Whitepaper
GDPR Technology Mapping Guide
Detect and respond to a data incident
Table of Contents

1. Executive overview 3
2. The implementation of timely personal data breach reporting 3
3. Using a security framework approach to benchmark data protection programs 5
4. DLP as a technical measure to assist with timely personal data breach reporting 5
   Where does DLP fit into the NIST Cybersecurity Framework? 5
   How can DLP assist with the breach response process? 6
5. Behavioral analytics as a technical measure to assist with timely personal data breach reporting 8
   Where does behavioral analytics fit into the NIST Cybersecurity Framework? 8
   How does behavioral analytics and security analytics support the breach response process? 8
6. CASB as a technical measure to assist with timely personal data breach reporting 9
   Where does CASB fit into the NIST Cybersecurity Framework? 9
   How does CASB support the breach response process? 9
7. Forcepoint Dynamic Data Protection technologies are fit for purpose 9
   Forcepoint DLP 10
   Data in Motion Report Catalogue: Custom group for GDPR-relevant reports 11
   Workflow 12
8. Next Steps 15

Disclaimer
Although Forcepoint has made every effort to ensure the accuracy of this paper which has been prepared in good-faith, Forcepoint cannot accept any responsibility whatsoever for any consequences that may arise from any errors or omissions, or any opinions given. This paper does not constitute legal advice and Forcepoint makes no representation or warranty, express or implied, regarding its products including without limitation fitness of its products for a particular purpose. In no event will Forcepoint be liable for any direct, indirect, incidental, consequential, special, or punitive damages related to this paper. The information provided in this paper is the confidential and proprietary intellectual property of Forcepoint, and no right is granted or transferred in relation to any intellectual property contained in this paper.
1. Executive Overview

The EU General Data Protection Regulation (GDPR) is now in effect, which requires organizations to put a much stricter focus on data protection.

The Official Journal of the GDPR provides broad guidance around all aspects of data protection, but is not prescriptive in terms of the information security requirements needed to adequately protect private data.

In this series of papers, we provide an interpretation of the regulation and how it maps to information security technology. More specifically, we introduce how Forcepoint technology can be used to help you prepare for the GDPR.

Each paper focuses on key areas where technical controls play a part in demonstrating compliance of the GDPR. In this paper we examine the need for timely reporting of personal data breaches.

- The key topics of this paper include:
  - The need to prepare to report personal data breaches in a timely manner
  - Using a security framework approach to benchmark data protection programs
  - Data Loss Prevention as a technical measure to assist with the preparation to report personal data breaches in a timely manner
  - Behavioral Analytics as a technical measure to assist with the preparation to report personal data breaches in a timely manner
  - Cloud Access Security Broker (CASB) as a Technical Measure to assist with the preparation to report personal data breaches in a timely manner
  - Why Forcepoint’s Dynamic Data Protection technologies are fit for purpose
2. The Implementation of Timely Personal Data Breach Reporting

There are specific articles within the GDPR Journal that relate specifically to the need to prepare to report personal data breaches in a timely manner.

Chapter 4 (Controller & Processor), section 2 (Security of personal data):

**Article 33** – (Notification of a personal data breach to the supervisory authority): (1) ‘In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.’

**Article 34** – (Communication of a personal data breach to the data subject):

(1) ‘When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay’.

(2) ‘The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:

(a) The controller has implemented appropriate technical and organizational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

(b) The controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;

(c) It would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.’ The articles above refer to breach notification, not only to the supervisory authority but also the data subject. The imposed 72 hour breach response timeline means controllers will be keen to gather as much forensic evidence and context surrounding every incident, to quickly understand the risk posed to data and the organization as whole.

Generic cybersecurity frameworks like NIST lend insight as to how information security leaders organize their personal data protection and insider threat programs in conjunction with the breach response process. (https://www.nist.gov/cyberframework)

This paper will focus on the technical measures that support and integrate into an organization’s breach response process and that map to the post breach aspects of the framework (e.g., Detect, Respond, Recover pillars).

4. DLP as a Technical Measure to Assist with Timely Reporting of Personal Data Breaches

DLP is relevant as a primary technical measure to assist an organization with their GDPR compliance efforts and can be used in the implementation of timely personal data breach reporting.

