

Features Guide

Version 1.6 (27 NOV 2023)



Table of Contents

1	Teramind DLP Features Overview		4	
2	Featu	res Comparison	5	
3	Monitoring and Detection Capabilities			
	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 I	oss 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 E	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	Work	force 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-I	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	Deplo	yment	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:



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, Professiona Services, Customizations
User Activity Monitoring				
Web pages & applications	\checkmark	\checkmark	\checkmark	√
OCR		\checkmark	\checkmark	√
Remote control	\checkmark	\checkmark	\checkmark	√
Email		\checkmark	\checkmark	1
Console commands		\checkmark	\checkmark	√
File transfers		\checkmark	\checkmark	\checkmark
Network		\checkmark	\checkmark	√
Instant messaging	\checkmark	\checkmark	\checkmark	\checkmark
Social media activity	\checkmark	\checkmark	\checkmark	\checkmark
Online meetings		\checkmark	\checkmark	\checkmark
Geolocation		\checkmark	\checkmark	\checkmark
Camera usage		\checkmark	\checkmark	1
Keystrokes		\checkmark	\checkmark	\checkmark
Clipboard (copy and paste)			\checkmark	\checkmark
Searches	\checkmark	\checkmark	\checkmark	√
Printing		\checkmark	\checkmark	√
Browser plugins	\checkmark	\checkmark	\checkmark	√
Registry	\checkmark	\checkmark	\checkmark	√
OS state	\checkmark	\checkmark	\checkmark	√
Custom website field capture				√
Custom app field capture				√
Data Loss Prevention				
Data discovery & classifications			\checkmark	1
Define content-based rules			\checkmark	√
Define file operation-based rules			\checkmark	√
Prevent malicious or negligent data exfiltration			\checkmark	√
Document and data fingerprinting			\checkmark	√
Regulatory compliance including HIPAA, GDPR, etc.			\checkmark	√
User Behavior Analytics				
Insider threat detection	\checkmark	\checkmark	\checkmark	\checkmark
Abusive behavior	\checkmark	\checkmark	\checkmark	1
Malicious behavior	\checkmark	\checkmark	\checkmark	1
Dynamic risk scoring		\checkmark	\checkmark	1
Anomaly detection		\checkmark	\checkmark	1
Workforce productivity analysis	\checkmark	\checkmark	\checkmark	√
Active vs idle time analysis	\checkmark	\checkmark	\checkmark	√
Template based scheduling	\checkmark	\checkmark	\checkmark	√
Interactive productivity reporting	√	√	\checkmark	√
Policy and Rules Management				
Policy manager	\checkmark	\checkmark	\checkmark	1
Visual rule editor	\checkmark	\checkmark	\checkmark	\checkmark
Regular expression support		\checkmark	\checkmark	√
Out-of-the box rule templates		√	\checkmark	√
Activity blocking + 7 other rule actions	Limited	√	\checkmark	√
Audit & Forensics				
Video recording of all user activity	\checkmark	\checkmark	\checkmark	\checkmark
Audio recording	\checkmark	\checkmark	\checkmark	\checkmark
OCR of screen content, OCR search, OCR rules		\checkmark	\checkmark	\checkmark
Option to record only during violation		\checkmark	\checkmark	\checkmark
Full text search of activities and meta-data		√	\checkmark	√
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	√	√	\checkmark	√
24x7 follow-the-sun support	√	√	\checkmark	√
Subscription includes software updates	\checkmark	√	\checkmark	√
Worry-Free Cloud Hosting				
No servers needed	\checkmark	\checkmark	\checkmark	√
			/	√
We set up and host for you Secure, Tier 3 data center	√ √	\checkmark	\checkmark	↓ ↓

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 preemptive actions such as warning a user, blocking an action, or taking control over their computers at any time.

3.1 Applications & Websites



- 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.

NO TRACK COP	ISOLE COMMANDS	
IONITOR ONLY THESE	APPLICATIONS	
Salesforce X Sr	Websites: Edit settings	×
USPEND MONITORI	MONITOR ONLY THESE WEBSITES	
facebook x me	Selesforce X SAP Logon 720 X Sage 50 Portal X	0
USPEND KEYSTROK	DON'T MONITOR WEB TRAFFIC FOR THESE WEBSITES	
	teramind.co X mail.google.com X	0
Skype × Firefo	SUSPEND MONITORING WHEN THESE WEBSITES ARE VISITED	
sope x men	gmail.com X mail.google.com X outlook.live.com X	0
	SUSPEND MONITORING WHEN WEBSITE CONTENT CONTAINS	
USPEND KEYSTROK	Text list - URL X	0
	DON'T MONITOR WEB TRAFFIC FOR THESE IPS	
	Network list - Safe sites 🗙	0
DLE TIME THRESHOL	SUSPEND MONITORING WHEN BROWSING TO THESE IPS	
10		0
	SUSPEND MONITORING WHEN BROWSING TO IPS NOT IN LIST	
	Network list - Blacklisted IPs 🔀	0
	SUSPEND KEYSTROKE MONITORING WHEN THESE WEBSITES ARE VISITED	
	sccounts.google.com x login.live.com x login.yshoo.com x login.sk	/pe.com X
	DON'T MONITOR PRIVATE BROWSING	
	WSS PORT	
	1501	

- 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?

Condition 1	×
Webpage Url 📀	
ONDITION	
Contains facebook.com 🗙 Contains instagram.com 🗙 Contains twitter.com 🗙	
Contains youtube.com 🗙 Contains pinterest 🗙 Contains tumblr 🗙	?
Contains facebook.com/business 🗙	(?)
	(?)
Contains facebook.com/business 🗙	?
Contains facebook.com/business x	
Contains facebook.com/business x Contains youtube.com/channel/UCSKRq9qTqFlyyQdovb01.g/ x condition 2	
Contains facebook.com/business x Contains youtube.com/channel/UCSKRq9qTqFjyyQdovb01.g/ x condition 2 Webpage Title ©	×
Contains facebook.com/business x Contains youtube.com/channel/UCSARg6gTqF}yy/Qdoxb0-Lg/ x Condition 2 Webpage Title ONDITION	
Contains facebook.com/business x Contains youtube.com/channel/UCSARg6gTqF}yy/Qdoxb0-Lg/ x Condition 2 Webpage Title ONDITION	×
Contains facebook.com/business x Contains youtube.com/channel/UCSiRiqbqTqFjyyjQdovb0-Lg/ x condition 2 Webpage Title Contains Equals int Shopping Sites x	×

- 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 <u>OCR</u> section for more information.

What are some useful resources for this feature?

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

3.2 Browser Plugins

What report can I access for this activity?

No dedicated report

What monitoring & tracking controls do I have?

No settings

- Browser Plugins activities can be monitored under the <u>Applications & Websites</u> and other related BI reports (e.g. the <u>Web File Events</u> report shows details for all the uploads/downloads done through the browser).
- The Browser Plugins does not have a dedicated settings panel and is controlled under the Websites settings panel. Check out the <u>Applications & Websites</u> monitoring and tracking controls for more information.

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

Condition 1	
Browser [×] Plugin permissions [×] ⊕	
CONDITION	
Opera 🗙 Firefox 🗙	0
EXCEPT	
Start typing	0

What are some sample rules using this feature?

	lle Block dangerous plugins Summary R Compliance Policy	
Ē	Category	
	Activity	
-	Users	
	Apply to Everyone	
2	Browser	
	Plugin permissions Proxy VPN	
8	Actions	
	After 2 violation(s) Block with message Potential dangerous plugin	

• 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.
- 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: <u>BI Reports > Applications & Websites</u>
- User Guide: <u>Monitoring Settings > Websites Settings</u>
- Rules Guide: <u>Activity Rules > Browser Plugins</u>

