# DLP w odniesieniu do wymagań GDPR

Maj 2017

**Alexander Raczynski**
araczynski@forcepoint.com

FORCEPOINT
POWERED BY Raytheon

# ZASTRZEŻENIE PRAWNE

Poniższa prezentacja nie stanowi ani nie zawiera porady prawnej.

W celu osiągnięcia zgodności z wymaganiami GDPR zalecamy dyskusję z Państwa zespołem prawnym, zespołem compliance oraz zespołem ochorny informacji.

FORCEPOINT
POWERED BY Raytheon

websense® → Raytheon → STONESOFT

**Commercial Leader**
*with*
Content Security & DLP
Cloud / On-Premise / Hybrid

**Pioneer on Cyber Frontlines**
*with*
Financial Resources
Deep Understanding of Threat Detection

**Networking Innovator**
*with*
Advanced Evasion Prevention
Security at Scale

# FORCEPOINT

POWERED BY Raytheon

Więcej informacji: https://www.forcepoint.com/history

# KLASYFIKACJA DANYCH vs. DLP

# KLASYFIKACJA DANYCH

RESTRICTED

CONFIDENTIAL

INTERNAL

PUBLIC


FORCEPOINT
POWERED BY Raytheon

# ILUZORYCZNA TECHNOLOGIA?



# TECHNOLOGIA DLP

# DLP

## Data in Motion

Dane płynące do wewnątrz i na zewnątrz organizacji

### Data Usage (Network)

Typowe kanały komunikacyjne

- ✓ HTTP(S)
- ✓ FTP
- ✓ SMTP
- ✓ Instant Messangers
- ✓ Network Printer

## Data in Use

Podczas manipulacji przez różne aplikacje

### Data Usage (Endpoint)

Monitorowane akcje (Endpoint)

- ✓ Cut / Copy / Paste
- ✓ Print
- ✓ Print Screen
- ✓ Access Files
- ✓ Endpoint LAN/Web
- ✓ Removable Media
- ✓ Outlook / Lotus Plugin
- ✓ Printers (local, net)

## Data at Rest

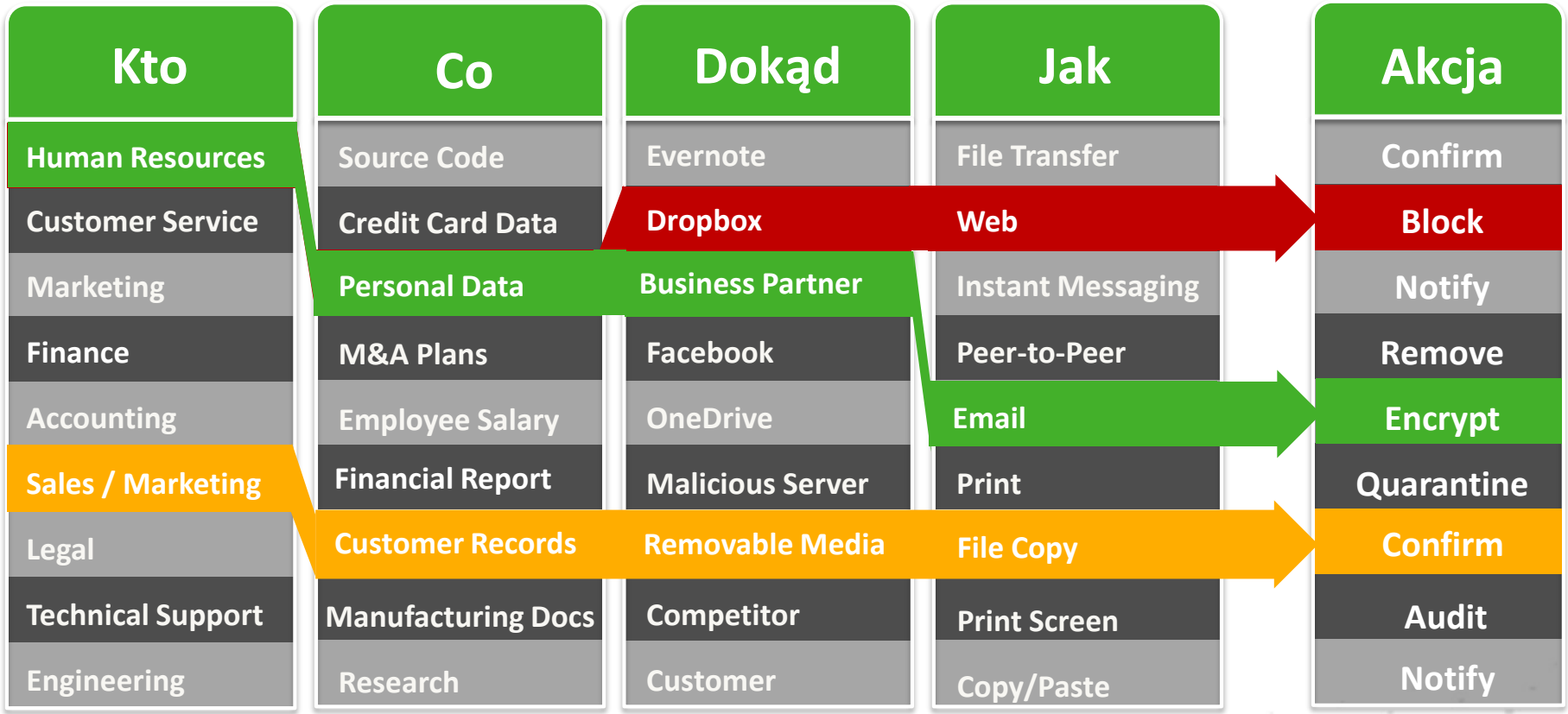
Dane przechowywane w granicach naszej infrastruktury

