Teramind for GDPR

Privacy and Data Breach Protection for GDPR Compliance

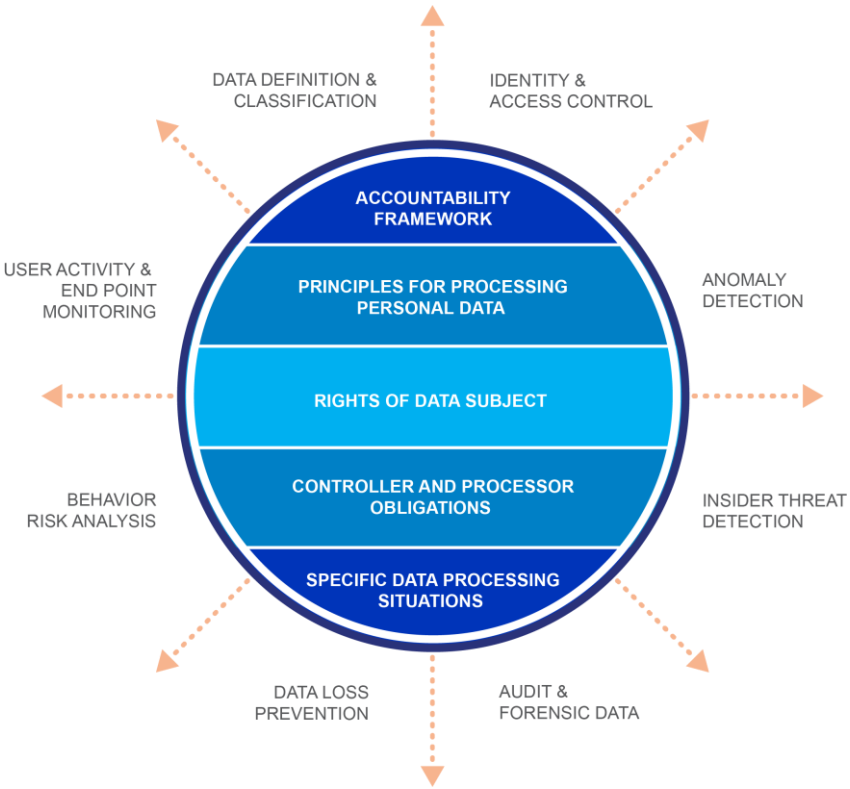
TERAMIND

www.teramind.co

Data privacy protection and data loss prevention on a unified platform

GDPR and similar laws such as CCPA, LGPD require organizations to implement policies and procedures with respect to collection, treatment and management of data, a plan to detect a data breach, regularly evaluate the effectiveness of security practices, and document evidence of compliance. With that, GDPR effectively mandates organizations to implement best practices for privacy and data security.

This is especially critical for companies engaged in employee monitoring as the privacy laws significantly impacts the way companies handle personal data. Whether evaluating employee productivity or guarding against insider threats, every company needs to incorporate employee privacy into its plans.



Teramind helps organizations deploy employee monitoring solution within the scope of the privacy and business as usual (BAU) restrictions set by compliance regimens. At the same time, its powerful DLP capabilities enable ongoing compliance monitoring and data breach prevention. Finally, if a breach does happen, Teramind's powerful auditing and repotting tools can help DPO, CSO and other security and risk management (SRM) leaders investigate, report on and prepare risk mitigation plans.

Data breach is a costly challenge facing privacy:

Organizations aren't prepared for GDPR

Only 35%

of them have a data breach reporting procedure that is aligned with GDPR requirements. Source: Deloitte.

Steep penalty for failing to comply with GDPR

$20M / 4%

of revenue is the maximum penalty for organizations who fail to comply with GDPR. Risk of litigation, loss of brand reputation and customer loyalty are also likely outcomes.

Data breaches are costly

$350M

damages is associated with a large data breach. For smaller breaches, the average is about $$3.86 Million. Source: IBM and the Ponemon Institute.

Loss of customers due to a breach incident

69%

A 2019 study found that 69% of customers would avoid a company that had suffered a data breach. Source: Verizon.