3.3 Emails

1. 2021 - Jan 16, 2021 🗃			and the second	Q 🚹 Sectoriarian	C C Electrone Genues Inc.
	5				
	n Sarat +				
				• near	
Net, whe Share from all the latest strategy from a latest provide the latest sectory factory (sector)	E Santa Alerena Digen alerena		There is a second secon		Pasar Pasar Pasar Pasar Pasar Pasar
		Contraction design		· barataireatera	
10 0N 161 0N	No. of the second				
-	Seatory's i Seato	Extintes (enterlying)	Separt (nuc) i hos	ning Outputs	
Carilleritaniae Provid Determinet			5 1		1
France Submercelle					1
Catana's parcea information dia			1 1	1	
Pationad					
Dellinati			1 1		
Buptowe animally					
The Set Environments					
family details and a state					
The Moto & Dallatante					(D and
EMAIL LOG body D coos Micahu Miram eb	on't count the days, make el Redmond ay@reply.ebay.co.uk		Jackson Gollan p	osted an updatejuly 19 at	œ > sp51 AM ViewSeitus →
EMAIL LOG body D coos Micahe M from eb E to micah	el Redmond ay@reply.ebay.co.uk teredmon-0 <mredmond8< td=""><td>Steramind-demo.com></td><td>Jøckson Gollen p</td><td>osted an updatejuly 19 at</td><td></td></mredmond8<>	Steramind-demo.com>	Jøckson Gollen p	osted an updatejuly 19 at	
EMAIL LOG body D coos Micahn from eb to micah subject	el Redmond ay@reply.ebay.co.uk teredmon-0 <mredmond8 @ Here we go Don't le</mredmond8 	Steramind-demo.com> et this get away!			951 AM View Status
EMAIL LOG body D coos Micahn from eb to micah subject	el Redmond ay@reply.ebay.co.uk teredmon-0 <mredmond8 @ Here we go Don't le</mredmond8 	Steramind-demo.com>			951 AM View Status
EMAIL LOG body D coos Micahn from eb to micah subject	el Redmond wy@reply.ebsy.co.uk teredmon-0 <mredmond@ @ Here we go Don't le st more of what you love '</mredmond@ 	Steramind-demo.com> et this get away!			9651 AM View Status
EMAIL LOG body D Micah from 60 micabject body Gs coss Ellis Ha	el Redmond wy@reply.ebsy.co.uk teredmon-0 <mredmond@ @ Here we go Don't le st more of what you love '</mredmond@ 	Steramind-demo.com> et this get away!			9651 AM View Status
EMAIL LOG body DA Micahn Micahn to micał subject body Ge Ellis Há Ellis Há	el Redmond ay@reply.ebsy.co.uk seredmon-0-threadmond@ @ Here we go Don't le ts more of what you love 's art fers@wish.com	Øseramind-demo.com> et this get away! View In Browser Fashion -			9651 AM View Status
EMAIL LOG body D coss Micaha aubject body Ge coss Ellis Hu to Elis H	el Redmond ay@reply.ebay.co.uk seredmon-0-onvedmond@ @ Here we go Don't le tr more of what you love h art fers@widh.com Her<@hart@teramind-der	@teramind-demo.com> et this get away! View In Browser Fashion - mo.com>	Home & Garden - Elect	ronics · Motors · Daily De	951 AM View Status
EMAIL LOG body D coss Micaha aubject body Ge coss Ellis Hu to Elis H	el Redmond ay@reply.ebay.co.uk seredmon-0-onvedmond@ @ Here we go Don't le tr more of what you love h art fers@widh.com Her<@hart@teramind-der	Øseramind-demo.com> et this get away! View In Browser Fashion -	Home & Garden - Elect	ronics · Motors · Daily De	951 AM View Status

- 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?

mails: Edit settings	^
YES CAPTURE INCOMING	
YES CAPTURE OUTGOING	
YES O SAVE ATTACHMENTS	
YES O CAPTURE EMAIL CONTENT	
NORE ATTACHMENTS WITH FILENAMES MATCHING (REGEX)	
APTURE EMAILS THROUGH	
APTURE EMAILS THROUGH Desktop Outlook x Outlook Web Access x Gmail x Yahoo Mail x Outlook.cm x	

Condition 1		×
Mail Direction		
INCOMING	OUTGOING	(?)
Condition 2		×
Mail To		
CONDITION		
Start typing		(?)
EXCEPT		
Contains teramind.co 🗙		(?)

What are some sample rules using this feature?

Ru	le Protect personal data Summary • Palicy Policy
	Category
-	Content sharing
	Users
	Apply to Everyone
	Content
	USA zip code and address matches 5 times
	Phones numbers matches 5 times
2	Emails Mail Direction is outgoing
0	Actions
0	Show warning with message Possible personally identifiable data. Please make sure you follow the company policy handling it.
	le Email with attachment to pen business address Summany
Den	le Email with attachment to non-business address Summary b blicy Pelcy
Den	to Policy Policy Category
Den	to Policy Policy
Den	to Policy Policy Category
Den	na Policy Category Activity
Den E	a Paling-Palicy Category Activity Users
Den E	a halap Palay Category Activity Users Apply to Everyone
Den E	an Palicy Pelicy Category Activity Users Apply to Everyone Emails
Den E	e Nelicy Pelicy Category Activity Users Apply to Everyone Emails Mail To contains @gmail. or contains @yahoo or contains @msn
Den	a haliay Paloy Category Activity Users Apply to Everyone Emails Mail To contains @gmail.or contains @yahoo or contains @msn Haia stachments

- 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.
- 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.
- 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.

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

Rule Prevents sending emails from non-approved email clien Demo Policy Policy	ts Summary
Category	
Activity	
🔹 Users	
Apply to Everyone	
🔤 Emails	
Mail Client excludes Outlook client or Outlook web client Mail Direction is outgoing	
⊗ Actions	
Block with message Please use Outlook to send any official emails.	

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

What are some useful resources for this feature?

- User Guide: <u>BI Reports > Emails</u>
- User Guide: <u>Monitoring Settings > Emails Settings</u>

•

- Rules Guide: <u>Activity Rules > Emails</u>
- Rules Guide: <u>Content Sharing Rules > Emails</u>

3.4 Online Meetings

What report can I access for this activity?

an 3, 2021 - Ja	n 9, 2021 🛅					Employees & Depts + Computers + D
Date/Sime *	Employee	Computer	Duration	Application	Direction	Perticipants
2021 01 08 03:48: 🝽		WN 0356H.	0.00.08	Zoom	incoming	Tia Sanders, +1
021-01-08 03-68 🗰	Tie Senders	WIN-035KH.	0.00-08	Zoom	Outgoing	Tia Sanders, Mohamed Krogh, jgollan
2021 01 08 031481 🗰	Mohamed Kregh	WN 03504.	0.00.08	Zoom	incoming	Tia Sanders, +1
2021-01-08 03:38: 🗰	Jackson Gollan	WN-035/01_	0.00.05	Zoom	Incoming	Tia Sandera, +1
021-01-08-03:37	Tie Sanders	WN-03561	0.01:01	Zoom	Outgoing	Tia Sanders, jgollan
2021 01 07 09:43: 🗰	Kate Sparrow	WIN 035KH	0.00.03	Zoom	Outgoing	Kate Sparrow
2021-01-07-09:20: =	Leo Stiles	WN-035/04_	0.00.04	Zoom	Incoming	Leo Stiles. Kate Sperrow
2021 01 07 09(20(🖝	Kate Sparrow	WIN 035KH	0.00/26	Zoom	Outgoing	Kate Sparrow
2021-01-07 09:00: 🗰	Kate Sparrow	WIN-035KH	0.02.13	Zoom	Outgoing	Kate Sparrow
2021-01-07 03:23:	Thomas Cook	WN-03501.	0.00.25	Zoom	incoming	Tia Sanders, +1
2021-01-07-03-23 🖝	Jackson Gollan	WN-035/04_	0.00.25	Zoom	Incoming	Tia Sanders. +1
2021-01-07 03:23: 🗰	Mohamed Krogh	WN-035/01_	0.00.13	Zoom	Incoming	Tia Sanders. +1
2021 01 07 03:23 🗰	Tia Sanders	WIN 035KH	0.00.26	Zoom	Outgoing	Tia Sanders, toook, Mohamed Kregh, jgollan
2021-01-07-02:111	Tie Sanders	WN-035KH_	0.01:29	Zoom	Outgoing	Tia Sanders
2021 01 05 13:58 🗰		WN 0358H	0.00.04	Zoom	Outeoing	Les Sties

What monitoring & tracking controls do I have?

Online Meetings: Edit settings	×
RACK THESE APPLICATIONS	
8x8 x Zoom x RingCentral x AirCall x	
	0

- 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 <u>Audit & Forensics</u> section to learn more).
- 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?

ondition 1		
Application Name	Time Active (min) 🎽 🕣	
CONDITION		
Contains aircall \times		3
EXCEPT		
Start typing		?

- 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?

Rule test Summar est Policy	у	
Category		
Activity		
Sers Users		
Apply to Everyone		
Applications		
Time Active (min)	>= 60min.	
Application Name	contains aircall	
Actions		
Record Smin be	ore and 5min after violation	

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

3.5 Console Commands

What report can I access for this activity?

