Teramind DLP

Features Guide

Version 1.6 (27 NOV 2023)

TERAMIND

Table of Contents

1 Teramind DLP Features Overview 4

2 Features Comparison 5

3 Monitoring and Detection Capabilities 6

3.1 Applications & Websites 6

3.2 Browser Plugins 8

3.3 Emails 9

3.4 Online Meetings 11

3.5 Console Commands 12

3.6 File Events 13

3.7 Web File Events 15

3.8 Instant Messaging 16

3.9 Social Media 18

3.10 Keystrokes 19

3.11 Clipboard (Copy and Paste) 20

3.12 Searches 21

3.13 Printing 22

3.14 Network 24

3.15 Geolocation 25

3.16 Camera Usage 26

3.17 OCR 27

3.18 Registry 29

3.19 OS State 30

3.20 Remote Control 30

4 Data Loss Prevention 31

4.1 Protect All Data Types and IP 31

4.2 Define Content-Based Rules 31

4.3 Define Fine Operation-Based Rules 32

4.4 Prevent Malicious and Negligent Data Exfiltration 32

4.5 Use Pre-Defined Data Categories 32

4.6 Leverage Document and Data Fingerprinting to Protect Sensitive Data 33

4.7 Ensure Regulatory Compliance Involving PII, PHI/HIPAA, GDPR, and More 33

5 User Behavior Analytics 34

5.1 Insider Threats 34

5.2 Abusive Behavior 34

5.3 Malicious Behavior 35

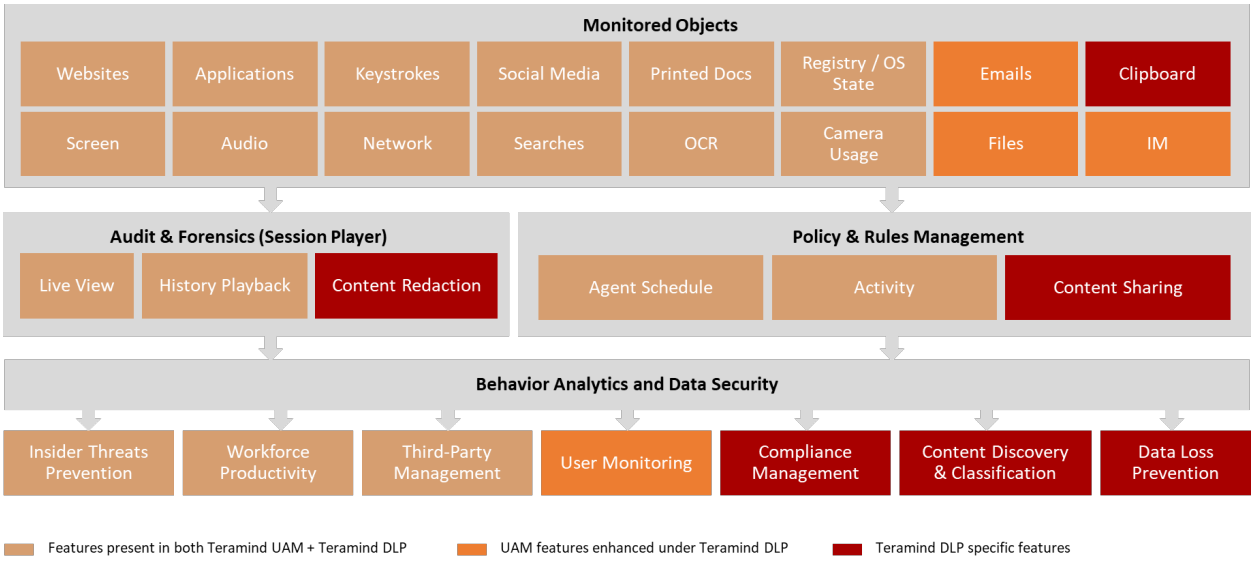
5.4 Dynamic Risk Scoring 36

5.5 Anomaly Detection 36
6 Workforce Productivity 38
6.1 Productivity Analysis & Reporting 38
6.2 Time Tracking 38
6.3 Template-Based Scheduling 39
6.4 Workflow Automation 39
7 Policy and Rules Management 40
7.1 Policy Manager 40
7.2 Visual Rule Editor 40
7.3 Regular Expression Support 40
7.4 Out-of-the-Box Rule Templates 41
8 Audit & Forensics 42
8.1 Real-Time Alerts & Audit Logs 42
8.2 Video Recording of All User Activity 42
8.3 Audio Recording 43
8.4 OCR of Screen Content 43
8.5 Option to Record Only During Violation 43
8.6 Full-Text Search 43
9 Role-Based Access Control (RBAC) 44
9.1 Standardized Account Roles and Profiles 44
9.2 Access Control Dashboard 44
10 Third-Party Integrations 45
10.1 SIEM / Threat Analytics Solutions 45
10.2 Project Management & Ticketing Solutions 45
10.3 Active Directory 45
10.4 Single Sign On (SSO) 46
10.5 API 46
11 Deployment 47
11.1 Supported Platforms 47
11.2 Hosting Options 47
11.3 Support 47

1 Teramind DLP Features Overview

Teramind DLP (Data Loss Prevention) solution allows you to implement effective protection against data exfiltration, IP loss, and various malicious or inadvertent security risks. Using automated data classifications, intelligent behavioral analysis, fingerprinting, and advanced OCR technologies, Teramind DLP can detect threats to your data in real time. Additionally, in case of a data breach incident, it provides you with the necessary tools to conduct forensic investigations and comply with breach reporting regulations.

Teramind DLP includes all the Teramind UAM features and adds content-based rules that control data sharing over the clipboard, files, emails, and IMs. The figure below shows the differences and similarities between the two products:



Contents highlighted in red color in this features guide are Teramind DLP-specific features.

Check out the Features Comparison table below to learn more about what features are available under each Teramind offer.

2 Features Comparison

	Starter	UAM	DLP	Enterprise
	Quick and easy screen recording and live view, website and app tracking	User activity monitoring at its fullest, audit, forensics, UBA, policies and rules	Content-based data exfiltration prevention plus stellar activity monitoring for forensics	For the most demanding enterprises and government organizations: SLA, Professional Services, Customizations
User Activity Monitoring				
Web pages & applications	✓	✓	✓	✓
OCR		✓	✓	✓
Remote control	✓	✓	✓	✓
Email		✓	✓	✓
Console commands		✓	✓	✓
File transfers		✓	✓	✓
Network		✓	✓	✓
Instant messaging	✓	✓	✓	✓
Social media activity	✓	✓	✓	✓
Online meetings		✓	✓	✓
Geolocation		✓	✓	✓
Camera usage		✓	✓	✓
Keystrokes		✓	✓	✓
Clipboard (copy and paste)			✓	✓
Searches	✓	✓	✓	✓
Printing		✓	✓	✓
Browser plugins	✓	✓	✓	✓
Registry	✓	✓	✓	✓
OS state	✓	✓	✓	✓
Custom website field capture				✓
Custom app field capture				✓
Data Loss Prevention				
Data discovery & classifications			✓	✓
Define content-based rules			✓	✓
Define file operation-based rules			✓	✓
Prevent malicious or negligent data exfiltration			✓	✓
Document and data fingerprinting			✓	✓
Regulatory compliance including HIPAA, GDPR, etc.			✓	✓
User Behavior Analytics				
Insider threat detection	✓	✓	✓	✓
Abusive behavior	✓	✓	✓	✓
Malicious behavior	✓	✓	✓	✓
Dynamic risk scoring		✓	✓	✓
Anomaly detection		✓	✓	✓
Workforce productivity analysis	✓	✓	✓	✓
Active vs idle time analysis	✓	✓	✓	✓
Template based scheduling	✓	✓	✓	✓
Interactive productivity reporting	✓	✓	✓	✓
Policy and Rules Management				
Policy manager	✓	✓	✓	✓
Visual rule editor	✓	✓	✓	✓
Regular expression support		✓	✓	✓
Out-of-the box rule templates		✓	✓	✓
Activity blocking + 7 other rule actions	Limited	✓	✓	✓
Audit & Forensics				
Video recording of all user activity	✓	✓	✓	✓
Audio recording	✓	✓	✓	✓
OCR of screen content, OCR search, OCR rules		✓	✓	✓
Option to record only during violation		✓	✓	✓
Full text search of activities and meta-data		✓	✓	✓
Professional Services				
Tailored deployment assistance				✓
Custom reporting configuration				✓
Custom behavior rules configuration				✓
Custom third-party integrations				✓
Availability in AWS GovCloud				✓
Availability in Azure Government				✓
Enterprise SLA				✓
On-Premise and Private Cloud Deployment				
Installation assistance	✓	✓	✓	✓
24x7 follow-the-sun support	✓	✓	✓	✓
Subscription includes software updates	✓	✓	✓	✓
Worry-Free Cloud Hosting				
No servers needed	✓	✓	✓	✓
We set up and host for you	✓	✓	✓	✓
Secure, Tier 3 data center	✓	✓	✓	✓
Data is encrypted in motion and at rest	✓	✓	✓	✓

3 Monitoring and Detection Capabilities

Teramind DLP monitors user activity for 13 system objects such as Websites, Applications, Social Media, IMs, Searches, Clipboard (copy & paste), etc. in real-time. The captured data is then presented on an enterprise-grade Business Intelligence (BI) dashboard. The BI tools allow you to customize, aggregate, or group data as you need and present them in visually engaging formats. Compare trends and data movement over time and view snapshots of key metrics and KPIs at a glance or drill down for in-depth analysis or export them to other applications.

Privacy Friendly Monitoring

While Teramind can capture virtually all computer activity, you have complete control over privacy. Each monitored object supports monitoring profiles and granular settings to ensure user privacy. You can track as much or as little as you want based on your organization's needs and alleviate any privacy concerns. Built-in Access Control panel lets you configure what admins can view or edit eliminating privilege abuse.

On Teramind DLP, you can create behavioral rules based on user activities, work schedules, and content sharing. Then, receive real-time alerts and notifications when any rule is violated. Using the smart policy and rules engine, you can prevent data breaches and malicious or accidental insider threats with pre-emptive actions such as warning a user, blocking an action, or taking control over their computers at any time.

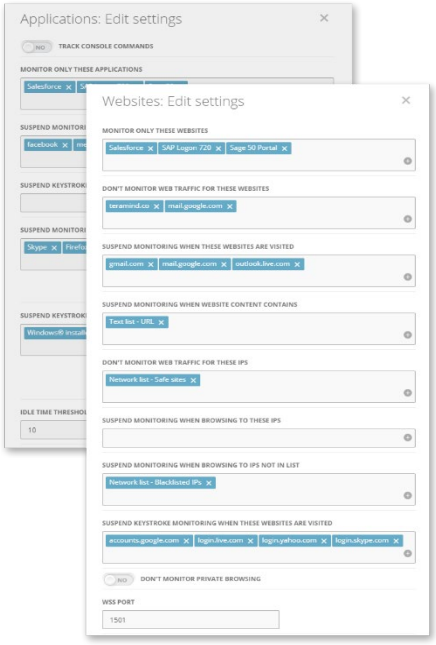
3.1 Applications & Websites

What report can I access for this activity?

- You can view the timestamp, employee, computer, process/URL, usage duration, idle time, active time, app/webpage, title, etc.
- View top employees, departments, app/domain, categories, browsers, security categories, reputations, classification timeline (e.g. productive vs. unproductive), etc.
- Automatically classify apps and websites based on inCompass® NetSTAR technology.
- View individual items or aggregate and compare them in different ways such as group by departments or compare app category vs. app reputation.
- Filter the report by the employee, department, computer, web/app, productive/unproductive, etc., and LDAP groups/attributes (if integrated with Active Directory).

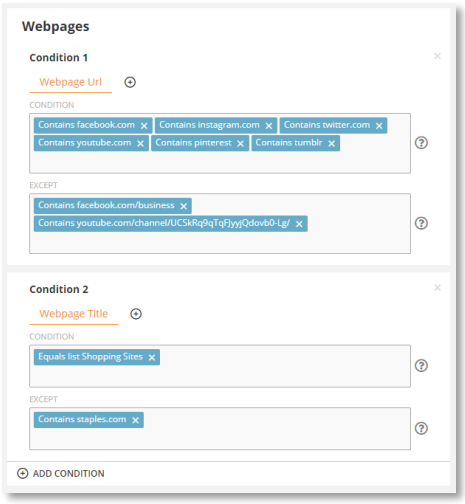
- Classify apps/websites into productive, unproductive, or custom categories.
- Print or export the reports as PDF/CSV files.
- Schedule regular report delivery to email addresses.
- View video records of the activities by date/time.
- Add real-time widgets on the dashboard or the BI reports.

What monitoring & tracking controls do I have?



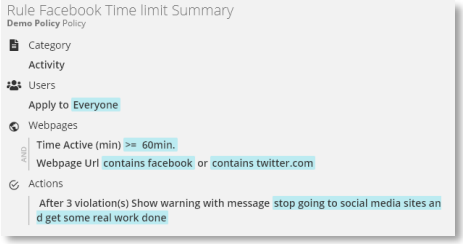
- Track all websites and applications and console commands. Or, you can configure the settings to monitor only select apps/websites.
- Monitor browser plugins and extensions.
- Suspend monitoring of keystrokes logging for certain applications/websites.
- Dynamically blackout screen recording when certain content is detected on a webpage. For example, when a user visits their bank's website or accesses a login page.
- You can suspend monitoring/keystrokes logging with extra conditions. For example, you can suspend monitoring Internet Explorer while it's used from an approved access control list (ACL).
- Option to monitor secure connections (HTTPS), SSH, and even private browsing sessions.
- Option to disable monitoring for password fields.
- Control the tracking of application idle time.

