observe IT
a division of Proofpoint

SOLUTION BRIEF

Insider Threat Management and Data Privacy Compliance

PREREQUISITES FOR PROPER USE

- Add to records of processing activities
- Implement internal control system
- Exclude personal data
- Handling electronic communication
- Pseudonymize PII Data for First Level Responders
- Categorization of employees
- Consideration of the Works Council
- Cross-border data-sharing considerations
- Exchanging data with third parties

Introduction

McKinsey estimates that more than 50% of all data breaches involve the action of an insider.[1] Colleagues and partners are more global, transitory, and connected than ever, not just from their respective offices, but often from a public place or home. The pressure to meet customer demands for organizations and their workforce is more significant than ever. It's no wonder as security mistakes and instances of users being compromised or impersonated are very common, not to mention data theft and system misuse. This calls for a people-centric solution that can protect both the organization and its workforce and their workforce. ObserveIT Insider Threat Management (ITM), a division of Proofpoint, helps organizations protect against data loss, malicious acts, and brand damage involving insiders acting maliciously, negligently, or unknowingly.

ObserveIT ITM: Data Privacy Compliance

TECHNICAL PRIVACY SAFEGUARDS IN OBSERVEIT	BUSINESS OPERATIONS ENABLERS THROUGH OBSERVEIT
✓ Anonymize data to avoid profiling	✓ Delegate Access to "Need to know" Users
✓ Exclude non-pertinent data from collection and alerts	✓ Support data subject requests in a human readable format
✓ Notify users proactively of security monitoring of risky user activity	✓ Decrease incident response & evidence gathering times
✓ Notify a user when an action breaches policy	✓ Facilitate faster and efficient audits
✓ Configure data retention policies	

Maintaining privacy is as much a cultural shift as regulatory compliance. Existing business and technology practices must be balanced with workforce best practices and organizational needs to protect itself. This cultural understanding will modify how any security technology is used. After all, standard security technologies today already collect sensitive employee information for legitimate employer interests.

In this document, we discuss the European Data Protection Directive (GDPR) & California Consumer Privacy Act 2018 (CCPA) as well as other relevant, unique obligations imposed by data protection regulations around the world. We respect the legitimate interests of employers and the reasonable expectations of employees around their personal data and their legal right of access to said data. We describe the risks that are inherent in the use of new technologies and addresses the proportionality of certain scenarios in which Proofpoint technologies are used.

THE DRIVE FOR INSIDER THREAT MANAGEMENT (ITM)

The Ponemon Institute found a 47% increase in insider-driven data breaches with their Cost of Insider Threats 2020 Report . When combined with the cost of dealing with each insider driven incident (on average, $645K) and the length of time to mitigate & contain (on average, 77 days), the total cost of insider threats for the median enterprise is $11.45M on an annualized basis.

Cybersecurity has traditionally focused on external threats with outside-in technologies. But, we cannot rely on preventative measures only to protect intellectual property, customer and employee information, and critical systems and manage insider risks. They're already inside, and it's hard to understand people through analyzing logs. With ObserveIT ITM, organizations can significantly reduce the risk of security incidents through contextual intelligence that ties risky user activity with data movement to quickly answer the "who, what, where, when, and why." This enables real-time detection and rapid response on top of any preventative measures of an insider threat management program.

Organizations face three primary challenges when it comes to effectively tackling risks from insiders to the organization's employees, systems, and data:

Alert Fatigue

As organizations use more and more security devices, the number of alerts increase as well. Each time, security analysts decide whether the warning is real, or not, and requires further validation. These decisions are more complicated when it comes to insider risk alerts. They need analysts to have user context around the alert, which is time-consuming and manual with traditional outside-in focused solutions.