Image: Compare Type: Compar	2021 - Jan 1	6. 2021 🗖							Last upto New 2021-01-02 2021
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1									
Image: Computer With 23501008FEIs Computer With 23501008FEIs Computer With 23501008FEIs Computer With 23501008FEIs Computer With 23501008FEIs Computer With 23501008FEIs Computer With 23501008FEIs Computer With 23501008FEIs Computer With 23501008FEIs Computer With 23501008FEIs Computer With 23501008FEIs Computer With 23501008FEIs Computer With 23501008FEIs Computer With 23501008FEIs Computer With 23501008FEIs Computer With 23501008FEIs Computer With 23501008FEIs Computer With 23501008FEIs Computer With 23501008FEIs Computer With 23501008FEIs Computer With 23501008FEIs Computer With 23501008FEIs Computer With 23501008FEIs Computer With 23501008FEIs Computer With 23501008FEIs Computer With 23501008FEIs Computer With 23501008FEIs Computer With 23501008FEIs Computer With 23501008FEIs Computer With 23501008FEIs Computer With 23501008FEIs Computer With 23501008FEIs Computer With 23501008FEIs Computer Mith 2350108FEIs Computer With 2350108FEIs Computer With 2350108FEIs Computer Mith 2350108FEI Computer With 2350108FEIs Computer With 2350108FEIs Computer Mith 2350108FEI Computer With 2350108FEIs Communer With 2350108FEIs <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th>									
Image: Computer With C3550/068PEI Image: Computer With C3550/068PEI<	114 -			• • •		-		e e turbrose	
Mark Mark <th< th=""><th></th><th></th><th></th><th>2.1.2</th><th></th><th></th><th></th><th></th><th>Gos</th></th<>				2.1.2					Gos
Community Computer				1m	factoria.				
Image: Section of the sectio									
Image: Section of the sectio									
Image: Computer Wirk 20300008PEI Computer Wirk 20300008PEI Computer Wirk 2030008PEI Computer Wirk 2030008PEI <t< td=""><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></t<>									
Image: Computer With Q33501ORPES Computer With Q3501ORPES									
Image: Section of the sectio									
with and the second se									
Name Name <th< td=""><td></td><td></td><td></td><td>guindeene areas</td><td>114</td><td>669</td><td></td><td></td><td></td></th<>				guindeene areas	114	669			
Image: Section of the sectio									
View View <td< td=""><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></td<>									
Image: Section of the section of t									
Image: Section of the sectio									
Image: Section of the sectio									
Commute Commute <t< td=""><td>10110-0112-011-010</td><td></td><td></td><td></td><td></td><td>000</td><td></td><td></td><td></td></t<>	10110-0112-011-010					000			
Community Computer VIII-0250/07887EI Computer VIIII-0250/07887EI					respect		reput		
COMMANDS LOG Tamar Loya Computer WH-0350H089E1 Computer WH-0350H089E1 Computer WH-0350H089E1 Computer WH-0350H089E1 Computer WH-0350H089E1 Computer WH-0350H089E1 Computer UNIV-0350H089E1 COMPUTER UNIV COMPUTER UNIV C									
COMMANDS LOG Tamar Loya Computer WIN-03050/085PEI Computer WIN-03050/085PEI Computer WIN-03050/085PEIS*CIUSers/tdoyeAppOex/Local/yehoomessenger/sp U-2 Tamar Loya Computer WIN-03050/085PEI Computer WIN-03050/085PEIS*CIUSers/tdoyeAppOex/Local/yehoomessenger/sp U-2 Tamar Loya									D out
Computer WH-0330x004PEI Commuter WH-0330x004PEI Commuter EXANIND EDMAWWW-0330x004PEIS' 'Cillsen'tidayeAppDexil.cosilyehoomessengerlep Duration 000001 Computer WH-0330x004PEIS Commuter WH-0330x004PEIS' 'Cillsen'tidayeAppDexil.cosilyehoomessengerlep Duration 000000 Duration 000000 Joan Tamar Loya									* ×
Command TERANINO-DEMO/WIN-035KHOR8PEIs; "CIUsersitoya/AppDatelLocallyahoomessengerlap Durstion 000001 Temar Loya Commune TERANINO-DEMO/WIN-035KHOR8PEIs; "CIUsersitoya/AppDatelLocallyahoomessengerlap Durstion 000000 Durstion 000000 Durstion 000000 Durstion 000000				EVHODODEI					
Duration 000001 10 Tamber 10y Computer WIN-03300108FEI Commant FEANIND-00400WIN-03300108FEIS: "CIUSers'stopyeAppOexil.cosilywhoomessengerlep Duration 000000 10 Tamber 10ye									
In 50 Tamar Loya Computer WIN-035KHOR8PEI Commune TEAMIND 26MO WIN-035KHOR8PEIs: "C/UsersidoyeAppDealLocallyshoomessengerApp- Duration 000000 Duration 000000 Tamar Loya		Comma	ind TERAM	IND-DEMO\WIN	1-035KH	OR8PE	\$: "C:\Users\t	loya\AppData\Lo	ocal\yahoomessenger\ap
Computer VIIN-035KHOR8PEI Command TERAMINO-DEMOVINN-035KHOR8PEIS: "CriUserstoloyelAppDatalLocallyshoomessengerlap Duration 00:00:00 Vmana Loya									
Command TERAMINO-DEMO/WIN-035KHOR8PEIS: "CilUsers'toloya'AppData/Locallyahoomessenger/ap Duration 00:00:00 Jon 2 Tamar Loya		Duratio	n 00:00:01						
Command TERANIND-DEMO1WIN-035KHOR8PEIS: "CriUsers'tdoya'AppData/Locallyahoomessenger/ap Duration 00:00:00 Jun 30 Tamar Loya	-								
Duration 00:00:00 Jun 30 Tamar Loya	Jun 30	Tamar	Loya						
Duration 00:00:00 Jun 30 Tamar Loya	Jun 30	Tamar Compu	Loya ter WIN-03						
	Jun 30	Tamar Compu	Loya ter WIN-03		I-035KH	OR8PE	S: "C:\Users\t	loya\AppData\Lo	ocallyahoomessenger\ap
	Jun 30	Tamar Compu Comma	Loya ter WIN-03 and TERAM	IND-DEMO\WIN	I-035KH	OR8PE	\$: "C:\Users\t	loya\AppData\Lo	ocallyahoomessengerlap
Computer WIN-035KHOR8PEI	jun 30	Tamar Compur Comma Duratio	ter WIN-03 Ind TERAM	IND-DEMO\WIN	I-035KH	OR8PE	\$: "C:\Users\t	loya\AppData\Lo	ocal\yahoomessenger\ap

What monitoring & tracking controls do I have?



- 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.
- 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?

ondition 1		
Application Name × Launched fro	m CLI [×] ⊕	
NO	YES	(?)

What are some sample rules using this feature?

Ru Den	le Preventing running of network sniffers from the console Summary No Policy Policy
ľ	Category
	Activity
:	Users
	Apply to Everyone
B	Applications
	Application Name contains nmap or contains wireshark or contains smartsniff
	Launched from CLI
8	Actions
	Lock user with message Dangerous console command detected. You are locked out of the system.

- Activity-based rules for console commands can be created under the Applications category and has the same capabilities as the applicationbased rules. For additional detection triggers, you can use the Launched from CLI condition.
- 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: <u>BI Reports > Console Commands</u>
- User Guide: <u>Monitoring Settings > Applications Settings</u>
- Rules Guide: <u>Activity Rules > Applications</u>

3.6 File Events



- 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.

File tra	nsfers: Edit settings	×
ASIC SETTINGS	ADDITIONAL SETTINGS	
WHAT TO TRA	СК	
YES T	RACK LOCAL FILES	
YES T	RACK NETWORK FILES	
YES T	RACK LOCAL DOCUMENTS	
YES T	RACK NETWORK DOCUMENTS	
YES T	RACK EXTERNAL DOCUMENTS	
YES T	RACK CD/DVD BURNING	
YES T	RACK EXTERNAL DRIVES	
YES T	RACK FILE SYNC WITH CLOUD SERVICES	
FILE TYPES TO	TRACK	
YES T	KT FILES	
YES D	OC(X) FILES	
YES X	LS(X) FILES	
YES PI	PT FILES	
YES ZI	P FILES	
YES PI	DF FILES	
FILE EXTENSIO	DNS LIST TO TRACK	
.odm 🗙 .	gdoc 🗙 .gsheet 🗙	
		0
TRACK DOWN	LOADS AND UPLOADS FROM THESE APPLICATIONS	
Google Driv	ve 🗙 OneDrive 🗙 Dropbox 🗙 Box 🗙	
		0
DO NOT MON	ITOR THESE LOCATIONS	
windows >	C	
		0

- 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?

File Prope	rties		*	?
ELD TYPE				,
ANY	STRING	INTEGER	DATE	?
IELD NAME				
watermark				?
ELECT MATCH	TYPE			J
Contains			•	?
ONTAINS				J
CONFIDEN	TIAL			

What are some sample rules using this feature?

Rule Protect confidential documents Summary Demo Policy Policy
Category
Content sharing
😩 Users
Apply to Everyone
Content
String document field named WATERMARK contains Confidential
Ries .
e File operation Write
External Drive
© Actions
Block with message Do not share confidential documents.

- 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.
- 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.

Nuic	File transfer rule Summary
Demo F	Policy Policy
C	ategory
A	ctivity
🛎 U:	sers
A	pply to Everyone
R, Fil	les
	Drive All drives
~	File path equals /path/to/sensitive/files
	File operation Access
⊘ A(tions
_	Block
Rule Demo I	Block external drives Summary
Rule Demo I	Block external drives Summary Magazing
Rule Demo I B Ci Ar	Block external drives Summary Miley Paley ategory ctivity
Rule Demol	Block external drives Summary Mily Policy ategory etnity sers
Rule Demol	Block external drives Summary Miley Paley ategory ctivity
Rule Demo I A A A	Block external drives Summary Nelsy Policy otkity sers pply to Everyone
Rule Demol	Block external drives Summary Nelsy Policy otkity sers pply to Everyone
Rule Demo I A A E E FI	Block external drives Summary Merg Poolsy tetwory sers poly to Everyone les
Rule Demo I A A E E FI	Block external drives Summary vitegory stregory sers pply to Everyone les Drive All external drives File operation Any

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

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
- 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?

