



---

# Practical Preparation for PDPA for Thailand Compliance

**Peera Denprayoonwong**

Security Consultant



Data Protection | Web Security | CASB | NGFW | Advanced Malware Detection | Behavioral Analytics | Insider Threat | Email Security | Data Guard | Cross Domain



## Practical Preparation for PDPA for Thailand Compliance

- ❑ DLP Gap analysis
- ❑ Building PDPA Policy Template and Discovery for PDPA Gap analysis
- ❑ Applying Data Classification Tools
- ❑ DLP Architecture and Cloud App Technology
- ❑ Managing DLP/PDPA incidents and engaging business user with User justification and Automated workflow
- ❑ Behavior Analytics / Dynamic User & Data Protection

# THE HUMAN POINT

PEOPLE



DATA



Understanding the intersection of people, critical data and IP over networks of different trust levels.

salesforce

amazon web services

box

Office 365

# 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**

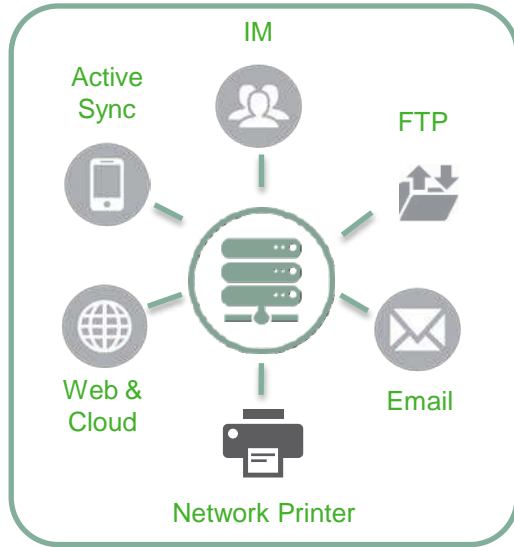
Risk adaptive protection to act on change in human risk to critical data in real time

## **Compliance**

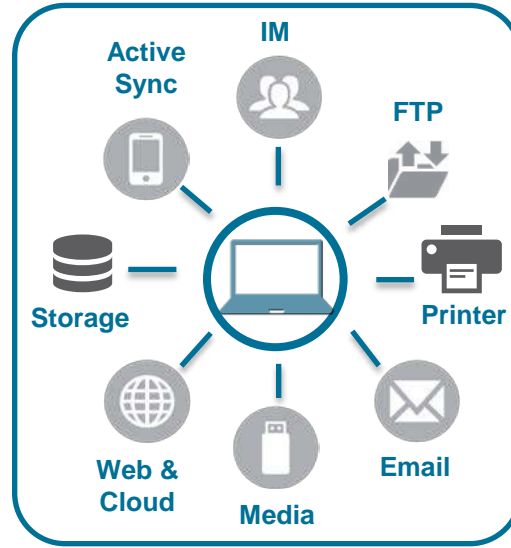
Effectively enforce compliance no matter where your data resides



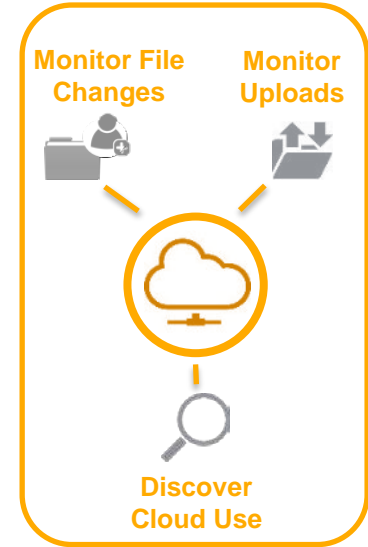
# CONSIDERATIONS FOR MONITORING DATA FLOWS



**NETWORK**  
Data in Motion



**ENDPOINT**  
Data in Use  
& in Motion



**CLOUD**  
Data In Use  
& in Motion



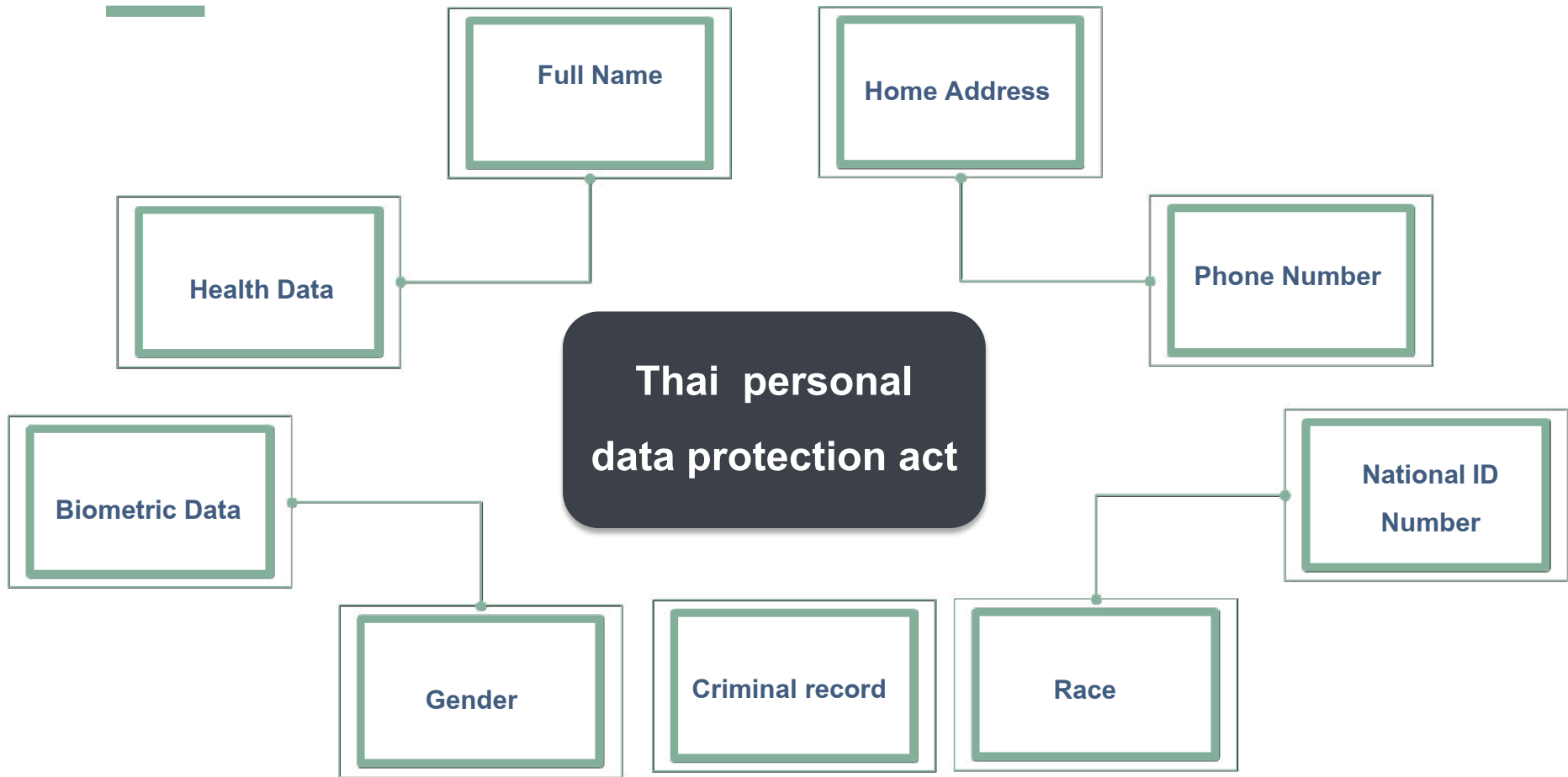
## Data Protection Technology for PDPA Implementation

- ❑ DLP Gap analysis
- ❑ Building PDPA Policy Template and Discovery for PDPA Gap analysis
- ❑ Applying Data Classification Tools
- ❑ DLP Architecture and Cloud App Technology
- ❑ Managing DLP/PDPA incidents and engaging business user with User justification and Automated workflow
- ❑ Behavior Analytics / Dynamic User & Data Protection