DLP is described as a top technical control for the GDPR, both in a recent study published by Osterman Research titled “GDPR Compliance and its Impact on Security and Data Protection Programs” and in a Gartner paper titled “Focus on Five High-Priority Changes to Tackle the EU GDPR.” In “Cost of a Data Breach,” a 2017 Ponemon report, it was found that the extensive use of DLP reduced the cost of a breach by $6.80 per capita.

Where does DLP fit into the NIST CyberSecurity Framework?

DLP helps organizations “IDENTIFY” their personal data risk posture, which we discussed in Part 1 of this report. In addition, DLP is designed to “PROTECT” organizations by safeguarding high risk personal data flows through actions like block, encrypt, or quarantine; this was discussed in Part 2 of this report.

DLP also plays a part in the “DETECT,” “RESPOND,” and “RECOVER” stages. During the response to an incident, gaining a full understanding of the personal data being processed is critical (i.e., who processed it, what was processed and how it was processed); DLP can provide this detail or context.
Identify: Understand how much personal data is held and where it resides

Protect: Protect critical data from malicious attack and misuse

Detect: Provide rapid detection of insider threats and data incidents

Respond: Reduce response times to insider incidents to comply and protect the brand

Recover: Get back to “normal” & learn from event feedback to “prepare”

---

**Pre-breach**

**Post-breach**

---

**Forcepoint GDPR use cases**

- Inventory for personal data
- Map, manage and control personal data flows
- Prepare to respond in a timely manner

**Forcepoint technologies mapped to the GDPR**

- Data Loss Prevention
- Behavioral Analytics
- Cloud Access Security Broker

---

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

---

**How can DLP assist with the breach response process?**

- **DLP can capture the following information about data at rest:**
  - Location
  - Access rights
  - Date of creation
  - Date of last modification

- **DLP can capture the following information about data in motion:**
  - Source and destination of the personal data flow (e.g., cloud application, email recipient, URL)
  - The channel it was transmitted over (e.g., email, web, endpoint, USB, local print, copy/paste)
  - The action taken by the DLP solution (e.g., encrypt, block, confirm action with employee, allow)
  - Forensic evidence (e.g., file that contained the data, email message body, web transaction)
In addition, DLP technology must be able to integrate with and assist existing controls and policies around the response process. There are a few key areas where DLP can plug directly into an incident response process.

1) **Integrated workflow**

This provides the ability for a data incident responder to assign a DLP incident to another employee, or to escalate an incident to an employee’s manager. Ideally, incident responders would have a limited view of the DLP management interface. Better still, workflow and remediation could be done outside of the DLP console and leverage more accessible channels like email.

2) **Hierarchical management**

This feature provides customized views and access to the DLP management interface (e.g., an incident responder who only has access to the reports and incidents list, an IT administrator who only has access to the system provisioning features).

3) **‘Anonymization’ or ‘masking’ of personal data**

DLP analyzes and collects sensitive and personal data (e.g., a data subject’s personal data is captured as part of the forensic evidence for an incident). In order to monitor personal data, employees and other data processors must also be monitored. The very regulation designed to protect the data subject, also exists to protect the employee, also a data subject.

Consider a system that provides a risk-based, prioritized view of data incidents. In the initial stage, all dashboards, reports, and incident lists should be anonymized; not only is the data subject’s personal data hidden, so is the processor’s identity. When an incident is discovered, it’s brought to a response committee. If an investigation is warranted and agreed on by the committee, more personal data can be exposed to identify the individual processor after secondary authorization. A further authorization stage could be used by Legal and the Data Protection Officer, enabling the investigation team to access the full data behind the incident, including the data subject’s personal data.
5. Behavioral Analytics as a Technical Measure to Assist with Timely Personal Data Breach Reporting

The GDPR makes a reference to “with due regard for state of the art.” With that in mind, technical measures such as behavioral analytics fall squarely into this camp.

Behavioral analytics is a “rapid detection” technology that addresses the shortfalls of many security technologies by providing organizations visibility into critical events across vast amounts of logging or incident data. Data protection technologies like DLP are often accused of being a “noisy” security control because they generate countless alerts as data processors interact with sensitive data. This overload often causes incident responders to miss critical events, as they are buried in thousands of other events produced from their security tools and technologies. However, it is still important to collect this management information because this level of detail is required during an investigation and for auditing purposes.

How does behavioral and security analytics support the breach response process?