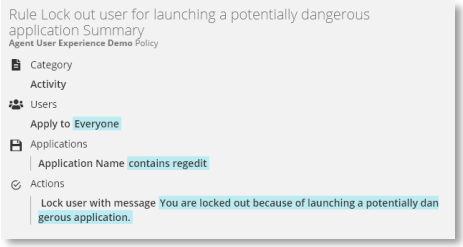
What rule and alert triggers can I use with this activity?



- On Teramind DLP, you can create Activity-based rules for the Websites and Browser Plugins.
- For the Webpages, you can use the Webpage Title, URL, and Query Arguments (URL variables) as inputs for the rule conditions.
- For the Applications, you can use the Application Name, Application Caption, Time Active, Time Idle, Focus Time, etc., and detect if it's launched from a CLI (Command Line Interface).
- For the Browser Plugin, you can use the Plugin Name, Browser (i.e. IE, Firefox), Plugin Permission (i.e. Proxy VPN, Requests, User Data) as inputs for the rule conditions.
- You can use all the available rule Actions, such as: Warn, Block, Notify, Lock Out User, Record Video, Execute Windows Command, etc., and additionally a Redirect action for webpages.

What are some sample rules using this feature?





- Restrict access to non-whitelisted/unauthorized applications or websites but allow managers to override if needed.
- Detect and block when a dangerous application (e.g., Windows Registry Editor) is launched.
- Warn users when spending excessive time on social media or entertainment sites such as YouTube.
- Find out potential turnover by checking if employees are searching on job sites. Get notified if the time spent on such sites exceeds a threshold.
- *While the Websites & Applications do not have a Content Sharing rule, you can use the OCR to detect content on web pages/apps and take appropriate actions. See the OCR section for more information.*

What are some useful resources for this feature?

- User Guide: BI Reports > Applications & Websites
- User Guide: Monitoring Settings > Applications Settings
- User Guide: Monitoring Settings > Websites Settings
- Rules Guide: Activity Rules > Applications
- Rules Guide: Activity Rules > Webpages

3.2 Browser Plugins

What report can I access for this activity?

No dedicated report

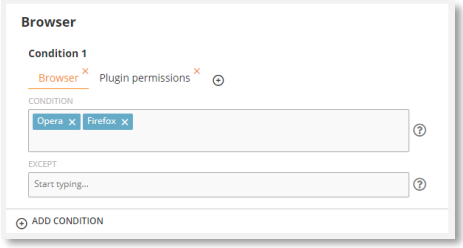
- Browser Plugins activities can be monitored under the Applications & Websites and other related BI reports (e.g. the Web File Events report shows details for all the uploads/downloads done through the browser).

What monitoring & tracking controls do I have?

No settings

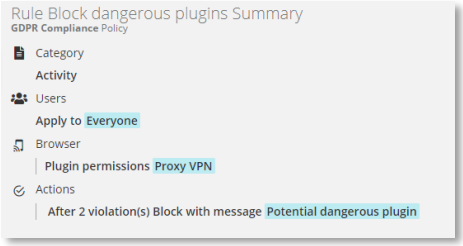
- The Browser Plugins does not have a dedicated settings panel and is controlled under the Websites settings panel. Check out the Applications & Websites monitoring and tracking controls for more information.

What rule and alert triggers can I use with this activity?



- On Teramind DLP, you can create Activity-based rules for the Browser Plugins.
- You can detect specific browser name (e.g. Chrome), plugin name, and plugin permission (i.e. Proxy VPN, Requests, User Data) as inputs for the rule conditions.
- You can use Warn, Block, Notify, Lock Out User, Execute Windows Command rule Actions.

What are some sample rules using this feature?



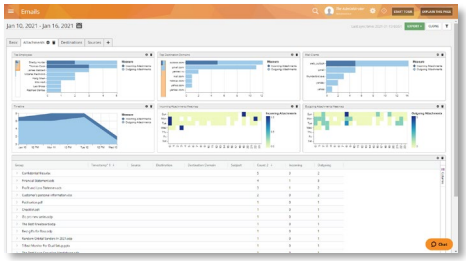
- Restrict use of certain browsers, e.g. old version of Internet Explorer.
- Block dangerous browser plugins and extensions to reduce the risk of malware infection or prevent a plugin from utilizing certain permissions such as the ability to access critical proxy settings or user data.

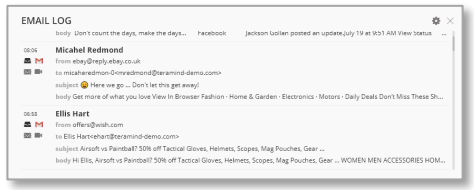
What are some useful resources for this feature?

- User Guide: BI Reports > Applications & Websites
- User Guide: Monitoring Settings > Websites Settings
- Rules Guide: Activity Rules > Browser Plugins

3.3 Emails

What report can I access for this activity?

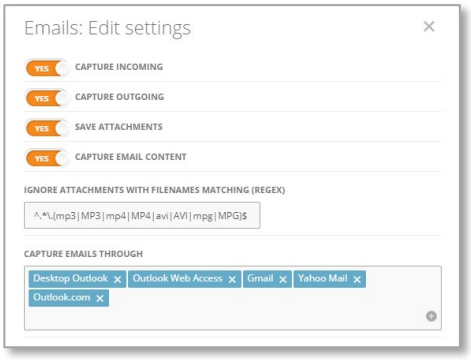




- View all emails and attachments being sent or received by employees and departments.
- View incoming/outgoing emails by timestamp, top employees/departments by no. of emails sent/received, attachment heatmaps, top domains, statistics for email sources, etc.
- Group email activities by the employee, departments, domain, source, etc. or compare trends such as outgoing vs. incoming emails.
- Save a copy of the email or attachments.
- Filter the report by the employee, department, computer, email direction, email client, etc. and LDAP groups/attributes (if integrated with Active Directory).
- Print or export the reports as PDF/CSV files.
- Schedule regular report delivery to email addresses.
- View video records of the activities by date/time.

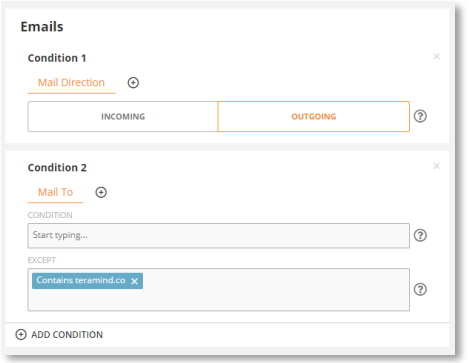
- Add real-time widgets on the dashboard or the BI reports.

What monitoring & tracking controls do I have?



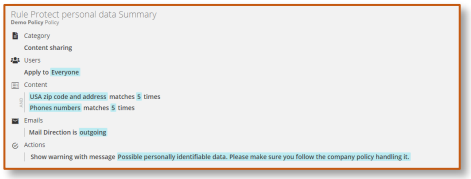
- You can select which emails to capture, incoming/outgoing, or both.
- You can decide if you want to capture the attachments or email content.
- You can use Regular Expressions (RegEx) to further filter or ignore any attachments you do not want to be captured. For example, video files.
- You can specify which email clients will be captured. Teramind supports popular clients such as Outlook, Gmail, Yahoo, etc. - both desktop and web versions.

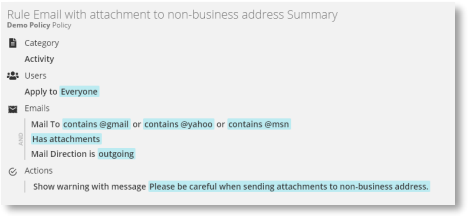
What rule and alert triggers can I use with this activity?



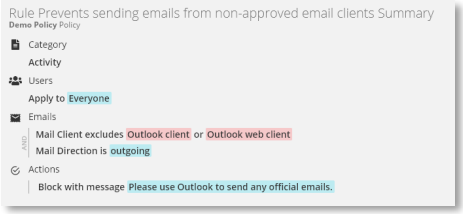
- On Teramind DLP, you can create Activity-based and Content-based rules for the Emails.
- You can use the Data Content to detect your own content or use the pre-defined Classified Data (Personally Identifiable Data, Financial Data, Health Data, Code) and File Origin.
- You can use the Mail Body, Subject, CC/To/From fields, Mail Direction, Mail Client, Mail Size fields and detect if the mail has any attachments as inputs for the rule conditions.
- You can use all the available rule Actions, such as: Warn, Block, Notify, Lock Out User, Record Video, Execute Windows Command, etc.

What are some sample rules using this feature?





- Detect sensitive information like Credit Card Numbers, Social Security Numbers, Health Records, or your own custom data types inside email body or attachments and act based on what's detected. For example, warn the user when sending out an email that contains a document containing contacts to prevent data exfiltration or comply with privacy laws.
- Prevent attaching files from a certain location(s) such as local, network, or cloud drives.
- Restrict sending work emails from personal email accounts.
- Prevent sending of attachments to non-business addresses.
- Detect if a competitor is contacting your employees or vice versa.



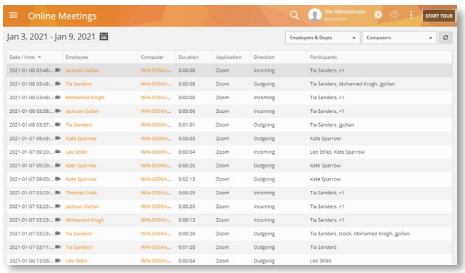
- Get notified if a user is sending emails with large attachments.

What are some useful resources for this feature?

- User Guide: BI Reports > Emails
- User Guide: Monitoring Settings > Emails Settings
- Rules Guide: Activity Rules > Emails
- Rules Guide: Content Sharing Rules > Emails

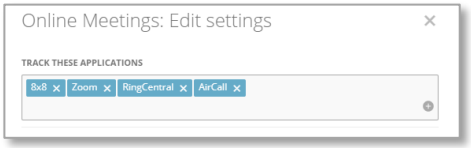
3.4 Online Meetings

What report can I access for this activity?



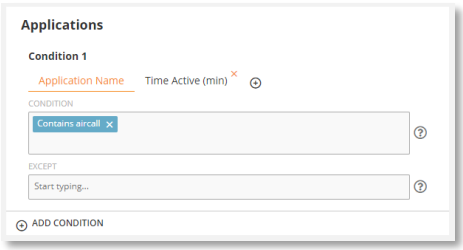
- Track online meeting activities for apps such as Zoom, AirCall, Microsoft Teams, etc.
- View employee/computer, when the meeting took place, duration, app, direction, participants, etc.
- Filter the report by employee, department, computer, etc.
- Optionally, view and/or hear the meetings (check out the Audit & Forensics section to learn more).

What monitoring & tracking controls do I have?



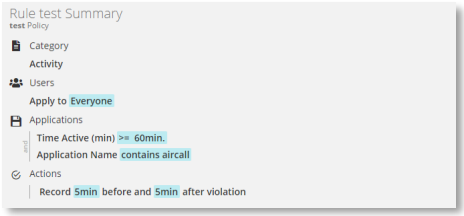
- You can select which online meeting applications to monitor such as, Zoom, Microsoft Teams, AirCall, etc.

What rule and alert triggers can I use with this activity?



- Online Meetings do not have dedicated rule triggers. However, you can use the Application category and use Activity-based rules for them.
- You can then use Warn, Block, Notify, Lock Out User, Execute Windows Command rule Actions.

What are some sample rules using this feature?



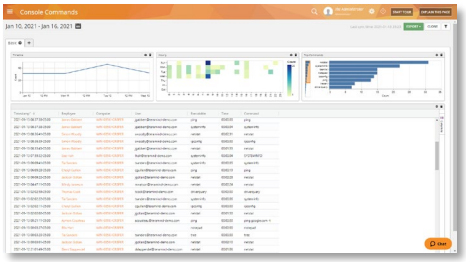
- Record the session if a user spending excess times in meetings.
- Get notified if the total meeting duration during a day is greater than a certain value.
- Detect what files are being shared at a meeting.

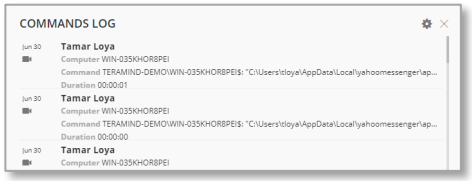
What are some useful resources for this feature?

- User Guide: Monitoring Reports > Online Meetings
- User Guide: Monitoring Settings > Online Meetings Settings
- Rules Guide: Activity Rules > Applications

3.5 Console Commands

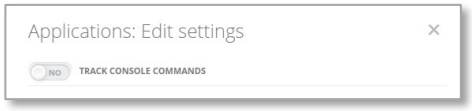
What report can I access for this activity?





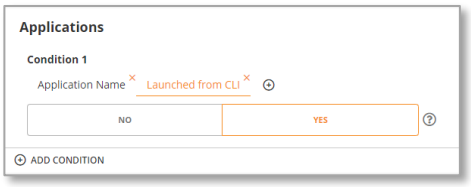
- Monitor any console commands executed by a user or an application from the command line.
- View date/time, employee, computer, username, PID (program ID), command heatmap by timeline, etc.
- Group activities by the employee, departments, app, etc. or compare trends such as top commands vs. top employees.
- Filter the report by the employee, department, computer, task, etc. and LDAP groups/attributes (if integrated with Active Directory).
- Print or export the reports as PDF/CSV files.
- Schedule regular report delivery to email addresses.
- View video records of the activities by date/time.
- Add real-time widgets on the dashboard or the BI reports.

What monitoring & tracking controls do I have?



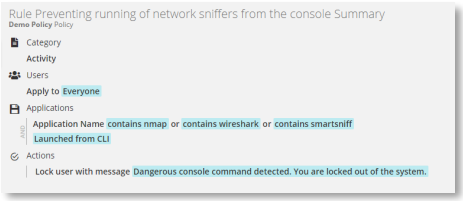
- Console Commands are tracked as part of the Applications object and can be turned on/off from the Applications settings.

What rule and alert triggers can I use with this activity?