# Personal Data Protection Act in Thailand

- ▶ สำหรับกฎหมายคุ้มครองข้อมูลส่วนบุคคลนั้น เป็นผลมาจากการเปลี่ยนผ่านเข้าสู่ดิจิทัล ซึ่งส่งผลให้มีการล่วงละเมิดสิทธิในข้อมูลส่วนบุคคลเพิ่มมากขึ้น จึงทำให้ภาครัฐต้องมีการคุ้มครองความเป็นส่วนตัวของประชากรในประเทศ ซึ่งถือเป็นส่วนหนึ่งของการรักษาความปลอดภัยของข้อมูล (Data Security) ครอบคลุมข้อมูลส่วนบุคคลประเภทต่างๆ ตั้งแต่ ชื่อ นามสกุล ที่อยู่ เบอร์โทรศัพท์ ไปจนถึงอีเมล หมายเลขบัตรประจำตัวประชาชน และ อื่นๆ
- ▶ นอกจากนี้ กฎหมายยังคุ้มครองไปถึงข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Data) เช่น เชื้อชาติ เผ่าพันธุ์ ความเห็นทางการเมือง ความเชื่อ ลัทธิ ศาสนา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลทางด้านสุขภาพ ข้อมูลทางพันธุกรรม และ ข้อมูลชีวภาพ
- ▶ บทลงโทษมีทั้งโทษทางแพ่ง ทางอาญา และทางปกครอง หากมีการฝ่าฝืนมีโทษจำคุกไม่เกิน 6 เดือนถึง 1 ปีหรือปรับไม่เกิน 500,000 ถึง 1 ล้านบาท หรือทั้งจำทั้งปรับ (สำหรับโทษทางอาญา) และโทษทางปกครองที่ถูกเพิ่มอัตราโทษจากเดิมที่ระหว่าง 100,000 ถึง 500,000 บาทเป็นระหว่าง 1 ถึง 5 ล้านบาท





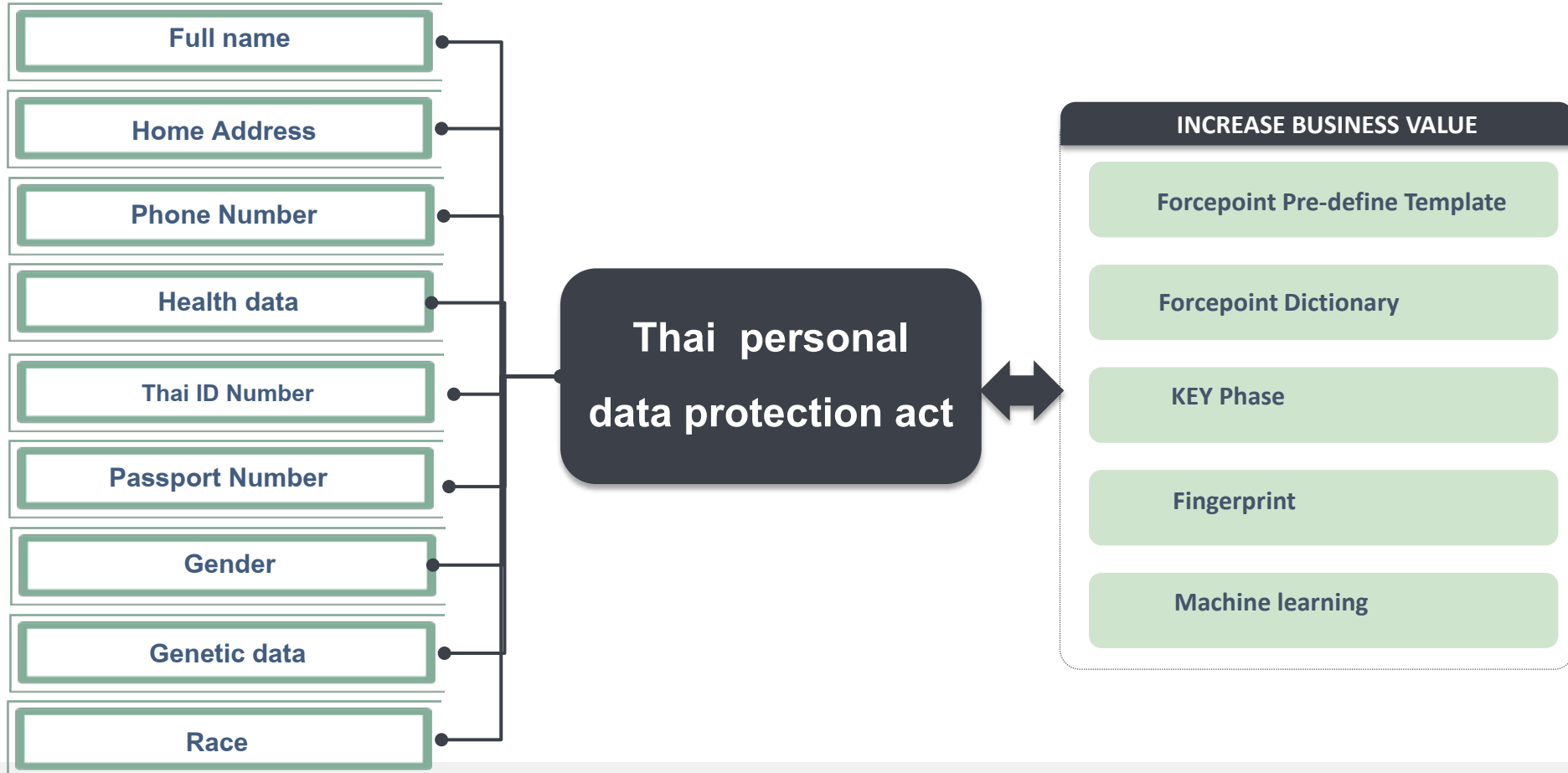




# Solutions to Locate, Manage, and Control Linkable to a specific individual

<b>Linked information:</b> Any piece of personal information that can be used to identify an individual	<b>Linked information:</b> information that on its own may not be able to identify a person, but serve as clues to your true identity when combined with another piece of information could identify, trace, or locate a person.	<b>Sensitive information :</b> (special personal data types)
<ul style="list-style-type: none"><li>• Full name</li><li>• Home Address</li><li>• Email Address</li><li>• Thai ID Number</li><li>• Social Security Number</li><li>• Passport Number</li><li>• Credit Card Number</li><li>• Date of birth</li><li>• Telephone number</li><li>• Log in details</li></ul>	<ul style="list-style-type: none"><li>• First or Last name</li><li>• Country, Province, City, Postcode</li><li>• Gender</li><li>• Race</li><li>• Non-specific age</li><li>• Job position and workplace</li><li>• IP address</li><li>• Device ID/Cookies ID</li></ul>	<ul style="list-style-type: none"><li>• Biometric Data</li><li>• Racial data</li><li>• Health data</li><li>• Ethnic origin</li><li>• Political Opinions</li><li>• Religious or philosophical belief</li><li>• Genetic data</li><li>• Sexual preference</li></ul>

# Thai Personal Data Protection Act



General Condition Severity & Action Source Destination

This rule monitors: specific data in: all parts of the transaction as a whole

Add or remove content classifiers or attributes to the condition.

<input type="checkbox"/>	18	Thai Mobile Number	Regular Expression	Threshold: At least 1 (unique values);
<input type="checkbox"/>	19	Thai Phone Number	Regular Expression	Threshold: At least 1 (unique values);
<input type="checkbox"/>	20	Common Medical Conditions (English)	Dictionary	Threshold: At least 1 (weighted score);
<input type="checkbox"/>	21	Credit Cards (Default)	Script	Threshold: At least 1 (unique values);
<input type="checkbox"/>	22	Common Medical Conditions (English)	Dictionary	Threshold: At least 5 (weighted score);
<input type="checkbox"/>	23	Credit Cards (Default)	Script	Threshold: At least 10 (unique values);
<input type="checkbox"/>	24	US Sensitive Diseases	Dictionary	Threshold: At least 1 (weighted score);
<input type="checkbox"/>	25	US Sensitive Diseases	Dictionary	Threshold: At least 5 (weighted score);

Add Remove

Condition Relations:

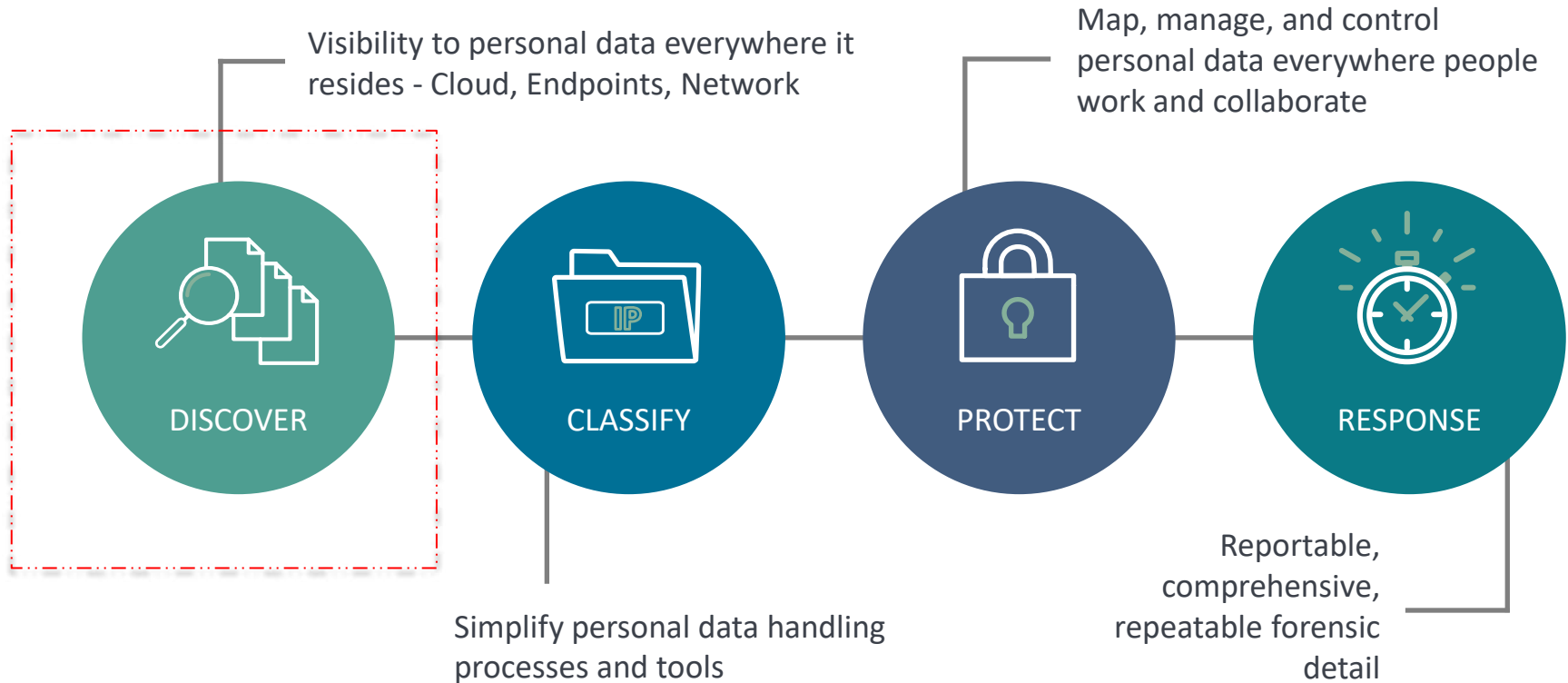
When do you want to trigger the rule?

Description:

<At least 1 (weighted score) 'Name'> AND <At least 1 (weighted score) 'Name\_Eng'> AND <At least 1 (weighted score) 'Address'> AND <At least 1 (weighted score) 'Address Content'> AND <At least 1 (unique values) 'Thailand ID number (Wide)'> AND <At least 1 'NIEM-Conformant XML'> AND <At least 1 'OASIS XML Common Biometric Format (XCBF)'> AND <At least 1 (unique values) 'CV and Resume in English'> AND <At least 1 (weighted score) 'Sex.1'> AND <At least 1 (weighted score) 'Sex.2'>

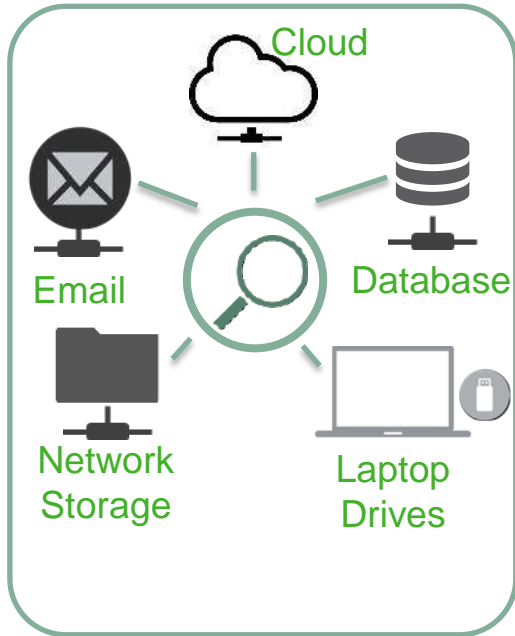


# Forcepoint's Approach to Thai Personal Data Protection Act

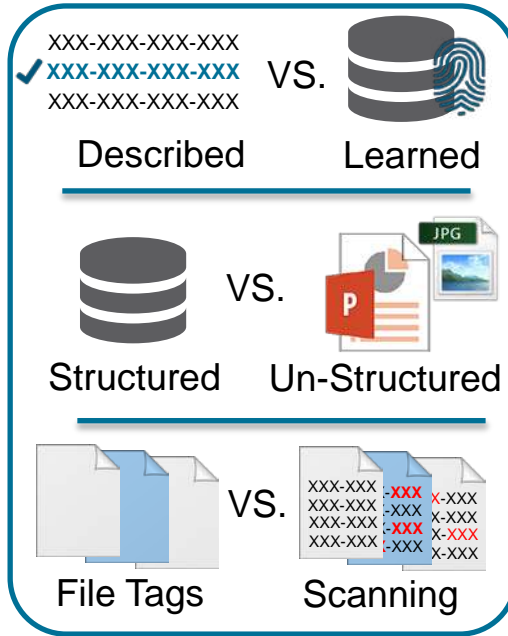




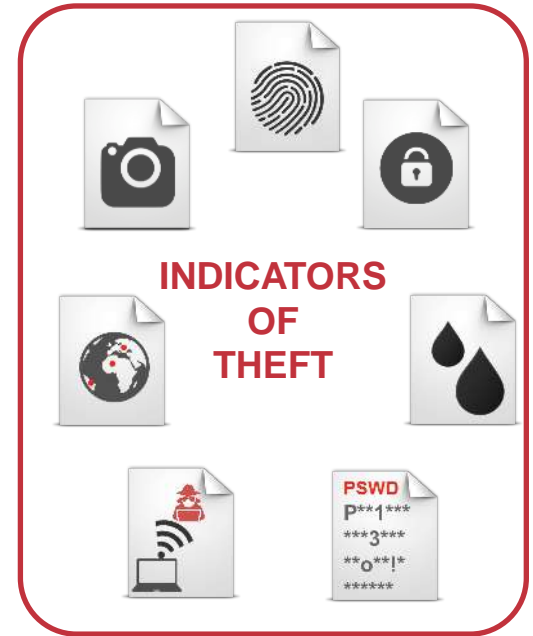
# PERSONAL DATA DISCOVERY



DATA IS EVERYWHERE



DATA IS NOT ALWAYS EASY TO FIND



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

FORCEPOINT PRODUCTS: DLP DISCOVER & DLP ENDPOINT

# DATA DISCOVERY RESULTS

The screenshot displays the Forcepoint Triton APX interface. At the top, the navigation bar includes 'Web', 'Data', 'Email', and 'Mobile'. The main header shows 'DLP Demo Discovery Incidents Report' with a 'Workflow' dropdown menu. A large green callout box points to this menu, containing the text: 'Workflow Remediate - Encrypt Escalate - Incident'. Below the header is a table of incidents. A second green callout box points to the 'Folder' column of the table, containing the text: 'Location'. A third green callout box points to the 'Discovered by' column, containing the text: 'Type'. The table lists several incidents, with one selected: ID 3641618, File Name 'Hojj kandidat...', Severity 'Medium', Folder '\\qastorage.webse...', Incident Time '2016-11-10 16:22:06', and Detected by 'Crawler E...'. Below the table, a detailed view of the selected incident is shown. A green callout box points to the 'File Details' section, containing the text: 'File Properties'. Another green callout box points to the 'File Permissions' section, containing the text: 'Access Control'. The interface also shows a left sidebar with navigation options like 'Main', 'Status', 'Reporting', 'Policy Management', 'Logs', 'Settings', 'General', 'Authorization', and 'Deployment'. The top right corner shows 'User name: admin' and 'Role: Super Administrator'. The bottom right corner has a 'Close' button.

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...	SlipjIBP1.txt	N/A	21.83 KB	Medium	\\GUYDEMO2016.QAE...	2016-11-13 20:41:28	Endpoint Agent	Endpoint
2.5.2	Windows Endpoint ...	3643572	Deep Web URLs for...	ter-unis.docx		225 24.13 KB	High	\\GUYDEMO2016.QAE...	2016-11-13 20:41:25	Endpoint Agent	Endpoint
2.4.2	Mac Endpoint Disc...	5722651	M&A Documents	djp-B067E4E...		1 76.87 KB	Medium	\\library\applicat...	2016-11-13 18:38:46	Endpoint Agent	Endpoint
2.4.1	Shared Storage DB...	3641618	Croetian Candidat...	Hojj kandidat...		16 456 B	Medium	\\qastorage.webse...	2016-11-10 16:22:06	Crawler E...	File System
2.1.1	Box Discovery Task	3384283	Japan Private Inf...	秘2 株式会社 小見隆...		5 62.87 KB	High	\\Box3@websearc...	2016-11-10 12:08:25	Crawler E...	Box Cloud
2.2.2	Box Discovery Task	3383493	Fingerprinted Doc...	2020_1rar		1 125.83 KB	Medium	\\Box3@websearc...	2016-11-10 12:08:15	Crawler E...	Box Cloud
2.3.2	Shared Storage Di...	3383505	US PHH For Discovery	bariatric fo...		1 200.77 KB	High	\\qastorage.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://websearc3...	2016-11-08 16:56:04	Crawler E...	SharePoint Online