No settings

 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 <u>Applications & Websites</u> and <u>File Events</u> sections for more information.

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

Condition 1	
File operation Download URL × ↔	
CONDITION	
Download X	0
XCEPT	
Start typing	?

What are some sample rules using this feature?

	le test Summary Policy
ľ	Category
	Activity
2	Users
	Apply to Everyone
	Files
	File operation Download
	Download URL contains https://rapidshare.com
\otimes	Actions
	Record Smin before and Smin after violation

What are some useful resources for this feature?

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

3.8 Instant Messaging

What report can I access for this activity?

												• •	194110.0
ct, 1	, 2023 - Oct 31,	2023									00007 + 10-0110	041 0.09	- 2
	0.8 1 And	nem i +											
IN I	EUNE			е т ×	TOP EMPLOYEES			0.01	HOURLY			0) е т »
1	1			1000				1000	275575		10		Ĩ
		nio Gir siz w	0.042		I .								
	INATIONS		07 043									c	а • т ×
		NO Ser so w		Branker Attacher		a j a				* * * * * * * * * * * *	Doging Dation	c	
	TINATIONS Warring Systems	Second 1	Daster		le l	Dester REP Mr. Dester			in a second			c	
	Maring Systems Warring Systems	Seminar's gate to the second	Doubse Dagery	Arelent	-	a a a a a a a a a a a a a a a a a a a	Tak M		in a second			c	
	Maring Systems Monorthers Monorthers	5 Transieny" 1. 2021 10 10 114202 1420 2021 10 10 114202 1420	Donates Datasena Income	Alta Selli Alta Selli		a p a construir alla font a construir alla font a construir font a construir font a construir	Train Sec		in a second	Insering Disalments 0 1 2		c	
	INATIONS Wave last Wave have Wave have Wave have Sample Out	- Territory' 1 2011/01/01/00/00 2011/01/01/00/00 2011/01/01/00/00	Emotion Dutyering Dutyering Dutyering	Afra Series Annues Series		a j a Josén Jili bel Des S Jili bel Josén Sel Andore	Tak Me On an	er er diabreet Jock its stabreet	Mariana Mariana Mariana Mariana	Insering Disalments 0 1 2		c	
	TINATIONS Weeks Application Weeks Harris Weeks Harris Geogle Clar. Despite Clar.	5 Streaming () (2023 - 10 N 174022 - 4400 2023 - 10 N 174024 - 4400 2023 - 10 N 174024 - 4400 2023 - 10 N 174020 - 4400 2023 - 10 N 174020 - 4400	Emotion Dolgang Dolgang Dolgang Dolgang	Advalantile Advances (20) Received 20)		i j ki j boli 201 ki jest 201 ki jest 164 kies 164 kies	tan be too an too too	er er diabreet jouk tra stabreet	Mariana Mariana Mariana Mariana	Insering Disalments 0 1 2		c	

- 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.
- 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.

- 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?

ACK THESE AF	PLICATIONS				
Facebook 🗙	Skype 🗙	Skype Web 🗙	Skype for Business	× Google H	angouts 🗙
WhatsApp We	eb 🗙 Slack	X Slack Web	X LinkedIn X		0
					1.0

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

Data content			• ?
ONTENT TYPE			
BOTH	TEXT	BINARY	
ELECT MATCH TYPE	I		
Regular expressio	on match		• ?
PECIFY VALUE			
.*will be hearing fi	rom my (attorney law	yer).*×	3
.*(I we) will sue.*	×		
.*(I we) will sue.* .*(I we) will take y			

What are some sample rules using this feature?

Provide Sector Sector

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

- Rules Guide: <u>Activity Rules > IM Instant Messaging</u>
- Rules Guide: Content Sharing Rules > IM Instant Messaging

3.9 Social Media

What report can I access for this activity?

2021 - Jan 9.3	ALL					Territor Toursen Laws T
, 2021 - Jan 9, 3	0.21					CALLER DATION CON Y
+						
		4.8 Initiation			e e lateres	
-		Non Internet Contract Section 1 Section 1		1	isellation -	<u> </u>
			Sec. Mate			
C. N. Strikerik		100	limite	Ref.	The set what you best of the trading if is an	
C-0170314-0101		1075	Long to	het.	Sector state) and is one for some in	and B
COLUMN TRAVEL		fact schen set	Tauton	ine.	New Appendix access to call to 2	
1.16.16.0.14.0.0			feature	Ref.	Webbare is being free and web	
		the life in the	Later .	24	Date from the lot of the of the	
C. 46 (875) (199)		make of th	Autor I	Red.	The runter are difficulty and party of	
0.00 10.00 0.00		utidation in plat photons	Instead	Det.	Labeled as in the share while the street	
1.00 0000000000		new sector and the sectors	feature	but.	An owner of standing a work many free has	
CONTRACTOR INCO.		have about a caller to have about a se-	Inches	Del.	Total advention space particular him for he	the Calebra Annual Residence of the Advance
		hadres, noting storads, from, income bach,	Long.	Red.	The local second second second second	A series where a provide the series had reard in the
		state and water water from Your a.	factors.	2.4	THE ARE TO DE A GROUP OF PROBATIO OF	FEEDBALE SHOEL - ACT, SA HOW MELL SHOE HORE
0.010004-010			intents.	in the	The first to be served in second with a	and it was the manufacture of the second
C-08 (0.004-050) C-08 (0.004-050)						
C-04 102204-0510 C-04 704204-0510 C-04 7040-04-0510		printer factories factor place, diamen factories	Unida	Ref.		test (
C-04 00204-0500 C-04 244/14-0500 C-04 244/14-0500 C-04 244/14-0500				Aut .		unad Analise is had as is the base is a sub-costs as and i
		press tepres	Inda			Applied to full you to the heart the area to cardin you and t
C-0 1004-000 C-0 30614-000 C-0 30614-000 C-0 30614-000 C-0 30614-000 C-0 30704-000		provide forgetones local analysis for the second for the second s	inds.	764	Elaberrise many and your hand varies	Applied to full you to the heart the area to cardin you and t
		process begines. Sense searce, hand normal, had hash similar mediat, tapay Tik, theory	inada Selar Restore	No. Raited	Edulations arens and pair hand coming Very Bills consolid to make a logge the En- Very Bills consolid to make a logge the	Applied to full you to the heart the area to cardin you and t

- 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?

TRACK THESE APPLICATIONS	
Facebook x Twitter x Linkedin x	¢
YES TRACK NEW COMMENT	
YES TRACK EDIT COMMENT	
YES 💽 TRACK NEW POST	

- 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?

ondition 1 Webpage Url Total Time Active (min) × 🕣	
NDITION	
Contains facebook.com x Contains instagram.com x Contains instagram.com x Contains instagram.com x Contains youtube.com x Contains pinterest x Contains tu	
CEPT	
Start typing	(?)

What are some sample rules using this feature?

 Social Media does not have a dedicated rules category. However, you can create rules to monitoring social media sites using the Activitybased 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.

Rule Excessive usage of social media Summary Experter Poly
Category
Activity
🛎 Users
Apply to Everyone
Webpages
Webpage Url contains facebook.com or contains instagram.com or contains twitter.com or contains youtube.com or contains nterest or contains tumbir
Total Time Active (min) > 15
© Actions
Show warning with message Please keep your social media usage to a minimum while at work
Rule test Summary Test Policy
Category
Content sharing
🔹 Users
Apply to Everyone
Content
All credit card numbers matches 1 times
Files
File operation Upload
Upload URL contains cdn.facebook.upload
& Actions
Block with message This file cannot be uploaded to this site

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

3.10 Keystrokes

Seth Mcgrego

), 2021 - Jan 1	-			Lad Sync Second SU25 45 43 2 Second C 19996
Comprise	+			
				11 (marine) 11
			Rent 1	ar Denirs atas management
	Bart 0.4	40 04 MG	in the second se	
		Counter		Topolar
10-11-11-11-11-11-11-11-11-11-11-11-11-1			0,0100	Anaditar R
D 12144X-018			whethe	the second se
ATTENDED AND ADDRESS OF ADDRESS O			uffeste.	a wy to prodify of prices destruct to set to a total two and the pair feet pair is the pair feet pair.
0.0108408			Afraha	s wy to properly of project or particle statement for address a full low regime equation of the statement of
0-9258-08			uffiate.	published from the section of the box regard device regard device regard over the state of the section of th
0.034006			and all and	dependencies for the exception of product the challphane for the control of our water is challphaney transmission is the top product to where
No. 1 Institute			and and a	inge weinning is miss to observing intergence to miss of charges in between independent pages and foregreen
ATTENDED AND A TOP OF			whate.	The second a new control of the part of th
0-010408-048			(Pate	All of the state of the register for any period of the the photoe sector paper. The the photoe of the state o
Ch-12 224525-0248			- Calo	Security of a security of the second sector of the
ACCOUNT OF A			urfunte.	- Angen - Sergen - S
And a second second			official a	pice Party and a second s
0-12010-008			(Pate	The State The main late to physical space of American and a state part of a manufactor or Accessing free
0.010000000			a finite	production of the product of the product of the product of the product of the sector of the interval product of the branch of the sector of the interval product of the branch of the sector of the interval product of the branch of the sector of the interval product of the branch of the sector of the interval product of the branch of the sector of the interval product of the branch of the sector of the sector of the interval product of the branch of the sector of the interval product of the branch of the sector of th
21-12-22-28-28-0100			urfunte.	standing of the second
APPLIE IN A PARTY OF A			demander.	Policing - 20 Mill Mongala, Milling Milling Philipping and an Ann an Angalan and an Ann Milling and and Anna Anna Angalan 19
COLUMN AND			official a	e bener bener with dense benere
			affects.	do black wholes a way and below of and ad
			Colora	al an a state of the state of t
KEYSTRO	DKE LOO			¢ :
• •	<ctrl> + <sh< td=""><td>ift> + t</td><td></td><td></td></sh<></ctrl>	ift> + t		
1	Seth Mcg	-		
		kspace>edge	Disseminat	tion
Jan 09	Seth Mcg	regor		

- 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?

