WHITE PAPER

exabeam

ADHERING TO GDPR SECURITY CONTROLS WITH EXABEAM

INTRODUCTION

The growing availability and potential rate of dispersion for personal data (name, address, transaction history, photographs, etc.) has generated new concerns over the security of its storage and handling. In 2016 The Council of the European Union responded with the European General Data Protection Regulation (GDPR), aimed at establishing a unified framework for securing every individual's right to the protection of personal data concerning him or her (Article 1). By May 2018, all organizations that collect, store, or process data on residents of the EU (including employees of the organization) will need to demonstrate full compliance. With an unprecedented financial penalty of up to 4% of global revenue for non-compliance, organizations must take swift and deliberate action to mitigate all potential risks.

While these standards apply specifically to holders and handlers of data, tools like Exabeam can be used by such organizations to reduce gaps in oversight and prevent threats to personal data. This solution brief will describe how Exabeam can help organizations implement effective security controls and best practices to achieve alignment with GDPR.

KEY POINTS IN GDPR

Existing Data Protection Standards across Europe are fractured and dated, failing to consider both technological and legislative advancements. The GDPR takes a fresh approach to new personal data protection requirements for all of Europe, including both technological and operational safeguards for data controllers (collection), data processors (processing, enhancement, and/or storage), and data subjects. Key points include the following:

Standardization- The GDPR aims to reduce ambiguity by providing a single data handling standard for all organizations that generate, process, enhance, or hold data on any EU citizen, regardless of where they are based (Article 3). This set of rules will be enforced equally by appropriate agencies from every country, with hefty fines for non-compliance.

Liability- The GDPR requires affected organizations to appoint an expert in the enforcement of these policies and procedures, known as a Data Protection Officer (DPO). It will be the responsibility of the DPO to:

- Oversee daily technical and operational data protection measures
- Carry out impact assessments for new handling or processing methodologies (Article 35)
- Serve as the first line of reporting after breach incidents (Article 33)

Additionally, both data controllers and data processors will share responsibility for the data transferred between them.

Risk Reduction- While roles and responsibilities are separately enumerated for controllers and processors, both parties are required to implement state of the art "technical and organizational measures," to mitigate the real risk to individuals incurred when handling personal data (Articles 25 and 32). These measures should include those that protect against the purposeful or accidental access, transmission, destruction, loss, alteration, or disclosure of personal data leading to physical or reputational damage of any EU citizen (Article 32).

Consent - Subjects of personal data are to be notified of the intent to collect and process relevant data, and organizations seeking use of this data must receive consent from affected individuals, except in cases where preserving the security of the individual overrides this contract. Individuals maintain ultimate "right of removal", i.e. extraction of such data at any point in time, as well as the right to not be the subject of automated decision making (i.e. wholly without human involvement), such as the analysis or prediction of aspects concerning the data subject's performance at work, unless authorized by the Union or Member State (Articles 5-22).

HOW EXABEAM CAN HELP

Exabeam is a Security Intelligence Platform that uses advanced data science to provide organizations with end-to-end detection, analytics, and response capabilities. Exabeam provides Data Protection Officers greater insight into network activity by using machine learning on existing data to establish behavioral baselines for all users and assets. By relying on a dynamic understanding of actual behavior, rather than hard-coded rules for expected activity, Exabeam fills a critical gap for organizations seeking comprehensive data access and controls monitoring. With specific regard to GDPR, Exabeam helps in three key areas:

1. External Threat Reduction- Exabeam works alongside existing security solutions, using machine learning and behavioral analytics to identify unusual activity that may be indicative of a hacker's attempt to find and access data.

2. Internal Threat Reduction- Exabeam works alongside identity and access management solutions to prevent security incidents resulting from the accidental or malicious abuse of allocated permissions. By flagging activity that falls outside the norm for a given user, Exabeam helps to detect potential data theft.

3. Oversight and Timely Notification- In additional to acting as a central point of intelligence in the customer's security ecosystem, Exabeam provides forensics and accurate reporting for better compliance reporting.