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

Display: Violation Triggers

Rule: Croetian Candidates information

- DB Fingerprint PII (Pre-SSID Fingerprinting - Database Records) 18  
Goudi, Stjepan, 87269108171, Kazalj, Tara, 24517049889, 37452260107, 62594481930, Varnek, Matija,

**File Details**

- File path: \\qastorage.websearc.com\Volume 1\Users\Public\Documents\hoj\kandidat.txt
- Hostnames: qastorage.websearc.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: bb06a739d439c0dafa072e2ecba11c1f
- Folder Owners: Unix User\501
- File Owners: Unix User\501

**File Permissions**

- Unix Group\fd\_1HS [RW]
- Everyone [RW]
- Unix User\501 [RW]

**Incident Details**

- Severity: Medium
- Status: New
- Channel: Discovery
- Analyzed by: Policy Engine: EIPMANAGER.togdom.com
- Detected by: Crawler: EIPMANAGER.togdom.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
- Discovery Type: File System

Showing 30 incident(s) / 1 selected

ID	Folder	File Name	Policies	File Size	Severity	Maximum Matches	Incident Time	Channel
192458	\Confidential\Con...	singapore names a...	US PII for Discovery	2.24 KB	High	11	2019-01-15 03:10:02	CASB Service
195456	\Confidential\Con...	Germany PII Crime...	Austria PII for D...	672 B	Medium	1	2019-01-14 03:06:12	CASB Service
194250	\Confidential\Con...	Germany PII CCN a...	Austria PII for D...	1.55 KB	Medium	1	2019-01-14 03:06:06	CASB Service
191709	\Confidential\Con...	singapore names a...	US PII for Discovery	2.37 KB	High	12	2019-01-13 03:09:06	CASB Service
182728	\Confidential\Con...	1-MB-Test.docx	Social Security N...	1023.76 KB	High	48	2019-01-13 03:03:38	CASB Service
195965	\Quarantine\perso...	10-MB-Test CCN an...	Social Security N...	1.62 MB	High	10000	2019-01-12 03:12:05	CASB Service
189801	\Quarantine\perso...	CCNs.txt	Credit Card Numbe...	498 B	High	20	2019-01-12 03:11:41	CASB Service

Incident: 195456 Severity: Medium Channel: CASB Service Discovery Type: Cloud Discovery

Tune Policy

Display: Violation triggers

## Properties

## History

## File Details

File path:	Documents\Confidential\Confidential\PII Data Sample\Germany PII\Germany PII Crime and Name.txt
File size:	672 B
Date Created:	04 Jan. 2019, 05:31:15 AM GMT+0000
Date Modified:	04 Jan. 2019, 05:31:15 AM GMT+0000
Checksum:	0b6e9580c758c7c54a5805e2a1976ad8
File owner:	Forcepoint Brasil
File-owner's email address:	admin@forcepointlab.onmicrosoft.com
Sharing status:	None

## Incident Details

Severity:	Medium
Status:	New

# INTEGRATED WORKFLOW

The screenshot displays the Forcepoint Triton APX interface, which is divided into several sections:

- Top Navigation:** Includes tabs for Web, Data (highlighted in green), Email, and Mobile.
- Left Sidebar:** Contains navigation options: Main, Status, Reporting, Policy Management, Logs, and Settings (General).
- Incidents (last 7 days):** A table listing incidents with columns for ID, Date/Time, and Name. A context menu is open over the table, showing options like Assign..., Change Status, Change Severity, Ignore Incident, Tag Incident..., Add Comments..., Download Incident..., Delete, and Edit Status... The 'Change Status' option is highlighted.
- Run Remediation Script:** A dialog box for selecting a script to execute on selected incidents. It includes fields for Script, Arguments, and Description, and a checkbox for 'Upon script execution change status to: Select'.
- Bottom Section:** Shows a detailed view of an incident (ID: 7667863, Severity: Medium, Action: Denied) and a table of incidents. A context menu is open over the table, showing options like 'Email to Manager...' and 'Email to Other...'.

**Remediation actions might include:**

- Escalate (to manager or another person)
- Move
- Delete
- Encrypt
- Apply DRM
- Apply masking
- Apply Categorisation
- Apply Pseudonymisation (for a test system for example)



