GDPR PRODUCT MAPPING OVERVIEW PAPER:

USING FORCEPOINT SOLUTIONS TO ASSIST WITH GDPR CONTROL REQUIREMENTS

FORCEPOINT
POWERED BY Raytheon

Protecting the human point.

Introduction

In this overview paper, we introduce three core DLP use-cases where Forcepoint technologies such as Forcepoint DLP and Forcepoint CASB are supporting organizations like yours prepare for the General Data Protection Regulation (GDPR):

- **The need to inventory personal data**
- **The need to map, manage & control the flow of personal data**
- **The need to respond to personal data breaches in a timely manner**

Security frameworks are a good way to align information security and data protection programs — preparing for GDPR is no different. For this paper we have chosen to use the NIST Cyber Framework[1] to map the three core Forcepoint GDPR use cases.

1 www.nist.gov/cyberframework

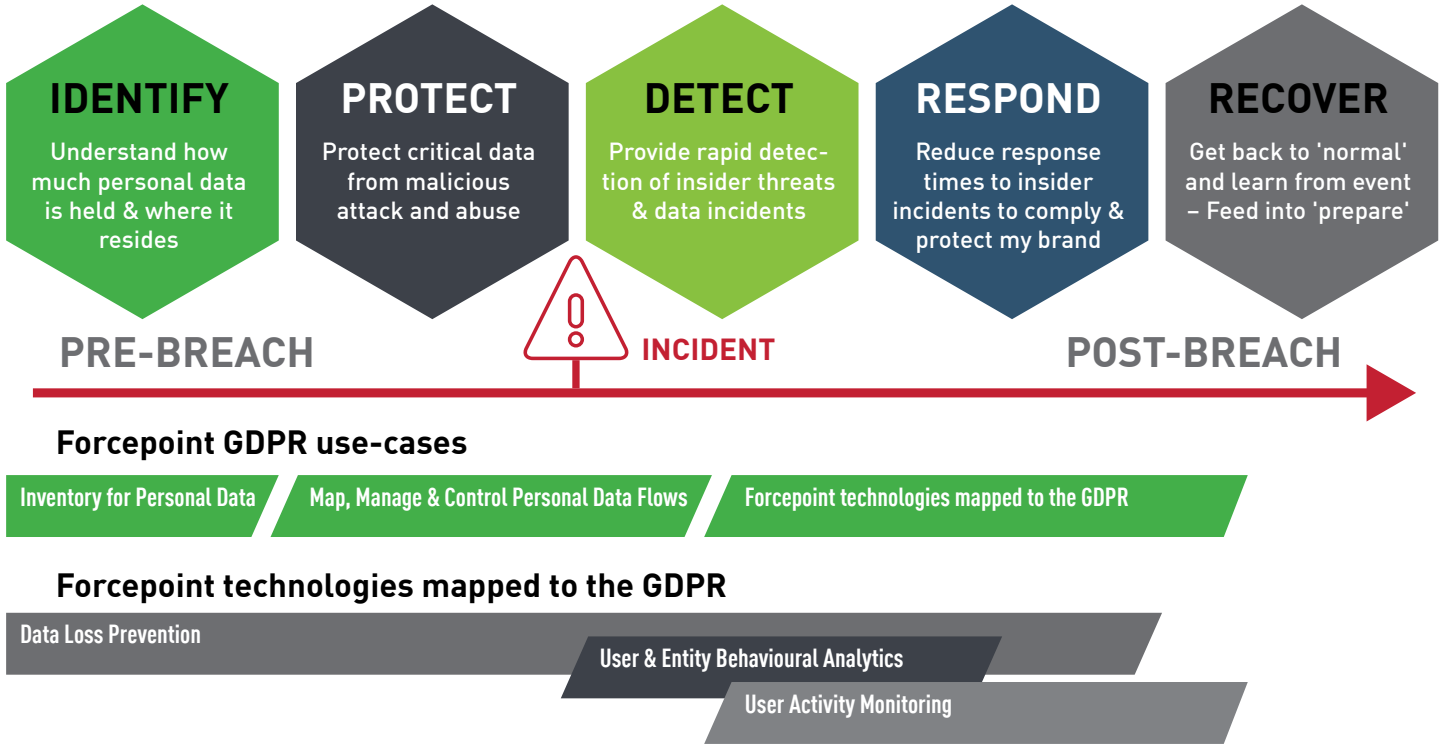

Figure 1 – Using a common security framework1 to map key GDPR & related Information security activities and the underlying technologies detailed in this overview paper.