- Activity-based rules for console commands can be created under the Applications category and has the same capabilities as the application-based rules. For additional detection triggers, you can use the *Launched from CLI* condition.

What are some sample rules using this feature?



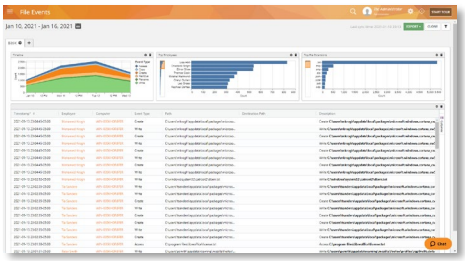
- Track privileged user activities for system-level applications.
- Block DOS commands such as *ren*, *del*, *attrib,* etc.
- Detect *ipconfig*, *nmap*, *WireShark*, or similar network scanning software.
- Prevent running of batch files and scripts.
- Block access to the command prompt entirely.

What are some useful resources for this feature?

- User Guide: BI Reports > Console Commands
- User Guide: Monitoring Settings > Applications Settings
- Rules Guide: Activity Rules > Applications

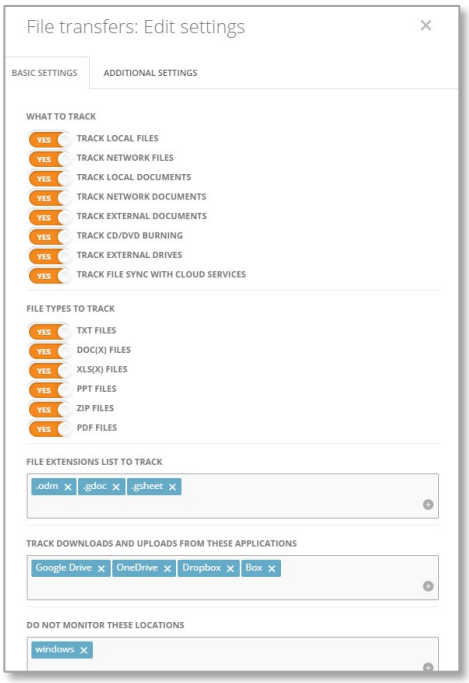
3.6 File Events

What report can I access for this activity?



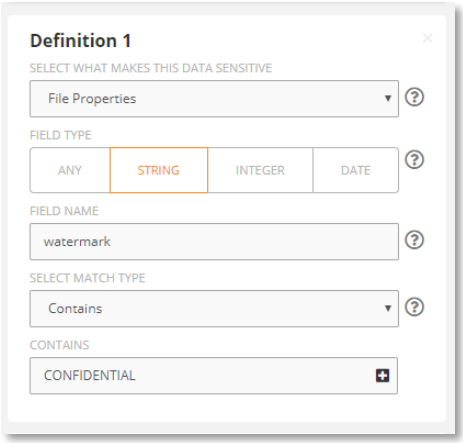
- View all file activities on the local, external, network, and cloud drives.
- View employee and computers for file actions (access, write, upload/download, etc.), source (i.e. local disk, network), the full path of the file, file name, extension, and what app initiated the file operation.
- Group by top employees/extensions or compare between two file activities such as Upload vs. Download.
- Filter the report by the employee, department, computer, task, etc. and LDAP groups/attributes (if integrated with Active Directory).
- Print or export the reports as PDF/CSV files.
- Schedule regular report delivery to email addresses.
- View video records of the activities by date/time.
- Add real-time widgets on the dashboard or the BI reports.

What monitoring & tracking controls do I have?



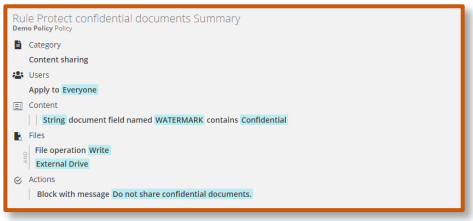
- You can specify what sources to track, such as local/network files, local/network documents, external documents, CD/DVD burning, external drives (i.e. USB / pen drives), etc.
- You can control which file types/extensions to track such as *doc*, *xls*, *ppt*.
- You can specify which applications should be monitored for upload/download activities.
- You can exclude select locations, folders, or drives from tracking.
- You can specify exactly what file operations to monitor, i.e. copy/move/upload/write.

What rule and alert triggers can I use with this activity?

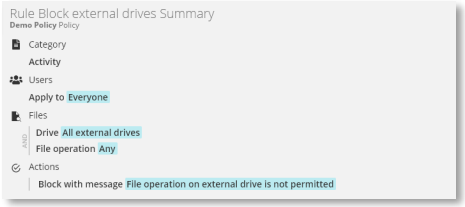


- On Teramind DLP, you can create Activity-based and Content-based rules for the File Transfers.
- You can use the Data Content to detect your own content or use the pre-defined Classified Data (Personally Identifiable Data, Financial Data, Health Data, Code), File Origin, and File Properties.
- You can use the File Operations such as access, write, rename, insert/eject), copy, upload/download, etc. as inputs for the rule conditions.
- Other conditions such as network host, file path, cloud provider, download file name, URL/size, etc. are available depending on which file operation is selected.

What are some sample rules using this feature?



- Prevent sharing of files that contain sensitive information, such as Credit Card Numbers, Social Security Numbers, Health Records, or your own custom data type.
- Prevent sharing of a file based on certain properties, such as, when a document contains a 'confidential' watermark.



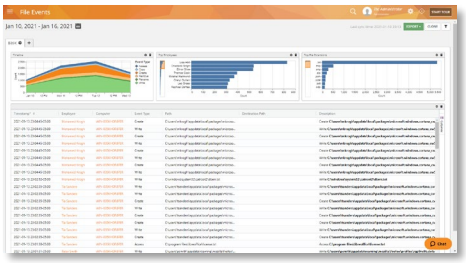
- Create rules based on file origin, such as, stop all network sharing from certain applications.
- Detect/block access to sensitive folders.
- Make a folder or drive ready only, preventing any changes to the files in that folder.
- Get notified when files are uploaded to Cloud sharing sites such as Google Drive, DropBox, OneDrive, etc.
- Block files from being copied to/from removable media such as USB drives.
- Prevent changes of program settings or tampering with configuration files.
- Stop transfer of large files.

What are some useful resources for this feature?

- User Guide: BI Reports > File Events
- User Guide: Monitoring Settings > File Transfers Settings
- Rules Guide: Activity Rules > Files
- Rules Guide: Content Sharing Rules > Files

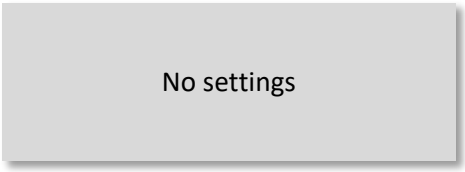
3.7 Web File Events

What report can I access for this activity?



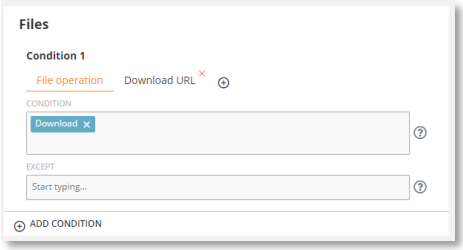
- View all web file events (upload/download, cloud sync, etc.).
- Group and compare events such as timeline (uploads vs. downloads), top employees, top domains, etc.
- Filter the report by the employee, department, computer, task, etc. and LDAP groups/attributes (if integrated with Active Directory).
- Print or export the reports as PDF/CSV files.
- Schedule regular report delivery to email addresses.
- View video records of the activities by date/time.
- Add real-time widgets on the BI reports.

What monitoring & tracking controls do I have?



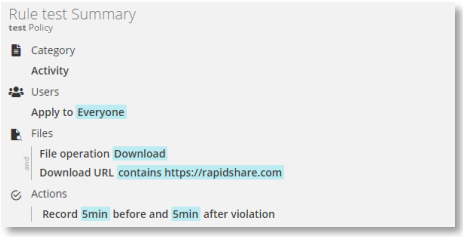
- Web File Events does not have a dedicated settings panel and controlled under the File Transfers and Websites settings panel to specify which URLs and files to track, when to track, etc. Check out the Applications & Websites and File Events sections for more information.

What rule and alert triggers can I use with this activity?



- Web File Events do not have dedicated rule triggers. However, you can use the Files category and use Activity-based rules or Content-based rules to detect file transfer activities including web uploads/downloads.
- You can then use Warn, Block, Notify, Lock Out User, Execute Windows Command rule Actions.

What are some sample rules using this feature?



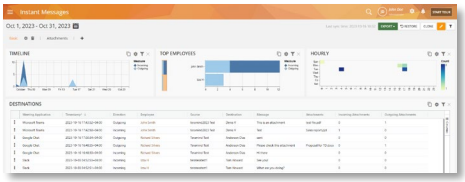
- Prevent upload or download of files to/from unknown or suspicious sites.
- Block torrent files.
- Limit the download/upload size to reduce abuse of bandwidth and storage.
- Prevent upload of sensitive files based on content.

What are some useful resources for this feature?

- User Guide: BI Reports > Web File Events
- User Guide: Monitoring Settings > File Transfers Settings
- User Guide: Monitoring Settings > Websites Settings
- Rules Guide: Activity Rules > Files
- Rules Guide: Content Sharing Rules > Files

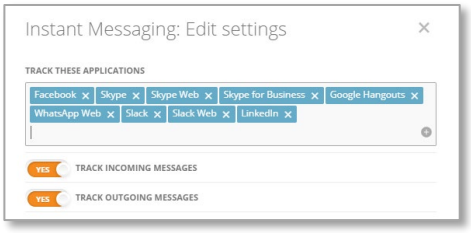
3.8 Instant Messaging

What report can I access for this activity?



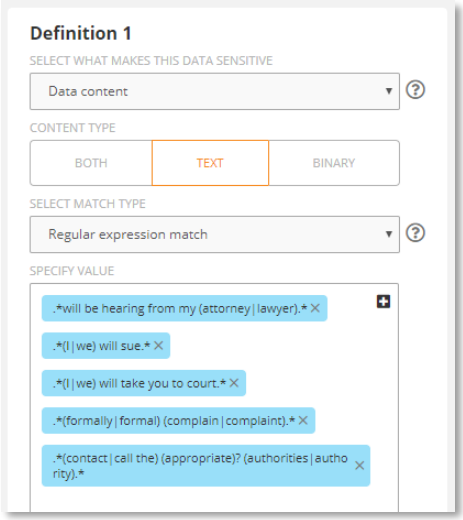
- Monitor detailed information about users instant messaging activities such as: *Employee*, *Computer*, *Metting App, Direction*, *Messages*, *Attachments*, etc.
- Add chart/grid widgets to analyze data and visually represent them. Compare or group activities such as outgoing messages trend by users, Attachments shared vs tasks, etc.
- Filter the report by the employee, department, computer, platform, etc. and LDAP groups/attributes (if integrated with Active Directory).
- Print or export the reports as PDF/CSV files.
- Schedule regular report delivery to email addresses.
- View video records of the activities by date/time.
- Add real-time widgets on the BI reports.

What monitoring & tracking controls do I have?



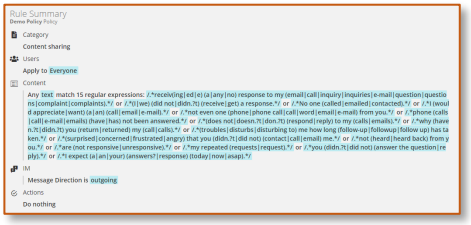
- You can select which messages to capture, incoming/outgoing, or both.
- You can specify which IM clients will be captured. Teramind supports popular clients, such as WhatsApp, Facebook Messenger, LinkedIn, Skype, Slack, Google Hangout, and Microsoft Teams - both desktop and web versions.

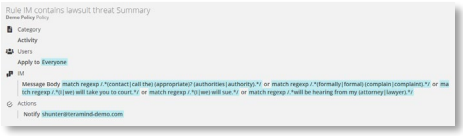
What rule and alert triggers can I use with this activity?

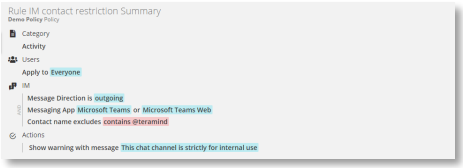


- On Teramind DLP, you can create Activity-based and Content-based rules for Instant Messaging.
- You can use the Data Content to detect your own content or use the pre-defined Classified Data (Personally Identifiable Data, Financial Data, Health Data, Code).
- You can use the Message Body, Message Direction, Messaging Application, and Contact Name as inputs for the rule conditions.
- You can use all the available rule Actions, such as: Warn, Block, Notify, Lock Out User, Record Video, Execute Windows Command, etc.

What are some sample rules using this feature?







- Improve productivity and data security. For example, detect if customer service agents are not responding to complaints or queries coming through your Instant Messaging channels.
- Create rules that warn HR about angry exchanges, harassment, or other potential negative sentiments in chat conversations.
- Detect if a user is targeted for phishing or social engineering online.
- Restrict messages to/from select contacts.
- Detect if a user is in contact with suspicious people or criminal groups.
- Monitor support chat conversations to improve the quality of customer service and SLA.
- Get notified if the chat body contains specific keywords or sensitive phrases such as lawsuit threats, angry sentiments, sexual harassment, etc.

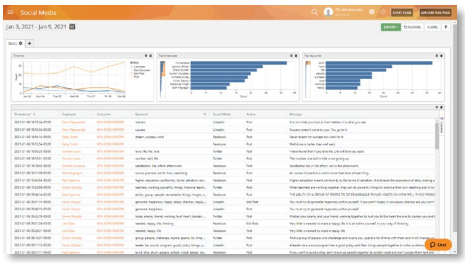
What are some useful resources for this feature?