Keystrokes: Edit settir	ngs	×
YES TRACK CLIPBOARD		
		_
		_
USPEND KEYSTROKE MONITORING WHEN accounts.google.com X login.live.co		

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

Condition 1	
Text Typed 💿	
ONDITION	
Contains <prtsc> X Contains <shift+prtsc> X</shift+prtsc></prtsc>	3
XCEPT	
Start typing	3

What are some sample rules using this feature?



- You can turn the Clipboard tracking on/off.
- You can automatically suspend keylogging for certain <u>Applications & Websites</u>.
- Automatically suspend keylogging when certain content is detected on <u>Applications & Websites</u>.
- 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.
- 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: <u>BI Reports > Keystrokes</u>
- User Guide: <u>Monitoring Settings > Keystrokes Settings</u>
- Rules Guide: <u>Activity Rules > Keystrokes</u>

3.11 Clipboard (Copy and Paste)

	THOE STWOOLS						
Activities	Q Employees	& Depts	•				
Employee	Computer	Keystrokes					
Tia Sanders	WIN-035KHOR8PEI	<control+v> How to make a financial pre</control+v>	sentation				
Michelle Hurley	WIN-035KHOR8PEI	responsibility typically resides in the Con	troller's gr				
Michelle Hurley	WIN-035KHOR8PEI	ny <back> , these responsibilities fall into</back>	departm				
Fang Shen	WIN-035KHOR8PEI	Now you offiver multiple products or se	vices you				
Jackson Gollan	WIN-035KHOR8PEI	<back> <control+v> How to make a finan</control+v></back>	cial prese				
Fang Shen	WIN-035KHOR8PEI	<control+b> create a target market state</control+b>	ment <ret< td=""></ret<>				

Ke	eystrokes: Edit settings	×
C	TRACK CLIPBOARD	
_		_

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

ondition 1	
Webpage Url 💿	
ONDITION	
Start typing	?
(CEPT	
Contains lightning.force.com 🗙	0

What are some sample rules using this feature?



What are some useful resources for this feature?

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

3.12 Searches

- There is no dedicated report for the Clipboard. However, you can use the <u>Keystrokes</u> report and search for hidden characters that indicate copy/paste operations, for example: <Control+C> or <Control+V>.
- Clipboard does not have a settings panel. However, you can turn it on/off from the <u>Keystroke</u>'s settings panel.
- 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.
- 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 monit		contro
	No settings	

- 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.
- 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.

You cannot create any Search-based rules

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

•

ondition 1	
Webpage Url [×] Webpage Title [×] ⊕	
ONDITION	
Match list Keywords 🗙	3
(CEPT	
Start typing	?

What are some sample rules using this feature?

- Rule Detect google search Summary Demo Palky Palky Category Activity Sers Apply to Everyone Webpages Webpage Url match list Keywords Webpage Title contains Google Search Actions Redirect to searchpolicy.teramind.co
- 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.
- 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: <u>BI Reports > Searches</u>
- User Guide: <u>Monitoring Settings > Websites Settings</u>
- Rules Guide: <u>Activity Rules > Webpages</u>

3.13 Printing

10, 100 1 - Jan 11	5, 2021 🛅						Card spectree 2025-01-05-25223	0.0% 7
in			· · helene				149	
		64 eV W	in the	ta ini a ta a ta a ta a ta a ta a ta a ta a t		a 11		Creft I
					Page	Capes		
101210-002			Manual Park is right	Orabilitati				10
05-10-06 10 60-21-00			famous Daritop log from	lief dan daran sta				5
45-10-00411-010			Manuel Parts Joy	Associate Disa Merupa Solt	4			1.0
10.1004041000			Manual Post is right	Frend Esternation				
-05-10-0140-0140			Manual Post 7, 107	10 feet Nambry Destanty	24			
			Manual Post in 198	Variating plan Loak				
			Manual Parch 207	increa ferene ell'est				
-0.1041030308			Manuel Port (p. 191	R.Naragened futuritercbit				
0.04 00.00 0.0200000 0.0200000			Manual Posts ADF	Robergenet Autorities	1.00			
			Manual Part 5, 107 Service Desitive Seg Front	The Bell Note Canadia pressignment of p Contract	1			11
			Manual Posts ADF	The Best Note Canadiag resultance with				L
			Monault Prot To HDF Remove Desitions any Port Remove Desition any Port Monault Post To HDF	The Back Note: Canobing Interpretation and g Contract 1 Contract 1 Interpret Contract plan - Industry Scherood				ł
			Manual Part 5, 859 Beneric Gelden Leg Part Beneric Leiter Leg Part Manual Part 5, 859 Manual Part 5, 859	The Back None Constructions into provide some state Destinal 1 Destinal 1 existing a business plan - Inclean Schwardt Phone is business a business plan and a contexpil.				ł
			Monault Prot To HDF Remove Desitions any Port Remove Desition any Port Monault Post To HDF	The Back Note: Canobing Interpretation and g Contract 1 Contract 1 Interpret Contract plan - Industry Scherood				
			Monard Post 5, 159 Remote Desires Jung Post Remote Desires Jung Post Monardt Post 5, 159 Monardt Post 5, 159 Monardt Post 5, 159	See Bar Nove Security institution may Contract 1 Contract 1 Institute of bolinary device for the soft Although bolinary plan and a minipal Although bolinary plan and a minipal Program provide statistical plan and a minipal Englance planets and institution planets due to				l
			Manual Feet 5, 199 Beneric Delition Day Port Beneric Delition Day Port Manual Feet 5, 199 Manual Feet 5, 199 Manual Feet 5, 199	Se fair faire freeding insighten sig Control 1 Control 1 Writing & Control physical School 1 Mining & Control physical School 1 Mining & Control School 1 Program (School School School 1)				

- 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.

RINTER TRACKING ACCOUNT USER	
demo@teramind.co	
RINTER TRACKING ACCOUNT PASSWORD	
VIS CAPTURE ACTUAL DOCUMENT	
MAXIMUM CAPTURE DOCUMENT SIZE (PAGES)	
50	
EXCLUDED PRINTER NAME (REGEXP)	
	0

- 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?

ondition 1	×
Printer name [×] Number of pages [×] ⊕	
CONDITION	
Contains HP_Color X	(?)
EXCEPT	
Start typing	0

What are some sample rules using this feature?

₹U Ner	le Print restrictions Summary 10 Policy Policy
i	Category
	Activity
	Users
	Apply to Everyone
à	Printing
	Matches any of 2 conditions:
	Number of pages >= 20
	Printer name contains HP_Color
	OR
	Number of pages >= 50
	Printer name excludes contains HP_Color
3	Actions
	After 2 violation(s) Show warning with message Please consider using the HP BW printers for large print jobs.

- 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.
- 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: <u>BI Reports > Printing</u>
- User Guide: <u>Monitoring Settings > Printed Docs Settings</u>
- Rules Guide: <u>Activity Rules > Printing</u>

3.14 Network

What report can I access for this activity?