Disparate Security Procedures

Responding to insider driven incidents is even more challenging than with a typical incident driven by an external threat. On top of manually correlating user context from multiple disconnected logs, the security team must collaborate with other teams, who typically don't understand log data. Organizations have neither the expertise nor the time to respond rapidly when faced with such threats. For example, in many banking institutions, the Anti-Money Laundering (AML) teams, cybersecurity operations, and investigative teams have separate reporting structures, although most laundering now occurs in the cyber realm.

Data Breach Notification

Under most data privacy laws, Data Controllers must notify the relevant national data protection regulators, and potentially the individual data subjects affected. Within a short period after a Personal Data Breach occurs, organizations must provide details of the breach, assess possible consequences, and initiate remedial action. A true criminal activity requires evidence to be presented within forty-eight hours of an incident, which means organizations cannot rely on existing forensic solutions that usually take days or weeks to provide answers.

Disclaimer: This whitepaper is provided for informational purposes only and should not be considered binding on Proofpoint. You should seek legal advice for your specific scenario.

The ObserveIT platform correlates user activity and data movement, empowering security teams to identify user risk, detect insider-led data breaches, and accelerate security incident response. The detection and response capabilities leverage a powerful contextual intelligence engine and a library of over 400 threat templates drawn from customers and leading cybersecurity frameworks. Thus, ObserveIT delivers a people-centric solution with rapid time to value and proven success streamlining insider threat programs.

PRIVACY CONSIDERATIONS

Lawfulness of Processing

For processing to be lawful, personal data must be processed with the consent of the data subject or unless there is another legitimate basis under governing law. Users within the organization must be informed of the security policies and of the monitoring of their business activity to protect against data exfiltration, system misuse, and policy violations. To achieve an adequate level of protection for companies, is it permitted by privacy laws to engage external experts, tools, or services to support internal security measures. For such use cases, there are stringent regulations within the laws to ensure that your infrastructure supports the required data protection level. Essential conditions for compliance fulfillment are described in this document under “Prerequisites for proper use.”

Employee Workplace Visibility

The visibility into electronic communications in the workplace is considered to be the main potential infringement of employee privacy. That said, organizations already have significant visibility into data movement, endpoint activity, and cloud usage from existing security solutions. Therefore, regulators recognize the need for visibility into risky employee actions as long as the solution meets certain conditions, listed below.

First, employers must weigh the proportionality of the security visibility measures they are implementing against the risks faced by the organizations and the impact on their users. Second, employers must explore additional ways to mitigate the impact or reduce the scale of the personal data processed. As an example of good practice, this consideration could be undertaken via a data privacy impact assessment before the introduction of any security technology.

An individual’s right to privacy is a cornerstone of today’s society. At the same time, an organization’s intellectual property and sensitive business information, built by the hard work of its workforce, is its lifeblood in today’s competitive world. A people-centric ITM program achieves a balance of user privacy and data security in adherence to data privacy regulations. This means ensuring user privacy while technology is in use while providing security teams have early warning and contextual awareness of data loss, risky behavior, and system misuse by insiders. We know the ObserveIT platform is powerful. But it’s also flexible enough that our customers achieve the balance of security and privacy with their security program.

Disclaimer: This whitepaper is provided for informational purposes only and should not be considered binding on Proofpoint. You should seek legal advice for your specific scenario.

More Information

To meet these strict data privacy requirements, Proofpoint offers the following documents for your records covering groups of related products. Proofpoint fully supports data privacy requirements and assists its customers in achieving the objectives of the regulation. Of particular importance are the data processing agreements (DPAs) that you need for your process directory.

You can find these on our website for Proofpoint Data Processing Agreements and related Standard Contractual Clauses (Model Clauses): https://www.proofpoint.com/us/legal/trust/dpa

PREREQUISITES FOR PROPER USE

Successful implementation of a people-centric security solution involves adapting the technology to comply with the requirements set forth below.

Add to Records of Processing Activities

Article 30 of the GDPR requires organizations that process personal data to maintain a record of their processing activities. Organizations need to maintain an internal record of processing activities and to have it readily available, in case a supervisory authority requests to review those records. The customer should add Insider Threat Management to its internal data processing directory.