- User Guide: Monitoring Reports > Instant Messaging (IM)
- User Guide: Monitoring Settings > Instant Messaging / IM Settings

- Rules Guide: Activity Rules > IM - Instant Messaging
- Rules Guide: Content Sharing Rules > IM - Instant Messaging

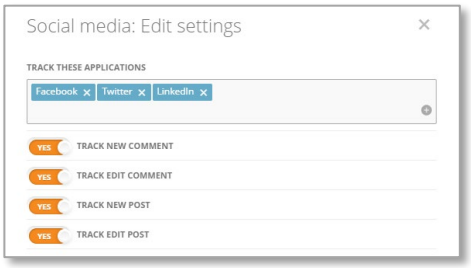
3.9 Social Media

What report can I access for this activity?



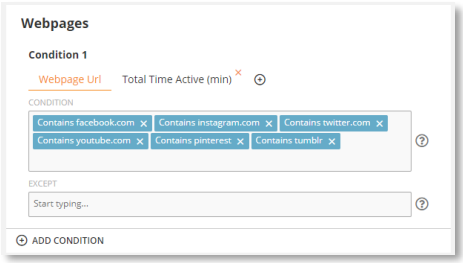
- View the source and action (post, comment, etc.) for the users' social media activities.
- View timeline (shows no. actions for a post, comment, edit post, etc.), top employees (by no. of social media activities), and top keywords, etc.
- See if any attachments are being shared.
- Aggregate or compare activities such as post vs. comments, Facebook vs. Twitter, etc.
- View the actual message.
- Filter the report by the employee, department, computer, platform, etc. and LDAP groups/attributes (if integrated with Active Directory).
- Print or export the reports as PDF/CSV files.
- Schedule regular report delivery to email addresses.
- View video records of the activities by date/time.
- Add real-time widgets on the BI reports.

What monitoring & tracking controls do I have?



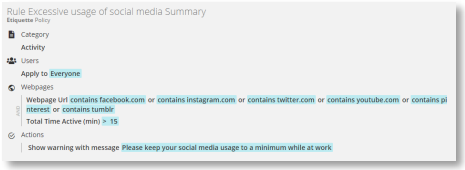
- You can specify which social media platforms to track. Teramind supports the most popular social media platforms, such as Facebook, Twitter, LinkedIn, etc.
- You can track New Comment, Edit Comment, New Post, and Edit Post activities in those applications.

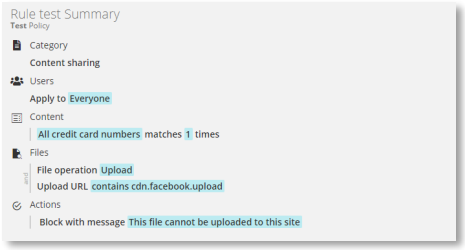
What rule and alert triggers can I use with this activity?



- Social Media does not have a dedicated rules category. However, you can create rules to monitoring social media sites using the Activity-based rules using the Webpages category. You can also create Content-based rules for social media. For example, using the Files category with a Content-based rule to detect sensitive contents and then use the *Upload URL* condition to block uploads of those files to a social media site.

What are some sample rules using this feature?





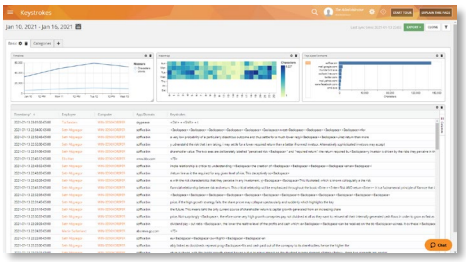
- Warn employees about excessive use of social media that might hamper productivity.
- Block posting of comments on certain social media sites such as Facebook but make an exception for the Marketing department.
- Monitor your corporate social channels. Get notified when any updates, posts, or comments are made on your social media accounts.
- Block uploading of sensitive files to a social media site.

What are some useful resources for this feature?

- User Guide: BI Reports > Social Media
- User Guide: Monitoring Settings > Social Media Settings
- Rules Guide: Activity Rules > Webpages

3.10 Keystrokes

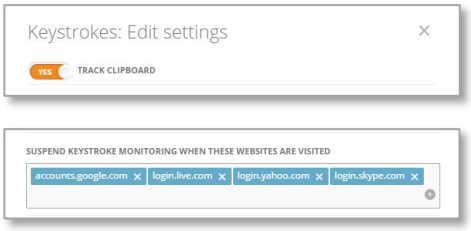
What report can I access for this activity?



- View all the keystrokes entered by the users in all apps/websites.
- In addition to regular keys, you can monitor the clipboard operations (copy/paste), use of special keys such as the Print Screen or key combinations.
- Compare items such as by timeline (e.g. no. of words vs no. of characters/letters typed for the duration), heatmap of keys pressed, top app/domains where the most keyboard activity occurred, etc.
- Group keystrokes by app/web categories, security categories, and reputation.
- Filter the report by the employee, department, computer, platform, etc. and LDAP groups/attributes (if integrated with Active Directory).
- Filter the report by the employee, department, computer, platform, etc. and LDAP groups/attributes (if integrated with Active Directory).
- Print or export the reports as PDF/CSV files.
- Schedule regular report delivery to email addresses.
- View video records of the activities by date/time.

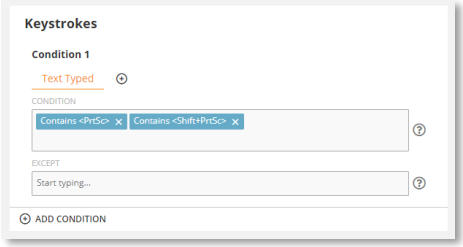
- Add real-time widgets on the dashboard or the BI reports.

What monitoring & tracking controls do I have?



- You can turn the Clipboard tracking on/off.
- You can automatically suspend keylogging for certain Applications & Websites.
- Automatically suspend keylogging when certain content is detected on Applications & Websites.

What rule and alert triggers can I use with this activity?



- On Teramind DLP, you can create Activity-based and Content-based rules for Keystrokes.
- You can use the Data Content to detect your own content or use the pre-defined Classified Data (Personally Identifiable Data, Financial Data, Health Data, Code).
- You can use Text Typed, Word Typed, Special Key Typed as inputs for the rule conditions.
- You can use all the available rule Actions, such as: Warn, Block, Notify, Lock Out User, Record Video, Execute Windows Command, etc.

What are some sample rules using this feature?

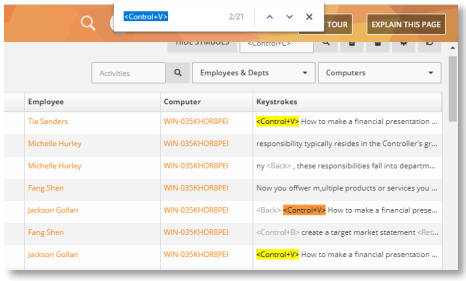
- Detect if someone is taking screenshots with the likely intention of stealing information.
- Detect if an employee is using unprofessional language with a customer on live chat.
- Detect PII, PHI, PFI or other sensitive contents to prevent data leaks in real-time, as the texts are types.
- A user repeating easy-to-guess passwords (hence, creating a security risk).
- Disable keyboard macros or select combo keys in certain applications or for some users.

What are some useful resources for this feature?

- User Guide: BI Reports > Keystrokes
- User Guide: Monitoring Settings > Keystrokes Settings
- Rules Guide: Activity Rules > Keystrokes

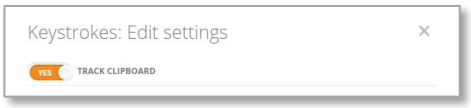
3.11 Clipboard (Copy and Paste)

What report can I access for this activity?



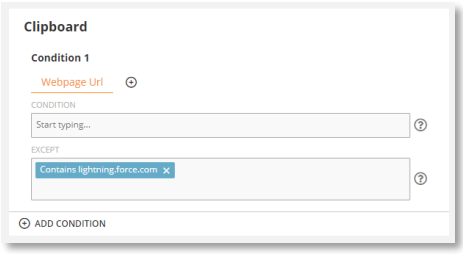
- There is no dedicated report for the Clipboard. However, you can use the Keystrokes report and search for hidden characters that indicate copy/paste operations, for example: `<Control+C>` or `<Control+V>`.

What monitoring & tracking controls do I have?



- Clipboard does not have a settings panel. However, you can turn it on/off from the Keystroke's settings panel.

What rule and alert triggers can I use with this activity?



- On Teramind DLP, you can create Content-based rules for the Clipboard.
- You can use the Data Content to detect your own content or use the pre-defined Classified Data (Personally Identifiable Data, Financial Data, Health Data, Code). You can also use Clipboard Origin to monitor clipboard activity on certain websites or applications.

What are some sample rules using this feature?

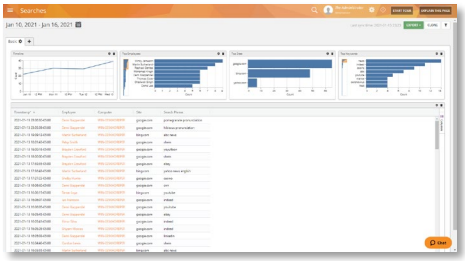
- Prevent sharing of customer data outside of your CRM site.
- Warn users when they copy social security numbers from an Excel spreadsheet and paste it on an email client like Outlook.
- Prevent data defined as sensitive on your *Classified List* to be pasted on an image application. So that the user cannot later upload the image to bypass your document upload rules.

What are some useful resources for this feature?

- User Guide: BI Reports > Keystrokes
- User Guide: Monitoring Settings > Keystrokes Settings
- Rules Guide: Content Sharing Rules > Clipboard

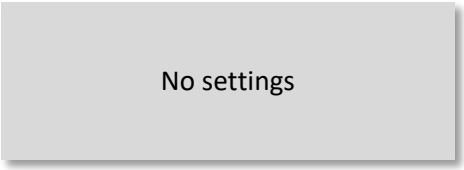
3.12 Searches

What report can I access for this activity?



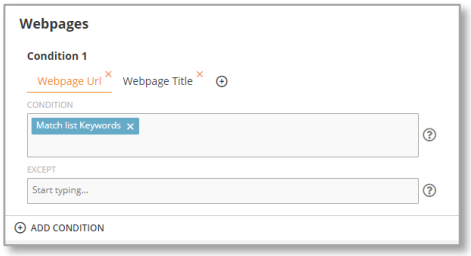
- View all the search phrases by timestamp, site, employee, department, computer, etc.
- Compare or group searches by timeline, top searches by employees, sites, keywords, etc.
- Filter the report by the employee, department, computer, platform, etc. and LDAP groups/attributes (if integrated with Active Directory).
- Print or export the reports as PDF/CSV files.
- Schedule regular report delivery to email addresses.
- View video records of the activities by date/time.
- Add real-time widgets on the BI reports.

What monitoring & tracking controls do I have?



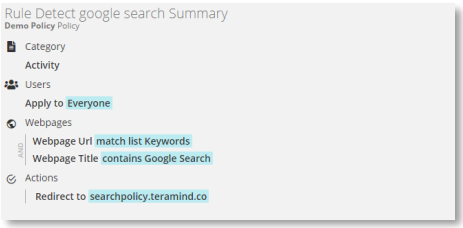
- Search does not have a dedicated settings panel. Search engines are treated like regular websites on Teramind. You can control the website settings from the Websites settings panel. See the Applications & Websites section for more information.

What rule and alert triggers can I use with this activity?



- You cannot create any Search-based rules directly. However, in Teramind DLP you can create Activity-based rules and use the *Website URL* and *Website Title* conditions to detect a search engine and the term(s) a user is searching for.

What are some sample rules using this feature?



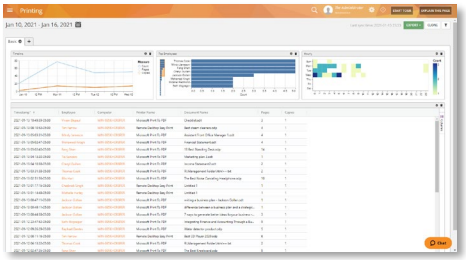
- Use the Webpages rules to detect when an employee searches for certain keywords.
- Redirect to another URL when a certain search engine is detected. For example, redirect all searches from Bing to Google.

What are some useful resources for this feature?

- User Guide: BI Reports > Searches
- User Guide: Monitoring Settings > Websites Settings
- Rules Guide: Activity Rules > Webpages

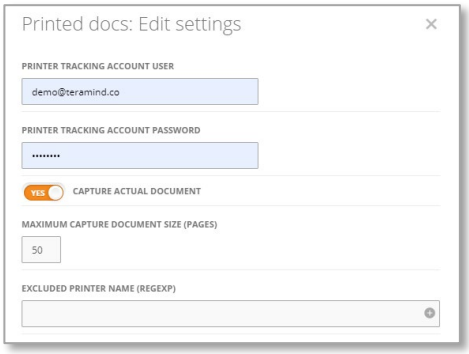
3.13 Printing

What report can I access for this activity?



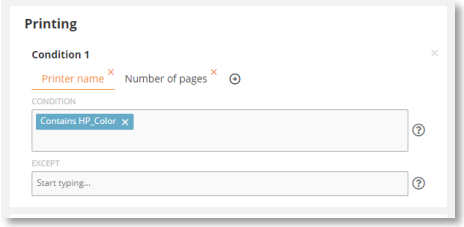
- Track all documents sent to the local or network printers including the name of the document, printer, pages, copies, computer, and the user initiating the print job.
- Compare or group print activities by timeline (e.g. no. of print jobs, pages, and copies), heatmap, etc.
- View or print a copy of the document or save it as a PDF file.
- Filter the report by the employee, department, computer, platform, etc. and LDAP groups/attributes (if integrated with Active Directory).
- Print or export the reports as PDF/CSV files.
- Schedule regular report delivery to email addresses.
- View video records of the activities by date/time.
- Add real-time widgets on the BI reports.

What monitoring & tracking controls do I have?



