GDPR:
The role of DLP and Incident Risk Ranking

February 2017

Neil Thacker, Deputy CISO
nthacker@forcepoint.com
@nt_hacker

DISCLAIMER

The following presentation does not represent direct legal advice.

We strongly recommend you discuss achieving compliance via your Legal/Compliance teams, Data Protection/Privacy Officer and work with the relevant workers councils.

UNIQUELY FORMED TO OFFER A NEW APPROACH TO SECURITY

websense®

Commercial Leader

with

Content Security & DLP
Cloud / On-Premise / Hybrid

Raytheon

Pioneer on Cyber Frontlines

with

Financial Resources
Deep Understanding of Threat Detection

STONESOFT

Networking Innovator

with

Advanced Evasion Prevention
Security at Scale

FORCEPOINT
POWERED BY Raytheon

AS AN ORGANISATION THAT HANDLES PII…

Are you a controller?

Are you a processor?

Are you both?

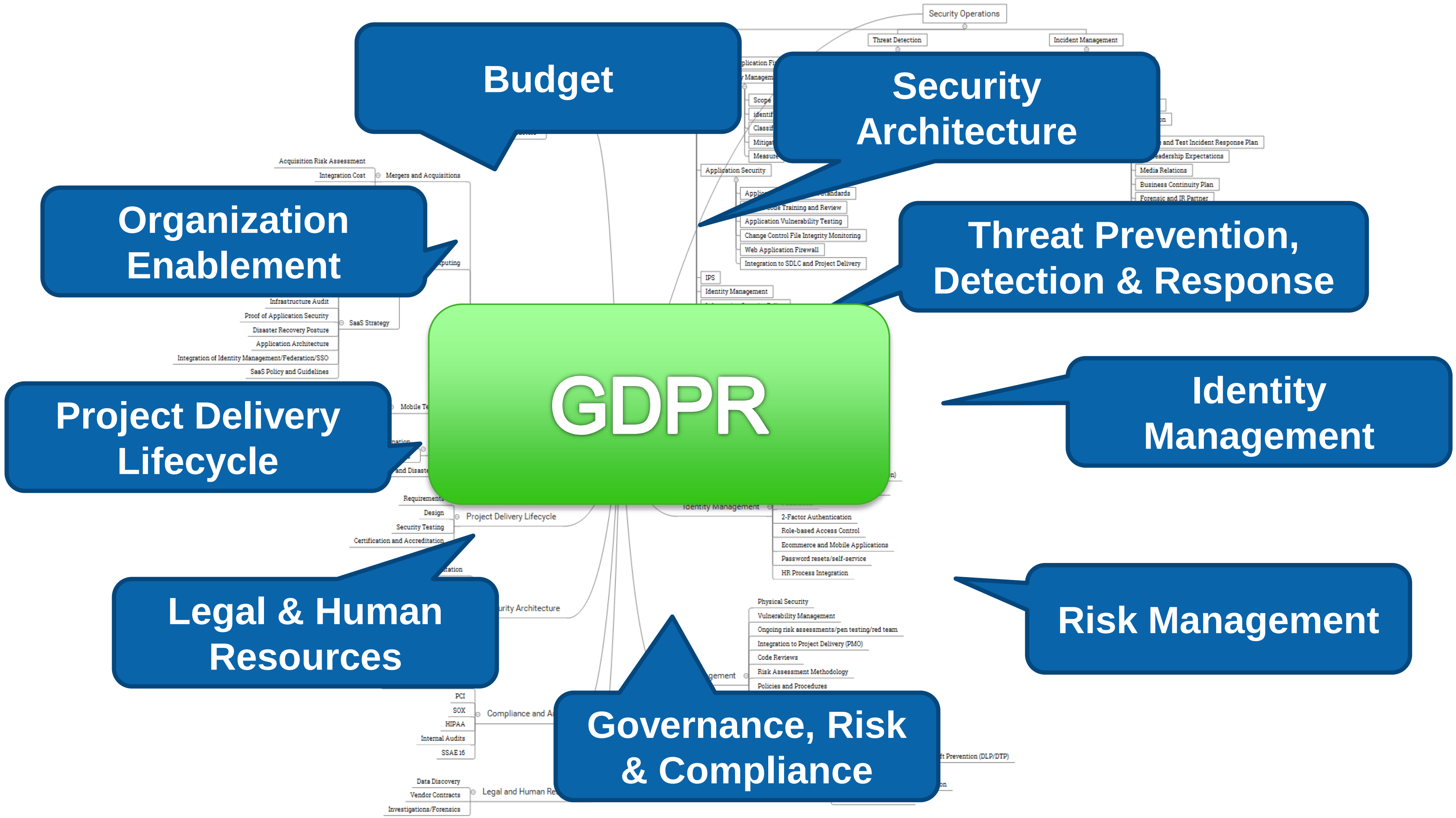
FORCEPOINT
POWERED BY Raytheon

ARTICLE 4 - DEFINITIONS

‘**controller**’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; *where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;*

‘**processor**’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

‘**personal data**’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;



GDPR

Budget

Security Architecture

Organization Enablement

Threat Prevention, Detection & Response

Identity Management

Project Delivery Lifecycle

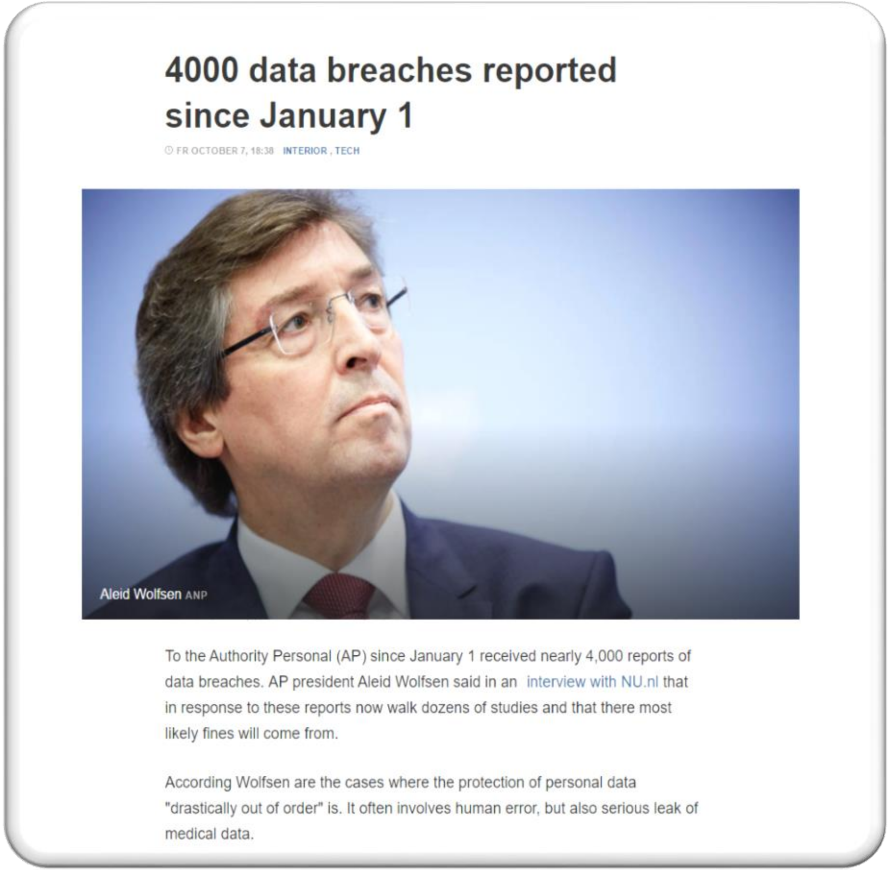
Risk Management

Legal & Human Resources

Governance, Risk & Compliance

Security Operations
Threat Detection
Incident Management
Scope
Classif
Mitigat
Measure
Application Security
Application Vulnerability Testing
Change Control File Integrity Monitoring
Web Application Firewall
Integration to SDLC and Project Delivery
IPS
Identity Management
and Test Incident Response Plan
Media Relations
Business Continuity Plan
Forensic and IR Partner
Acquisition Risk Assessment
Integration Cost
Mergers and Acquisitions
Infrastructure Audit
Proof of Application Security
Disaster Recovery Posture
Application Architecture
Integration of Identity Management/Federation/SSO
SaaS Policy and Guidelines
SaaS Strategy
Requirements
Design
Security Testing
Certification and Accreditation
Project Delivery Lifecycle
2-Factor Authentication
Role-based Access Control
Ecommerce and Mobile Applications
Password resets/self-service
HR Process Integration
Physical Security
Vulnerability Management
Ongoing risk assessments/pen testing/red team
Integration to Project Delivery (PMO)
Code Reviews
Risk Assessment Methodology
Policies and Procedures
PCI
SOX
HIPAA
Internal Audits
SSAE 16
Data Discovery
Vendor Contracts
Investigations/Forensics

NETHERLANDS - GDPR READY



4000 data breaches reported since January 1

FR OCTOBER 7, 18:38 INTERIOR , TECH

Aleid Wolfsen ANP

To the Authority Personal (AP) since January 1 received nearly 4,000 reports of data breaches. AP president Aleid Wolfsen said in an interview with NU.nl that in response to these reports now walk dozens of studies and that there most likely fines will come from.