Privacy: Data vs People

Privacy isn't just about 'data-privacy. A data-breach impacts your employees and customers and in turn, effect your business indirectly. Some of these can be significantly damaging than direct penalties.

For example, A recent Gartner survey found top three concerns of businesses in respect to data breaches were brand damage, loss of costumer trust, and financial impact post-incident.

Teramind helps you guard your customer data, protect your financial interest and IP while at the same time, ensures that your employees' privacy is upheld.

Key privacy challenges and how Teramind can help

With the introduction of GDPR and similar upcoming laws, companies are tasked with walking a tightrope, simultaneously balancing their business interest, customers' data security and their employees' privacy. Here are some key challenges they are facing and how Teramind can help find a balance between privacy and security:

Privacy challenge	How Teramind can help
Broad scope, BAU and legal complexity	
Territorial scope, difficulty of demonstrating business as usual (BAU) intent etc. make it difficult to implement a cohesive privacy strategy.	Teramind's employee monitoring features are tied to specific productivity, threat prevention and other well-defined business objectives helping you demonstrate BAUs.
Conflicting interests of privacy, security and productivity	
Companies use employee monitoring to protect their IP and business, yet such software can introduce divergent interests among stakeholders, customers and employees.	Autonomous features such as auto-reduction, access control on a need-to-know basis, automated-data purge etc. limit the amount of information collected without compromising the fundamental purpose of monitoring.
Disparate technology	
There are hundreds of solutions in the market promising privacy compliance, from FA, DLP, UEBA, PAM, CASB, DCAP, etc. confusing customers about which solution to use.	Teramind combines user activity monitoring, data loss prevention, audit and reporting capabilities all in a single product. Additionally, Teramind can be combined with your existing SIEM, PM and HRM system to orchestrate security and privacy.
Difficulty of PII data classification	
PII, PHI, PFI data are difficult to detect especially when scattered among unstructured datasets or in motion making them harder to protect.	Teramind's intelligent classification engine automatically discovers privacy data on-the-fly, reducing effort and difficulty of data classifications.
Continuous fnforcement	
Ensuring continuous compliance is difficult to achieve without a monitoring policy in place.	'Always-on' system ensures employees and admins are following company policy and privacy regulations all the time even when offline.
Stakeholder engagement	
Implementing a privacy policy is an organization-wide measure, but existing solutions are often highly technical and often designed for specific users.	Teramind is designed to be used by DPO, security analyst, HR manager, CIOs, CEOs. The dashboard can be configured for each user's specific information requirements, security privilege and privacy.

Teramind for GDPR: Features at a glance

Privacy-focused monitoring:

Real-time monitoring protects sensitive data from insider threats while dynamic blackout and selective recording features ensure privacy for personal data.

Ongoing compliance enforcement:

Behavior and activity monitoring platform continuously enforces policies and takes immediate action on detection of anomalies or rule violations.

Data discovery and classification:

Find and categorize personally identifiable data to apply data privacy and data exfiltration rules.

Authentication and access control:

Identity based authentication and segregated access control prevent unauthorized PII access or sharing.

Data risk mitigation:

Identify high risk employees, policies and system components that may put your GDPR and other compliance initiatives at risk.

Collect evidence with conformance:

Screen recording only during policy violation incidents allows for collection of forensic data, while conforming to the privacy and record keeping boundaries set by GDPR.

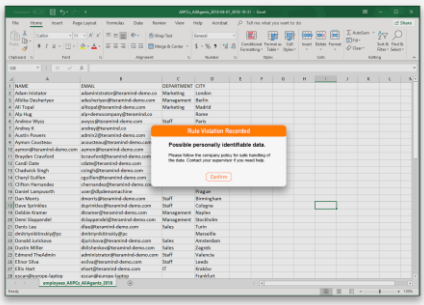
Audit ready:

Session recording and immutable logs keep track of access, entitlement and rectification related information.