### Data Discovery

Repozytoria danych

- ✓ Network Shares (NTFS, NFS, Novell)
- ✓ SharePoint
- ✓ Databases (via ODBC)
- ✓ Exchange
- ✓ Lotus Domino
- ✓ Pst files
- ✓ Endpoint

# DATA IN USE & IN MOTION



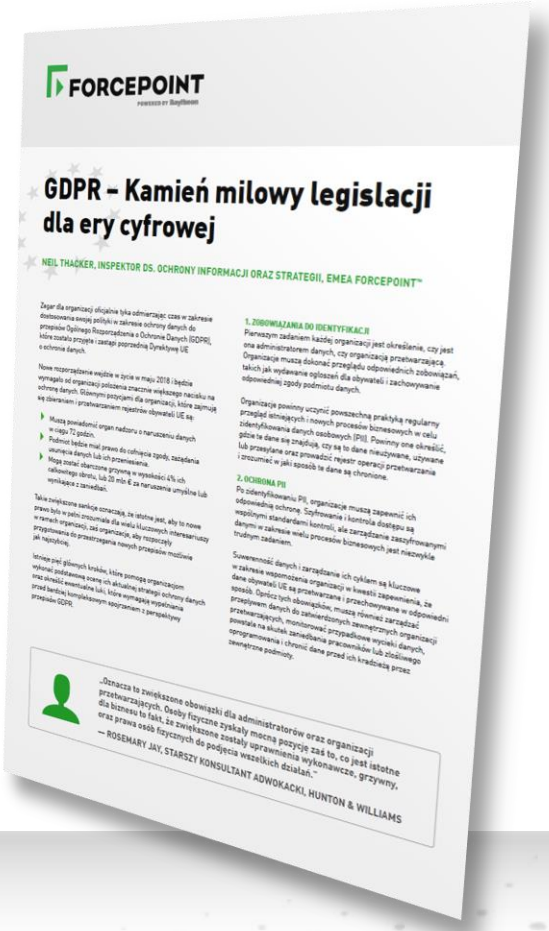

FORCEPOINT
POWERED BY Raytheon


General
Szeroki zasięg
Data
Dane osobowe (PII)
Protection
Dane / Prywatność
Regulation
Prawo / Instrukcja
FORCEPOINT
POWERED BY Raytheon

# GDPR - PORADY PRAKTYCZNE

- Ocena obecnych praktyk w zakresie ochrony danych
- Tworzenie struktury zarządzania w zakresie ochrony danych
- Przeprowadzenie inwentaryzacji zasobów danych osobowych
- Stworzenie narzędzi informacyjnych
- Weryfikacja mechanizmów zezwoleń
- Implementacja sterowników technicznych i organizacyjnych
- Przeprowadzenie oceny skutków ochrony danych
- Zgłoszenie naruszenia danych osobowych do organu nadzoru



FORCEPOINT

GDPR – Kamień milowy legislacji dla ery cyfrowej

NEIL THACKER, INSPEKTOR DS. OCHRONY INFORMACJI ORAZ STRATEGII, EMEA FORCEPOINT™

Żegar dla organizacji oficjalnie tyka odmierzając czas w zakresie dostosowania swojej polityki w zakresie ochrony danych do przepisów Ogólnego Rozporządzenia o Ochronie Danych (GDPR), które zostało przyjęte i zastąpi poprzednią Dyrektywę UE o ochronie danych.