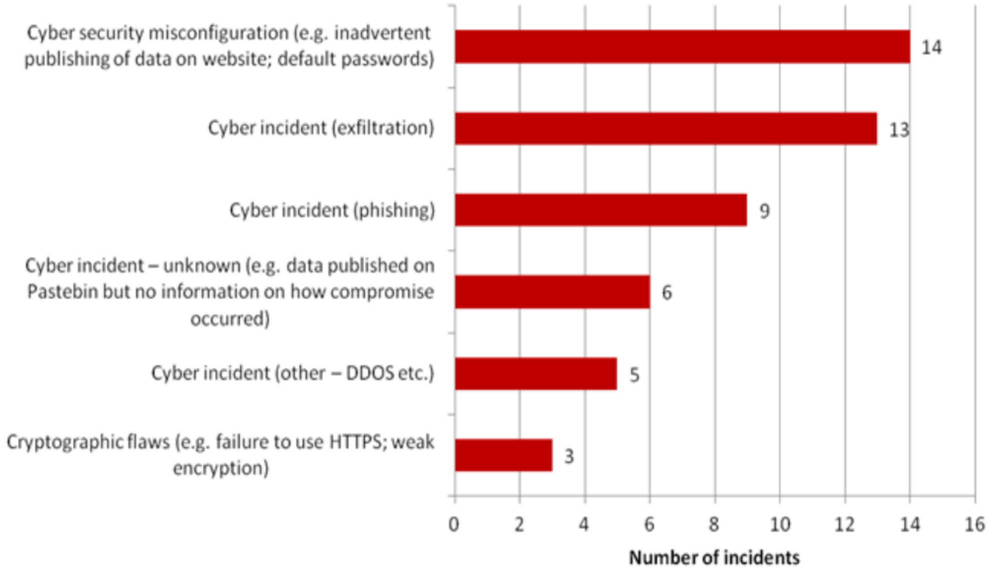
According Wolfsen are the cases where the protection of personal data "drastically out of order" is. It often involves human error, but also serious leak of medical data.

- Netherlands introduced a new Data Protection law in 2016. A head-start to GDPR
- 4000+ data breach incidents reported to authority personal since 1st January 2016
- >50% of Dutch Government agencies reported a data breach in 2016
- Breach causality involved human error in majority of cases

Source: http://nos.nl/artikel/2136510-4000-datalekken-gemeld-sinds-1-januari.html

ICO REPORT 2016

Cyber incidents by type



'Other principle 7 failures' are security incidents that cannot be categorised as one of the other types. Examples include failure to password protect emails containing personal information and processing personal data relating to work on a non-business computer.

FORCEPOINT
POWERED BY Raytheon

Source: https://ico.org.uk/action-weve-taken/data-security-incident-trends/

TECHNOLOGIES CHANGE

PEOPLE ARE THE CONSTANT IN SECURITY

FORCEPOINT
POWERED BY Raytheon

TECHNOLOGIES CHANGE

ACCIDENTAL INSIDER

Inadvertent Behaviors

Poorly communicated policies and user awareness

Broken Business Process

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

MALICIOUS INSIDER

Rogue Employee

Leaving the company, poor performance review

Criminal Actor Employees

Corporate espionage, national espionage, organized crime

COMPROMISED INSIDER

Malware Infections

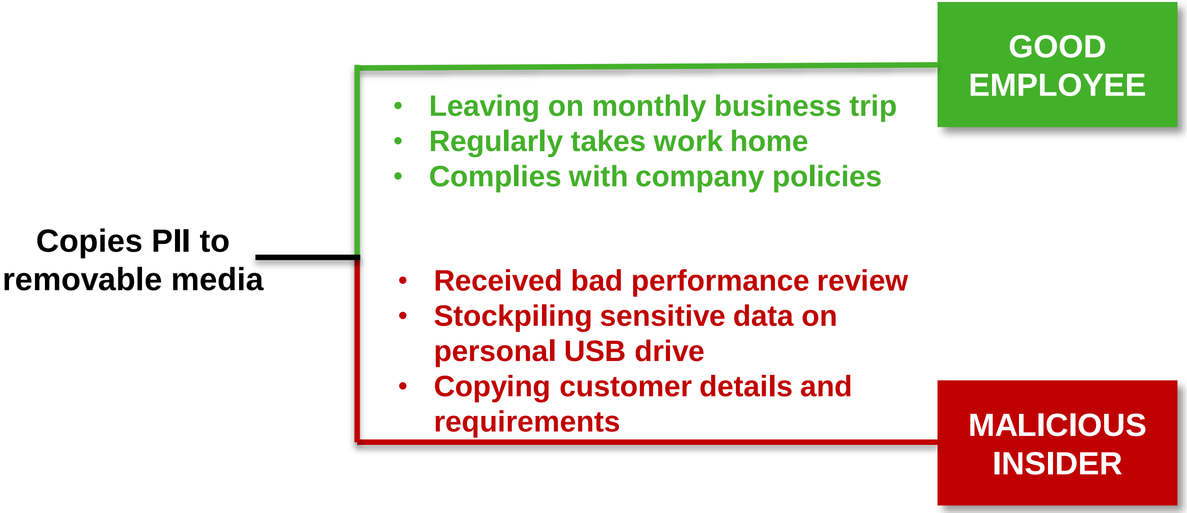
Phishing targets, breaches, BYOD contamination

Stolen Credentials

Credential exfiltration, social engineering, device control hygiene

YOU MUST UNDERSTAND INTENT
TO INTERPRET AN ACTION

John A.
Actuary
Global Insurer



Copies PII to removable media

- **Leaving on monthly business trip**
- **Regularly takes work home**
- **Complies with company policies**

GOOD EMPLOYEE

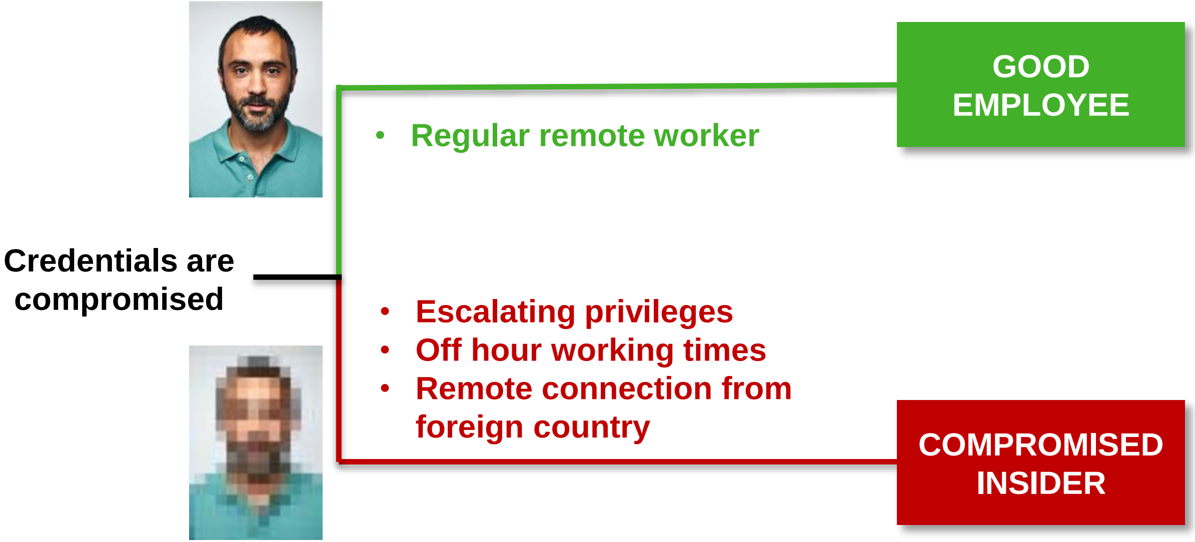
- **Received bad performance review**
- **Stockpiling sensitive data on personal USB drive**
- **Copying customer details and requirements**

MALICIOUS INSIDER

FORCEPOINT
POWERED BY Raytheon

YOU MUST UNDERSTAND INTENT
TO INTERPRET AN ACTION & IDENTIFY IMPERSONATORS

Roberto S.
Scientist
Pharmaceutical
Company



Credentials are compromised

- Regular remote worker

GOOD EMPLOYEE

- Escalating privileges
- Off hour working times
- Remote connection from foreign country

COMPROMISED INSIDER

RECOMMENDED ITEMS

35-50L Rucksack
Mountain Boots
Crampons
Gaiters
Helmet
Harness
Ice axe
Waterproof Jacket and Trousers
Mountain Trousers
Thermal Layer
Mid-Layer Jacket
Light Weight Duvet Jacket