1, 2023 - Nov 30,	2023 📋				07081+ 0	RISTORE BLOWL AND	CLENE	о 🖊 т
0 (+								
GOING TRAFFIC	0.	o Y × INCOMING	TRAFFIC	0	ο τ × cor	INECTION BY PROCE	55	D O T X
047100- pr/1000- pr/1000- 10- 10- 10- 10- 10- Carea	1441 0 3 0 3 0 3 0 3 0 3 0 3 0 3 0 3	utenĝa steinteroj urestitojn urestitojn	itig clano			ng-bhilte- ng-charue- tu-fscigh No- g-28,802 (4),80 Coreation	1 10,000	ann Tratar Ann Ann Ann Ann Ann Ann Ann Ann Ann Ann
NGRID								
N GRID								DOTX
Timesterg* 4	Department	Imployee	Computer	Seit	(braincini p	Destination Port	Pressel	Sett
Timestenp* 4 2023-11-0 121742+0400	No Department	Altha Danmaria	serviced 111	Default link	210 253 235 250	1800	Retucal NP	5ert 10
Timestany' à							Patricel	Sett
Timestenp* 4 2023-11-0 121742+0400	No Department	Altha Danmaria	serviced 111	Default link	210 253 235 250	1800	Return 1	5ert 10
Timesterio* 4 2023-11-15 12-1748+0400 2023-11-15 12-1748+0400	No Department No Department	Adva Sammona Adva Sammona	network2335	Default lask Default lask	210 255 235 250	1900 443	Postcol TCP 1/CP	5ect 780 1936
Timesteng* 4 2023-11-10 12/17-41-0400 2023-11-10 12/17-41-0400 2023-11-10 12/17-41-0400	No Department No Department No Department	Julia Serenara Julia Serenara Julia Serenara	nerwane2185 nerwane2185 nerwane2185	Defect link Defect link Defect link	200.255.216.259 236.56.212.150 15.52.52.5	1900 443 53	Postucal NCP NCP	5ect 0 790 1826 79
Tenensey" 4 2023-11-01 12/1742-0400 2023-11-01 12/1741-0400 2023-11-01 12/1741-0400 2023-11-01 12/1741-0400	No Department No Department No Department No Department	Adha Samana Adha Samana Adha Samana Adha Samana Adha Samana	nerwand100 nerwand200 nerwand200 nerwand200	Defect last Defect last Defect last Defect last	200.255.235.250 236.58.232.131 15.52.52.5 15.52.52.58	1800 440 53 440	Postcol 309 109 509 109	Sect 1 790 1936 78 1939
Tenenary" 4 2023-11-01 (217542-0400 2023-11-01 (217542-0400 2023-11-01 (217542-0400 2023-11-01 (217542-0400 2023-11-01 (217542-0400	No Department No Department No Department No Department No Department	Adm Samon Adm Samon Adm Samon Adm Samon Adm Samon Adm Samon	network2333 network2333 network2333 network2333 network2333	Default last Default last Default last Default last Default last	200203208200 2063029230 1532323 1532323 15323230 2965329230	1800 440 53 440 440	Postocal 509 509 509 609 609	Sect 1 720 1836 78 1989 641
Timetersy" 4 2020-01-01 12/14/24/04/00 2020-01-01 12/17/24144/00 2020-01-01 12/17/24144/00 2020-01-01 12/17/24144/00 2020-01-01 12/17/24144/00 2020-01-01 12/17/24144/00	No Department No Department No Department No Department No Department No Department	Adm Semons Adm Semons Adm Semons Adm Semons Adm Semons Adm Semons semedia @dealay=b158e	nerwano2185 nerwano2185 nerwano2185 nerwano2185 nerwano2185 nerwano2185 nerwano2185	Default last Default last Default last Default last Default last Default last	200.203.208.200 206.50.212.130 1532.52.5 1532.52.50 206.50.212.136 150.577.136.500	1900 443 53 443 443 440 5008	Protocol 109 109 109 109 109 109	Sect 1 720 938 73 939 640 84
Timestenny" - 8 2020 - 11-01 12/1748-9840 2020 - 11-01 12/1748-9840	No Separtment No Separtment No Separtment No Separtment No Separtment No Separtment No Separtment	Adva Serenova Adva Serenova Adva Serenova Adva Serenova Adva Serenova Adva Serenova ovrednik (dodaškoje bil takije serednik (dodaškoje bil takije	nmand333 nmand333 nmand333 nmand333 nmand333 debtp-1248m debtp-1248m	Default Leak Default Leak Default Leak Default Leak Default Leak Default Leak Default Leak	200295205290 2065022335 1552535 15525350 20650222355 20650222355 150577356300 20650223510	1800 440 53 441 441 5328 441 5328	Pretocol 1029 1029 1029 1029 1029 1029 1029	5ert 720 1826 73 1939 5939 640 24
Timesterny" - 8 2020-11-101 12/1748-98400 2020-11-01 12/1748-98400 2020-11-01 12/1748-98400 2020-11-01 12/1748-98400 2020-11-01 12/1748-98400 2020-11-01 12/20148-98400 2020-11-01 12/20148-98400	No Separtment No Separtment No Separtment No Separtment No Separtment No Separtment No Separtment No Separtment	Alth Services Alth Services Alth Services Alth Services Alth Services and Self deblog-b*58the served ind deblog-b*58the	Amand III Amand	Default last Default last Default last Default last Default last Default last Default last Default last	200255235259 2053023235 10532325 10532335 10532335 20550232355 20550232356 2055023356 2055023356 2055023356 2055023356	1000 440 53 441 441 5028 441 5028 441 443	Pretocol 509 509 509 509 509 509 509 509 509 509	5ert 720 1826 73 1939 5939 641 34 34 22

What monitoring & tracking controls do I have?

Network: Edit settings	×
YES SSL	
YES TRACK NETWORK CONNECTIONS	
YES O DON'T DISABLE TEREDO	
TRACK ONLY THESE IPS	
	0
DO NOT TRACK THESE IPS	
	G
TRACK ONLY THESE PORTS	
	0
DO NOT TRACK THESE PORTS	
	0
TRACK PROCESSES	
Network Process List 🗙	
	0

What rule and alert triggers can I use with 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.
- 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.

ondition 1	×
Remote host [×] Bytes sent [×] ⊕	
CONDITION	
Match 1.1.1.1/32 ×	(?
XCEPT	
Start typing	(2)

What are some sample rules using this feature?

PCI	le PCI-DSS 1.3.4 - Unauthorized traffic from cardholder environment Summary DSS Compliance Policy
B	Category
	Activity
	Users
	No one selected
ų,	Networking
	Remote host excludes match 192.168.0.0/18 or match 10.0.0.1/8
8	Actions
	Block with message Outbound internet traffic from cardholder data environment hosts is not allowed per PCI-DSS 1.3.4 and Notify mredmond@teramind-demo.com
1	
	Io 0/1 DSS 7.1 Limit access - Iodicula DDD Summany
20	le PCI-DSS 7.1 - Limit access - login via RDP Summary 98 Compliante Pricy
a	le PCI-DSS 7.1 - Limit access - login via RDP Summary Sis emplane hito: Category
C	DSS Compliance Policy
PCI	255 Compliance Policy Category
	DSS Compliance Policy
	086 cm/laten hity Cdggoy Arthify Usdrs Apdy ta Affordi
	DSC complexer helps Category Activity Uper Apply to AM Topal Networking Application Name <u>contains metocone</u>
	OSC complexes heley Activity Usors Apply to Affitopal Asplication Name contains motic one Asplication Name contains motic one Asplication Name contains motic one
20 10 11	DSC complexer helps Category Activity Uper Apply to AM Topal Networking Application Name <u>contains metocone</u>

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.
- 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



- 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.

Geolocation: Edit settings	>
TIME THRESHOLD (S)	

• 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: <u>BI Reports > Geolocation</u>
- User Guide: Monitoring Settings > Geolocation Settings

3.16 Camera Usage

What report can I access for this activity?

ct 2	29, 2023 - Nov 27, 2	023 箇					U DPOU	• 9 ALSTON	85%	+ WIDS(T	CLOW:	0	1	т
lesic	0 +													
MEE	TING APP USAGE				οv×	WEEKLY USAG	ie.					0	0 T	
-	ent rintencamp			Empoyee + rogro - servaling	and the second states	1.00								
	Sec. ex-					2100								
						1								
		630 Else Bills 1 Time Journ	546 55° 546 549			1	-it	3	3	1	į		ŝ	
PLA			546 35° 346 349			Å	â	3	1	2	ż	0	з от	×
PLA	130 0.07 0.02		Sid Sir Sid Set		Computer	Å	i g) (rm)		ž	0		
PLA	10000 au	Tare (sourt)		hape 5 feller	Computer Andrey MCARe	Å 1.0 100 Å	ĝ Meriog le Danuer		Caract		Time	0		
PLA I I	iture au 50 bit 620 IN GRID	Tex huri)	Engliger	kapa 348 v		Å 1.0 100 Å			Caract	tene Anal USI Ve	Time	0		
PLA	10000 and 500 0.01 0.02 IN GRID Transform" -1 2015-11-11 01 0.01-30.20	The basel Department No Department	Engliger samelding-bed	kapat 7.68%	average definition	A 100 100 Š	Summer decrease		Carwood Wheater HP Turei	tene Anal USI Ve	Tirse 08/08/24	0		
PLA	1999 201 201 201 201 1999 201 201 201 Terestory? + 2010 17.11 21 2017-2020 2015 17.13 12-2020	Ten Jose) Department No Department No Department	Engliger sameldeißdesk hoßtp	hg 0388v	nearry shrider	A 110 120 Sex Defail GA Defail GA	hansee daoneer Moneth	photoe	Carwood Wheater HP Turei	lane Asud USI Ve Non HD I-D Withom C	Tirse 08/08/24	0		

- 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?

