regulations no matter where your data resides



Visibility

**Users &
Critical Data**

**Investigate
& Act**

A busy city street scene with many pedestrians walking across the frame. In the background, there is a traffic jam with cars and a white van with a logo. The scene is slightly blurred, emphasizing the movement and density of the urban environment.

Tack för att ni har lyssnat

**PROTECTING THE
HUMAN POINT.**



Thank you