Gloves
Warm Hat, Sun Hat & Buff
Socks
Sun Glasses & Goggles
Sun Cream & Lip Protection
Water & Water Bottle
Snacks / Hill food
Head Torch
Personal Medical Items
Money
Passport
Mobile phone
Map

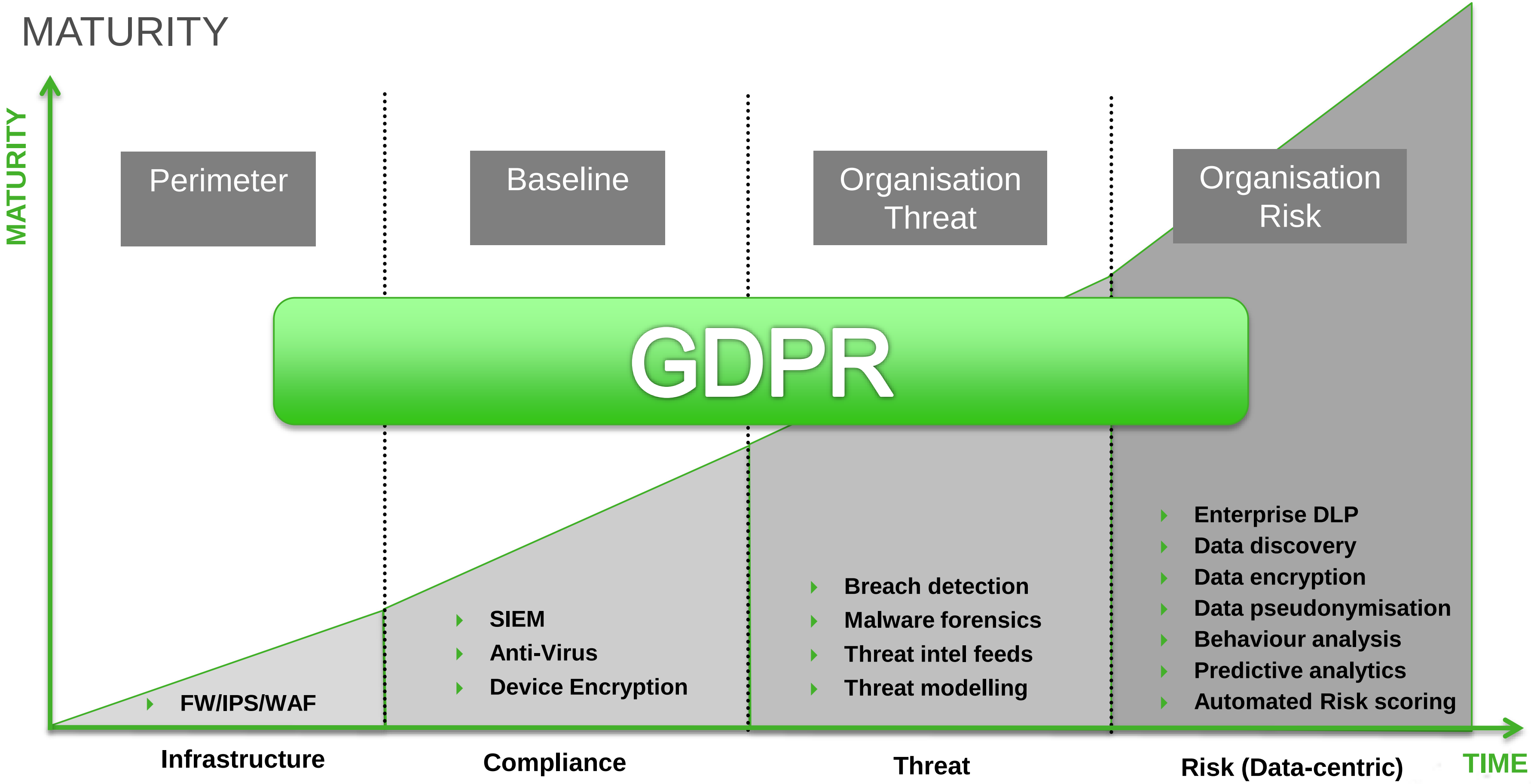
ASSUMED ITEMS

ITEM	NEED
Passport	Allows me to travel Proves I’m authorised
Mobile phone	If I need help I can call – selfie at summit to prove I made it
Map	Allows me to set a route and check on progress. Make Day 1 hut

ASSUMED ITEMS

ITEM	NEED
Certification (ISO27018)	Allows us to operate Proves we're authorised
Supervisory Authority	If we need help we can call – selfie at summit to prove we made it
Data protection strategy	Allows us to set a route and check on progress. Make Day 1 hut (25th May 2018)

MATURITY



FORCEPOINT
POWERED BY Raytheon

GDPR

❑ Assessment of current data protection practices

❑ Creation of a data protection governance structure

❑ Maintaining a personal data inventory

❑ Creating information notices

❑ Maintaining consent mechanisms

❑ Application of technical and organisational controls

❑ Performing Data Protection Impact Assessments (DPIA)

❑ Preparation to report personal data breaches

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

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 KEY ARTICLES

- ❑ Article 6 – Lawfulness of processing
- ❑ Article 17 – Right to Erasure
- ❑ Article 25 – Data Protection by Design/Default
- ❑ Article 32 – Security of Processing
- ❑ Article 33 – Data breach Notification <72hrs
- ❑ Article 35 – Data Protection Impact Assessments (DPIA)
- ❑ Chapter V (Article 44-50) - Data Transfers
- ❑ …many more!!

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.

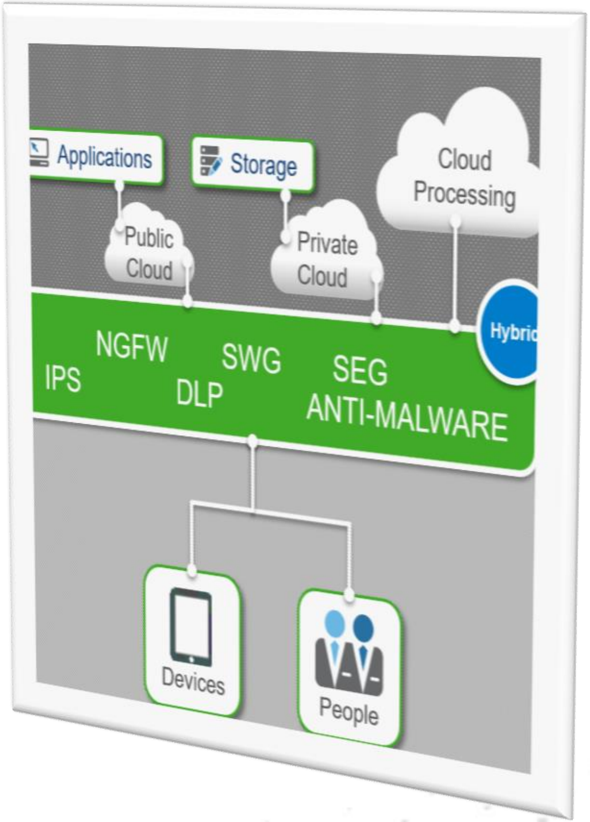
The investigation will focus on identifying the source and destination of the breach through event and incident information from Data Leakage Prevention (DLP) and Data Theft Prevention (DTP) tools. Data forensics will then help to pinpoint the stolen data, at which time the organisation will be required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

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 GUIDANCE FOR CLOUD

- ❑ Assess where PII data is stored/processed for each cloud service/application
- ❑ Enforce policies on processors that process PII data in non-EU locations to ensure Data Transfer rules are met
- ❑ Track use of PII data through behaviour analytics from endpoint, network and cloud
- ❑ Align organizational, governance and technical controls to identify misuse, mishandling, unlawful processing or profiling
- ❑ Review model contracts, consider Privacy Shield, understand other national data protection laws
- ❑ Educate employees on the correct use of cloud services/applications. Provide measurement and metrics to the Data Protection Officer