Behavioral analytics UEBA technology can be either a stand-alone solution programmed to work with specific data sources from multiple security controls, or purpose-built and integrated into individual security technologies. For example, some DLP technologies already leverage security analytics and machine learning to provide a risk-based prioritization of DLP incidents in order to help reduce the operational burden of managing these systems.

A malicious insider is one of the best examples at demonstrating why behavioral analytics technologies are well suited at detecting an insider threat that might lead to a breach. For example, an employee receives a bad performance review, their intent might change from good to malicious. Before their review, they worked within normal behavior patterns, accessing specific data in specific locations. After their poor review, they begin to access new servers, different types or volumes of data, and hoard this data into specific locations as they prepare to take this data off-site through various means.

In the event that an incident occurs or an investigation is warranted, investigators or responders are able to use this technology to dramatically speed up their investigation because they are able to see more context around the data incident and gain better understanding of intent.

Where does behavioral analytics fit into the NIST CyberSecurity Framework?

Behavioral and security analytics in general span across multiple stages of the NIST framework. This technology can speed up the detection of personal data incidents by analyzing network traffic, security events (including DLP incidents), and machine or employee activity to “baseline” normal behavioral patterns and flag up abnormal behavior. Machine learning is then used to provide operators with a risk-based and prioritized view of top security incidents that require further investigation, avoiding the aforementioned lengthy alert lists. In the event that an incident occurs or an investigation is warranted, investigators or responders are able to use this technology to dramatically speed up their investigation because they are able to see more context around the data incident and gain better understanding of intent.

While security analytics has definitely helped reduce the time to detection and the cost per breach, it is not the silver bullet that some might think. The detection of a breach is also done through other means, such as a fellow employee noticing unusual behavior, or by an outside entity (e.g., a local data protection authority or law enforcement agency). The changes in behavior, and the actions, are captured and provided in the entity timeline response to understand how behavior changed over time.
6. Cloud Access Security Broker (CASB) as a Technical Measure to Assist with Timely Personal Data Breach Reporting

A Cloud Access Security Broker (CASB) is software that monitors and controls access to cloud applications to enforce security policies.

Knowledge workers are avid consumers of a variety of different cloud applications to help increase their productivity and innovation. However, with the strict guidelines laid out in GDPR, these cloud services may pose a risk to maintaining compliance to that directive. Many organizations simply don’t have the visibility into the use of unsanctioned IT applications, referred to as “Shadow IT,” or for that matter, even the use of sanctioned IT. This is a major blind spot that creates a security gap for IT organizations when they must research a potential data breach.

Where does CASB fit into the NIST cybersecurity framework?

CASB spans across multiple tiers of the NIST framework. With an integrated DLP and CASB solution, organizations gain full visibility into where their data is located, the importance of that data, attempts to move it, and the circumstances of how it’s being accessed, which is critical when responding to an incident, and possibly preventing incidents before they even occur.

How does CASB support the breach response process?

One of the most compelling features of a CASB deployment is the ability to analyze the previous six months of a user’s cloud activity. This includes identifying sanctioned and unsanctioned applications accessed, the duration of use, and the different devices being used for access.

Most data breach investigators will agree the majority of incidents are, in fact, due to human error or a broken business process. Very few employees are consciously putting personal data at risk. CASB combined with DLP allows investigators to create a baseline of normal activity as it relates to cloud usage and then identify abnormal activity which can help them to determine if a user is a malicious insider, if they have been compromised, or are simply inadvertently not following policies or best practices.

7. Forcepoint Dynamic Data Protection Technologies are Fit for Purpose

Forcepoint User & Data Security technologies are formed of three products: Forcepoint DLP, Forcepoint Behavioral Analytics, and Forcepoint CASB.

The combination of these three technologies provides organizations with a comprehensive solution that lends insight into people’s behavior and motivations as they interact with critical data and IP everywhere. These solutions include all of the core capabilities listed above: Data Loss Prevention, Behavioral Analytics, and Cloud Access Security Broker.
**Forcepoint DLP**

Forcepoint has been a global leader in the DLP market for many years, both in terms of market share and feature set. In fact, Radacati rated Forcepoint as a Top Player in their DLP Market Quadrant report published October 2017.

**Management, monitoring, reporting and incident response capabilities**

Forcepoint DLP can streamline the response and remediation efforts during a data incident.