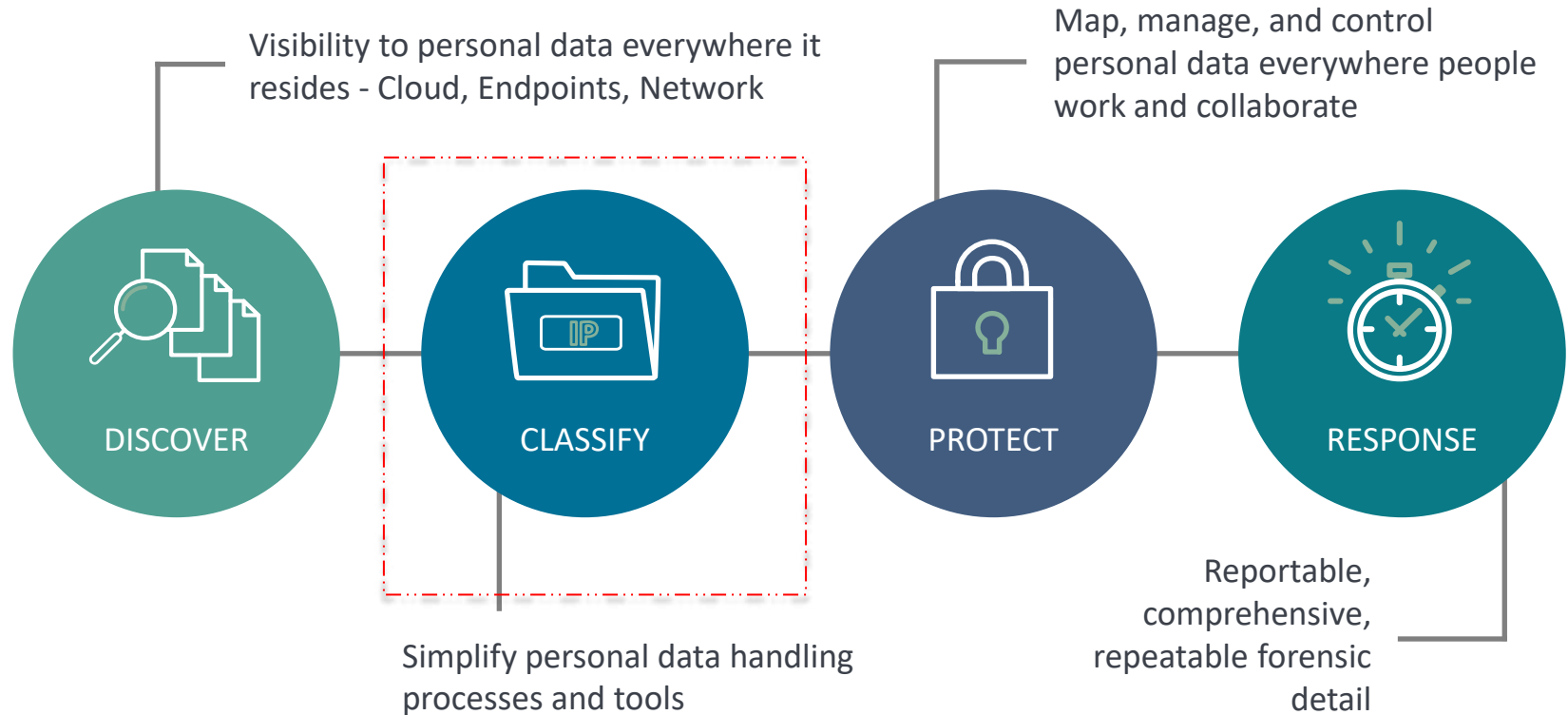


## Data Protection Technology for PDPA Implementation

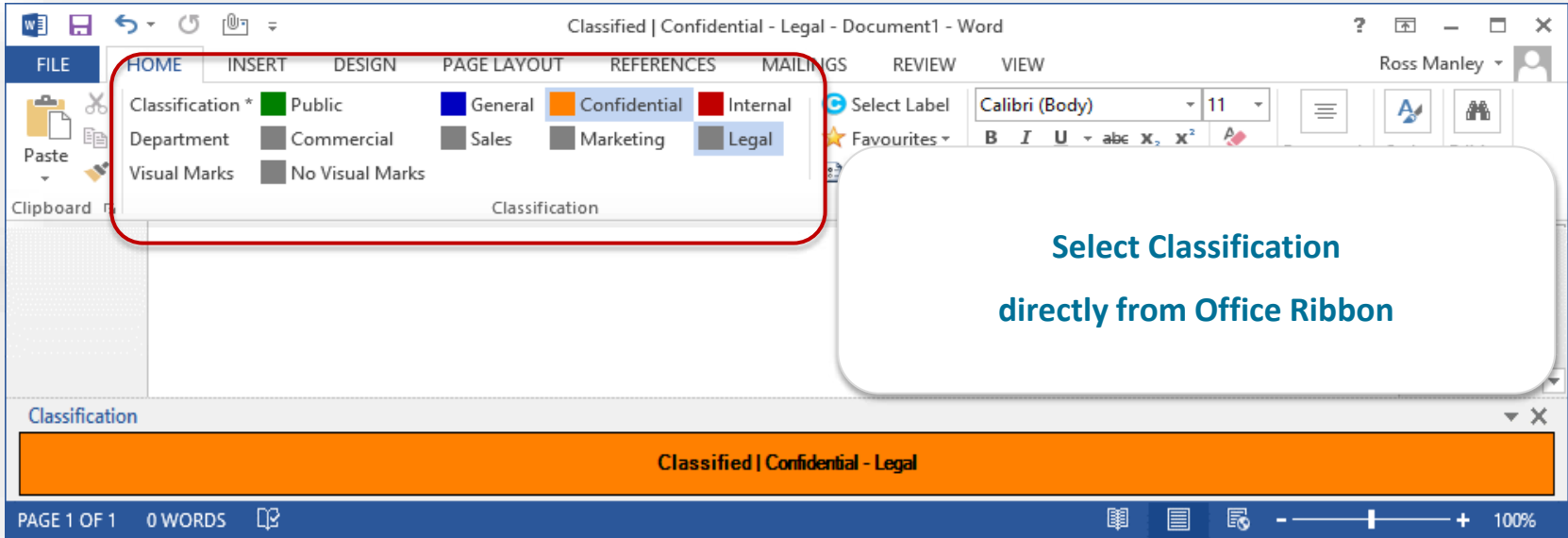
- ❑ DLP Gap analysis
- ❑ Building PDPA Policy Template and Discovery for PDPA Gap analysis
- ❑ Applying Data Classification Tools
- ❑ DLP Architecture and Cloud App Technology
- ❑ Managing DLP/PDPA incidents and engaging business user with User justification and Automated workflow
- ❑ Behavior Analytics / Dynamic User & Data Protection



# Forcepoint's Approach to Thai Personal Data Protection Act



## Multiple selectors of various types to support advanced classification schemes



The screenshot shows the Microsoft Word ribbon with the 'HOME' tab selected. A red box highlights the 'Classification' group, which includes the following options:

Classification *	Public	General	Confidential	Internal
Department	Commercial	Sales	Marketing	Legal
Visual Marks	No Visual Marks			

The 'Confidential' option is currently selected, indicated by an orange background. A callout box on the right contains the text: **Select Classification directly from Office Ribbon**.

At the bottom of the ribbon, a 'Classification' task pane is visible, showing the selected classification: **Classified | Confidential - Legal**.



# Policy design & implementation

## Employees



Public

General Business  
Default Label

Confidential

Internal Only

## HR



Public

General Business

Confidential

Internal Only    HR  
Default Label

## Finance



Public

General Business

Confidential

Internal Only    Finance  
Default Label

## C-Level



Public

General Business

Confidential

Internal Only    M&A  
Internal Only    Project Phoenix

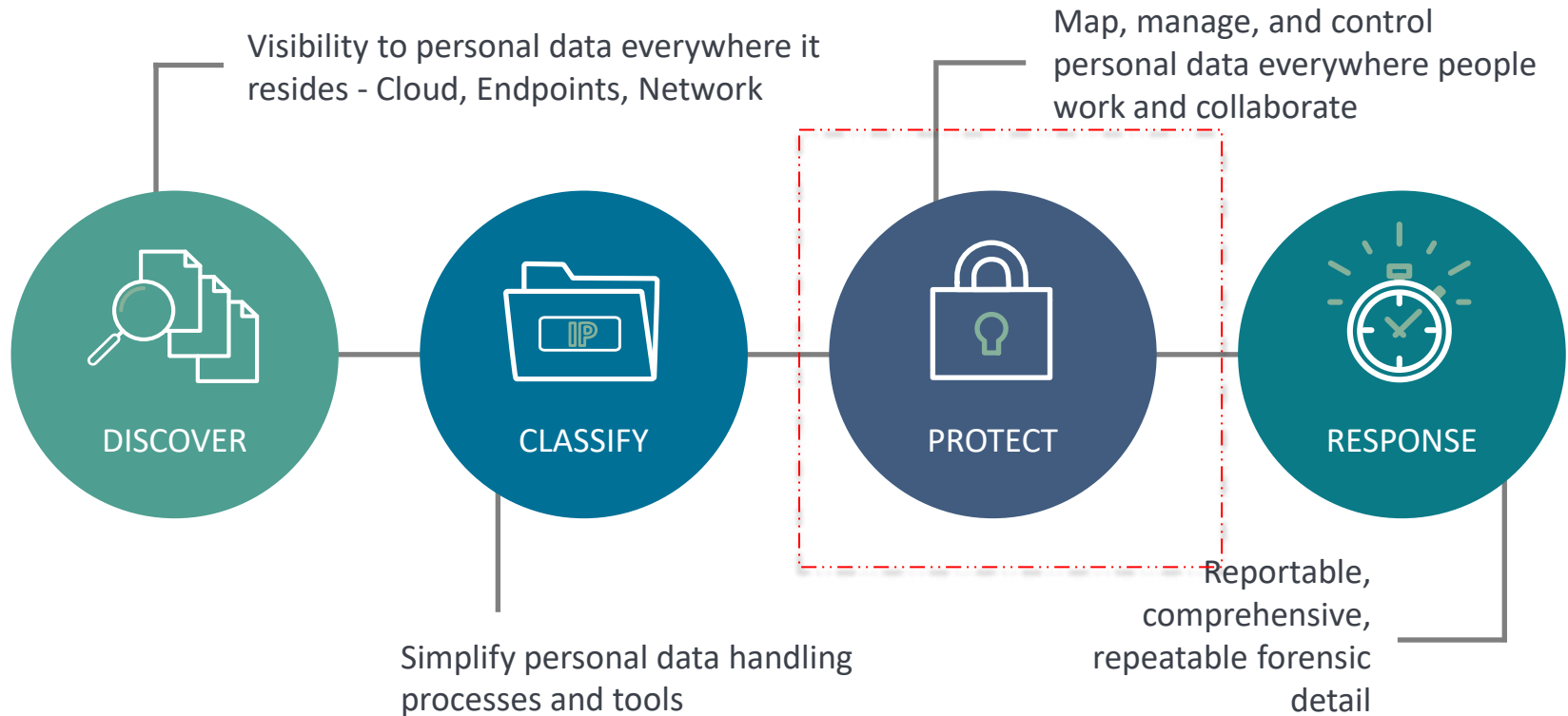


## Data Protection Technology for PDPA Implementation

- ❑ DLP Gap analysis
- ❑ Building PDPA Policy Template and Discovery for PDPA Gap analysis
- ❑ Applying Data Classification Tools
- ❑ DLP Architecture and Cloud App Technology
- ❑ Managing DLP/PDPA incidents and engaging business user with User justification and Automated workflow
- ❑ Behavior Analytics / Dynamic User & Data Protection



# Forcepoint's Approach to Thai Personal Data Protection Act



---

## Protect Sensitive Data

- Email
- Web
- Share Drive
- USB
- Cloud Application



Your Firefox is critically out of date. An update is required to stay secure. Update Now

Independent Data Theft Prevention [DTP], Data Loss Prevention [DLP]

Your public IP address is: 125.25.144.119 [more info](#)

[Data Leak Testing](#)

[Industry Information](#)

[Sample Data](#)

[Session Info](#)

[Contact](#)

# Are you leaking data through web "File Uploads"?

File Upload should be detected by all Data Security tools for both Endpoint and Network based tools [more info](#).

HTTP/S File Upload [22MB max] should be detected by all Data Security tools for both Endpoint and Network based tools [more info](#)

Browse... CreditCard.txt

Upload File

**Warning**

Forcepoint DLP Endpoint has blocked you from uploading sensitive information to the remote host DATALEAKTEST.COM, because it is in violation of corporate policy.