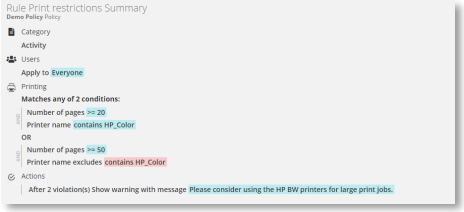
- Specify which printer account will be used for printers that require login (e.g. network printers).
- Turn the capture of actual documents on/off.
- Specify the maximum size of the document (pages) to be captured.
- Exclude printers you do not want to track.

What rule and alert triggers can I use with this activity?



- On Teramind DLP, you can create Activity-based rules for the Printer.
- You can use the Document Name, Printer Name, and Number of Pages as inputs for the rule conditions.
- You can use all the available rule Actions, such as: Warn, Block, Notify, Lock Out User, Record Video, Execute Windows Command, etc.

What are some sample rules using this feature?



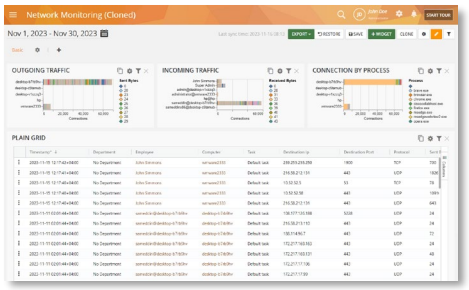
- Warn the user about large print jobs to reduce waste.
- Prevent data leaks over hardcopies by restricting what documents can be printed.

What are some useful resources for this feature?

- User Guide: BI Reports > Printing
- User Guide: Monitoring Settings > Printed Docs Settings
- Rules Guide: Activity Rules > Printing

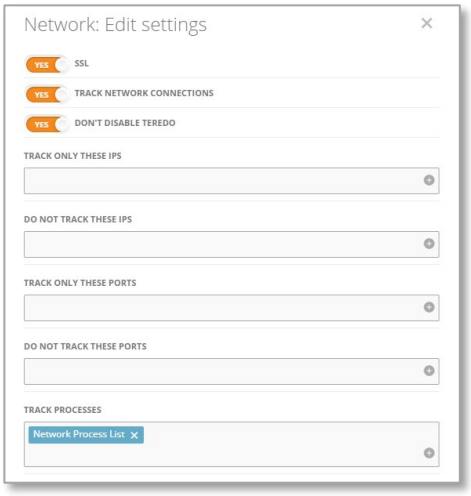
3.14 Network

What report can I access for this activity?



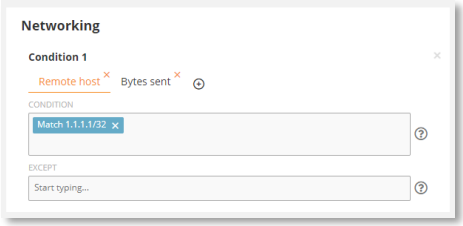
- Monitor detailed information on the camera usage such as: *Employee*, *Computer*, *Source/Destination IP*, *Ports*, *Hosts*, *Bytes Sent/Received*, etc.
- Add chart/grid widgets to analyze data and visually represent them. Compare or group activities such as outgoing traffic trend by users, most used host vs computers, etc.
- Filter the report by the employee, department, computer, platform, etc. and LDAP groups/attributes (if integrated with Active Directory).
- Print or export the reports as PDF/CSV files.
- Schedule regular report delivery to email addresses.
- View video records of the activities by date/time.
- Add a real-time *Network Usage* widget on the dashboard.

What monitoring & tracking controls do I have?



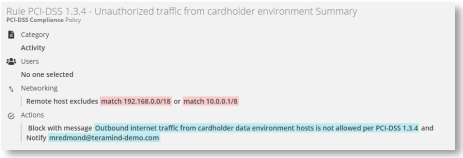
- You can turn SSL on to monitor secure connections (i.e. HTTPS).
- Select which IPs and Ports you want to track. For example, you can decide to track only external IPs or connections.
- Similarly, you can specify which network processes to track. You can use names (i.e. `svchost.exe`), Regular Expressions, Network Shared Lists, etc. to fine-tune the processes to track.

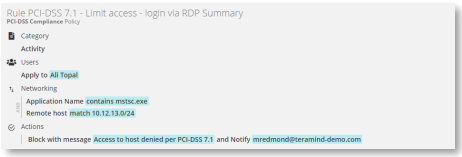
What rule and alert triggers can I use with this activity?



- On Teramind DLP, you can create Activity-based rules for the Network.
- You can use the Application Name, Remote Host and Port, Bytes Sent and Received, Local IP, etc. as inputs for the rule conditions.
- You can use these rule Actions: Warn, Block, Notify, Lock Out User, Execute Windows Command, etc.

What are some sample rules using this feature?





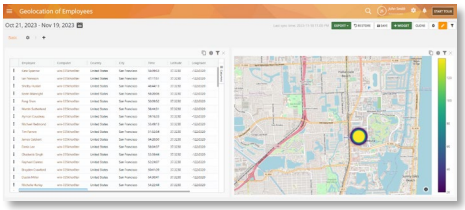
- Implement network security-related rules, for example, restrict outgoing internet traffic from the payment server (to comply with PCI DSS regulation).
- Limit network access such as, disable login via RDP (Remote Desktop Protocol).
- Detect if a user has established a connection to a peripheral local or VPN network or has changed the network route to bypass your corporate VPN.
- Get notified when abnormal network activity (i.e. sudden spike in network traffic) is detected which might indicate an intrusion.

What are some useful resources for this feature?

- User Guide: Monitoring Reports > Network Monitoring
- User Guide: Monitoring Settings > Network Settings
- Rules Guide: Activity Rules > Networking

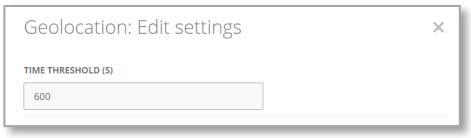
3.15 Geolocation

What report can I access for this activity?



- Monitor detailed information about the users' location such as: *Employee*, *Computer*, *Latitude*, *Longitude, Country, City,* etc.
- Plot coordinates and chart *Dimensions* and *Measures* on a map.
- Compare or group locations by timeline (e.g., by remote vs on-site employees), create charts, etc.
- Filter the report by the employee, department, computer, platform, etc. and LDAP groups/attributes (if integrated with Active Directory).
- Print or export the reports as PDF/CSV files.
- Schedule regular report delivery to email addresses.
- View video records of the activities by date/time.

What monitoring & tracking controls do I have?



- You can set a time threshold before a location is reported.

What rule and alert triggers can I use with this activity?

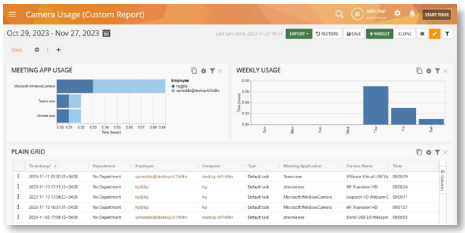
- Currently you cannot create any behavior rules/alerts based on Geolocation.

What are some useful resources for this feature?

- User Guide: BI Reports > Geolocation
- User Guide: Monitoring Settings > Geolocation Settings

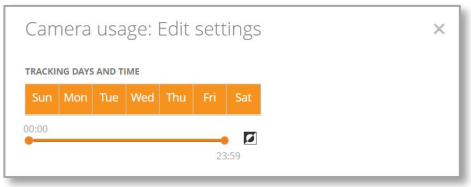
3.16 Camera Usage

What report can I access for this activity?



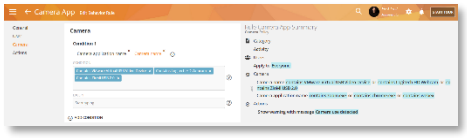
- Monitor detailed information on the camera usage such as: *Employee*, *Computer*, *Duration*, *Time Started*, *Meeting Application*, *Camera Name*, etc.
- Add chart/grid widgets to analyze data and visually represent them. Compare or group activities such as camera usage by apps, usage timeline by employees, etc.
- Filter the report by the employee, department, computer, platform, etc. and LDAP groups/attributes (if integrated with Active Directory).
- Print or export the reports as PDF/CSV files.
- Schedule regular report delivery to email addresses.
- View video records of the activities by date/time.

What monitoring & tracking controls do I have?



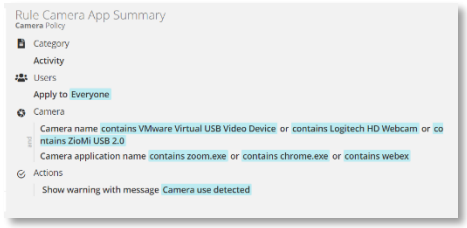
- You can toggle the Camera Usage monitoring on/off or set up a monitoring schedule.

What rule and alert triggers can I use with this activity?



- You can detect the camera name and in which application the camera is being used.
- You can use the Notification, Lock Out User, Warn, Set User's Active Task, Record Video and Command Actions with the Camera.

What are some sample rules using this feature?



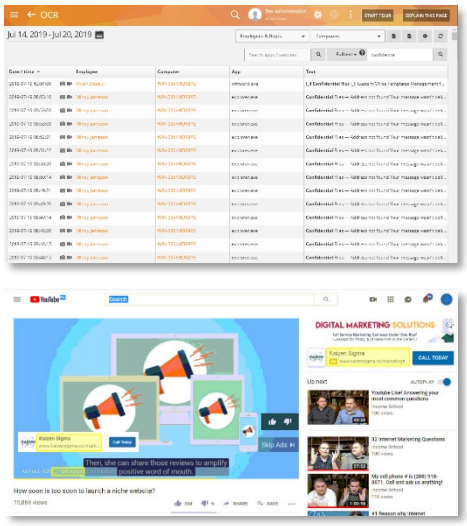
- Allow webcam usage only in your company's approved apps such as Webex and block other apps to reduce security and privacy risks.
- Respect user privacy by only recording video for a specific camera. For example, record screen sessions of remote users by tracking the camera supplied by the company and not record when the user is using their personal/built-in webcam.

What are some useful resources for this feature?

- User Guide: Monitoring Reports > Camera Usage
- User Guide: Monitoring Settings > Camera Usage Settings
- Rules Guide: Activity Rules > Camera

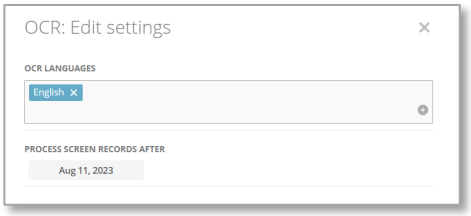
3.17 OCR

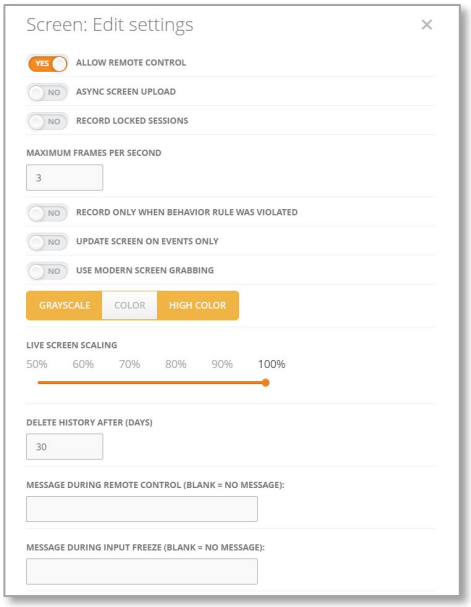
What report can I access for this activity?



- Detect on-screen text in real-time, even inside images or videos.
- Quickly search for information using powerful search features, such as Full Text, Wild Cards, Regular Expressions.
- Automatically identify the areas of the screen where OCR text was detected using OCR Snapshot.
- Works with multi-screen setups, virtual desktops, and Terminal Servers.
- Filter the report by employee and computer and LDAP attributes (if integrated with Active Directory).
- Print or export the reports as PDF/CSV files.
- Schedule regular report delivery to email addresses.
- View video records of the activities by date/time.

What monitoring & tracking controls do I have?

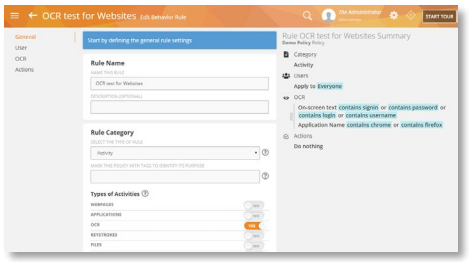




OCR settings can also be affected by *Monitoring Settings > Screen*.

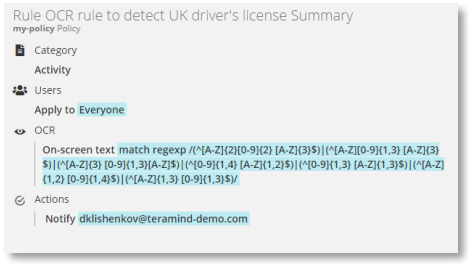
- You can specify which language will be used for the OCR. Default is English. Teramind also supports Hebrew, Russian, Dutch, Spanish, and Turkish.
- You can set asynchronized upload of OCR captured videos in case you have a slower server or limited bandwidth.
- You can enable recording only when a rule is violated to reduce the storage requirement or for privacy reasons.
- You can also control the FPS, color mode, size, bit-depth, compression, etc.
- You can specify when the recordings will be automatically deleted to reduce storage needs or to comply with privacy regulations.

What rule and alert triggers can I use with this activity?



- You can detect any text displayed on the screen by using keywords, lists, or regular expressions.
- You can use the Application Name as input for the rule condition.
- You can use the Notification Action with the OCR.

What are some sample rules using this feature?



- Generate an alert when a user sees a full credit card number on the screen violating the PCI DSS compliance requirements.
- Get notified when your employees visit sites that contain questionable content, such as hacking, pornographic, or piracy-related topics.
- Prevent steganographic data exfiltration by detecting information hidden inside images or videos.