GDPR STRATEGY

Preparation

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

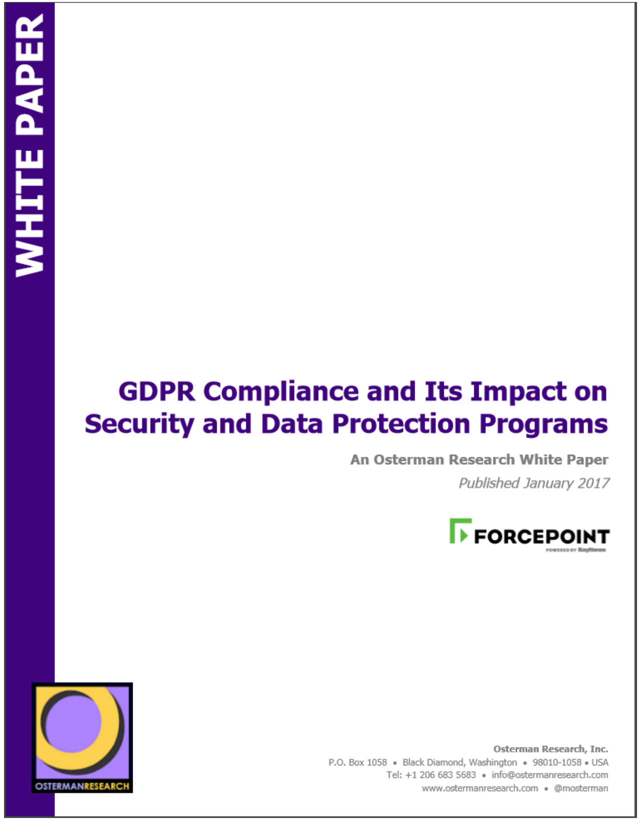
<12 Months

- 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

NEW OSTERMAN REPORT



WHITE PAPER

GDPR Compliance and Its Impact on Security and Data Protection Programs

An Osterman Research White Paper

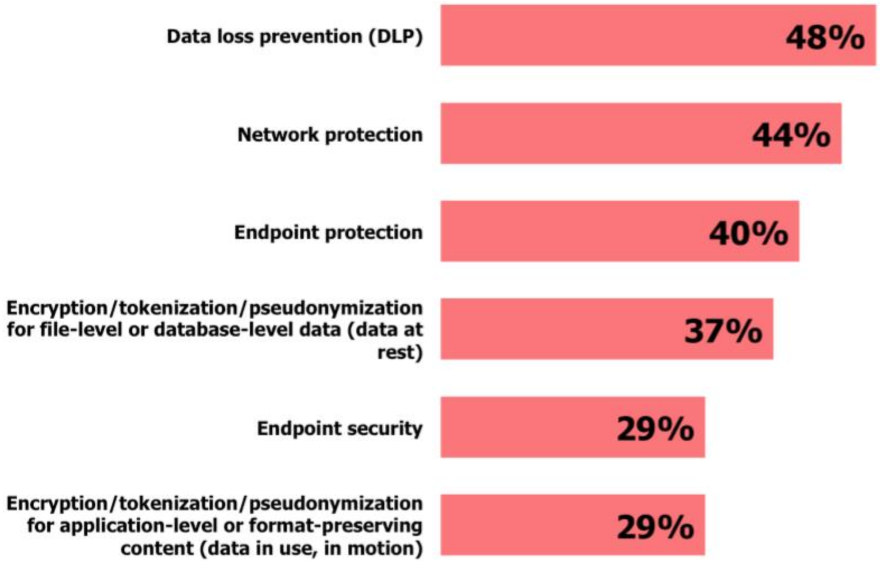
Published January 2017

FORCEPOINT
POWERED BY Raytheon

OSTERMANRESEARCH

Osterman Research, Inc.
P.O. Box 1058 • Black Diamond, Washington • 98010-1058 • USA
Tel: +1 206 683 5683 • info@ostermanresearch.com
www.ostermanresearch.com • @mosterman

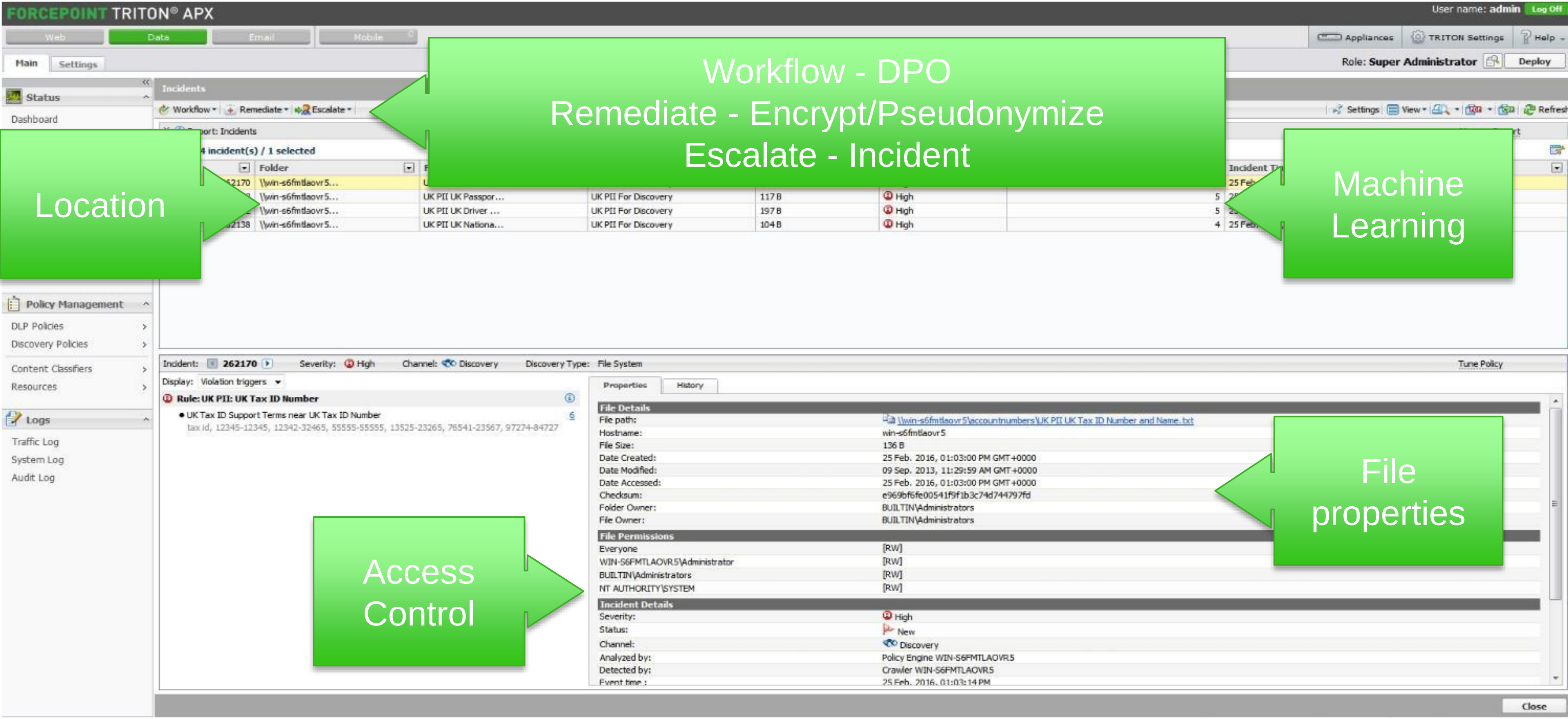
Figure 2
Data Protection Technologies That Organizations Will Spend More On During the Next 12-18 Months to Specifically Address the GDPR



Source: Osterman Research, Inc.

Source: http://www.forcepoint.com/ostermanGDPR

DATA DISCOVERY



Report: Incidents

4 incident(s) / 1 selected

	Folder						Incident Ti
2170	\\win-s6fmtlaovr5…	U					25 Feb
	\\win-s6fmtlaovr5…	UK PII UK Passpor…	UK PII For Discovery	117 B	High	5	2
	\\win-s6fmtlaovr5…	UK PII UK Driver …	UK PII For Discovery	197 B	High	5	2
2138	\\win-s6fmtlaovr5…	UK PII UK Nationa…	UK PII For Discovery	104 B	High	4	25 Feb

Incident: 262170 Severity: High Channel: Discovery Discovery Type: File System Tune Policy

Display: Violation triggers

Rule: UK PII: UK Tax ID Number

- UK Tax ID Support Terms near UK Tax ID Number 6
  tax id, 12345-12345, 12342-32465, 55555-55555, 13525-23265, 76541-23567, 97274-84727

Properties | History

File Details	
File path:	\\win-s6fmtlaovr5\accountnumbers\UK PII UK Tax ID Number and Name.txt
Hostname:	win-s6fmtlaovr5
File Size:	136 B
Date Created:	25 Feb. 2016, 01:03:00 PM GMT+0000
Date Modified:	09 Sep. 2013, 11:29:59 AM GMT+0000
Date Accessed:	25 Feb. 2016, 01:03:00 PM GMT+0000
Checksum:	e969bf6fe00541f9f1b3c74d744797fd
Folder Owner:	BUILTIN\Administrators
File Owner:	BUILTIN\Administrators
File Permissions	
Everyone	[RW]
WIN-S6FMTLAOVR5\Administrator	[RW]
BUILTIN\Administrators	[RW]
NT AUTHORITY\SYSTEM	[RW]
Incident Details	
Severity:	High
Status:	New
Channel:	Discovery
Analyzed by:	Policy Engine WIN-S6FMTLAOVR5
Detected by:	Crawler WIN-S6FMTLAOVR5
Event time :	25 Feb. 2016, 01:03:14 PM