Why inventory for personal data?

Organizations will need to understand how much personal data exists within their organization in order to quantify their exposure to the GDPR. Invariably, an organization will discover that they have more data than they thought and in places they were not expecting. Additionally, knowing where personal data resides will also prove useful during data subject access requests; for example, where they are looking to have their personal data rectified or erased.

Data Loss Prevention (DLP) is an excellent technical measure to assist organizations to inventory for personal data. DLP solutions are able to detect many types of data, including personal data, in many different formats (e.g., structured and unstructured). They can also determine file ownership, access rights and age of data files; in order to be effective, it must be able to look for personal data across the organization, within laptop devices, local file shares, mailboxes and databases to network and cloud storage. Today, data is more distributed than ever as organizations encourage more flexible working practices and move towards a cloud-first IT strategy.

Leading DLP technologies integrate with 3rd party technologies like file classification tools to take action on personal data found at rest. for example, mis-classified files or unclassified files can be re-routed to classification tools and have the correct file classification tag applied.

Forcepoint DLP can scan many different locations to find sensitive data

Endpoint Devices (Windows & macOS)

Microsoft Exchange (inc. online version)

Microsoft SharePoint (inc. online version)

Shared Storage

Box (Cloud scan)

Databases

Map, manage and control the flow of personal data

Once you understand where your data is and who has access to it, an organization will look to create policies around the lawful processing of data. Employees need to interact with personal data as part of their normal working duties. Data flows across organizations in many ways: employees move files from a network share to a laptop drive in order to work remotely; email data to a supplier; copy and paste data between applications; or upload data to cloud file sync and share services.

DLP solutions understand how to recognise personal data; therefore, it can be configured to perform particular actions or work with other IT systems to instruct them to perform actions on its behalf. DLP solutions must be in the flow of personal data to take this action, and are most effective when deployed on the endpoint, the network and in the cloud.

Understanding data flows to 3rd parties is a critical part of preparing for the GDPR. Forcepoint's experience of running cloud application risk assessments with large enterprises often uncover as many as 600 cloud applications in use. Many organizations will first look to inventory their sanctioned and unsanctioned cloud usage; Cloud Access Security Brokers (CASB) play a key role in helping organizations achieve this goal.

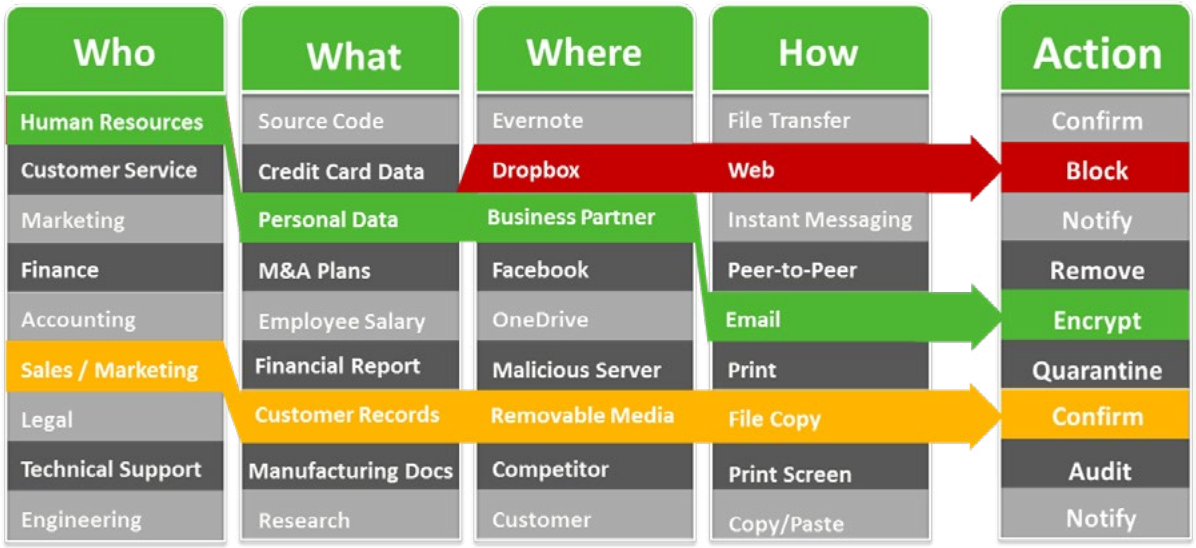

Figure 2 – Outlines common data flow examples and actions that can be taken using DLP as an enforcement point.