Reporting for the entire compliance team:

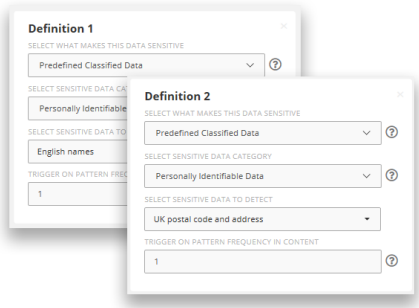
User activity and rule/policy conformance and violation reports are available for the Controller, DPO, auditors and other members of the compliance team.

Teramind for GDPR delivers immediate business benefits



Protecting the principles relating to processing of personal data

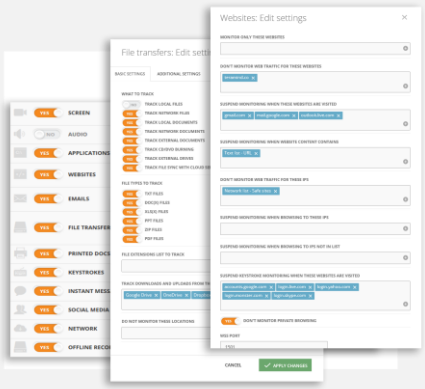
Teramind ensures data is processed lawfully and not exfiltrated to unauthorized systems and mediums. Data classification can be set to identify personal data and then policies and rules can be created using advanced OCR and fingerprinting features to detect and restrict access to such data automatically.



Going beyond personal data

Different privacy laws may require treatment of special categories data. For example, GDPR's treatment of processing of genetic data, biometric data or HIPAA's requirements for health data vs., PCI DSS impose on personal financial data.

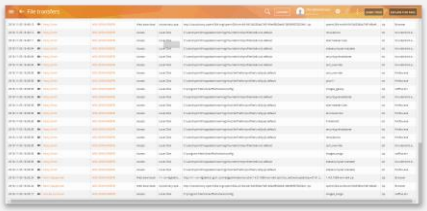
Teramind features built-in classifications for many types of PII, PFI, PHI data as well as the ability to define custom data types using keywords, regular expressions, and patterns. Custom data types can be created for your unique needs.



Data protection by design

Teramind ensures data is processed only in the context it is required to be processed under the relevant privacy laws. Monitoring settings can be configured to only record the necessary information. For example, keystrokes or screen capture can be disabled when a user enters their personal banking site or personal emails.

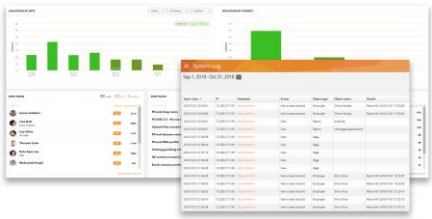
Organizations can implement Teramind with specific monitoring features and recording of events only at policy violations, narrowing the scope of user activity recording and ensuring a privacy-friendly implementation. Administrators' privileges can be limited with tiered access to only view specific sets of data. Custom alerts and prompts can be set up to inform users what data is collected and allow them to acknowledge any action being taken.



Privacy governance and record keeping

Privacy regulations including GDPR requires organizations to maintain an up-to-date record of the locations and usage of personal information and demonstrate safeguards used to protect the data. This could be information in files, databases, email, unstructured data, backups, DMS, knowledge bases, or anything else that houses data.

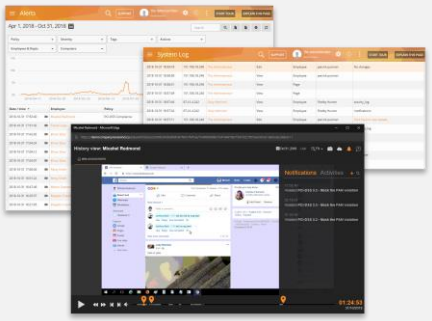
Teramind keeps detailed logs of information and record who's accessing what data, how the data is flowing through the organization and then create perimeter rules to safeguard their access or usage.



