Teramind DLP

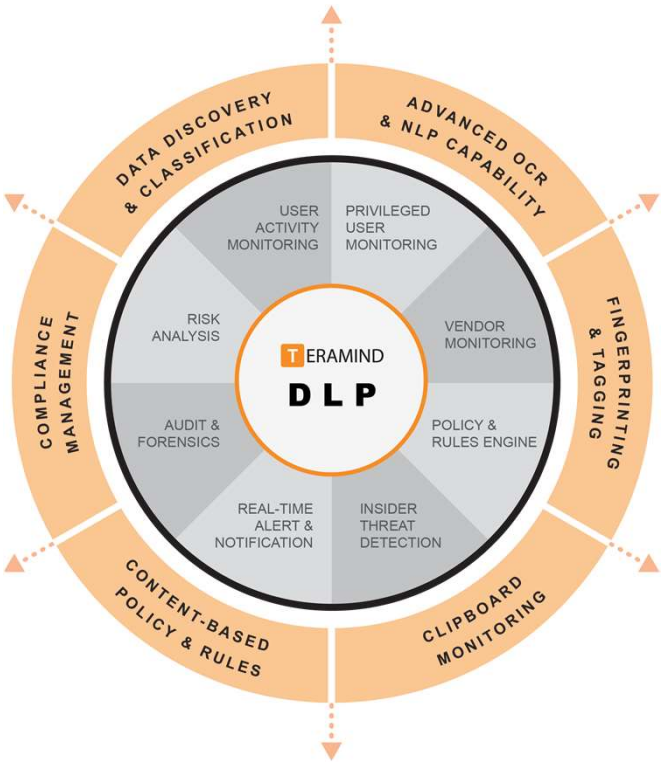
Effective Endpoint Data Loss Prevention

TERAMIND

American Technology Solutions

Effective defense against data breaches, data leaks and IP theft

Data Loss Prevention (DLP) is a strategy for ensuring your employees and vendors do not accidentally or intentionally share sensitive and company confidential data outside your organization. A DLP solution utilizes content discovery, digital inspection techniques and contextual analysis to identify and categorize sensitive data and IP. Next, policies and rules are created for data usage scenarios. The system then monitors user actions; validates them against the DLP rules and takes appropriate action if and when a rule condition is triggered. Actions could include stopping the action, blocking the user, alerting an administrator, requesting management override and more.



Teramind DLP: Data loss prevention, user activity monitoring and insider threats detection in a single platform

Teramind's 'user-centric', endpoint Data Loss Prevention solution goes beyond traditional DLP approaches by adding intelligent behavioral analysis to identify human factors like malicious intent, errors or accidents allowing you to implement effective protection against data breaches and other exfiltration attempts. Teramind DLP provides the best return of investment for organizations of any size. It's designed to assist SMBs, enterprises and the public sector address data loss, cybersecurity and insider threats. Additionally, Teramind's compliance management features help you conform with compliance regulations including GDPR, HIPAA, PCI DSS, and ISO 27001.

Teramind DLP: Features at a glance

User activity monitoring:

Monitors all user activity including third-party vendors and privileged users for 12+ system objects like: website, application, keystroke, IM, email, network etc.

Powerful policy and rules engine:

Teramind comes with hundreds of pre-built rules, templates and data categories. Create your own rules with an intuitive, visual Policy & Rules editor.

Insider threat detection:

Intelligent user behavioral analysis combined with session recording & playback, real-time alerts, immutable logs etc. help identify insider threats before they become critical issues.

Content discovery and classification:

Discover and identify sensitive information from structured and unstructured sources. Built-in classification templates for Personally Identifiable Information (PII), Personal Health Information (PHI), Personal Financial Information (PFI) etc.

Advanced OCR:

'On the fly' content discovery with advanced OCR, natural language processing (NLP) and RegEx. Detect sensitive data inside images, applications and even videos preventing steganographic data exfiltration.

Clipboard monitoring:

Teramind's Clipboard Monitoring and Interception feature allows you to protect sensitive data from being shared through the clipboard copy/paste operations.