Camera		Fulls Campaia App Summary Second Rep.
Carables 1		B Giapop
Conversion and Baltion server." Conversion of Co.		Activity
196125		Anthe Decem
Final Association Review Sole of Technological Philameters		449 C C C C C C C C C C C C C C C C C C
Parial Realistics a	8	The same interviewed of a first linearity is a construction of which is a 1 minuted 2020
		Core copplication accelerations so more or consider described or consider where
Arrest Control of Cont	Q	g alws
() -32 CHIMIDH		Show warning with manage Grown Les childred

What are some sample rules using this feature?

Ru Cam	e Camera App Summary era Policy
B	Category
	Activity
2	Users
	Apply to Everyone
ø	Camera
	Camera name contains VMware Virtual USB Video Device or contains Logitech HD Webcam or co ntains ZioMi USB 2.0
	Camera application name contains zoom.exe or contains chrome.exe or contains webex
8	Actions
	Show warning with message Camera use detected

What are some useful resources for this feature?

- 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.
- 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.
- User Guide: <u>Monitoring Reports > Camera Usage</u>
- User Guide: <u>Monitoring Settings > Camera Usage Settings</u>
- Rules Guide: <u>Activity Rules > Camera</u>

3.17 OCR

What report can I access for this activity?

ul 14, 2019 - Jul	20, 2019 🔳		Englopers & Day is	- Compations - B B 0 27
			Search apps. Postburger.	Q Fallent • O confidence Q
Sate/filese +	Employme	Computer	A	Text
ana	B D THE DEC	WTV-249-C-808-870	virrorit.ara	UI Confidential flag (J. Suns in VI or Lampings Heregoment 1.
0144-07-14 06:02-10	B Be Minasjamano	W39-2250 K003PD	#12000.408	Confidential $5~{\rm ev}-4dd$ we not found like memory were's tak .
9944-02-14-08-58-08	8 M 18-19 karran	WW9-385-0408394	rectanges.	Gerfilertial Sec Address of Incol New record reactions .
2010-07-10 18:00:00	B B Vincy Kencom	WW 2014 WHITE	113 000.0xE	Certificated ht co - Address not found Your mosego wants coll .
212-07-12 06:52:21	R Dr. Vince, jamason	WE9-338 0 8083P3	412 0091498	Confidential Tret - Address not found Your manage warn's cell.
044-05-14.06/01/22	B Dr. Marry Jameson	W89-315 C400398	PUBLIC AND	Cardidential for the field would find that convergences to take
2112-07-10-06-06-20	a a Westances	WWW DESKEDBORD	osuo.oc	Confidential Riss - Address not found Your resultance in
212-07-12 05-08-14	B Br. Vérayjersson	W39-220-04083PD	612 0/01 BIG	Confidential II as - Address not to, nd Your manage waar's call.
DIRATING DEVICT: 0	a la Massarian	W89-335 0 808390	ALLINGUM .	Confidential 5 et- Address for four d'har metage seech cet.
241-0211-05-05-05-08	I In Marginster	WW03330406356	neianose	eq:Gaselikerikelikerikerikerikerikerikerikerikerikeriker
210/07/10/06/014	B Br. Missourcem	WW 224 14 Million	011010-04	Confidential Hiss - fold-participants found flow management cost .
010-07-1010-022	and the state of the second	W79-328 C 808.870	era brestere	Confidential 1 at \sim 4dd are not found 10ar metage wards rate .
	In Maryleneses	was-2120406370	nilonen	Genfidential Sec. – fold would found Your consequences (Sec.
210-0210-064015	am Westkerow	WW 255-0408276	minore	Confidential Riss - Address of Interal Rev repuigt work (1918)



- 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: Edit settings	×
OCR LANGUAGES	
English ×	0
PROCESS SCREEN RECORDS AFTER	
Aug 11, 2023	
c	
Screen: Edit settings	×
YES ALLOW REMOTE CONTROL	
ASYNC SCREEN UPLOAD	
RECORD LOCKED SESSIONS	
MAXIMUM FRAMES PER SECOND	
3.	
RECORD ONLY WHEN BEHAVIOR RULE WAS VIOLATED	
UPDATE SCREEN ON EVENTS ONLY	
USE MODERN SCREEN GRABBING	
GRAYSCALE COLOR HIGH COLOR	
LIVE SCREEN SCALING	
50% 60% 70% 80% 90% 100%	
DELETE HISTORY AFTER (DAYS)	
MESSAGE DURING REMOTE CONTROL (BLANK = NO MESSAGE):	
MESSAGE DURING INPUT FREEZE (BLANK = NO MESSAGE):	

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

i

- 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, bitdepth, 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: <u>Monitoring Reports > OCR</u>
- User Guide: <u>Monitoring Settings > Screen Settings</u>
- Rules Guide: <u>Activity Rules > OCR</u>

3.18 Registry

What report can I access for this activity?



What monitoring & tracking controls do I have?



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.

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?



What are some sample rules using this feature?



- 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.
- 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: <u>Activity Rules > Registry</u>

3.19 OS State

What report can I access for this activity?

elect o	sion +								Licenses i	1 use: 53 /	500
Lock		11 Not deleted			rs. Employee		cionenta				0
Unloc		The Protoented		Administratio	rs, preproyee	Uepa	interna •	۹			
Restor			Depart	ment	Last login time		Last login from	Status	Monitored	27A	1
	Monitoring	amind-demo.com			2020-08-05 16	:15:39	WIN-035KHORBPEI	Locked	No	No	
Disabl Bulk e	e Monitoring dit	dteramind-demo.com	Arick1		Online		win-035khor8ter	Active	Yes	No	1
Ber	Th_ bendter	amind.co	my dep	artment				Active	No	No.	
Dot	Pine bobricki	Steramind-demo.com	Staff		2022-01-04 15	:24:13	WIN-035KHOROPER	Active	765	No	
812	rde_ bcrawfo	rd@teramind-demo.com	arick-te	982	2022-08-27 23	:00:17	win-035khoröter	Active	Yes	No	
Cat	her catherin	e@teramind.co						Active	Yes	No	
Cha	dw csingh@	teramind-demo.com	Sales		Online		win-035khor@ter	Active	Yes	No	
04	ol. coullent	pteramind-demo.com	Staff		Online		wn-035khor8ter	Active	185	N0	

 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 <u>Employees</u> report.

What monitoring & tracking controls do I have?

OS State: Edit settings	×
VES SLEEP	
YES SCREENSAVER	

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

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

eral	Registry		Rule Registry changes Summary Sample Bake Policy
r Istry ons Overges saved	Condition 1 Kay Name ^X Value ^X Program ^X connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connexts Connext	•	Cotegory Activity Activity Activity Apply to IT Registry Program Contains regedit Key contains Nexy Scal machinet
	Start typing	0	Value equals Starts Value equals 3 G Actions

• You cannot use any rules directly with the OS State. However, you can monitor <u>idle time</u> 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: <u>Employees</u>
- Rules Guide: <u>Agent Schedule Rules > Idle</u>

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 <u>Audit & Forensics</u> section for more information.

4 Data Loss Prevention

Teramind data loss prevention feature utilizes automated data discovery, classification, and contentbased 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



4.2 Define Content-Based Rules

SELECT THE TYPE OF RULE	
Content sharing	•
MARK THIS POLICY WITH TAGS TO IDENTIFY ITS PU	JRPOSE
Types of Content ⑦	
OCR	YES
OCR CLIPBOARD	YES
CLIPBOARD FILES	YES
Types of Content ⑦ OCR CLIPBOARD FILES EMAILS	YES

- 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.
- 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

File Origin			• ?			
SELECT FILE ORIGIN						_
SHARE	CLOU	Definition	n 1			- 1
		SELECT WHAT	MAKES THIS DAT	A SENSITIVE		
SELECT MATCH TYPE		File Prope	rties		*	?
All shares		FIELD TYPE				
		ANY	STRING	INTEGER	DATE	?
	_					- 1
		FIELD NAME				
		departmen	t			3
		SELECT MATCH	I TYPE			
		Equals			٠	?
		SPECIFY VALUE				- 1
		HR				

- 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



4.5 Use Pre-Defined Data Categories

ELECT WHAT MAKES THIS DATA SENSITIVE	
Predefined Classified Data	• ?
ELECT SENSITIVE DATA CATEGORY	
Code Snippets	• ?
Financial Data	
Health Data	
Personally Identifiable Data	
Code Snippets	
RIGGER ON PATTERN FREQUENCY IN CONTENT	
1	0

- 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.
- Teramind has built-in templates for many predefined 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

operty	Value	^				
Description — Itle iubject	PowerPoint Presentation	Describe the	sensitive cor	itent that Terai	mind will pro	tect
Tags Categories Comments	CUSTOMER_CONFIDENTIAL	Definition SELECT WHAT	n 1 MAKES THIS DAT	A SENSITIVE		
Origin	Teramind	File Prope	rties		*	0
Last saved by	Teramind	RELD TYPE				
Revision number Version number	1	ANY	STRING	INTEGER	DATE	?
Program name Company	Microsoft Office PowerPoint					
Manager						0
Content created	2019-07-22 7:43 PM	Tags				9
Date last saved Last printed	2019-07-22 7:45 PM	SELECT MATCH	H TYPE			
Total editing time	00:01:00	Equals				?
lemove Properties	and Personal Information	SPECIFY VALU				
			R CONFIDENTIA			