Nowe rozporządzenie wejdzie w życie w maju 2018 i będzie wymagało od organizacji położenia znacznie większego nacisku na ochronę danych. Głównymi pozycjami dla organizacji, które zajmują się obrazowaniem i przetwarzaniem rejestrów obywateli UE są:

- Muszą powiadomić organ nadzoru o naruszeniu danych w ciągu 72 godzin.
- Podmiot będzie miał prawo do cofnięcia zgody, zażądania usunięcia danych lub ich przeniesienia.
- Mogą zostać obarczone grzywną w wysokości 4% ich całkowitego obrotu, lub 20 mln € za naruszenia umyślne lub wynikające z zaniedbań.

Takie zwiększone sankcje oznaczają, że istotne jest, aby to nowe prawo było w pełni zrozumiałe dla wielu kluczowych interesariuszy w ramach organizacji, zad organizacje, aby rozpoczęły przygotowania do przestrzegania nowych przepisów możliwie jak najszybciej.

Istnieje pięć głównych kroków, które pomogą organizacjom wykonać profesjonalną ocenę ich aktualnej strategii ochrony danych oraz określić niezbędne luki, które wymagają wypełniania przed bardziej kompleksowym spojrzeniem z perspektywy przepisów GDPR.

1. ZOBOWIĄZANIA DO IDENTYFIKACJI

Pierwszym zadaniem każdej organizacji jest określenie, czy jest ona administratorem danych, czy organizacją przetwarzającą. Organizacje muszą dokonać przeglądu odpowiednich zobowiązań, takich jak wydawanie ogłoszeń dla obywateli i zachowywanie odpowiedniej zgody podmiotu danych.

Organizacje powinny uczynić powszechną praktyką regularny przegląd istniejących i nowych procesów biznesowych w celu zidentyfikowania danych osobowych (PII). Powinny one określić, gdzie te dane się znajdują, czy są to dane nieużywane, używane lub przesyłane oraz prowadzić rejestr operacji przetwarzania i zrozumieć w jaki sposób te dane są chronione.

2. OCHRONA PII

Po zidentyfikowaniu PII, organizacje muszą zapewnić ich odpowiednią ochronę. Szyfrowanie i kontrola dostępu są współczesnymi standardami kontroli, ale zarządzanie zaszyfrowanymi danymi w zakresie wielu procesów biznesowych jest niezwykle trudnym zadaniem.

Suwerenność danych i zarządzanie ich cyklem są kluczowe w zakresie wspomożenia organizacji w kwestii zapewnienia, że dane obywateli UE są przetwarzane i przechowywane w odpowiedni sposób. Oprócz tych obowiązków, musza również zarządzać przesyłaniem danych do zatwierdzonych zewnętrznych organizacji przetwarzających, monitorować przypadkowe wyniki danych, powstałe na skutek zaniedbania pracowników lub złośliwego oprogramowania i chronić dane przed ich kradzieżą przez zewnętrzne podmioty.

„Oznacza to zwiększone obowiązki dla administratorów oraz organizacji przetwarzających. Osoby fizyczne zyskały mocną pozycję zaś to, co jest istotne dla biznesu to fakt, że zwiększone zostały uprawnienia wykonawcze, grzywny, oraz prawa osób fizycznych do podjęcia wszelkich działań."