Fingerprinting and tagging:

Teramind's powerful fingerprinting and tagging features identify important documents and files and then monitors their usage so that you can keep track of your data even when modified or transferred.

Compliance management:

Teramind has built-in support for compliance and standards like GDPR, HIPAA, PCI DSS, ISO 27001 etc. and can be adapted to support other regulatory requirements with its powerful Policy & Rules editor and various monitoring and reporting capabilities.

Risk management:

Identify high risk users, policies and system objects on the dedicated Risk Dashboard. Sophisticated risk scoring helps identify and focus on high risk areas.

The causes, impacts and frequency of data leaks prove businesses need data loss prevention:

Financial loss due to a data breach is huge

According to a 2018 study conducted by the Ponemon Institute, the average cost of a data breach rose by 6.4% with a range of $3.86M - $350M.

$3.86M avg. cost of a breach

$350M for larger breaches

User Privilege Puts Sensitive Data at Risk

According to a survey of 400,000 member online by Cybersecurity Insiders published on The Insider Threat 2018 report.

37% excess privilege

34% increased amount of sensitive data

Data leak incidents are growing at an alarming rate

The rate of data breaches in 2018 reported by federal survey respondents is 57%, more than 3x higher than what they measured 2 years ago.

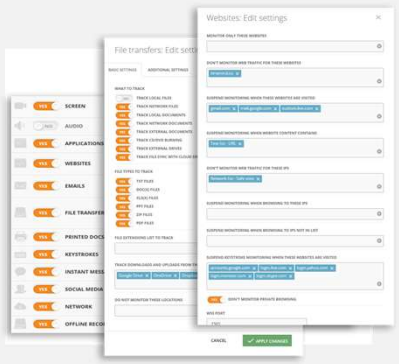
300% increase in data breaches in two years

IP losses due to cyber crime is hurting companies globally

McAffe estimated that annual losses for the US from cyber crime targeting IP is about $12B and perhaps $50B to $60B world-wide.

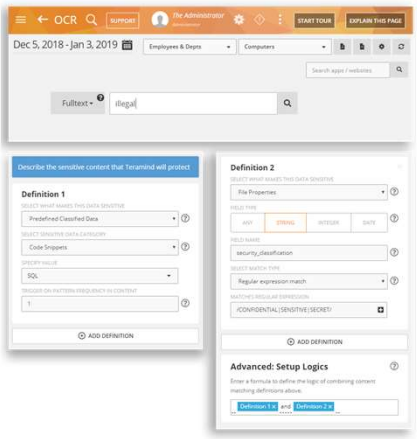
~60B is the upper range for annual global loss in IP

Teramind DLP delivers immediate business benefits



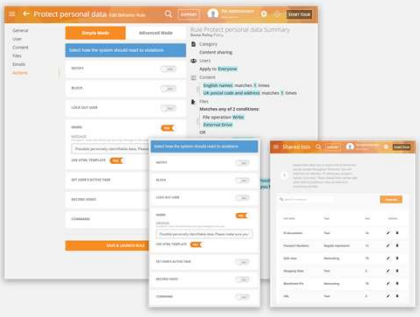
Organization-wide data visibility and control

Teramind monitors every action that a user makes for over 12 objects including screen, apps, websites, files, emails, etc. You can view the user activity with associated security KPIs, alerts and logs on a central console. Control who can access what information, when and how – all from the industry's most powerful and user-friendly DLP Management Dashboard. Drag-and-drop widgets to build your own enterprise dashboard to have organization-wise data visibility and control even from your mobile phone or tablet.