Forcepoint DLP provides organizations with a comprehensive set of tools in order to visualize, manage, and respond to data protection incidents. The solution centralizes policy management and reporting within the Forcepoint Security Manager. In this same console, existing Forcepoint customers are able to manage their Web and Email security gateway policies.

**Incident Risk Ranking (IRR)**

IRR is an industry-first, purpose-built DLP analytics tool that significantly reduces response times and focuses response teams on areas posing the greatest risk. It applies analytics and machine learning to cluster DLP incidents into cases of suspected data theft or broken business processes in order of business risk.

For more information on Incident Risk Ranking, please review a report by 451 Research®.

**Hierarchical management and access to management information and reporting:**

- While monitoring employees as they process personal data, organizations will generate and collect personal data on the processor (i.e., employee). The privacy laws designed to protect the citizen's personal data are also applicable to the employee.

- Forcepoint DLP has support for tiered access to the management console, including reporting and incident work flow.

- During a violation, sensitive data referenced within the report can be masked or anonymized to prevent system administrators and incident responders from identifying specific data or employees.

- Organizations can then put in place comprehensive policies and processes around who can access the non-anonymized data. The responder can only unlock the identity of the employee behind the breaches or view the incident’s PII data with the authorization of the DPO, HR, Legal, or the Workers Councils.

**Reporting, logging, and alerting:**

Forcepoint DLP comes with over 20 pre-built reports. Forcepoint DLP administrators can also create customized reports tailored to their needs.

**Data incident forensics**

Forcepoint DLP provides detailed information about the data around the incident.
During an incident, Forcepoint DLP provides the following information about data at rest:

- Owner
- Location
- Access rights
- Date of creation
- Date of last modification
- Direct access to copy of the file in question for more inspection
- Details on the policies that were violated and record counts by violation

Figure 3 – A Forcepoint IRR Report
Figure 4 - Forcepoint Security Manager provides anonymization capabilities to protect the privacy of employees and data subjects within the DLP Incidents.

Figure 5 - Data at Rest (Discovery) Report Catalogue: Custom group for GDPR-relevant built-in reports.

Figure 6 - Data in Motion Report Catalogue: Custom group for GDPR-relevant built-in reports.
The Properties tab provides more detail around the discovery incident. The level of detail varies depending on the file system the personal data is stored on.
During an incident, Forcepoint DLP provides the following information about data in motion:

- Source and destination of the personal data flow (e.g., cloud application, email recipient, URL)
- The channel it was transmitted over (e.g., email, web, endpoint, USB, local print, copy/paste)
- The action taken by the DLP solution (e.g., encrypt, block, confirm action with employee, allow)
- Forensic evidence (e.g., file that contained the data, email message body, web transaction)
- Access to other incidents from the same source or destination
- Details on policies violated and record counts by violation

Figure 10 - Data in Motion drill-down incident list showing Forensics tab

Figure 11 - From the Forensics tab, investigators are able to click on the source, destination or the channel to find other incidents that match these values as part of their investigation.
Detect and respond to a data incident

The History tab allows the responder to understand the audit trail of a particular incident and what action was taken, including those taken during the workflow, escalation, and remediation phases.

Figure 12 - The Properties tab provides more detail about the incident

Figure 13 - Details the history of an incident
Workflow

An incident responder can use the integrated workflow features to manage incidents; in addition, Forcepoint DLP provides the ability to use email for workflow purposes.

Remediate:
- A responder can remediate an incident (e.g., release from quarantine, run a remediation script to tag a file using an integrated data classification provider, or move a file to a safe location and leave a “stub” in its place).

Escalate:
- A responder can also escalate an incident to the employee’s manager or other function, like Data Controller or DPO.

Forcepoint DLP Summary

Forcepoint DLP enables organizations to identify the personal data “attack surface” through the inventory of personal data at rest across an organization’s infrastructure, which includes laptop devices, on-premises systems, and cloud storage.

Forcepoint DLP provides visibility and enforcement of how data is used and where it flows polices to reduce the risk of data loss. In the act of performing both of these tasks, Forcepoint DLP captures detailed information about how personal data is processed. This information is critical for incident responders as they go about their investigations. Forcepoint’s integrated DLP security analytics, Incident Risk Ranking, simplifies the job of DLP by automating the review of potentially thousands of DLP incidents to uncover patterns pointing to data loss or theft.