— ROSEMARY JAY, STARSZY KONSULTANT ADWOKACKI, HUNTON & WILLIAMS

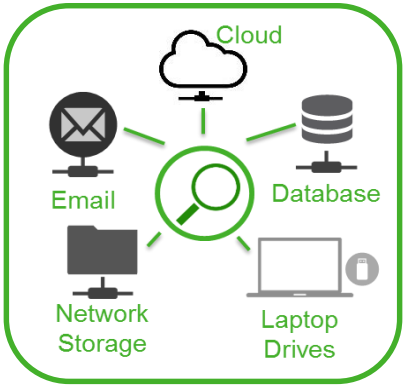
FORCEPOINT POWERED BY Raytheon

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

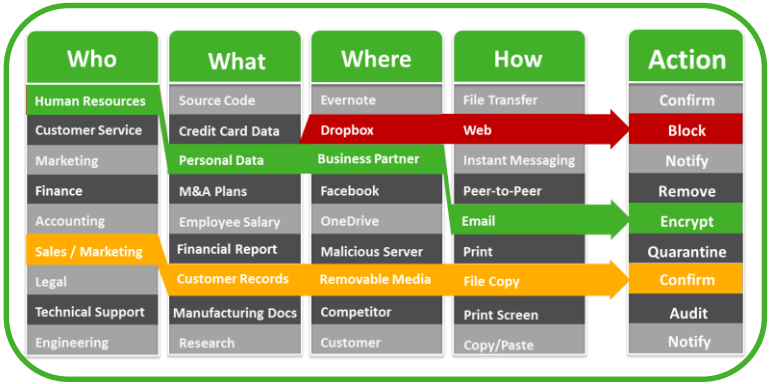
 

# JAK DLP MOŻE POMÓC?

## INWENTARYZACJA DANYCH OSOBOWYCH




## KONTROLOWANIE PRZEPŁYWU I UŻYCIA DANYCH OSOBOWYCH



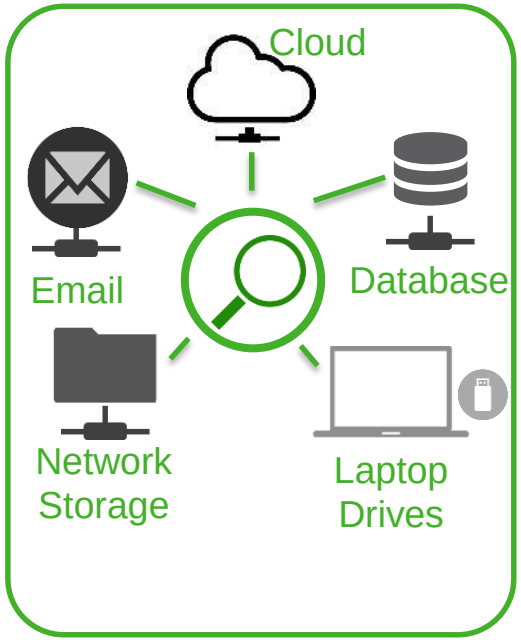

## BĄDŹ GOTOWY ODPOWIEDZIEĆ NA CZAS


DLP: Discover, Endpoint

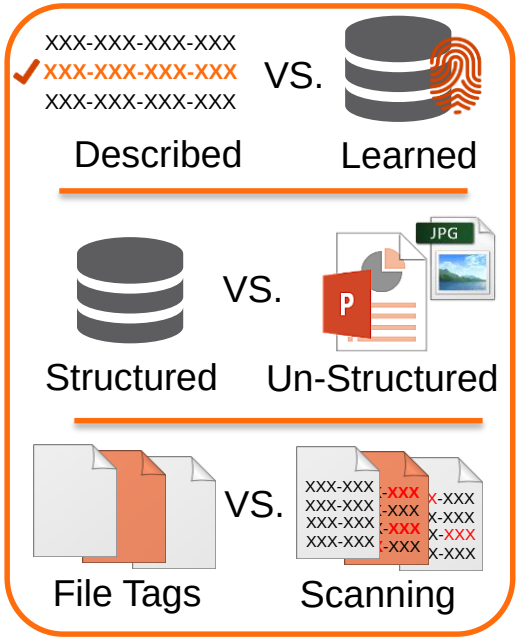
DLP: Gateway, Endpoint

Incident Management

# INWENTARYZACJA DANYCH OSOBOWYCH




DANE SĄ WSZĘDZIE




NIE ZAWSZE ŁATWE DO ZNALEZIENIA

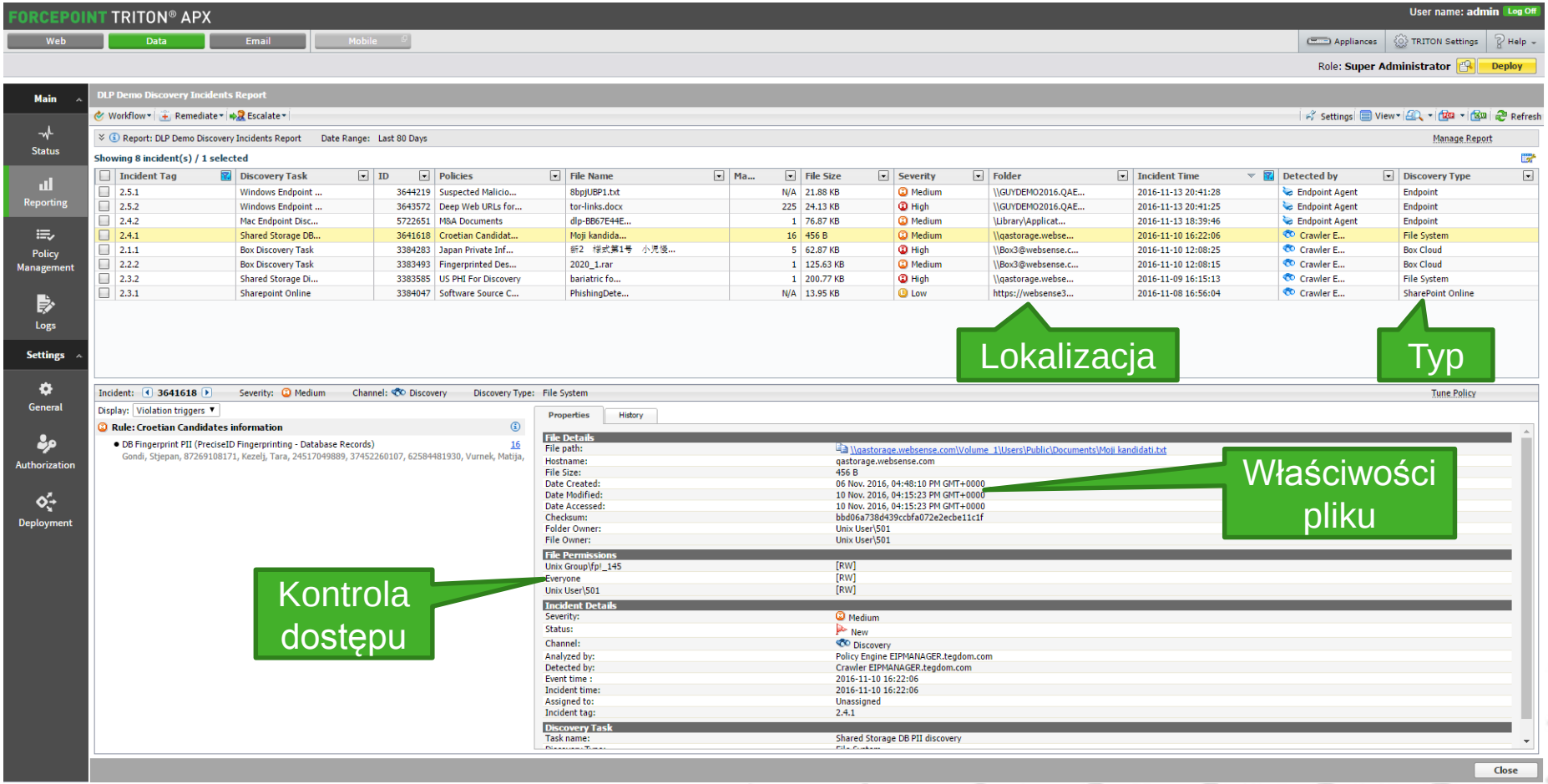

NIE TYLKO UTRATA, CZASEM CELOWE DZIAŁANIE

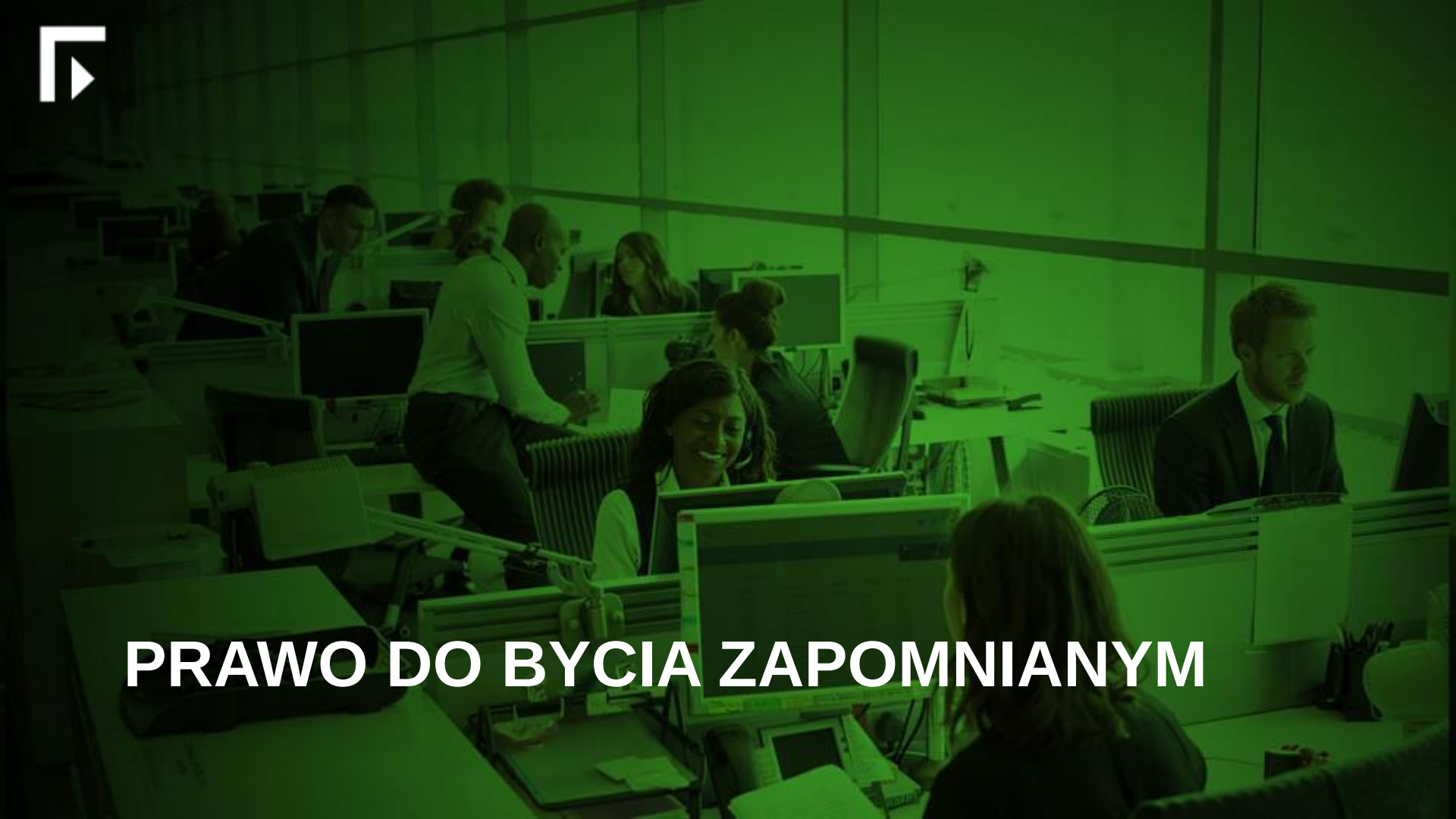
**FORCEPOINT DLP: DLP DISCOVER & DLP ENDPOINT**

FORCEPOINT