Workflow - DPO
Remediate - Encrypt/Pseudonymize
Escalate - Incident

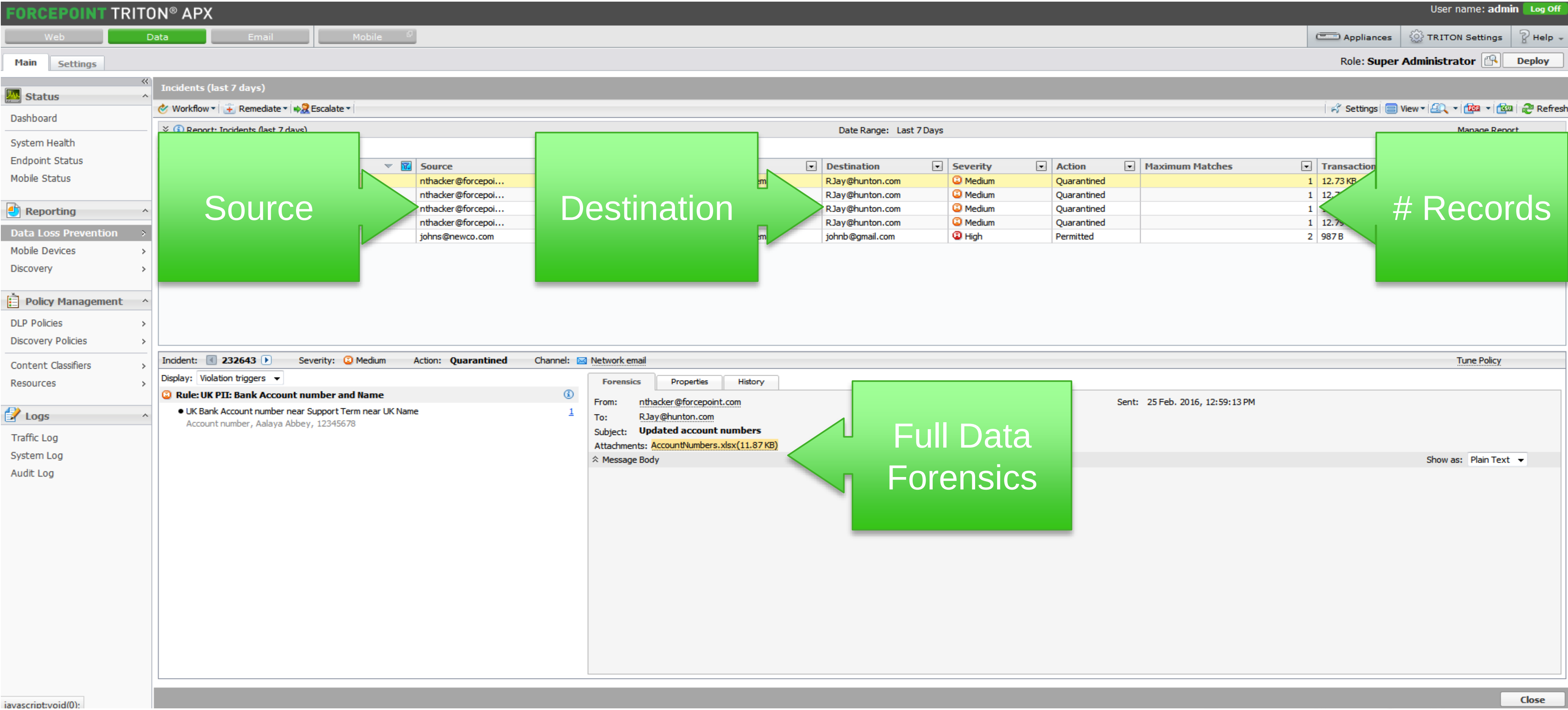
Location

Machine Learning

File properties

Access Control

DATA BREACH NOTIFICATION



Role: Super Administrator

Incidents (last 7 days)

Report: Incidents (last 7 days)

Date Range: Last 7 Days

Source	Destination	Severity	Action	Maximum Matches	Transaction
nthacker@forcepoi...	RJay@hunton.com	Medium	Quarantined	1	12.73 KB
nthacker@forcepoi...	RJay@hunton.com	Medium	Quarantined	1	12.
nthacker@forcepoi...	RJay@hunton.com	Medium	Quarantined	1	
nthacker@forcepoi...	RJay@hunton.com	Medium	Quarantined	1	12.7
johns@newco.com	johnb@gmail.com	High	Permitted	2	987 B

Incident: 232643 Severity: Medium Action: **Quarantined** Channel: Network email

Display: Violation triggers

Rule: UK PII: Bank Account number and Name

- UK Bank Account number near Support Term near UK Name 1
  Account number, Aalaya Abbey, 12345678

From: nthacker@forcepoint.com

To: RJay@hunton.com

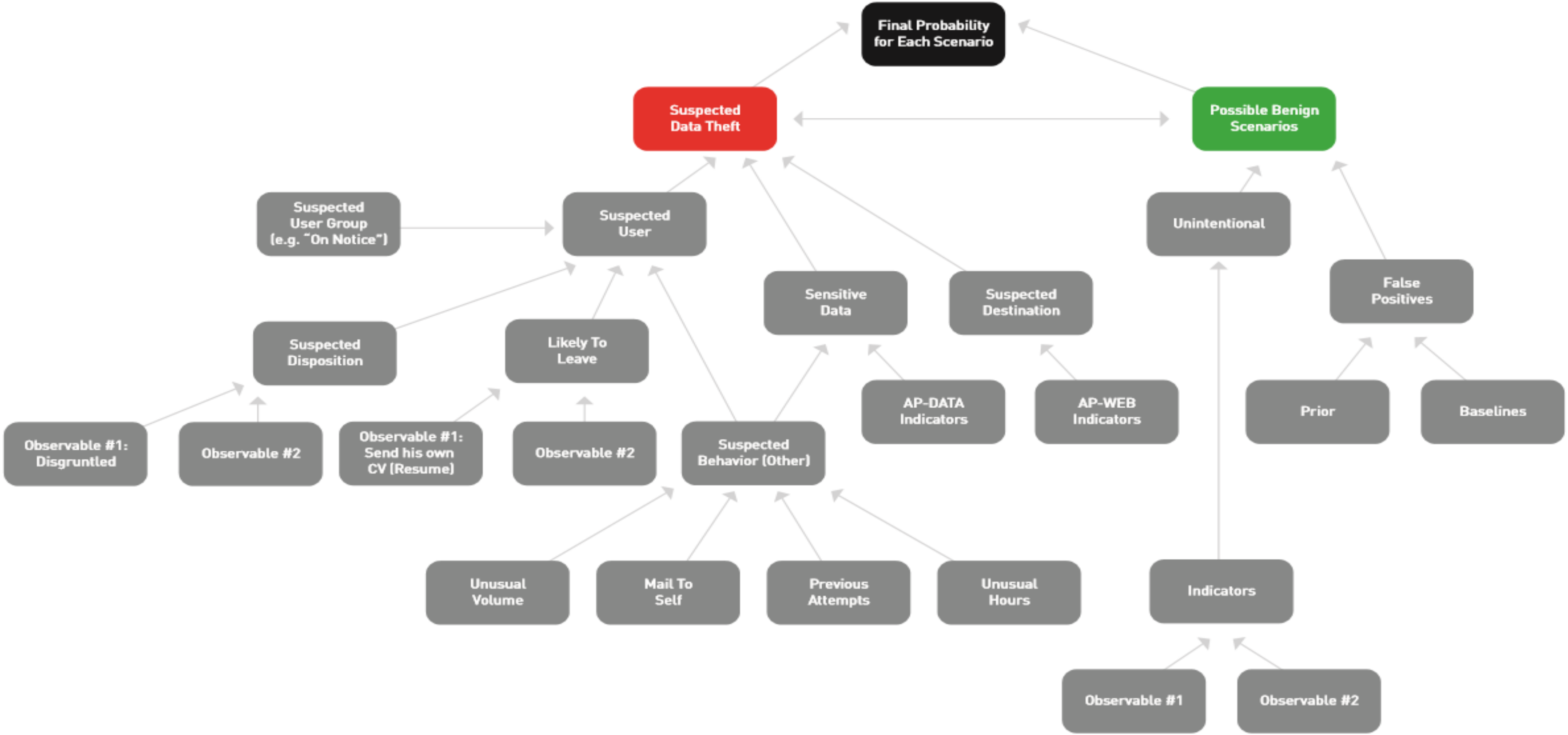
Subject: **Updated account numbers**

Attachments: AccountNumbers.xlsx(11.87 KB)