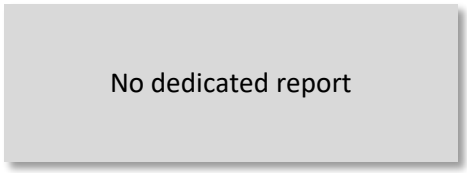
What are some useful resources for this feature?

- Video: Intelligent User Session Mining with Teramind's patent-pending OCR features

- User Guide: Monitoring Reports > OCR
- User Guide: Monitoring Settings > Screen Settings
- Rules Guide: Activity Rules > OCR

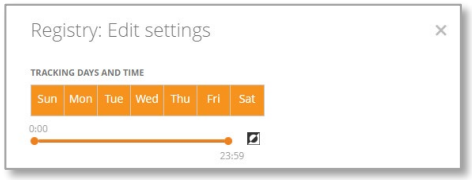
3.18 Registry

What report can I access for this activity?



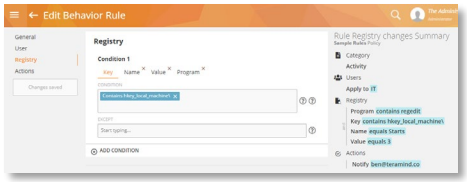
- Registry changes aren't tracked on a dedicated report but you can view rule violation incidents related to the registry on the Behavior Alerts report.

What monitoring & tracking controls do I have?



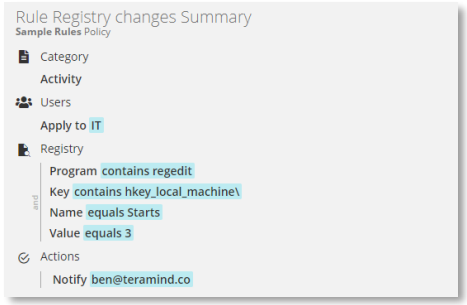
- You can toggle the registry monitoring on/off or set up a monitoring schedule.

What rule and alert triggers can I use with this activity?



- You can detect changes to registry keys, names, values and programs.
- You can use the Notification, Block, Lock Out User, Warn, Set User's Active Task, Record Video and Command Actions with the Registry.

What are some sample rules using this feature?



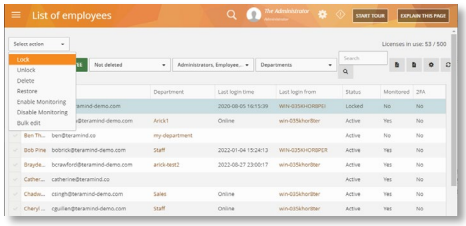
- Prevent changes to sensitive keys/programs or other items in the registry. For example, network or internet settings, security policies, etc.
- Detect/prevent unauthorized changes of permissions or privileges of files, folders, drives or applications. For example, a malicious user or intruder can change the USBSTOR values to enable the use of external drives compromising security. By monitoring the registry key, you can prevent such changes.
- Detect if a user is trying to install a dangerous or problematic software by monitoring what changes the software is making to the system.

What are some useful resources for this feature?

- User Guide: Monitoring Settings > Registry Settings
- Rules Guide: Activity Rules > Registry

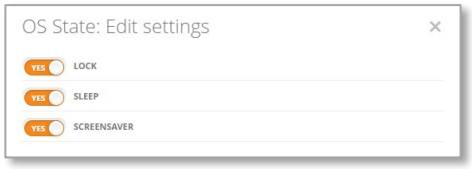
3.19 OS State

What report can I access for this activity?



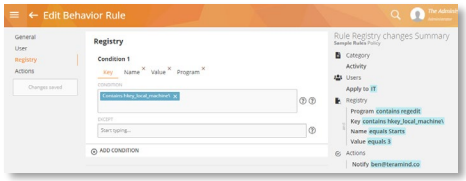
- OS State changes aren't tracked on a dedicated report but you can view a user's OS State and change the "Lock" state under the *Status* column of the Employees report.

What monitoring & tracking controls do I have?



- You can toggle the monitoring of Lock, Sleep and Screensaver states.

What rule and alert triggers can I use with this activity?



- You cannot use any rules directly with the OS State. However, you can monitor idle time with the Agent Schedule-based rules. You can also use the Lock Out action with some rules to lock out the user's computer (Windows only).

What are some useful resources for this feature?

- User Guide: Monitoring Settings > OS State Settings
- User Guide: Employees
- Rules Guide: Agent Schedule Rules > Idle

3.20 Remote Control

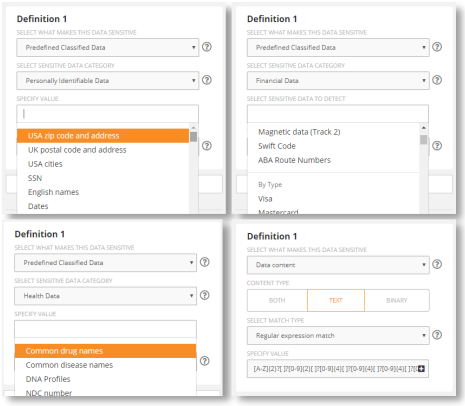
The Remote Control feature allows you to take full control of a user's computer over the internet. Additionally, you can block the user's input or freeze their screen remotely.

Remote Control is available through Teramind's Session Player and is part of Teramind's audit and forensics capabilities. Please check out the Audit & Forensics section for more information.

4 Data Loss Prevention

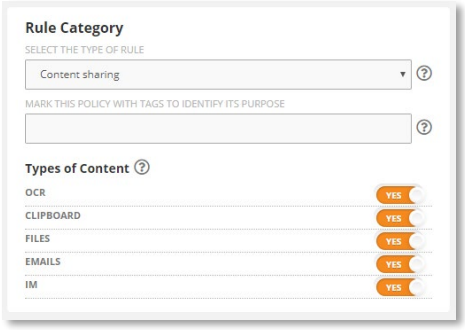
Teramind data loss prevention feature utilizes automated data discovery, classification, and content-based rules to protect your sensitive data and IP from exfiltration. Additionally, built-in support for PII, PHI/HIPAA, PFI/PCI DD, and GDPR-regulated information means your data protection and security policies conform with regulatory standards and compliances.

4.1 Protect All Data Types and IP



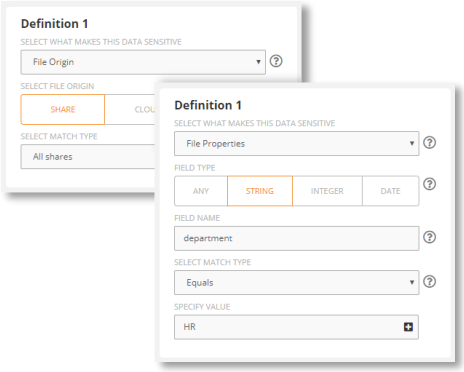
- Teramind has built-in templates for many classified and sensitive data types you can use to protect your confidential data and IP.
- You can create custom data types specific to your organization easily using Regular Expressions (RegEx) and natural language definitions. For example, billing/invoice numbers, signup, enrollment and payment data, OGD, GSCP, special codes, etc.
- Protect your IP data such as Deal Management Information, Trading Algorithms, Financial Modeling, Code Snippets, IPO Plans, M&A Plans.

4.2 Define Content-Based Rules



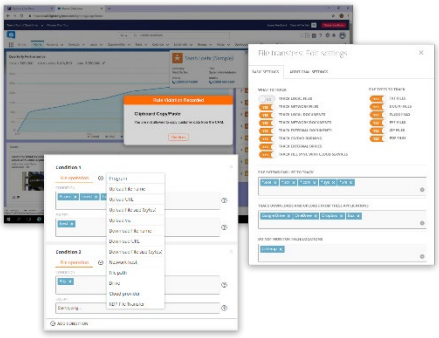
- In addition to defining activity-based rules, you can create Content-based rules in Teramind DLP to protect important information from malicious or accidental data leaks.
- You can create content-based rules for Files, Emails, IMs, Clipboard, and OCR.
- Content rules detect sensitive content anywhere: from applications, websites, IM chats, and email attachments to 'on-the-fly' information, displayed on the screen.

4.3 Define Fine Operation-Based Rules



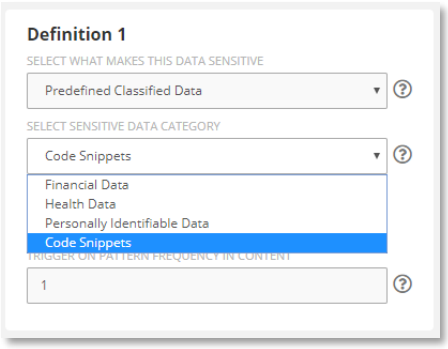
- In addition to the regular file activities (i.e. read/write, upload/download, etc.), Teramind DLP comes with two special types of content categories for file operations: File Properties and File Origin.
- *File Properties* lets you create rules to detect file properties/meta tags against any string (text), integer (number), or date.
- *File Origin* lets you create rules based on the file source, such as Cloud, URL, or all shares.

4.4 Prevent Malicious and Negligent Data Exfiltration



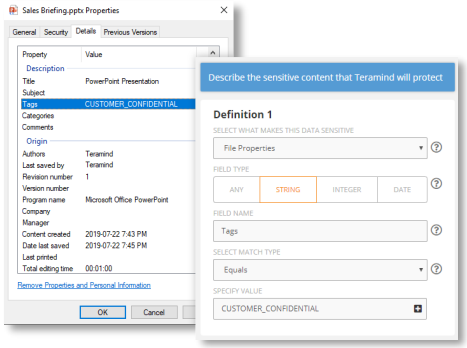
- Use the File Transfer rules to block external drives, Clipboard rules to prevent sharing of confidential information across apps and websites, Use OCR to keep an eye on emails or IMs and block them automatically if a potential data leak event is detected.
- There are hundreds of use cases where Teramind DLP can proactively defend your data from malicious or accidental leaks or misuse.

4.5 Use Pre-Defined Data Categories



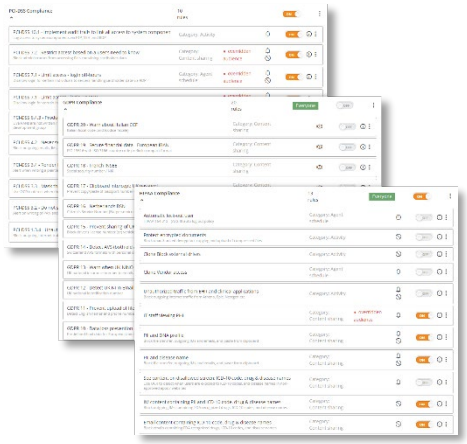
- Teramind has built-in templates for many pre-defined data categories to help you classify information automatically and in real-time.
- *Financial Data* allows you to detect credit card numbers, Swift codes, ABA Route Numbers, etc. for PCI DSS.
- *Health Data Category* allows you to identify common drug/disease names, DNA profiles, HICN, ICD codes, etc. for HIPAA compliance.
- *Personally Identifiable Data* allows you to detect names, addresses, birth dates, zip codes, etc. for privacy such as GDPR compliance.
- *Code Snippet* allows you to prevent source code leaks for SQL and many other popular languages.

4.6 Leverage Document and Data Fingerprinting to Protect Sensitive Data



- This feature is useful to secure patents or legal documents, government forms, HIPAA data, HR records, etc.
- In Teramind DLP, *File Properties* and *File Origin* allow you to identify files based on their tags and sources, allowing you to track them even when changed or shared across users.
- *Data Content* allows you to track any text or binary patterns in a file, allowing you to create document signatures that can be tracked to ensure data integrity.

4.7 Ensure Regulatory Compliance Involving PII, PHI/HIPAA, GDPR, and More



- Teramind DLP has built-in support for many regulatory compliances 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 data security best practices and fulfill breach reporting and burden of proof requirements.
- Additionally, your can configure Teramind's monitoring features to meet privacy requirements set by GDPR and similar regulations.

What are some useful resources for this feature?

- Video: Teramind How-To Series: Preventing data loss with Teramind
- Video: Teramind DLP or Teramind DLP?
- Video: Teramind for HIPAA Compliance
- Product Brochure: Teramind DLP
- Knowledge Base Article: How to Detect and Prevent Data Leaks with Teramind

5 User Behavior Analytics

Teramind comes with powerful User & Entity Behavior Analytics (UEBA) to identify and alert you about a wide range of anomalous behavior and potential threats by either a malicious, inadvertent, or compromised employee or third-party entity. Predictive and situational threat information derived from machine learning, regression analysis, and risk analysis helps you detect vulnerabilities early; identify security weak spots, and develop risk mitigation plans for the future.

5.1 Insider Threats

In Teramind DLP, insider threat detection works utilizing a combination of monitoring, authentication, data classification, risk analysis, and behavioral rule features. For example:

- 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.
- Clipboard monitoring and interception feature allow you to protect sensitive data from being shared through the clipboard copy/paste operations.
- 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 by insiders.
- Conduct OCR search for confidential information and see who had access to such information and when.
- Establish organization-wide visibility and control for over 12 objects including screens, apps, websites, files, emails, etc. Locate suspicious activity in real-time.
- Detect activities of all types of insiders: employees, third-party vendors, freelancers, contracts, etc.
- Activity, Agent-Schedule-based rules to automatically detect when users violate rules.
- Utilize sophisticated anomaly rules to identify user activities outside the normal behavior.
- Real-time alerts and notifications immediately warn you about harmful insider activity.
- Use session playback, monitoring reports, and logs to investigate data breaches and identify what happened, who, and what caused the incidents.
- Risk analysis to identify security gaps & vulnerabilities.

What are some useful resources for this feature?

- Video: Teramind: Insider Threat Prevention

5.2 Abusive Behavior

These are user behaviors that, while not malicious or particularly dangerous, still can cause your organization loss of productivity and in some cases, other damages. With Teramind DLP, you can create Content, Activity, and Agent Schedule-based rules to detect abusive behaviors easily. For example:

- Sign of discontent, harassment, legal threats, or other sentiments in emails or IM chats indicating underlying issues.