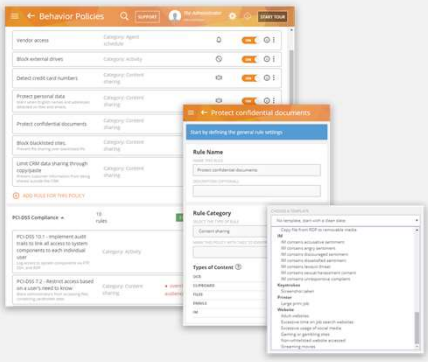
Auto discovery and classification of sensitive data

Teramind has built-in templates for many classified and sensitive data types like Personally Identifiable Information (PII) Personal Health Information (PHI), Personal Financial Information (PFI), OGD, GSCP, Special codes etc. Custom categories can be created Regular Expression (RegEx) and Natural Language Processing (NLP). Combine advanced OCR, fingerprinting and tagging technology with multiple logic, file origin, file properties and data content to discover classified information in structured/unstructured data or even images 'on the fly'.



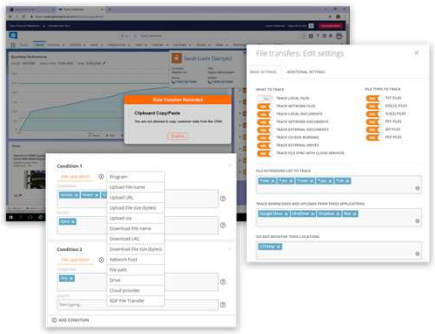
Powerful policy & rules editor

Teramind's flexible platform and powerful rules engine allows for creation of rules and policies to easily address data loss prevention needs of any organization. The visual Policy and Rules Editor enables administrators to define highly complex rules for very specific use cases with oversight on all internal and external disk activity, keystrokes, application usage, instant message, social media posts, and much more. Use built-in shared list or upload your own data/text patterns, regular expressions, or networking protocols to create IP black/white listing, define safe or restricted app and websites and do much more.



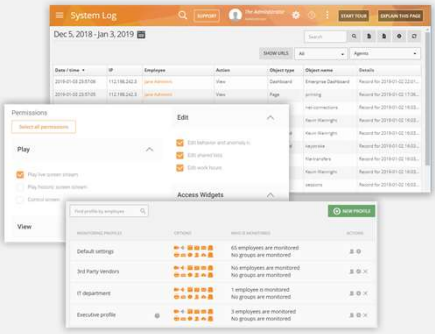
Predefined DLP policies and rules

The core of the Teramind platform is its automation. Teramind comes with over 200 pre-defined policies and rules. For example: block email containing sensitive keywords, stop uploading of a confidential document, detect screen capture, prevent use of external drives etc. The templates cover virtually every use case of data loss prevention, insider threat detection and compliance requirements. Just pick a policy or rule template and all the data definition, content source, condition will be set automatically for you to edit.



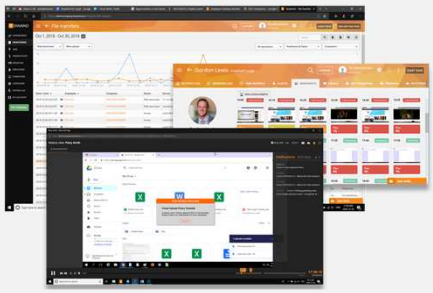
Prevent data leaks over external drives, network and Cloud services

Use file transfer rules to block external drives, clipboard rules to prevent sharing of confidential information like customer data outside the CRM or restrict download/upload operations in the Cloud for certain file types or all files. Keep an eye on the social media or IMs and block them automatically if a potential data leak event is detected. There are hundreds of use cases where Teramind can proactively defend your data from malicious or accidental leaks or misuse.



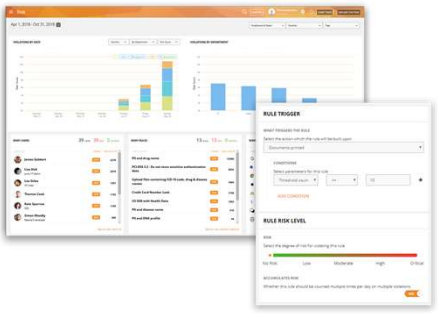
Data loss prevention from insider threats

Teramind allows organizations to create profiles for regular, privileged and contract/external users and then define what information and system resources each profile can access. Further rules can be set up by behavior policies so that access to sensitive information is segregated by the organization's security policy, or on a need-to-know basis. Rules can also be created to notify the authorities of any suspicious privileged user activity, such as unscheduled and/or unauthorized changes to system configuration, and creation of backdoor accounts.