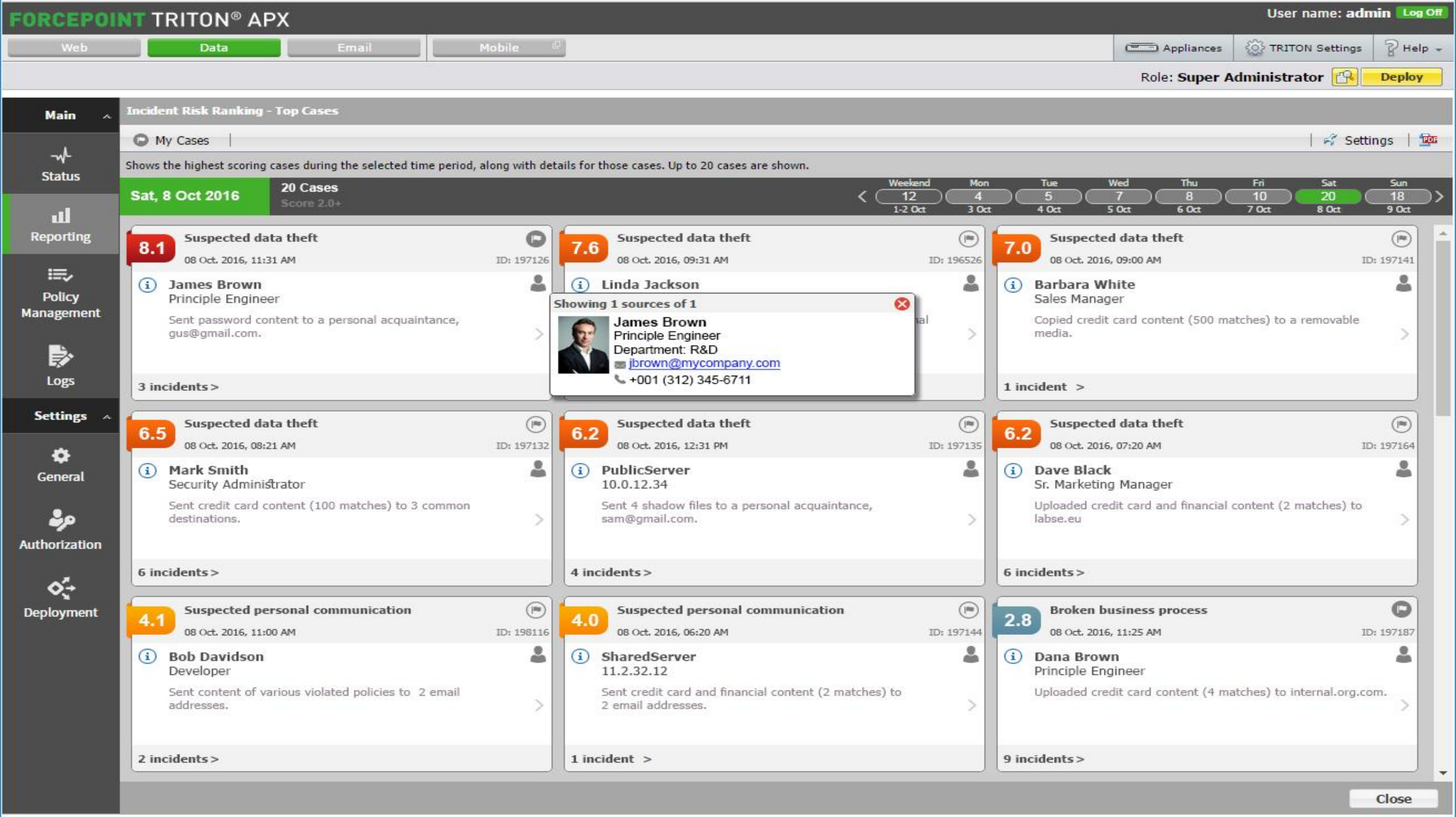
Sent: 25 Feb. 2016, 12:59:13 PM

Show as: Plain Text

FORCEPOINT
POWERED BY Raytheon



FORCEPOINT
POWERED BY Raytheon



Incident Risk Ranking - Top Cases

Shows the highest scoring cases during the selected time period, along with details for those cases. Up to 20 cases are shown.

Sat, 8 Oct 2016 — 20 Cases, Score 2.0+

Weekend	Mon	Tue	Wed	Thu	Fri	Sat	Sun
12	4	5	7	8	10	20	18
1-2 Oct	3 Oct	4 Oct	5 Oct	6 Oct	7 Oct	8 Oct	9 Oct

8.1 Suspected data theft
08 Oct. 2016, 11:31 AM — ID: 197126
James Brown
Principle Engineer
Sent password content to a personal acquaintance, gus@gmail.com.
3 incidents >

7.6 Suspected data theft
08 Oct. 2016, 09:31 AM — ID: 196526
Linda Jackson
...al

Showing 1 sources of 1
James Brown
Principle Engineer
Department: R&D
jbrown@mycompany.com
+001 (312) 345-6711

7.0 Suspected data theft
08 Oct. 2016, 09:00 AM — ID: 197141
Barbara White
Sales Manager
Copied credit card content (500 matches) to a removable media.
1 incident >

6.5 Suspected data theft
08 Oct. 2016, 08:21 AM — ID: 197132
Mark Smith
Security Administrator
Sent credit card content (100 matches) to 3 common destinations.
6 incidents >

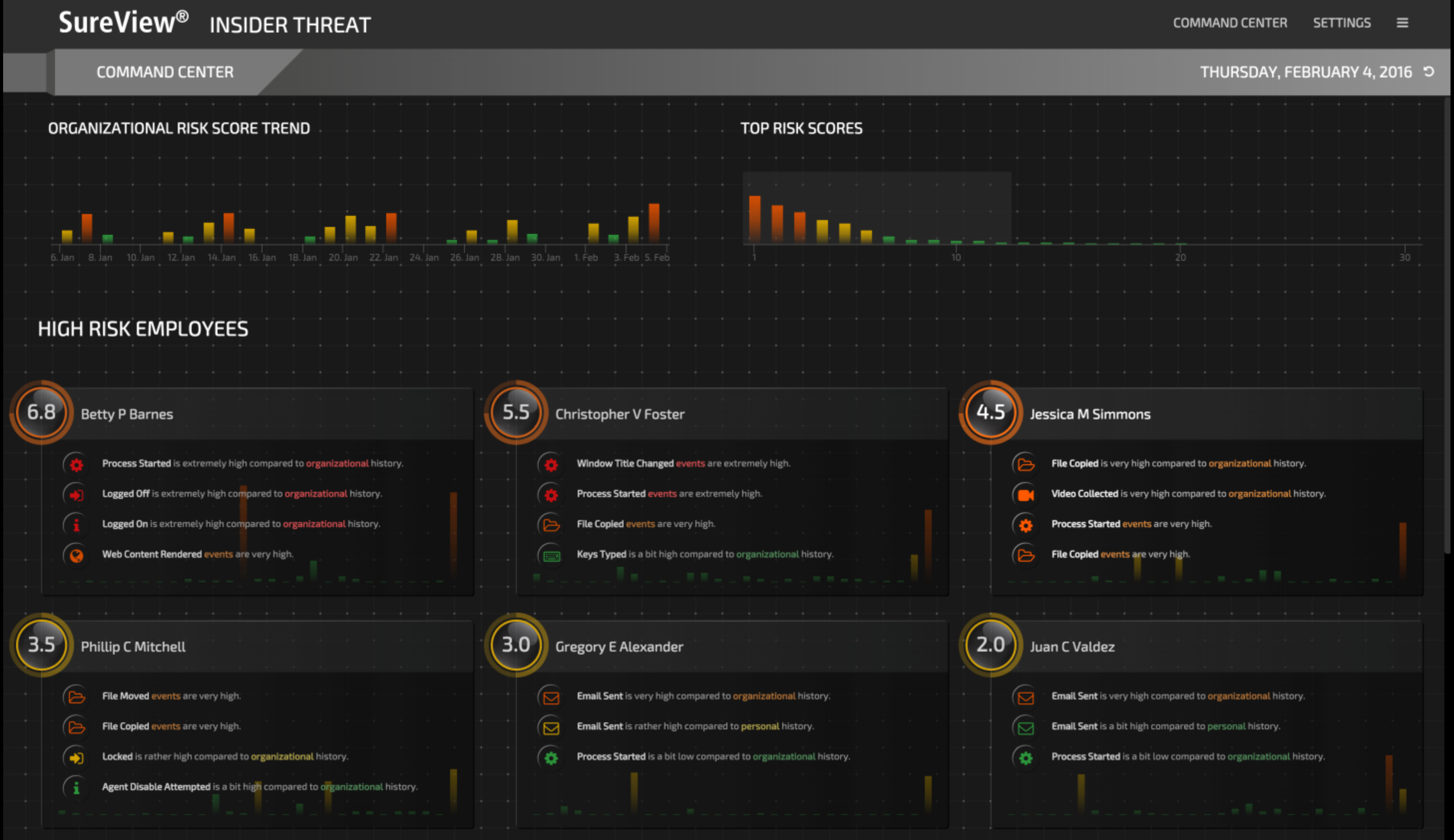
6.2 Suspected data theft
08 Oct. 2016, 12:31 PM — ID: 197135
PublicServer
10.0.12.34
Sent 4 shadow files to a personal acquaintance, sam@gmail.com.
4 incidents >

6.2 Suspected data theft
08 Oct. 2016, 07:20 AM — ID: 197164
Dave Black
Sr. Marketing Manager
Uploaded credit card and financial content (2 matches) to labse.eu
6 incidents >

4.1 Suspected personal communication
08 Oct. 2016, 11:00 AM — ID: 198116
Bob Davidson
Developer
Sent content of various violated policies to 2 email addresses.
2 incidents >

4.0 Suspected personal communication
08 Oct. 2016, 06:20 AM — ID: 197144
SharedServer
11.2.32.12
Sent credit card and financial content (2 matches) to 2 email addresses.
1 incident >

2.8 Broken business process
08 Oct. 2016, 11:25 AM — ID: 197187
Dana Brown
Principle Engineer
Uploaded credit card content (4 matches) to internal.org.com.
9 incidents >



ORGANIZATIONAL RISK SCORE TREND

TOP RISK SCORES

HIGH RISK EMPLOYEES

6.8 Betty P Barnes

- **Process Started** is extremely high compared to organizational history.
- **Logged Off** is extremely high compared to organizational history.
- **Logged On** is extremely high compared to organizational history.
- **Web Content Rendered** events are very high.