- Development team using production data for testing and development.
- IT department storing authentication information such as credit card magnetic data which is prohibited in PCI DSS regulation.
- User entering sensitive data such as passwords or personal details on potentially harmful or unsecured sites.
- Employees looking at materials online that are questionable, suspicious, or otherwise dangerous. For example, hacking sites, pornography, or piracy content.
- Workers spending too much time on Facebook, watching YouTube videos, or surfing online shopping sites.
- Employees idling too much, coming to work late, frequently absent, etc.
- Spending excess time on personal tasks such as applying for jobs.
- Abusing company resources, such as printing unnecessary copies of documents, throttling the network, etc.
- Using applications or sites that are unproductive or unauthorized.
- Not following prescribed policy when dealing with customers.
- Not following corporate etiquette policy, for example, visiting gambling sites.
- Using browser's incognito/private mode.
- Contractor submitting invoices that do match work hours or task completion status.

5.3 Malicious Behavior

With Teramind DLP you can create Activity, Agent Schedule, and Content-based rules to detect malicious behavior or suspicious intents easily. For example:

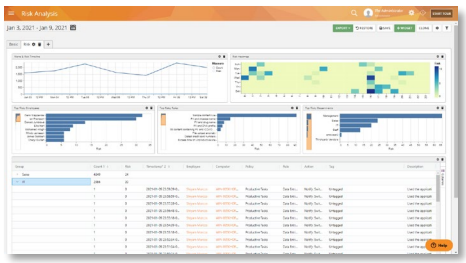
- Customer agent asking for credit card numbers in unsecured email or support chat.
- Sales rep copying customer data from the CRM site and emailing it outside.
- Uploading documents that contain sensitive data to personal Cloud drives.
- Unauthorized users reading documents they should not have access to.
- An employee participating in insider trading by sharing embargoed information.
- A user trying to hide information in an image.
- Sending out emails with sensitive files to non-corporate emails.
- The non-authorized use of cloud sharing drives as an attempt to exfiltrate data.
- Sharing 'not for the pubic' files on social media or IMs.
- Running network snooper, registry editor, or other dangerous applications.
- Running software from external media or cloud services.
- Changing the configuration of the network or system settings.
- Saving files on removable media.
- Employees communicating with competitors.
- RDP connection attempts to forbidden hosts or unauthorized use of RDP applications.
- Sudden change in schedules or work patterns.

What are some useful resources for this feature?

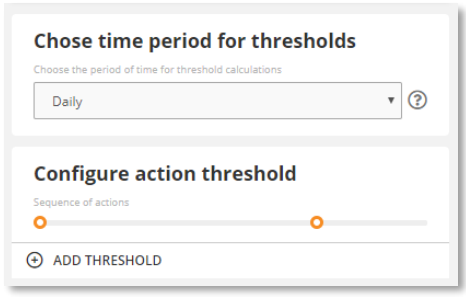
- Video: How to use Teramind to monitor and block data exfiltration attempts to USB/external drives

- Video: Teramind How-To Series: Block clipboard copy/paste actions for sensitive data
- Video: Teramind How-To Series: Preventing data loss with Teramind
- Knowledge Base Article: How to Detect and Prevent Data Leaks with Teramind

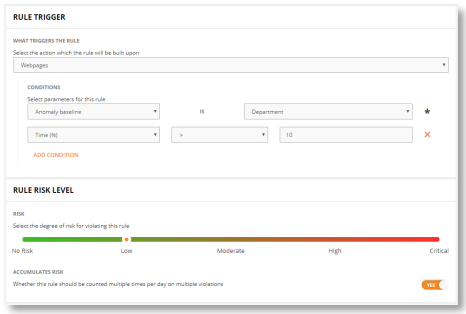
5.4 Dynamic Risk Scoring



Conduct Risk Analysis:
You can use the BI Reports > Behavior Alerts > Risk screen or create your own risk analysis reports to conduct an organization-wide risk assessment. You can find out top risky users, rules, and objects (applications and websites). You can plot risk trends, for example, by department, severity, number of violations, tag, etc. Unique risk score helps you identify high-risk users or policies so that plans can be developed for treating the risks.

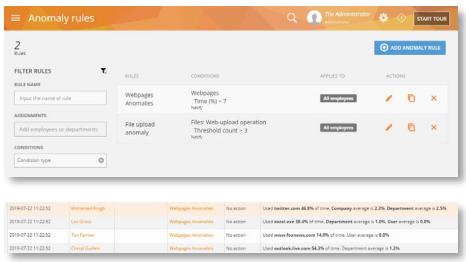


Assign Risks to Rules:
Each rule has an Advanced Action tab where you can assign risk to an activity based on frequency. You can add multiple thresholds, assign risk levels and take different actions depending on how often the rule is violated. For example, you can set an email rule that sets a Low risk when a user sends 5 emails in a day. However, if they send more than 10 emails a day, then the rule will set a Moderate risk level and trigger a Notification action.

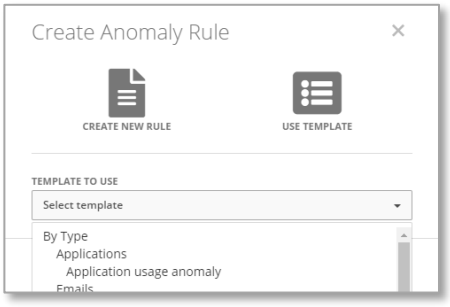


Assign Risks to Behavioral Baselines:
With the Anomaly Rules, you can assign dynamic risks to anomalous behaviors based on time and baseline compared at user, departmental, or organization level. For example, you can set up a website anomaly rule that assigns a high risk to a user's behavior if they spend more than 20% of their time over their departmental baseline. The risk score will then auto-adjust over time as both the user's and the department's activities change. The risk score will also reflect this on the Risk report.

5.5 Anomaly Detection



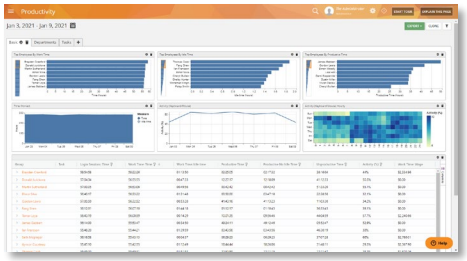
Anomaly Rules (On-Premise):
Anomaly Rules are special types of rules available on Teramind UAM and Teramind DLP. They allow you to identify anomalies in user behavior or application activities by utilizing behavioral baselines. An anomaly rule also allows you to assign risk levels to the behavior and a notification action to inform admins or managers about such anomalies. You can view the anomalies on the Alert report along with the rule violation incidents.

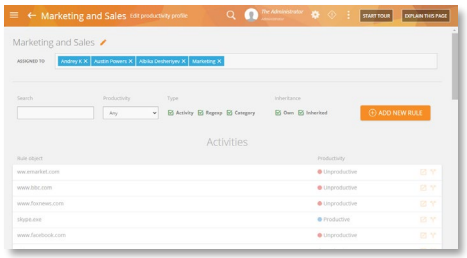


Built-in Templates:
Teramind DLP comes with many anomaly rule templates for Applications, Emails, Files, Instant Messages, Networking, Printing, etc. Using the templates, you can start creating sophisticated anomaly rules in no time.

6 Workforce Productivity

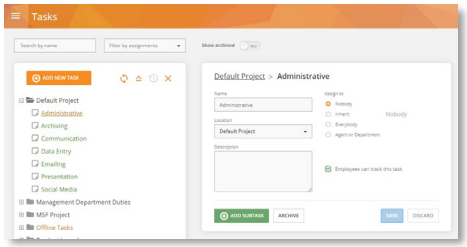
6.1 Productivity Analysis & Reporting

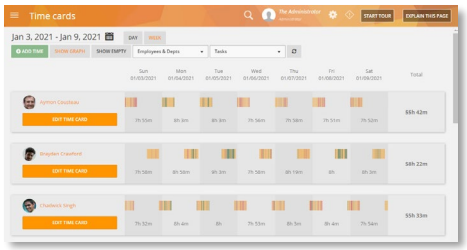




- Productivity reports allow you to track productive, unproductive, active, and idle time and performance KPIs for employees and departments.
- Classify apps/websites as productive, unproductive or into custom categories.
- Identify top employees by Work Time, Idle Time, Productive Time, Session Time, Activity %, etc.
- Track time spent and wages on different employees, departments, projects, or tasks.
- Understand exactly how shifts are spent through minute-by-minute activity monitoring to best utilize your workers.

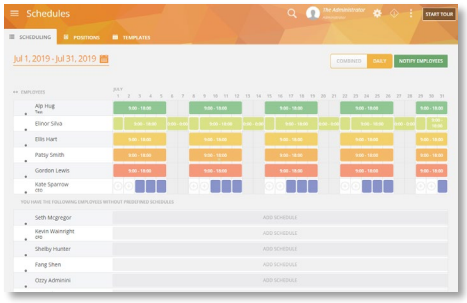
6.2 Time Tracking

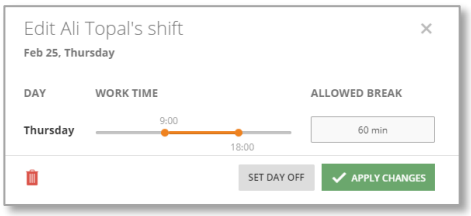




- Automatically assign tasks to employees and track time based on their activity or let them manage their clock-in.
- Comes with Time Tracker, Employee Cost, Task Cost, Time Records, and Time Card reports.
- Add missing time entries and notes such as PTO/time off, accruals, etc. for auditing and compliance purposes.
- Analyze payroll and discover your cost drivers such as unproductive hours and absence.
- View screen snapshots and session records of the selected time period.
- Import projects and tasks from PM solutions such as Zendesk, JIRA, etc.

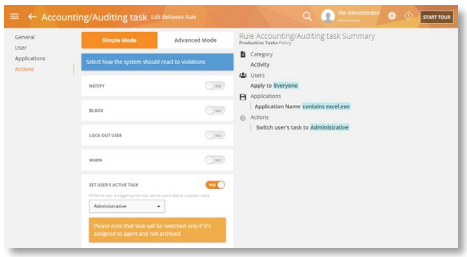
6.3 Template-Based Scheduling

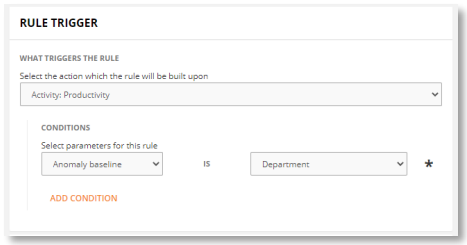




- Create daily and weekly schedules for your employees and contractors.
- Notify employees about their schedule changes automatically.
- Configure worktime, launch breaks, days off, etc.
- See who is late, stays overtime, or leaves early.
- Prevent users from using their computers or access certain apps when they are not scheduled to work.
- Batch-assign schedules to multiple employees at once.
- Create schedule-based rules such as late, absent, early start, late shift, etc.

6.4 Workflow Automation



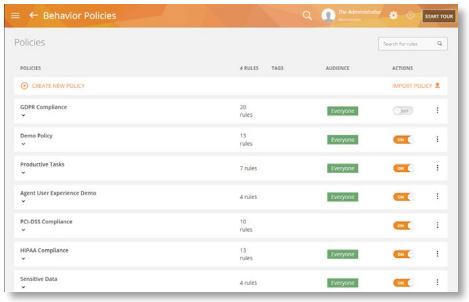


- Create productivity rules. For example, if an employee is idle for longer than a certain time, send them a warning automatically.
- Create anomaly rules to get early warning on fringe cases. For example, employee productivity dropping below their own, departmental or organizational baseline.
- Train new staff or provide job shadowing support using the Remote Control feature. Develop training materials, demo, tutorials, etc. using the Screen and Audio recording features.
- Provide on-demand feedback and gamify performance reviews utilizing custom alert messages. For example, automatically send a congratulatory message to an employee when their productivity reaches the Top 10 spot.

7 Policy and Rules Management

The core of Teramind is its policy and rules engine which can automatically detect malicious, inadvertent, or accidental threats. You can get started right away with hundreds of pre-built rule templates, activity classification lists, and data categories. Create your own policies and rules with an intuitive, visual rule editor. Use natural English, regular expressions, and sample conditions to easily define your requirements. Create monitoring profiles for individual employees, groups, or departments all from a wizard-like interface.

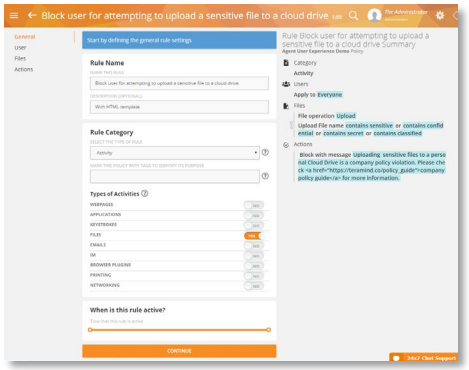
7.1 Policy Manager



Policies help you organize similar rules together or apply a set of rules to some particular users. For example, you can have all your HR-specific rules such as 'Preventing email harassment', 'Limiting social media use' etc. under the 'Business Etiquette' policy.

- You can create as many policies as you want.
- Import or export policies and share rules across them.
- Teramind DLP comes with a sample policy with some rules for you to experiment with.

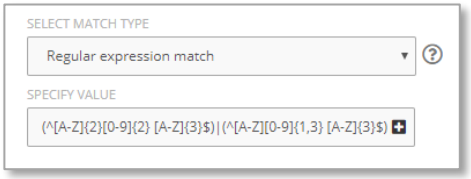
7.2 Visual Rule Editor



The Rules Editor is an intuitive, visual editor where you can create even complex rules easily without going through multiple screens or coding.