When combined with technologies like CASB, web and email security gateways or encryption solutions, DLP solutions can apply policies to allow the flow of data in a safe and measured way. One way they do this is by applying encryption as an employee copies files to USB. In addition, they can educate employees on the safe processing of personal data by using "pop-up" messages, providing feedback and asking for justifications for particular actions. DLP solutions can also instruct systems to block or quarantine the transfer of personal data to high risk locations, or move data when it's found in the wrong location.

What technical measures assist in the response process to a data breach?

Detection:

Security analytics tools like User & Entity Behaviour Analytics (UEBA) can assist with the detection of an incident. UEBA ingests thousands of security incidents or events and applies analytic algorithms to look for patterns of behaviour that are leading indicators of data risk. This approach is compelling, compared to the manual alternative of assigning individual operators the task of scanning through huge volumes of alerts, an approach which puts a huge burden on already over-stretched security operations teams. Additionally, DLP solutions such as Forcepoint DLP use pre-defined policies to detect indicators of risk (e.g., looking for data movement out of hours, looking for employee-encrypted files being transmitted across networks, looking for personal data contained in images such as screenshots).

Response:

In assisting with the response process, DLP solutions can provide valuable forensics around data incidents (e.g., where the data came from, where it went, the action taken, whether it was encrypted, what personal data was subject to the incident)

In addition, User Activity Monitoring (UAM) technologies are very effective at supporting the response process. These technologies are designed to monitor specific observables of privileged users as they access personal data. Some of these systems can take a series of screenshots of an employee's desktop during specific events, and more importantly, as data processors access personal data. In the event of a breach or data incident, investigators are then able to access this deep level of forensics to assist in the investigation. Getting to the truth as quickly as possible is critical, not only to protect the individual but also the organization; and of course, in order to meet the strict timescales defined in the GDPR.

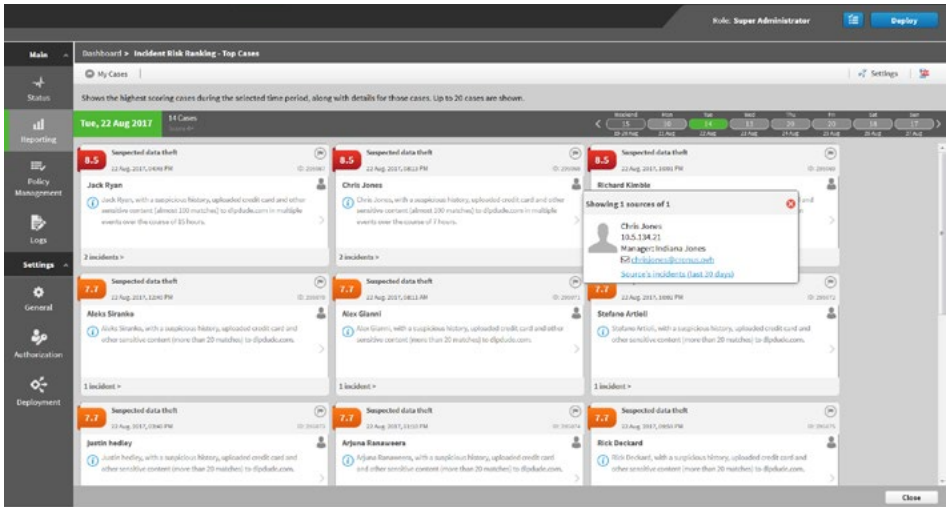

Figure 3 – shows a Forcepoint Incident Risk Ranking report that leverages security analytics and machine learning to cluster DLP incidents into cases ranked in order of priority

Recover:

Once the investigation is completed and the intent behind the breach is clarified (i.e., was it an accident, were credentials compromised or was the intent to take data?), remediation actions becomes more accurate. Whether it's fixing a broken business process, raising awareness with processors, repairing an infected machine or updating data protection polices, technical measures can be used to further test and enforce these new outcomes.

Summary & Next Steps

Forcepoint provides market leading technologies and solutions to protect personal data and other critical data, such as intellectual property. For more information on the GDPR or for details on how to build DLP or broader insider threat programs, please visit our website: www.forcepoint.com/gdpr

To learn why organizations should inventory personal data — to both scope initial compliance efforts and to understand "sensitive data drift", or as part of the day to day tasks when responding to Data Subject Access Requests, please read paper 1 entitled, "Personal Data Inventory".