EXTERNAL THREAT REDUCTION

Exabeam improves insight into external threats by providing:

- Vulnerable account monitoring
- Anomalous account activity monitoring
- Threat vector monitoring

Hackers have a variety of motives for accessing an organization's network. The most familiar might include the exploitation of personal data for direct financial gain such as in the case of card skimmers that steal individual account details, point-of-sale compromise at a major retail provider, or even internal-based threats like creating new accounts to steal data and sell externally. However, financial institutions aren't the only ones at risk. In fact, any organization handling customer or employee data is a prime target, regardless of how that information might be used. Ransomware attacks, for example, are not just about the data itself, but also the reputational damage organizations would incur from jeopardizing the privacy and security of affected persons. Without appropriate controls in place to reduce the likelihood of such attacks, organizations create vulnerabilities for customers and employees.

Though attackers continue to refine their methodologies, the GDPR mandates that organizations keep up with evolving threats by employing "state of the art" technologies capable of scaling with the problem (Articles 25 and 32). Exabeam can bridge this growing gap between prevention and detection using the power of machine learning and intelligent alert prioritization. By highlighting deviation from observed behavior, Exabeam helps organizations quickly subvert previously unfamiliar attacks, and improve future defenses.

The following examples illustrate how Exabeam can enhance existing security measures and provide gapless coverage for external threats seeking access to sensitive personal data.

1. Proactively monitoring vulnerable accounts to detect unauthorised access- Vulnerable accounts may fit into one of three broad categories: 1) Accounts with access to the most sensitive data and systems, like account administrators; 2) Accounts that have high reputational visibility, like executive users, or 3) Accounts that are not typically closely monitored, like service accounts. All three types are prime targets for external threat actors seeking to acquire valuable personal data. Exabeam allows organizations to apply more focused attention to these accounts by monitoring their behavior compared to a baseline of their normal and expected activity.

2. Flagging unusual account activity to contain attacks before data is compromised- During or after breach by an external threat actor unfamiliar with the organization's systems and protocols, a compromised account will typically exhibit variation in routine behavior while the threat actor explores the network. This might include access from atypical locations, or access of databases and systems not relevant to the individual's usual duties. Exabeam uses machine learning to highlight this anomalous activity, helping organizations respond quickly and keep valuable personal data secure.

3. Highlight risky events in typical threat vectors (email/web) to prevent data loss- Many complex attacks start not with the compromise of user credentials, but with the receipt of dangerous malware that makes credential compromise and system breach possible. Where firewall, DLP, and proxy solutions may fail to recognize indicators of 'bad coming in' or 'good going out', Exabeam uses machine learning to flag access to bad domains, email phishing attacks, anomalies in data uploads, etc. to help identify threats earlier in the attack lifecycle and prevent compromise of personal data wherever it resides.

INTERNAL THREAT REDUCTION

Exabeam improves insight into internal threats by providing:

- High Risk account monitoring
- High Risk application monitoring
- Physical threat monitoring

Threats originating from within the organization are often the most difficult to detect, due to the intimate knowledge of systems and processes most malicious insiders use to cover their tracks. The GDPR directs organizations to carefully consider the risk of unauthorized access, alteration, destruction, or exfiltration of personal data at every stage of handling (Article 24). While identity and network access controls help organizations create a framework for how systems should be protected, they fail to account for the innumerable ways savvy, (or sometimes oblivious) employees will manage to disrupt these plans. This creates a gap in security that leaves sensitive systems and data highly vulnerable, risking the security of customers and employees alike.

Whether it's simply forgetting to remove access rights for a departing employee, or the deliberate attempt to steal customer data before heading to a competitor, employee-related compromise is a complex problem to manage. Exabeam helps address both accidental and intentional data compromise by highlighting unusual departures from normal behavior so that organizations are better prepared to investigate and mitigate the unexpected.