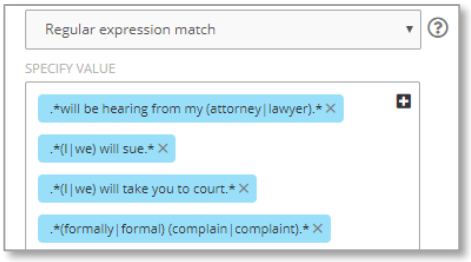
- A step-by-step wizard guides you through the entire rule creation process.
- The editor shows an easy-to-read natural language summary of the rule so anyone can follow how it works and what it does.
- Hundreds of built-in templates to choose from.
- Simple and Advanced modes for beginners and experienced users.

7.3 Regular Expression Support



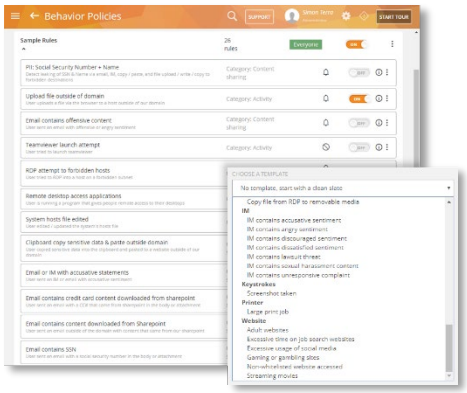
A Regular Expression or RegEx is a sequence of characters that define a pattern. Such patterns are very powerful compared to keywords or simple text searches in locating hard-to-find, repetitive information.

- Teramind DLP allows you to use Regular Expressions in rule conditions, searches, filters, monitoring settings, etc.
- You can use it to detect numeric or structured data such as credit card numbers, zip/postal codes, account numbers, etc.



- You can also detect sensitive words or phrases such as harassment or angry sentiment in emails.
- Find all pages that contain a certain set of words in a specific order in web pages or documents.

7.4 Out-of-the-Box Rule Templates

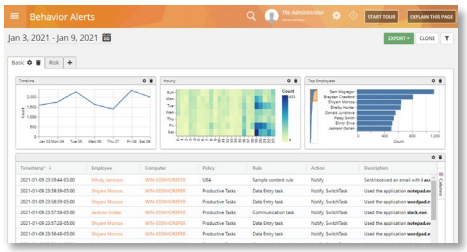


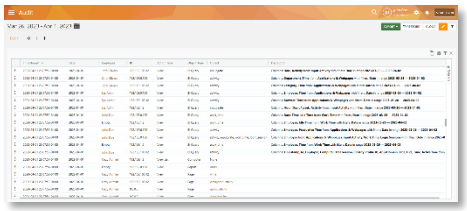
- Teramind DLP comes with hundreds of pre-defined policies and rules. For example block email containing sensitive keywords, stop the uploading of a confidential document, detect screen capture, prevent the use of external drives, etc.
- MITRE ATT&CK Detection & Prevention Library with over 350 behavior policies and rules
- Other pre-packaged sample rules ready for use.
- Unlike Teramind Starter or Teramind UAM, there are no restrictions on which of the templates/rules you can use on Teramind DLP.

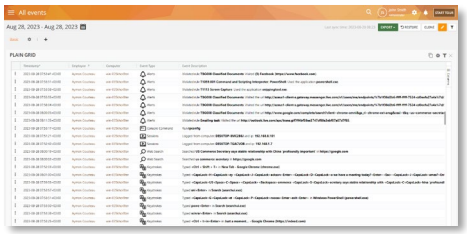
8 Audit & Forensics

In addition to the monitoring and alert reports, Teramind DLP comes with a Session Player that allows you to access a user's desktop live or view recordings of previous sessions. You can see all the notifications the user received and conduct powerful on-screen content search with OCR.

8.1 Real-Time Alerts & Audit Logs

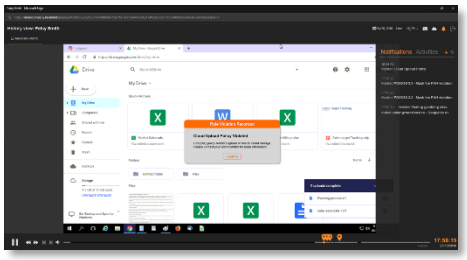


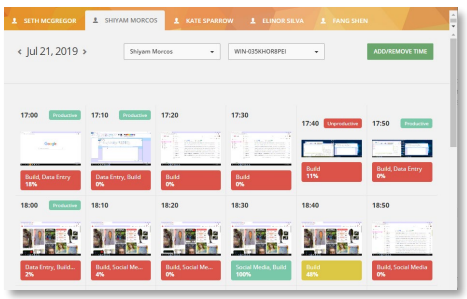




- View all rule violation incidents and alerts, actions taken by the system, alerts trend, and timeline, most violated policy & rules, most risky users, etc.
- Click on an alert to view the session recording or to investigate an employee.
- Prioritize alerts to prevent false alarms.
- Get scheduled alert digest and email notifications.
- Configure alert messages and templates with HTML.
- View and analyze immutable system and user logs with the built-in *Audit*, *All Events*, *Computer*, *Employee* and *Session Logs* reports.
- Export the alerts and logs as CSV or PDF.
- Integrate with SIEM and log analytics systems such as Splunk to send alerts and event logs.

8.2 Video Recording of All User Activity





- Teramind visually captures every action that a user makes in real-time.
- Live View or History Playback of the user's desktop.
- Take remote control or freeze input.
- Precisely locate when a rule violation incident occurred and view the user activities leading up to the event.
- Take screenshots or export the recordings as MP4 files.
- Supports multi-screen setups and virtual desktops.
- View user activity at a glance with Live Montage and Screen Snapshots with simple color-coding.
- Access the recordings from the Monitoring Reports, Alerts, and Session Logs for any date/time and activity.

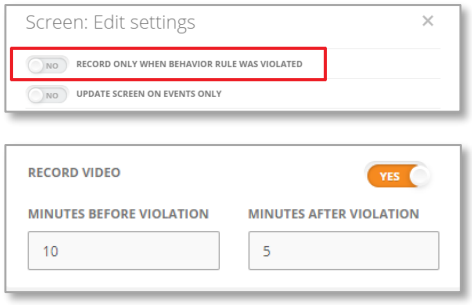
8.3 Audio Recording

When enabled, Audio Recording captures both input (Microphone, Line-in) and output (Speakers, Line-Out, Application Sounds), etc. The audio recording is available as part of the video recordings and can be played back with the video player. Please see the Video Recording of All User Activity section above for more information.

8.4 OCR of Screen Content

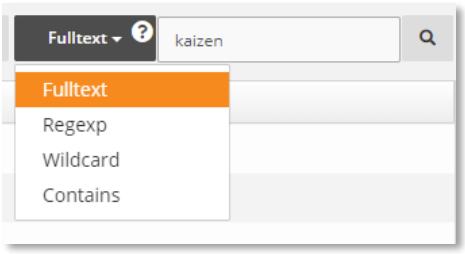
Teramind saves all the screen recordings with meta-data and indexes so that you can conduct a high-speed OCR search in the captured recordings. See the OCR section above for more information on how the OCR feature works.

8.5 Option to Record Only During Violation



- Teramind can be configured to record the Screen/Desktop only during a rule violation incident (by default Teramind records for 24/7).
- Additionally, Teramind UAM and Teramind DLP allow dynamic recording on a rule-by-rule basis. You can control how long it will record both before and after the rule violation incident.

8.6 Full-Text Search



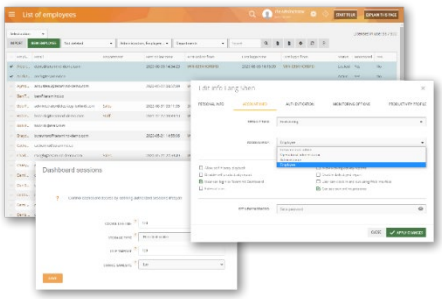
In Teramind UAM and Teramind DLP, you can conduct OCR text searches using:

- **Fulltext:** Full-text search with natural language processing (NLP).
- **Regexp:** Regular expressions, e.g. `[a-zA-Z]{4}[0-9]{12}`.
- **Wildcard:** Use '*' as a wildcard, e.g. `*doe` will match `John doe`, `jdoe`, `ddoe`, etc.
- **Contains:** Find any phrase that contains the text specified. Same as `*term*`.

9 Role-Based Access Control (RBAC)

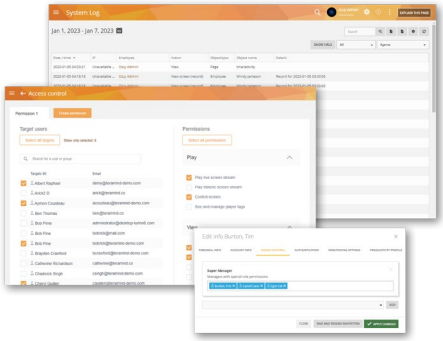
Teramind comes with a comprehensive set of access control features to help you monitor and manage access to critical systems and data to prevent privilege misuse and abuse. A dedicated Access Control Dashboard allows you to create customized access control policies and rules to manage user privileges.

9.1 Standardized Account Roles and Profiles



- Use built-in account types such as Admin, Ops Admin, Sys Admin, Employee, Department Managers, etc.
- Control monitoring settings, authentication and productivity profiles of users or groups.
- Enforce password policy, expiry and complexity requirements.
- Enforce session policy, time out, lifespan, etc.

9.2 Access Control Dashboard

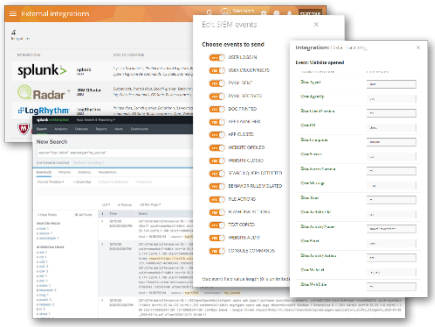


- Implement multi-layered identity authentication, authorization, and access control policies.
- Create access permissions, view and edit controls for privileged users.
- Apply special role permissions to department managers, supervisors, etc.
- Audit admin activities with immutable system logs.

10 Third-Party Integrations

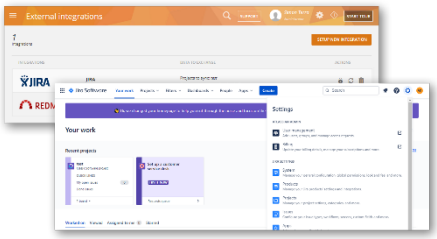
Teramind comes with built-in integration support for Security Information and Event Management (SIEM) and Project Management (PM) software. You can send real-time event and meta-data from Teramind to the integrated software. Teramind can also be integrated with Active Directory and Single Sign On (SSO) solutions. Here's a quick overview of the integration options.

10.1 SIEM / Threat Analytics Solutions



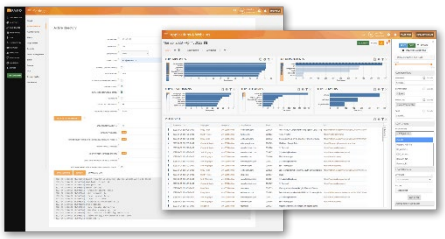
- Built-in integration support for Splunk, HP ArcSight, IBM QRadar, LogRhythm, etc.
- Send real-time event telemetry and meta-data.
- Common Event Format (CEF), Common Information Model (CIM) and JSON formats enable integration with virtually any solution in minutes.
- Customizable field mapping.
- Customized business process tracking.
- Secure connection option over TCP, TLS, UDP.

10.2 Project Management & Ticketing Solutions



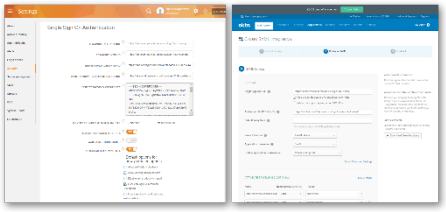
- Built-in integration support for JIRA, Redmine, Zendesk, etc.
- Sync projects, task statuses and test statuses.
- Import time tracking information directly to Teramind.
- Assign users, testers and supervisor roles.
- Customizable field mapping.
- Launch the Revealed Agent from your existing solution to track time with special launch parameters.

10.3 Active Directory



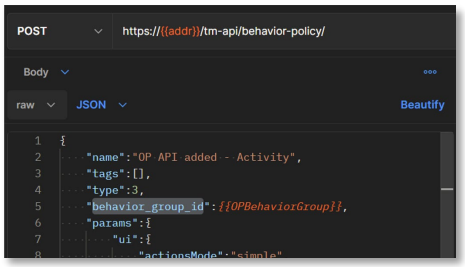
- Built-in integration with Active Directory over LDAP.
- Import users, computers, groups/OUs, attributes.
- Filter reports with attributes and groups.
- Apply rules to OU's and/or groups.
- Remote install using Group Policy (GPO).
- Use Teramind only on a specific group.
- Use your own custom AD sync profiles.
- Sync with multiple AD domains/servers.

10.4 Single Sign On (SSO)



- Authenticate to the Teramind Dashboard using a Single Sign On (SSO) service such as Okta, One Login etc.
- Support for SAML 2.0 protocol, X.509 certificate.
- Auto register new agents and configure default options.

10.5 API



- View and control most aspects of the solution with a set of robust APIs.
- Secure connectivity with your own JW access tokens.
- Use Teramind with any web services solution to push/pull data.

11 Deployment

11.1 Supported Platforms

Windows 8 & Up	Citrix XenApp® & XenDesk®	Windows Server 2012 & Up	VMware Horizon	macOS 10.14 & Up

11.2 Hosting 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.

11.3 Support

- Installation assistance
- We set up the host for you (for the Cloud deployment option)
- 24x7 follow-the-sun support
- Option for Enterprise SLA
- Subscription includes software updates