To learn why organizations must ensure they understand data flows, and how DLP technology can assist them to manage and control personal data flows as part of meeting GDPR requirements, please read paper 2 entitled, "Data Flow Mapping & Control".

To learn which technologies can assist organizations to respond to data breaches in a timely manner (i.e., within 72 hours of the controller becoming aware of the data breach), please read part 3 entitled, "Detect & Respond To A Data Incident".

To arrange a demonstration of the technologies detailed in this paper, please contact your local Forcepoint sales office. www.forcepoint.com/company/contact-us

Forcepoint Products:

Forcepoint technology mapped to the 5 pillars of the security framework

	Prepare	Protect	Detect	Respond	Recover
Forcepoint DLP	●	●	●	●	
Forcepoint UEBA			●	●	
Forcepoint Insider Threat			●	●	●
Forcepoint Cloud Access Security Broker	●	●	●		
Forcepoint Web Security		●	●		
Forcepoint Email Security		●	●		
Forcepoint Next Generation Firewall		●	●		

Forcepoint Products:

Forcepoint DLP

provides security focused on people's interaction with data, including creation, storage, email, webmail, personal devices and cloud applications. The industry's most complete data protection platform, Forcepoint DLP is recognized as a market leader by industry analysts for its robust coverage of data discovery, endpoint control, network enforcement and extension into cloud applications.

When combined with Forcepoint Web and Email Security technology, organizations benefit from centralised management, policy enforcement and reporting across critical communication channels.

Forcepoint UEBA

(User & Entity Behavior Analytics) identifies the human risk to cyber security by monitoring and providing visibility into the cyber activity of people. Forcepoint UEBA prioritizes cyber risk and assigns a risk score for every user by analysing large amounts of complex data from your existing IT environment and understanding the actions of users that may put critical data at risk.

Our security analytics platform provides unparalleled context by fusing structured and unstructured data to identify and disrupt malicious, compromised and negligent users. We uncover critical problems such as compromised accounts, corporate espionage, intellectual property theft and fraud.

Forcepoint Insider Threat

enables organizations to protect data and guard their most critical systems against the broad spectrum of insiders, including accidental, compromised and malicious employees. Forcepoint Insider Threat automatically identifies high risk users and provides deep context into unusual behaviour to proactively and authoritatively address threats from within. This "high definition" context greatly reduces data incident investigation times by providing investigators and responders with clear, actionable information across many systems from a single console.

By focusing on peoples' interactions with data through deep integration with Forcepoint DLP and Forcepoint UEBA, Forcepoint Insider Threat prevents behavioral-based data loss and exposes other insider threats that present risk to critical systems, such as fraudulent transactions or cyber sabotage.

Forcepoint CASB (Cloud Access Security Broker)

provides organizations with visibility and control over cloud applications. Forcepoint CASB provides both the ability to discover the use of unsanctioned cloud applications and assess associated risk, as well as the ability to control how sanctioned cloud applications (e.g., Office 365, Google Suite, Salesforce, Box, Dropbox) are used in order to prevent the loss of critical data.

Forcepoint Web Security

is a cloud or hybrid deployed Secure Web Gateway that stops advanced threats from getting in and sensitive data from getting out – whether an organization's users are in the office, working from home or on the road.

Forcepoint Email Security

stops the spam and phishing emails that introduce ransomware and other advanced threats before they can infect systems with malware that lead to data loss.

Comprehensive defenses integrate highly effective analytics and advanced malware sandboxing for inbound protection, DLP as an outbound control and email encryption for secure communications.

Forcepoint NGFW (Next Generation Firewall)

connects and protects people and the data they use throughout your offices, branches, and the cloud – with the greatest efficiency, availability and security.

ABOUT FORCEPOINT

Forcepoint is transforming cybersecurity by focusing on what matters most: understanding people's intent as they interact with critical data and intellectual property wherever it resides. Our uncompromising systems encompass Cloud, data and network security, and enable companies to empower employees with unobstructed access to confidential data while protecting intellectual property and simplifying compliance. The combination of UEBA technology (RedOwl acquired in August 2017), Forcepoint DLP and Forcepoint Insider Threat provide the industry's only comprehensive solution for understanding and responding to the behaviors and intent of people.

CONTACT

www.forcepoint.com/contact

For more about Forcepoint, visit www.forcepoint.com and follow us on Twitter at @ForcepointSec.

[EBOOK_PROD_MAP_GUIDE_OVERVIEW_ENUS] 400021.02NOV17