Data breach audit with forensic evidence

Detailed alerts for all users can be viewed including any breach events and what actions were taken. Warning messages can be configured to inform the users about nonconformity as it pertains to handling sensitive data. Influence corrective behavior with on-time feedback and notifications. Session recordings and history playback can be used to view user's desktop for audit and evidence gathering purposes.

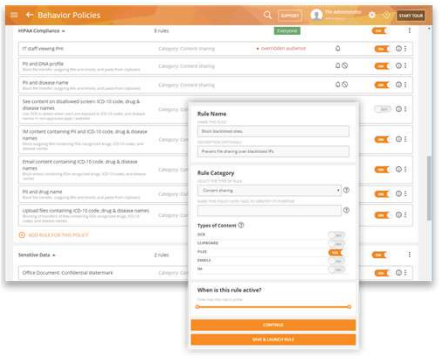


Data risk identification and management

Teramind has a dedicated Risk dashboard where supervisors can conduct organization-wide risk assessment. Risk can be profiled by users, departments or by content. Reports can be derived by severity of risks or by how many times security violations occurred. Unique Risk Scores helps you identify high-risk users or policies so that plans can be developed for treating the risks.

Unified security orchestration with SIEM and threat analytics systems

Event triggers and logs from Teramind can be sent to SIEM and other analytics tools like HP ArcSight, Splunk, IBM QRadar, McAfee Enterprise Security Manager, LogRhythm, NetIQ Sentinel etc. allowing you to share reports and threat intelligence with your security team or other departments. Teramind also has a set of RESTful APIs utilizing a simple token/endpoint framework that can be easily utilized by an application supporting webservice connections.



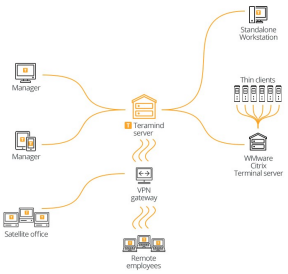
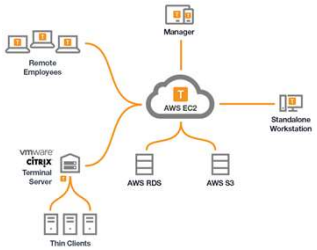
Compliance and privacy management

Teramind has built-in support for many regulatory compliance standards including GDPR, HIPAA, PCI DSS, ISO 27001, NIST, FISMA etc. Teramind's detailed alerts, session logs, anomaly and risk analysis, and incident reports help you demonstrate that you have established data security best practices and are ready to fulfill breach reporting and burden of proof requirements. Additionally, your can configure Teramind's monitoring features to meet the personal data privacy requirements set by GDPR and similar regulations.

Supported on all major platforms

Windows 7 & Up	Citrix XenApp® & XenDesk®	Windows Server 2008 & Up	VMware Horizon	Mac OSX

Flexible deployment options

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

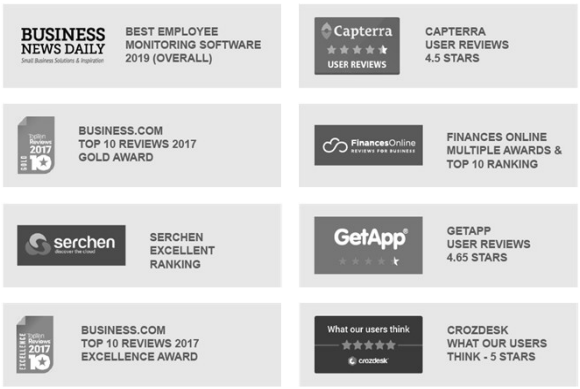
About Teramind

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 2,000 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:



www.americantechnology.com

sales@americantechnology.com

1-800-955-5790

Live Demo

www.teramind.co/sim