5.5 Christopher V Foster

- **Window Title Changed** events are extremely high.
- **Process Started** events are extremely high.
- **File Copied** events are very high.
- **Keys Typed** is a bit high compared to organizational history.

4.5 Jessica M Simmons

- **File Copied** is very high compared to organizational history.
- **Video Collected** is very high compared to organizational history.
- **Process Started** events are very high.
- **File Copied** events are very high.

3.5 Phillip C Mitchell

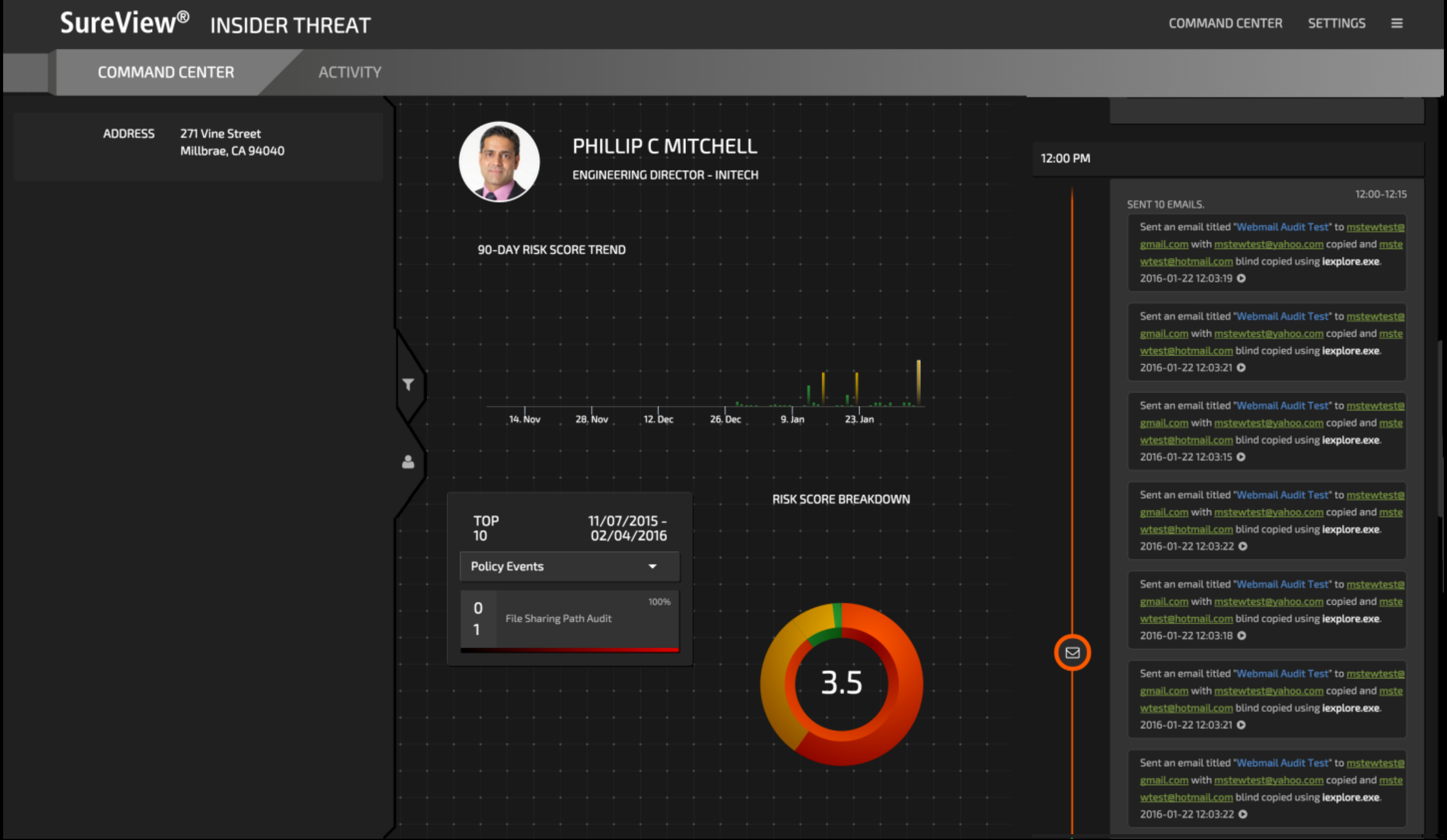
- **File Moved** events are very high.
- **File Copied** events are very high.
- **Locked** is rather high compared to organizational history.
- **Agent Disable Attempted** is a bit high compared to organizational history.

3.0 Gregory E Alexander

- **Email Sent** is very high compared to organizational history.
- **Email Sent** is rather high compared to personal history.
- **Process Started** is a bit low compared to organizational history.

2.0 Juan C Valdez

- **Email Sent** is very high compared to organizational history.
- **Email Sent** is a bit high compared to personal history.
- **Process Started** is a bit low compared to organizational history.



ADDRESS 271 Vine Street
Millbrae, CA 94040

PHILLIP C MITCHELL

ENGINEERING DIRECTOR - INITECH

90-DAY RISK SCORE TREND

TOP 10 11/07/2015 - 02/04/2016

Policy Events

0 1	File Sharing Path Audit	100%

RISK SCORE BREAKDOWN

12:00 PM

SENT 10 EMAILS. 12:00-12:15

Sent an email titled "Webmail Audit Test" to mstewtest@gmail.com with mstewtest@yahoo.com copied and mstewtest@hotmail.com blind copied using Iexplore.exe.
2016-01-22 12:03:19

Sent an email titled "Webmail Audit Test" to mstewtest@gmail.com with mstewtest@yahoo.com copied and mstewtest@hotmail.com blind copied using Iexplore.exe.
2016-01-22 12:03:21

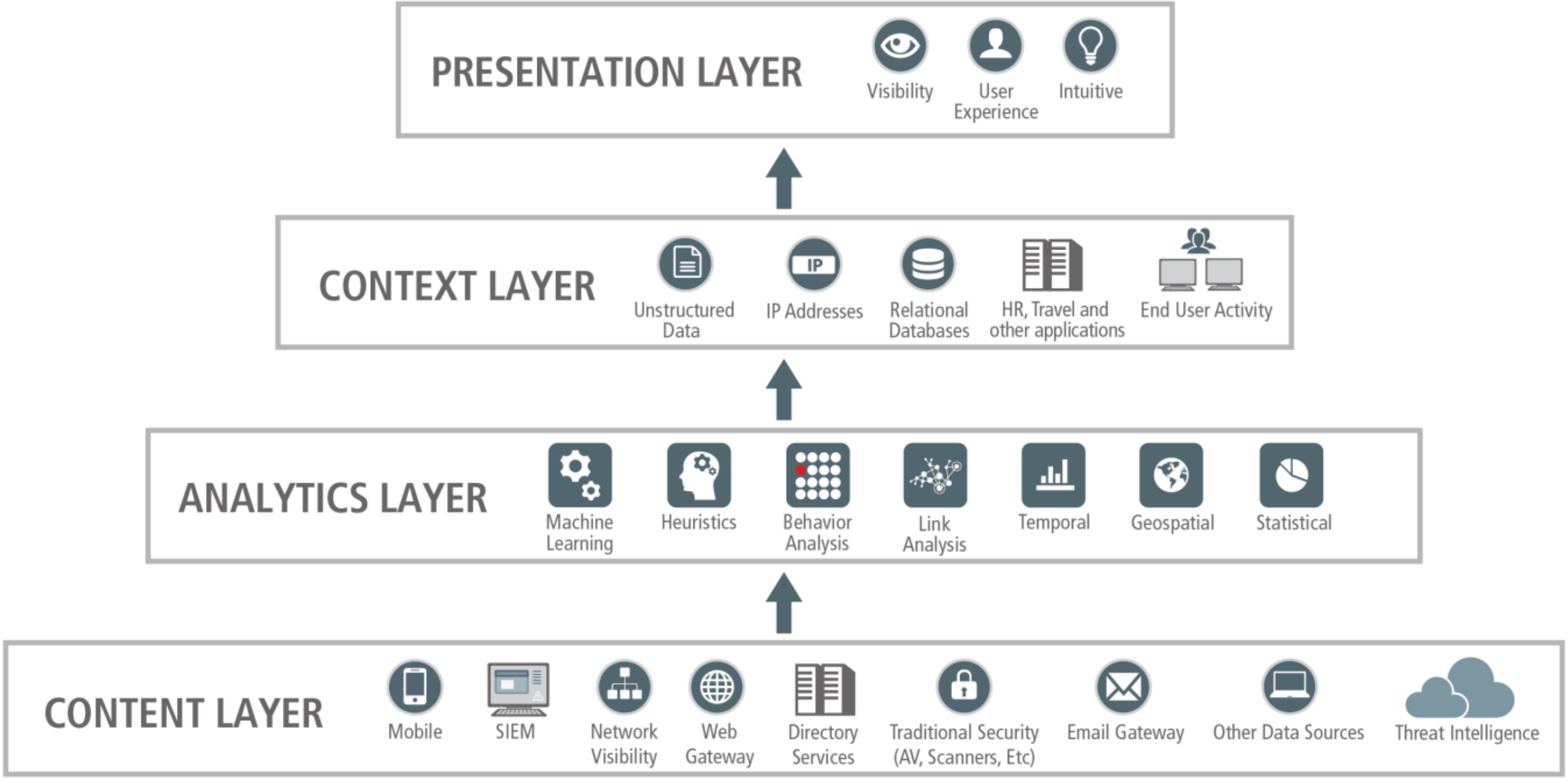
Sent an email titled "Webmail Audit Test" to mstewtest@gmail.com with mstewtest@yahoo.com copied and mstewtest@hotmail.com blind copied using Iexplore.exe.
2016-01-22 12:03:15