# INVESTIGATING A DATA INCIDENT IN *Forcepoint Security Manager*

**FORCEPOINT TRITON® APX** User name: admin [Log Off](#)

Web **Data** Email Mobile

Appliances TRITON Settings Help

Role: Super Administrator [Deploy](#)

Main **DLP Demo Incidents Report**

Workflow Remediate Escalate

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

Showing 10 incident(s) / 1 selected

Incident ID	Incident Time	Source	Policies	Channel	Destination	Severity	Action	Transaction Size	Status
3.1	2016-11-14 20:44:26	Nathalie Derby	PCI; Peoples Repu...	Network email	barackadama@yahoo...	High	Permitted	17.5 KB	New
3.2.1	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	2016-11-09 18:45:42	Linda Jackson	Suspected Mail to ...	Network email	linda.jackson1976...	Medium	Quarantined	34.95 KB	New
3.4	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	2016-11-13 17:01:02	10.0.140.183	3M Product Numbers	HTTPS	safebrowsing.goog...	Medium	Permitted	23.97 KB	New
3.6	2016-11-10 16:56:21	10.0.140.183	Galaxy Note 7 doc...	FTP	10.11.2.47	Medium	Permitted	8.47 MB	New
3.7	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	2016-12-22 16:54:15	Barbara White	Information Gover...	Network email	knelson@qaxech201...	Medium	Permitted	283.94 KB	New
OneDrive	2016-11-06 11:32:56	cloud@forcecloud...	PCI; Credit Cards	File Sync and Shari...	forcecloud-my.sha...	High	File deleted	468 B	New
RMS	2016-11-03 16:12:34	QAS...	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, 1895-8-25

Forensics Properties History

From: Barbara White  
To: knelson@qaxech2010.mbsn  
Subject: Automatic Email Subject with <keyword>  
Attachments: optima\_m450w\_with\_oem\_suite\_m450wswan\_ex433\_clinical.ipa(282.88 KB)  
Message Body

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

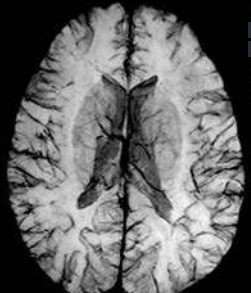
Ex: 313226  
T1 SAG POST  
C:20 omniscan  
Se: 9/10  
Im: 6  
Seg: R19:9

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



Source

Channel

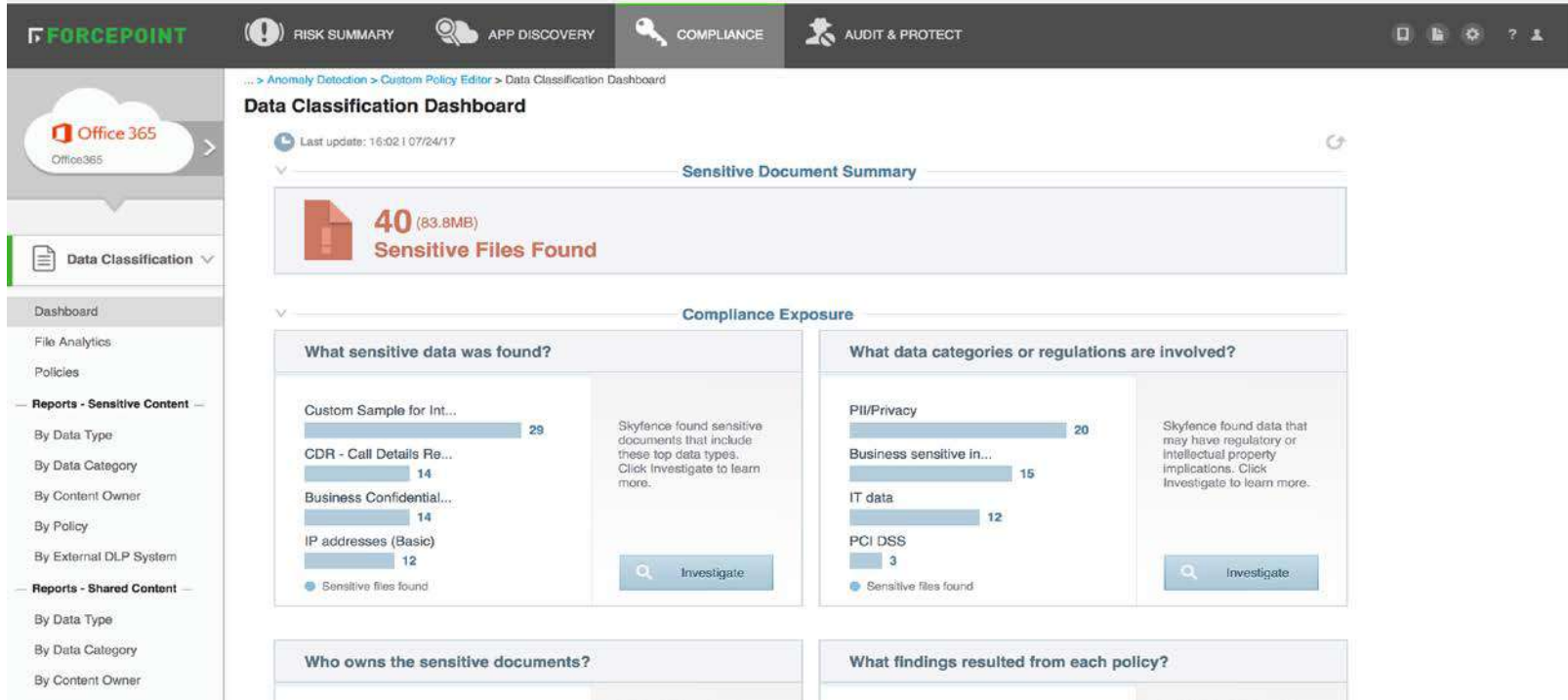
Destination

Action

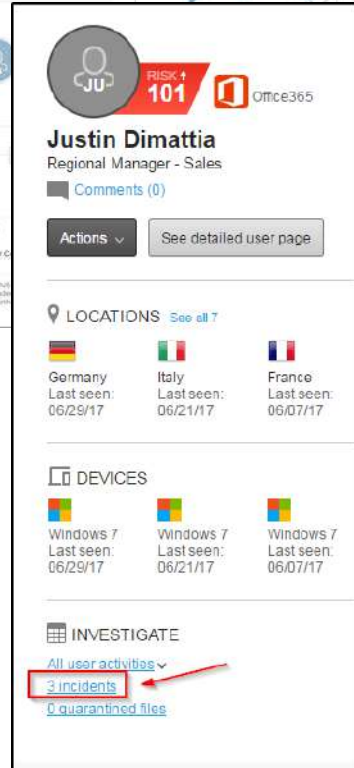
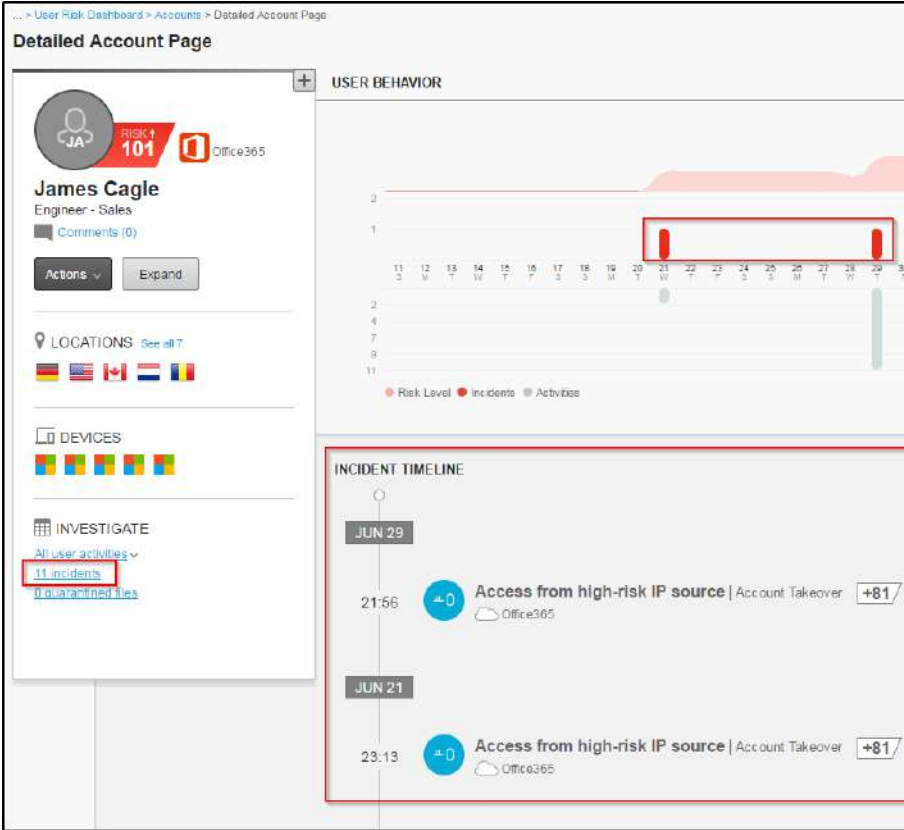
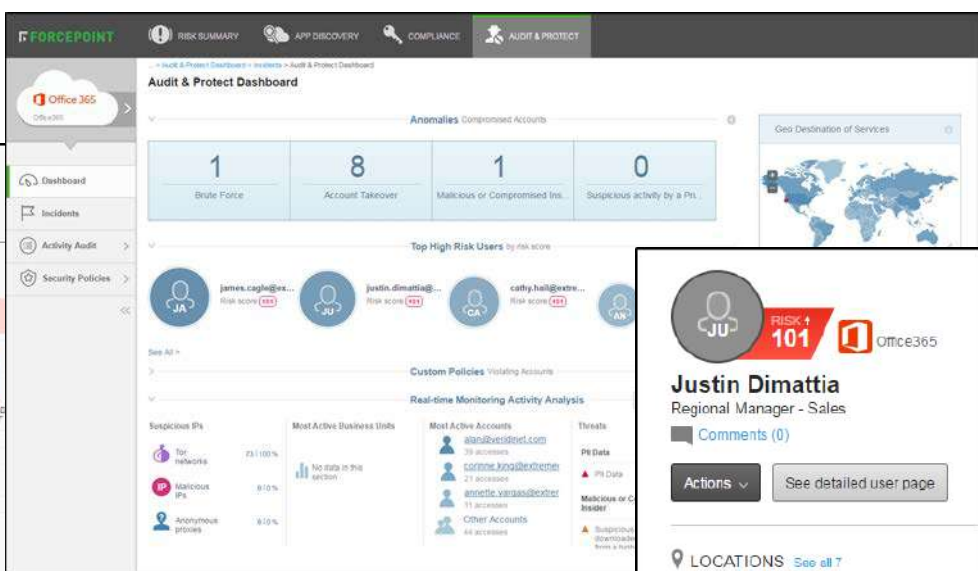
Forensics