Implement Internal Control System

Misuse of an organization's data by employees, whether the data is internal to the organization or related to its stakeholders, would cause that organization to be in violation of GDPR and other privacy laws, even if it had put in place appropriate security measures. Implementation of an internal control system (ICS) supports the organization's regulatory compliance efforts. This consists of internal control and monitoring systems. The control system provides the measures to review the organization's activities and ensures the proper recording of business transactions and compliance with privacy principles. The control system makes sure that only staff who need to view this data are given access to it and are trained on how to use it properly.

Private Use and its Intensity

Current IT operating guidelines range from a complete ban on personal usage to specific framework conditions for permissible private use. IT operating policies should include clear rules on whether private use of corporate IT is permitted. If this is the case, the scope to which private use is allowed must be regulated. For example, companies can exclude sensitive applications and personal information from being captured.

Handling Electronic Communication

Communication within a company today is predominantly electronic. It is recommended to specify how these communication means will be processed and to inform the employees how and to what degree the activities will be monitored and the purpose of that monitoring. Typically, there are regulations for emails, chats, file directories, which are indispensable for fulfilling accounting, corporate, and other regulatory obligations.

Pseudonymize PII Data for First Level Responders

Anonymize personal data where possible and only use information that identifies an individual when the risk to the organization's security is clear and documented. ITM can completely obfuscate and anonymize user data such as name, computer, and relevant metadata. A Chief Privacy Officer or equivalent would then have to approve any request for revealing a user's data.

Categorization of Employees

When implementing an ITM solution, it is not advisable to handle the data of all employees the same way. The employees should be categoritzed and divided into target groups with individual guidelines. Confidential emails from certain recipient groups (e.g., works council) can be excluded from processing by these systems or be processed under other rules. More specifically, merger and acquisition (M&A), investment banking and sales teams are often communicating with entities (such as outside legal counsel, M&A targets, customers, and partners) outside the organization, yet their email communication and document sharing are of the highest value. In such cases, traditional data classifications are less relevant than the context of the data movement and communications. An ITM solution provides that contextual awareness.

Disclaimer: This whitepaper is provided for informational purposes only and should not be considered binding on Proofpoint. You should seek legal advice for your specific scenario.

Consideration of the Works Council

Every company that is big enough to have a Works Council in Germany would have had to get specific approval or operate under some other permission from their works council to deploy any security services. Regarding concerns of privacy, customers can find related information on our Trust Site. There are a series of whitepapers outlining Proofpoint's commitment to GDPR compliance in general, as well as product-specific whitepapers showing how certain Proofpoint products can support a company's privacy compliance.

The Works Council as Part of the Internal Control System

The purpose of this right to supervise activities is to protect individual workers against anonymous inspection systems. Employees compliance with the IT operating guidelines and the guidelines themselves should be reviewed regularly. In this role, the works council can fulfill its duty to participate and monitor the proper operation of the security solution in terms of IT guidelines and employee rights through an auditing function.

Cross-Border Data-Sharing Considerations

GDPR Article 47, "Binding corporate rules," allows internal international information sharing. These corporate rules should include all essential data privacy principles and enforceable rights to ensure appropriate safeguards for transfers or categories of transfers of personal data.

Exchanging Data with Third Parties

Where the processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organizational measures, in such a manner that processing will meet the requirements of the regulation and ensure the protection of the rights of the data subject.

LEARN MORE

For more information, visit **observeit.com**.

ABOUT OBSERVEIT

The ObserveIT platform correlates user activity and data movement, empowering security teams to identify user risk, detect to insider-led data breaches, and accelerate security incident response. Leveraging a powerful contextual intelligence engine and a library of over 400 threat templates drawn from customers and leading cybersecurity frameworks, ObserveIT delivers rapid time to value and proven capability to streamline insider threat programs.

observe IT
a division of Proofpoint