Exabeam's Advanced Analytics solution has been used to identify insider threats in financial institutions, retail, online service providers, telco, oil & gas, and many other verticals. Some examples of how Exabeam helps address insider threats to personal data specifically, includes the ability to:

1. Proactively monitor high risk / revoked access accounts to protect vulnerable personal data- Exabeam allows customers to prioritize accounts that are known to be at higher risk based on past performance. Rather than rely on rules for these known activities, such as an employee that's been warned for accessing sensitive personal data, Exabeam focuses exclusively on new and unusual risky behavior, elevating the risk score accordingly.

2. Proactively monitor applications containing personal data- Common applications like HR and CRM systems often have several levels of security with different functionality throughout. The most privileged layer often contains employee information like home address and phone number, and is only accessible by a specific set of authorized users for tasks like approving time sheets or referencing emergency contact information. In situations where greater account access is mistakenly allocated, sensitive personal data is put at risk. Exabeam identifies activity in applications that might appear normal for authorized users like HR or line managers, but unusual for others, like a junior engineer or sales rep. This type of anomalous activity can be an indicator of a potentially serious data breach.

3. Flag unusual physical events for signs fo personal data compromise- Many times malicious insiders attempt to evade digital footprints by relying on 'low-tech' methodologies for data exfiltration which are historically more difficult to track. This might include email or USB transfer of sensitive documents, or entering the office after hours to print client files. Exabeam can track all of these events to provide a holistic view of all activities to reduce gaps in secure data handling.

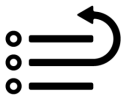
OVERSIGHT AND TIMELY NOTIFICATION

Exabeam improves operational efficiency by providing:

- Intelligent alert prioritization
- Automatic context enrichment
- Automatic timeline reconstruction
- Proactive threat hunting

The GDPR stipulates that collector and processor organizations must appoint a Data Protection Officer to assume responsibility for all technologies and processes implemented to ensure data security. The primary requirement for this role is to report breach incidents to local authorities within 72 hours (Article 33), and to affected persons as soon as possible. In order to provide accurate information, these Officers must first ascertain the breach's full scope and impact. Exabeam eases this burden by automatically connecting critical entities and events across data sources, identifying anomalous behavior which could indicate a breach and creating comprehensive event timelines for every potentially compromised user and asset.

In addition to forensic analysis of known breaches, Exabeam provides users the insights necessary to ensure daily alignment with security processes and procedures. Some examples of how these capabilities help organizations meet GDPR reporting compliance include the ability to:



1. Prioritize alerts to address serious breach incidents first- Exabeam takes in multiple data feeds including alerts from third party monitoring tools to help analysts and incident responders reduce the number of alerts they must review, and to prioritize those that represent the highest risk to the organization. With relation to GDPR, this should include those incidents with the highest likelihood of a breach.

2. Automate context enrichment and improve alert accuracy- Exabeam uses machine learning and statistical analysis to learn and enrich information available about an IT environment such as asset ownership, machine type, etc. This helps DPOs quickly understand the context in which an incident has occurred so they can ascertain the scope of the breach.

3. Automatically construct incident timelines to reduce response and reporting time- To provide comprehensive, end-to-end analysis of security risks, DPOs require insight into the full incident timeline. To manually construct this artifact, for every risk, would be a daunting task. To speed-up the process, and reduce potential human error- Exabeam automatically reconstructs each incident in the form of a timeline which includes all user behavior (both normal and anomalous) surrounding an incident. This shortens investigations from several days to seconds and makes it easier for DPOs to meet their 72-hour time limit on reporting.

4. Proactively search for similar schemes to reduce vulnerability- Sometimes the best defense is a good offense. With heavy fines looming for non-compliant organizations, DPOs should seek cost-effective solutions for threat prevention, in addition to those designed for detection and mitigation. Exabeam's Threat Hunter allows users to search for threat indicators, or behaviors characteristic of the formative phases of attacks. This allows

CONCLUSION

While the task of updating data protection policies and practices might appear daunting, employing tools specifically designed to improve ecosystem vigilence gets organizations a long way towards securing sensitive assets and information. By equipping Data Protection Officers with the ability to more effectively monitor and respond to all data access activities, Exabeam helps organizations to meet both technological and operational requirements of GDPR.

For more information, please visit www.exabeam.com, or send an email to info@exabeam.com.