ISMS/ISO 27001-based data security

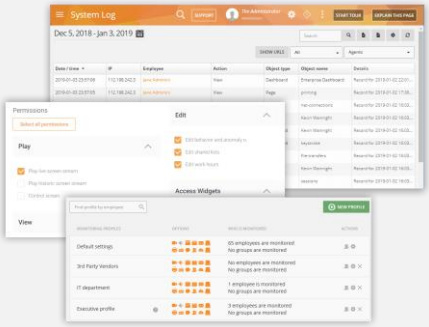
GDPR, CCPA, LGPD all require companies to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

Teramind is well suited to help implement many of these security requirements. For example: implement access profiles for each staff, restrict or block sharing of encrypted content, limit use of FTP/Cloud sharing sites, prevent the viewing of sensitive data by employees, prevent unauthorized decryption operations on files and more. Additionally, Teramind is an ISO 27001 certified company and as such ensures that our own security and privacy policy can meet our customers requirements.



Breach notifications and reporting

Teramind protects you from insider threats and data breaches. However, on the worst happens, Teramind can provide full forensics with respect to a data incident, and a video recording of the event. Detailed alert reports can be exported including any security incidents and what actions were taken in minutes superseding the 72-hour limit set by GDPR. Session recordings and history playback can be used to provide proof for further forensic investigation.



Serving the needs of security and risk management (SRM) leaders

Some key responsibilities of SRM leaders such as the DPO, CSO, HR and other privacy officers are to monitor the effectiveness of the compliance measures and identify any risk associated with a company's data processing operations.

To help these various stakeholder, Teramind employs a role-based access management system ensuring that both internal and external users are monitored and audited properly. Additionally, there's a Risk dashboard that identifies policies, rules, personnel and system objects that are at risk.

Continues monitoring of privacy codes of conduct

Teramind monitors all employee, contractor and third-party vendor activity including file access, apps and website usage and all other interactions within the local, network or Cloud environments. Business etiquette rules can be created to train the users about nonconformity and influence corrective behavior.

Supported on all major platforms

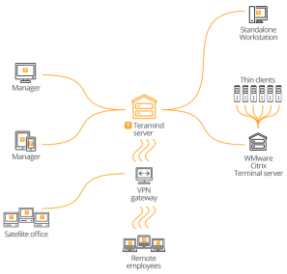
Windows 8 & Up	Citrix XenApp® & XenDesk®	Windows Server 2012 & Up	VMware Horizon	Mac OSX

Flexible deployment options

Cloud

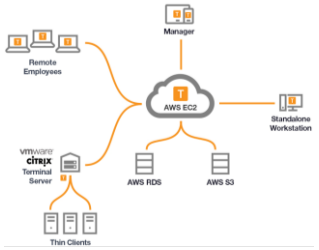
No server maintenance, only install Teramind Agents on the machines you want to monitor and set up your users, policies and rules and let us take care of the rest.

On-Premise



Control your Teramind implementation in its entirety. Leverage LDAP groups and users to identify which users and groups to apply which policies and rules to.

Private Cloud



Use your own secure, scalable private cloud implementation including AWS, Google Cloud, Azure and more.

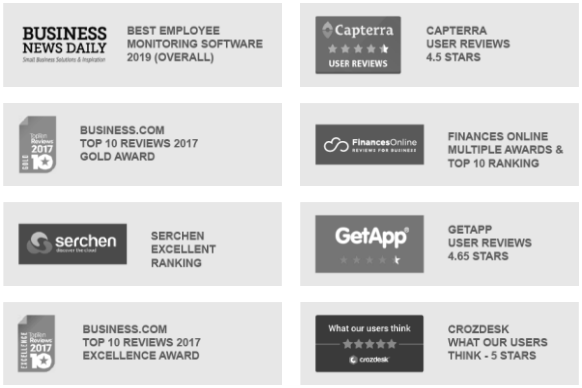
About Teramind

Founded in 2014, Teramind is a leading, global provider of employee and user activity monitoring, user behavior analytics, insider threat detection, forensics and data loss prevention solutions.

Over 4,000 organizations in finance, retail, manufacturing, energy, technology, healthcare and government verticals across the globe trust Teramind's award-winning platform to detect, record, and prevent malicious user behavior in addition to helping teams drive productivity and efficiency.

Teramind is headquartered in Miami, Florida, with sales and support operations around the world.

Teramind is Ranked #1 by:



Live Demo

www.teramind.co/sim

www.teramind.co

hello@teramind.co

+1-212-603-9617