# CLOUD APPLICATION ACCESS SECURITY CONTROL (CASB)

- Dashboard



# INCIDENTS ARE EVERYWHERE

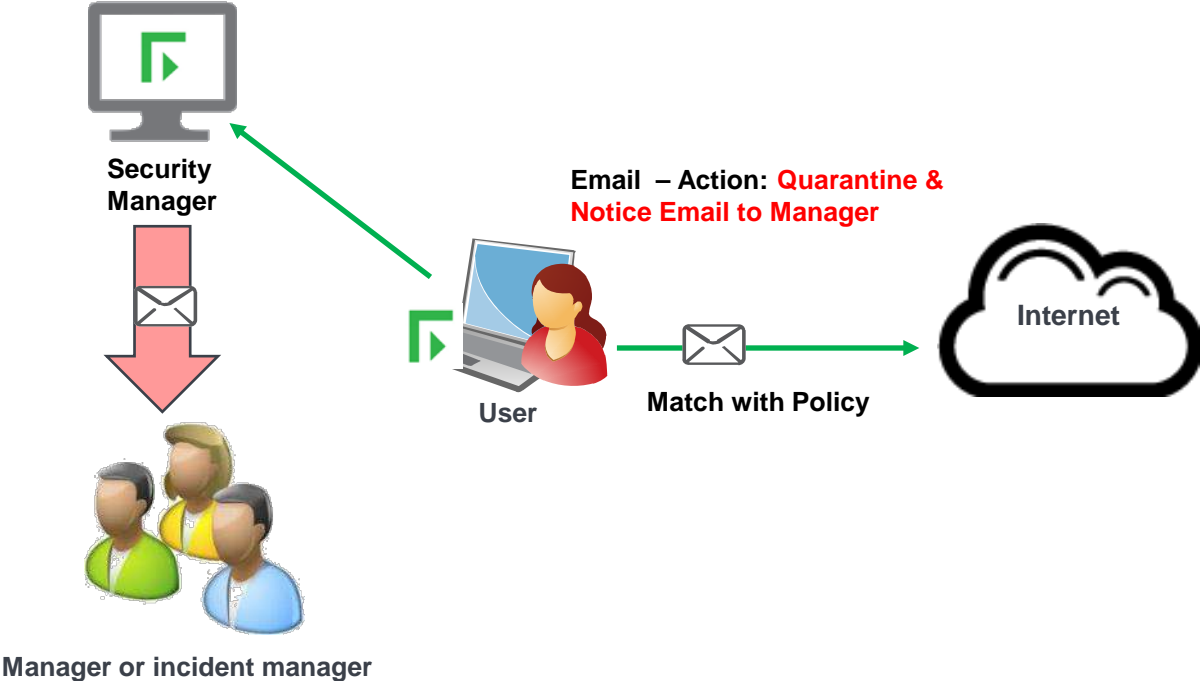




## Data Protection Technology for PDPA Implementation

- ❑ DLP Gap analysis
- ❑ Building PDPA Policy Template and Discovery for PDPA Gap analysis
- ❑ Applying Data Classification Tools
- ❑ DLP Architecture and Cloud App Technology
- ❑ Managing DLP/PDPA incidents and engaging business user with User justification and Automated workflow
- ❑ Behavior Analytics / Dynamic User & Data Protection

# EMAIL INCIDENT WORKFLOW





COMPOSE

Inbox (43)

Starred

Sent Mail

Drafts (6)

More ▾



Peera ▾

**Violation triggers:**

Policy: ·POC-EU GDPR  
Rule: ·POC-EU GDPR  
> Classifier: UK Names (Wide) (Script)  
> 5 match(es): Finlay Ryan, Lydia Shah, Kacie Coleman, Summer Hanson, Ryan Mahmood  
> Classifier: UK National Insurance Number - no proximity (Regular Expression)  
> 5 match(es): TW 76 03 79 D, ZR 48 75 03 C, JN 67 20 73 , AS 99 41 79 D, RT 65 48 76

**Actions**

Click one of the links and fill the needed details in the email window that will be opened. Send the email and the action will be activated.

**Change severity to:**

- [High](#)
- [Medium](#)
- [Low](#)

**Escalate to:**

- [Source's manager](#)

**Change status to:**

- [New](#)
- [In Process](#)
- [Closed](#)
- [False positive](#)
- [Escalated](#)

**More actions:**

- [Release to all recipients](#)
- [Assign](#)
- [Ignore](#)
- [Add comments](#)

**Release instructions**

You are authorized to release this quarantined message.

To release this message, simply reply to this email making sure that the following **Quarantine release code** appears in the body of your reply.

Quarantine release code: <!-- \_\_\_Block Start\_\_\_ Do not alter this block #%H^BBB {2:X}prRirrV8JEw5b/G8qyluaC86SsYQTE/vXOLixg8X99Bewx6G+tHrpZ4nO41Dwk+ecWX80pJ549h03LAN4le5ryn5VJaB9A19ebyyw/AamUp4ITXFXBbzxbqIB6juC9OpygKR0ADY



No recent chats

[Start a new one](#)



# 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	One-Drive	Web	Block
Marketing	Personal Data	Business Partner	Instant Messaging	Notify
Finance	M&A Plans	Facebook	Peer-to-Peer	Remove
Accounting	Employee Salary	OneDrive	Email	To Approve
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

# Data Flow Mapping

The screenshot displays the Forcepoint Triton APX interface. A green callout box at the top center contains the text: "Workflow Remediate – Encrypt Escalate - Incident".

The main interface shows a table of incidents. The selected incident (ID 7667629) is highlighted in yellow. The table columns are: Incid..., ID, Incident Time, Source, Policies, Channel, Destination, Severity, Action, Transaction Size, and Status.

Annotations with green callout boxes point to specific data in the table:

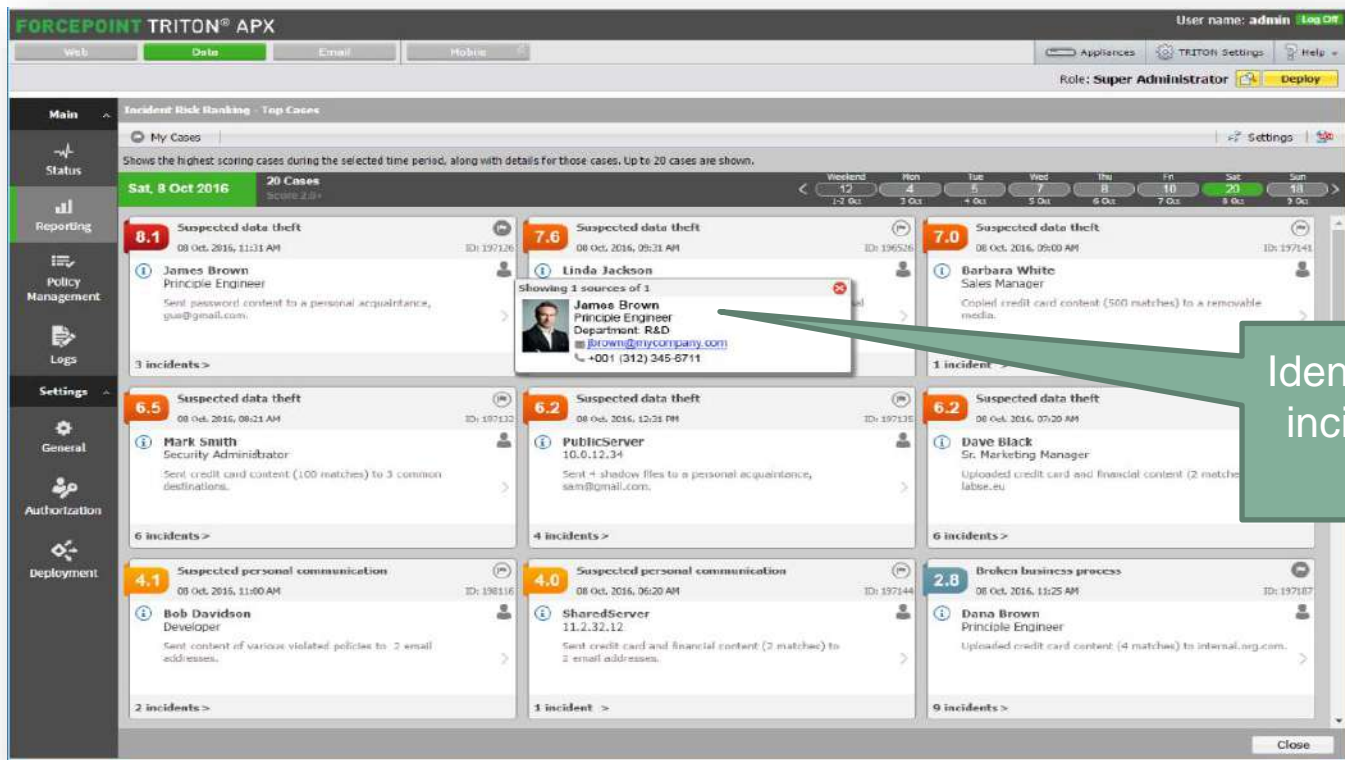
- Source:** Points to the "Source" column for incident 5.2, which is "Barbara White".
- Channel:** Points to the "Channel" column for incident 5.2, which is "Network email".
- Destination:** Points to the "Destination" column for incident 5.2, which is "knelson@qaexch201...".
- Action:** Points to the "Action" column for incident 5.2, which is "Permitted".
- Forensics:** Points to the "Attachments" field in the incident details, specifically to the file "epdima\_mcs50w\_with\_0pm\_suite\_mr450v0wan\_ex433\_clinical.jpg(282.88 KB)".