POWERED BY Raytheon

# WYNIKI INWENTARYZACJI





# PRAWO DO BYCIA ZAPOMNIANYM

# ARTYKUŁ 17 – PRAWO DO USUNIĘCIA DANYCH („PRAWO DO BYCIA ZAPOMNIANYM”)

1. Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:

   a) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
   b) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie zgodnie z art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a), i nie ma innej podstawy prawnej przetwarzania;
   c) osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 1 wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 2 wobec przetwarzania;

   …

# JAK TO ZREALIZOWAĆ? PRZYKŁAD

1. Data Discovery w oparciu o konkretne dane klienta:

| Nazwisko | Imię | PESEL | Nr dow. | Telefon |
|---|---|---|---|---|
| Raczyński | Aleksander | 67042818958 | ANU959154 | 606 430 403 |
| Domagalski | Jan | 97050510553 | AFE550845 | 656 237 493 |
| Nierozważna | Krystyna | 90021705440 | AFZ842190 | 565 238 783 |

2. Wykonaj zadanie „Discovery” w poszukiwaniu danych

- Serwery plików
- SharePoint
- Zasoby w chmurze (Box Cloud / SalesForce / Dropbox)
- Exchange
- PST-Files
- Lotus Domino
- Stacje Robocze (Endpoints)
- Bazy danych

# CZY UDAŁO SIĘ TO ZROBIĆ SKUTECZNIE?

Wyszukiwanie danych działa poporawnie dla zasobów, które są dostępne w czasie procesu „discovery”.

Należy jeszcze zwrócić uwagę na:

- Sekwencyjny backup systemów i danych
- Zasoby szyfrowane
- ...

Możliwe rozwiązania:

- Zdefiniowanie procesów integrujących przywracanie backupu i zasobów danych z ponownym zadaniem „discovery”
- Monitorowanie za pomocą narzędzi „Data-in-motion” (Dane w ruchu)

FORCEPOINT
POWERED BY Raytheon


# Dziękuję