Forcepoint Behavioral Analytics

Forcepoint Behavioral Analytics enables security teams to proactively monitor for high risk behavior inside the enterprise. This security analytics platform provides unparalleled context by fusing structured and unstructured data to identify and disrupt malicious, compromised, and negligent users.

Forcepoint uncovers critical problems such as compromised accounts, corporate espionage, intellectual property theft, and fraud. This technology builds on the analytics found in Forcepoint DLP by drawing in more structured and unstructured data sets to apply advanced analytics and accurately identify employees putting the organization at risk.
Forcepoint Behavioral Analytics allows organizations to rapidly detect a broad array of insider threats that put personal data at risk through a combination of user activity monitoring, advanced analytics and DLP integration. In many cases, this detection can be done even before a breach occurs because an employee’s behavior change elevates risk to initiate early intervention.

Forcepoint Behavioral Analytics greatly reduces investigation time, enabling responders to ‘get to the truth’ much more quickly. It provides detailed forensics and associated context to investigators from multiple IT systems and from the endpoint. One of the most compelling features for investigations is video playback (i.e., a series of screenshots of the user’s desktop) because it provides the responder clear and unequivocal understanding of the employee’s intent. Was the user compromised or was this action intentional?

Forcepoint Behavioral Analytics use cases include privileged user auditing and compliance, internal and financial fraud monitoring, protecting critical infrastructure systems and acceptable usage policy enforcement.

Management, monitoring, reporting, and incident response capabilities
To start, incident responders will log into the analytics dashboard in order to get an executive overview of insider risk. If an investigation is warranted, they are able to drill down to specific employees and then into the entity timeline, where they have access to a deeper level of tools and evidence to support their investigation process.

Initially, this dashboard view can be anonymized, and, after a strict authorization process that might include involving stakeholders like Legal, HR or Workers Councils, an investigator can remove the anonymization to access the user details and start the investigation process.

The investigator can see which activities in the entity timeline contributed to the risk score and if necessary, they can drill down further into each activity. If the investigator needs additional detail, they can then click on the activity in question to get additional detail.
In addition, investigators can export the evidence that has been collected into a case file, which can be used to pass on to HR and legal teams in the event that further action is required.

**Forcepoint Behavioral Analytics Summary**

High assurance organizations use Forcepoint Behavioral Analytics to extend their personal data protection programs into broader insider threat programs that cover more use cases than that of data protection alone. Integrated state-of-the-art analytics bring additional value to an organization by highlighting employees behaving in ways that put the organization at risk. Identifying these employees early on and gaining clarity around the intent behind their actions results in a proactive data protection stance that reduces the risk of a breach, whether those actions are accidental, compromised, or malicious. Providing this tool to investigators significantly reduces their investigation times, which in turn reduces the liability to employers. The tool protects employees by better identifying mistakes and broken business processes.

Figure 16 - Event Issue Investigation

Unlike many other UEBA providers, Forcepoint Behavioral Analytics is able to analyze unstructured data, such as email and voice transcripts or instant messaging chat sessions.

This broader visibility means Forcepoint Behavioral Analytics is able to detect human indicators of risk which might result in a personal data incident, which can then be used to take proactive and preventative action. Forcepoint Behavioral Analytics assists investigators as they respond to incidents by presenting the deep contextual data collected as part of the analytic process in a single dashboard.
8. Next Steps

For more information on the GDPR, please visit our website: www.forcepoint.com/gdpr

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 1, "Inventory of Personal Data."

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 part 2, "Data Flow Mapping & Control."
About Forcepoint

Forcepoint is transforming cybersecurity by focusing on what matters most: people’s behavior as they interact with critical data and systems. This human-centric approach to cybersecurity frees employees to innovate by understanding the normal rhythm of user behavior and the flow of data in and out of an organization. Forcepoint behavior-based solutions adapt to risk in real time and are delivered via a converged security platform to protect network users and cloud access, prevent confidential data from leaving the corporate network, and eliminate breaches caused by insiders. Based in Austin, Texas, Forcepoint protects the human point for thousands of enterprise and government customers in more than 150 countries.

forcepoint.com/contact

© 2019 Forcepoint. Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint. All other trademarks used in this document are the property of their respective owners.