The incident details pane shows the following information:

- Incident: 7667629
- Severity: Medium
- Action: Permitted
- Channel: Network email
- Rule: IG Toolkit: DOR and Name
- From: Barbara White
- To: knelson@qaexch2010.wb9n
- Subject: Automatic Email Subject with <keyword>
- Attachments: epdima\_mcs50w\_with\_0pm\_suite\_mr450v0wan\_ex433\_clinical.jpg(282.88 KB)



# DATA BREACH NOTIFICATION - INCIDENT RISK SCORING RANKING REPORT



Identify high risk data incident cases over last 24 hours

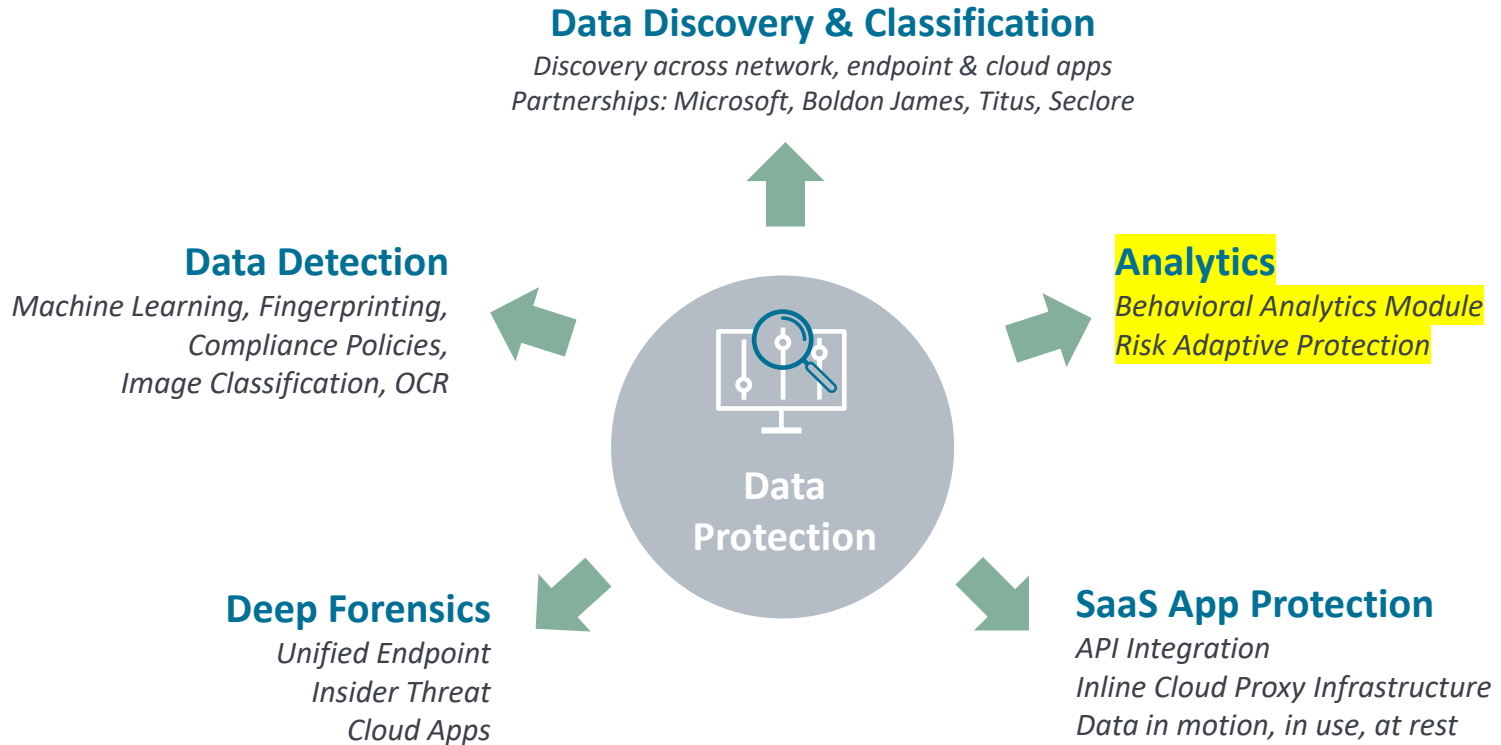
Utilizes Machine Learning and Security Analytics to cluster incidents into cases



## Data Protection Technology for PDPA Implementation

- ❑ DLP Gap analysis
- ❑ Building PDPA Policy Template and Discovery for PDPA Gap analysis
- ❑ Applying Data Classification Tools
- ❑ DLP Architecture and Cloud App Technology
- ❑ Managing DLP/PDPA incidents and engaging business user with User justification and Automated workflow
- ❑ Behavior Analytics / Dynamic User & Data Protection

# Data Protection Point of View



A person wearing a blue long-sleeved shirt is standing at a desk, using a grey printer. The printer is on a dark wooden desk. In the background, there is a laptop and some papers. The scene is brightly lit, suggesting an office environment.

## Better Understanding of Intent

An employee tries to print customer's credit card data and the DLP solution blocks it.

Is this employee a risk?

# Introducing Dynamic Data Protection (DDP)

Delivering Risk-Adaptive Protection

Forcepoint DLP

Forcepoint Behavioral Analytics



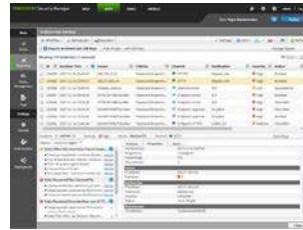
Endpoint monitoring,  
Collection and enforcement



Endpoint  
Server



Set dynamic  
enforcement  
action plan



View DLP  
incidents  
with end-user  
risk level



Automatically  
analyze DLP  
data for identity  
risk calculation



Investigate  
high-risk entity  
activity



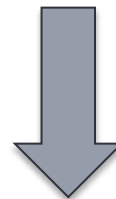
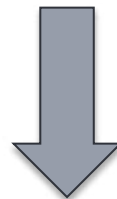
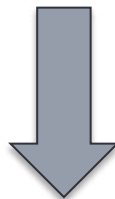
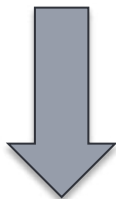
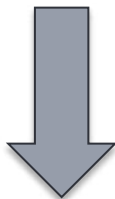
# Graduated Enforcement Based on Risk

*Removing friction to “free the good, while stopping the bad” ...*

**From  
blocking**

For Risk Adaptive Protection users, determine actions according to the source's risk level:

Risk level 1	Risk level 2	Risk level 3	Risk level 4	Risk level 5
Action plan: Block All	Action plan: Block All	Action plan: Block All	Action plan: Block All	Action plan: Block All



**To  
Empowering**

For Risk Adaptive Protection users, determine actions according to the source's risk level:

Risk level 1	Risk level 2	Risk level 3	Risk level 4	Risk level 5
Action plan: Audit Without Forensics	Action plan: Audit Only	Action plan: Audit and Notify	Action plan: Drop Email Attachments	Action plan: Block All

Follow us!



@Forcepoint



Forcepoint



@ForcepointSec  
@ForcepointLabs



Forcepoint LLC



Forcepoint



Data Protection | Web Security | CASB | NGFW | Advanced Malware Detection | Behavioral Analytics | Insider Threat | Email Security | Data Guard | Cross Domain