Sent an email titled "Webmail Audit Test" to mstewtest@gmail.com with mstewtest@yahoo.com copied and mstewtest@hotmail.com blind copied using Iexplore.exe.
2016-01-22 12:03:22

Sent an email titled "Webmail Audit Test" to mstewtest@gmail.com with mstewtest@yahoo.com copied and mstewtest@hotmail.com blind copied using Iexplore.exe.
2016-01-22 12:03:18

Sent an email titled "Webmail Audit Test" to mstewtest@gmail.com with mstewtest@yahoo.com copied and mstewtest@hotmail.com blind copied using Iexplore.exe.
2016-01-22 12:03:21

Sent an email titled "Webmail Audit Test" to mstewtest@gmail.com with mstewtest@yahoo.com copied and mstewtest@hotmail.com blind copied using Iexplore.exe.
2016-01-22 12:03:22



PRESENTATION LAYER

Visibility

User Experience

Intuitive

CONTEXT LAYER

Unstructured Data

IP Addresses

Relational Databases

HR, Travel and other applications

End User Activity

ANALYTICS LAYER

Machine Learning

Heuristics

Behavior Analysis

Link Analysis

Temporal

Geospatial

Statistical

CONTENT LAYER

Mobile

SIEM

Network Visibility

Web Gateway

Directory Services

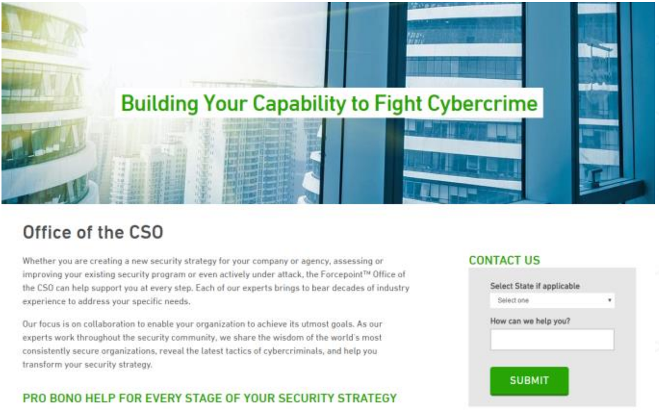
Traditional Security (AV, Scanners, Etc)

Email Gateway

Other Data Sources

Threat Intelligence

OUR COMMITMENT – OOCSO, TRUST PROGRAM, FEDRAMP, CSA STAR 2, ISO27001, ISO27018



Building Your Capability to Fight Cybercrime

Office of the CSO

Whether you are creating a new security strategy for your company or agency, assessing or improving your existing security program or even actively under attack, the Forcepoint™ Office of the CSO can help support you at every step. Each of our experts brings to bear decades of industry experience to address your specific needs.

Our focus is on collaboration to enable your organization to achieve its utmost goals. As our experts work throughout the security community, we share the wisdom of the world's most consistently secure organizations, reveal the latest tactics of cybercriminals, and help you transform your security strategy.

PRO BONO HELP FOR EVERY STAGE OF YOUR SECURITY STRATEGY

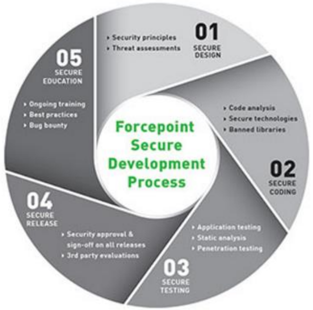
CONTACT US

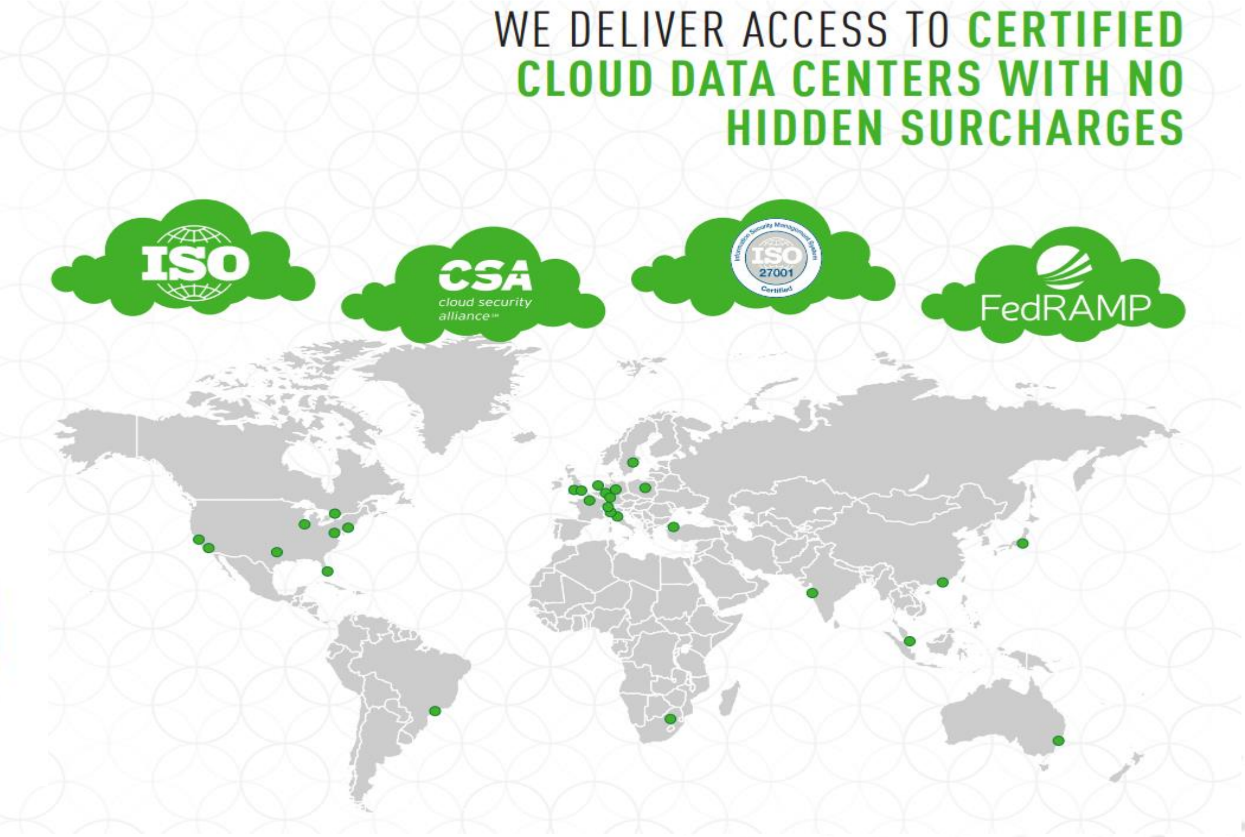
Select State if applicable

Select one ▾

How can we help you?

SUBMIT




WE DELIVER ACCESS TO CERTIFIED CLOUD DATA CENTERS WITH NO HIDDEN SURCHARGES
ISO
CSA cloud security alliance℠
ISO 27001 Certified
FedRAMP

Questions

February 2017

Neil Thacker, Deputy CISO
nthacker@forcepoint.com
@nt_hacker