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

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: <u>Teramind: Insider Threat Prevention</u>

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: <u>How to use Teramind to monitor and block data exfiltration attempts to USB/external</u> <u>drives</u>

- 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: <u>How to Detect and Prevent Data Leaks with Teramind</u>

5.4 Dynamic Risk Scoring



Chose time period for thresho	lds
Choose the period of time for threshold calculations	
Daily	• ?
Configure action threshold	
Configure action threshold	
Configure action threshold	

GAT TRIGGERS THE RULE					
lect the action which the rule wi	I be built upon				
Webpages					*
CONDITIONS					
Select parameters for this ru					
Anomely baseline	*	15	Department		*
Time (%)	*	>	* 10		×
JLE RISK LEVEL					
X lets the degree of risk for violati	ng shia rule				
ect the degree of risk for violati	Low	Mode	arate	High	Critic
	•	Mode	arata	High	Critic

5.5 Anomaly Detection

■ Anomal	, raies				Q	And a second			TART TOUR
2 RUNES							@ AD0	ANOM	LY RULE
FILTER RULES	τ	RULES	CONDITIONS			APPLIES TO	ACTIO	15	
Input the name of r	ule	Webpages Anomalies	Webpages Time (%)			All employees	1	0	×
Add employees or	departments	File upload anomaly		-upload opera d count > 3	ition	All employees	1	0	×
CONDITIONS									
Condition type	0								
019-07-22 11:22:52	Mohamed Kragh		Webpages Anomalies	No action	Used twitter.com	45.8% of time. Company average i	2.3%, Depar	General P.	erage is 2.5%
019-07-22 11-22-52	Les Gress		Webpages Anomalies	No action	Used excellence 38.	Ph of time. Department average i	s 1.0%, User a	verage 5	0.0%
019-07-22 11:22:52	Tim Farrow		Webpeges Anomalies	No action	Used www.foxner	n.com 14.0% of time. User allerap	1.025		
019-07-22 11:22:52			Webpeers Anomalies	Nawaran		care 54.3% of time. Department av			

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.

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



6.2 Time Tracking



- 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.
- 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



6.4 Workflow Automation

	Simple Mode	Advanced Mode	Rule Accounting/Auditing task Summary Pretention Tasks Printy				
er plications	Select how the system should a	mart to violations	Category Activity				
tions			ALL Users				
	NOTRY	() NO	Apply to Everyone Applications				
	BLOCK	()N2)	Application Name contains excel exe & Actions				
	LOCK OUT USER	<u>(10</u>)	Switch user's task to Administrative				
	WARN	<u>()</u> m)					
	SET USER'S ACTIVE TASK	(11)					
	Administrative •						
		-					
	Please note that task will be assigned to agent and not a						
RULE TRIG		e built upon					
Select the action							
Select the action Activity: Proc	Juctivity		~				
			~				
Activity: Proc			~				
Activity: Proc CONDITIO Select par	INS	15	V Department V *				

- 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.
- 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.

Policy and Rules Management 7

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

olicies			Search for rules Q
POLICIES	# RULES TAES	AUDIENCE	ACTIONS
CREATE NEW POLICY			
GDPR Compliance	20 rules	Everyone	()#E) I
Demo Policy V	13 rules	Everyone	.
Productive Tasks	7 rules	Everyone	.
Agent User Experience Demo	4 rules	Everyone	 1
PCI-DSS Compliance	10 rules		.
HIPAA Compliance	13 rules	Everyone	.
Sensitive Data	4 rules	Everyone	•••

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.

7.3 Regular Expression Support

			~
Regular exp	pression match	•	(?)
PECIFY VALUE			
	9]{2} [A-Z]{3}\$) (^[A-Z][0		

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.

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.

7.2 Visual Rule Editor



7.4 Out-of-the-Box Rule Templates



- 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.

- Teramind DLP comes with hundreds of predefined 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

Behavio	or Alerts	÷				Q 🕐 The Ado	- 🔅	START TOUR	HIS PA
3, 2021 - Ja	an 9, 202	1 🛅						EXPORT + CLO	£ 1
c 🗢 🗑 Risk	+								
maine				elv.			Tea Brainpeer		
			\sim			Court	an ingage		
2,000	\frown	/				40	Braysen Crawler Snigen Woose	the second se	
1.500		~	1					the second se	
							Denaid Juneau Party Smith		
500							Jacket One	Concession of the local division of the loca	
an Citter D	1 7.420 10	10 101	Fride Sector			F2 FF8222		0 400 800 Covri	(200
inestery" +		Employee	Computer		Policy	. No.	Action	Description	
101103000 · ·			WN-0504		una			Sent/received an email with i are	
						Sample content rule	Nutrity		
021-01-09 23:59:39		Shiyam Morcos	WN-65504		Productive Tasks	Data Entry task	Notify SwitchTask	Used the application notepad.en	3
521 01 09 29 58 59		Shyam Moncos	WN 0550-9		Productive Tesks	Data Entry task	Notify Switchlink	Used the application wordpad.e	
021-01-09 23:57:58		fackson Golfan	WN-03504		Productive Tasks	Communication task	Nosty Switchfack	Used the application stack.ese.	11
021-01-09 23:57.20		Shijan Morcos	WN-60504		Productive Tasks	Data Entry tack	Nastly SwitchTack	Used the application notepad.ex	
021-01-09 23:56-48	105:00	Shiyare Morcos	WN-050H	CASPER.	Productive Tasks	Data Entry task	Notify, SwitchTask	Used the application wordpad.e	
udit				/				9. (a) entre • •	-
3021-April 3								GANT- Prettone Co	
	523 🖬							CASE STOR C	•
									ат
Contract to		Testal.	I MON						
contact protocolem	100.00	Constant.	KITCHIG MM	0.045	to year	Concernant, and			
100-04110-050-010	1010-01	0.0 Minu	NAMES OF	# forty	1014			10 10 10 10 10 10 10 10 10 10 10 10 10 1	
CONTRACTOR OF STREET	N	and the second second	NAMES OF	100	and the second	California Company, Ca		A DESCRIPTION OF TAXABLE PROPERTY.	
15%-Data 25/540 Sola	and in a	Spilling)		Atop	-			And the second s	
CONTRACTOR OF THE PARTY OF THE	2010	ta Mari	NAMES OF	-	And all a	Star Liber Dev	Coll faile from tool of the o	The Data constrained and the second sec	
CONTRACTOR OF THE	2.00	1.00	MARK OF	2540	10.21			An ora MD-10-D04-0	
110-0412-070-0-08	3010-01	and a	sceam or	Attack	-			Nampa Alattica Bankway 200 Ci 12 - 1201	
100000203000	8027	ade Das	NUMBER OF STREET	U Gara	England the sol		in the local data and the second	Only he can be be be an a the can be	*004
COLOR DOCTOR	A.44	abe for	ACCORD 140	0.005	1005			Contraction and the second second second	
0000000000	2014	544 Ar 16	ana sea	Service.	here				
CONTRACTOR PARTY	2011	and the second	NUMBER OF	inger Top	-				
contact of the last		17,078	010 KP	147	-				
CONTRACTOR NO.	20.00	Markine .	P.0. 544	200	eccelers				
Statistics and sea	107.5.5	740 (C-146)	1947 - 1946	1	and the factor				_
Il events			-					9 0 0 .	CMIT
									-
8, 2023 - Aug 28	, 2023 🛅							0.00.00.000 EPERF 0.000000 EA	e 🖊
0 + 0									
680									
		Geographic	lan las						OT
						a miner (It Fantuck (Hyper Sume hot	hadi.com		
Terement*	Erglager *		- A						
Teranary* 2011/02/07/15/24* 4/140 2025/08/28/17/24* 4/140	Agreen Course Agreen Course	n extined	- Q	Weiderley Ar		ipting interpreter Passedfack Cast fre-	sector parentel car		
2023 OR 2017 State - Cont	Agreen Courte Agreen Courte Agreen Courte	n en 1750el n en 1750el	- 0	Tubberk	THE Server Capture Lord	to autoine enteringted and	options periodal car		
2013 OF 2017 STATE OF B	Agreen Courte Agreen Courte Agreen Courte	n an Olived n an Olived n an Olived n an Olived	0	Patrick Patrick	1913 Survey Capture Unit 1900 Statuted Document	in automore enteringinal see	neng mananga bas son/Milanny	na kalanina "i "referita del del rista attache	wante
2023 OR 2017 State - Cont	Agreen Courte Agreen Courte Agreen Courte	n an Olived n an Olived n an Olived n an Olived	0000	Total Colorado Total Colorado Total Colorado	1913 Seven Capture Cont 1905 Stanford Document 1905 Stanford Document	in autorian angeingteid an 1996 the of Map (Second Second pr 1996 the of Map (Second Second pr	trog nasarga ka sos/M/sang trog nasarga ka sos/M/sang	na valjačna, i Tertholisti M. M. Tile atavite na valjačna, i Tertholisti M. M. Tile atavite nikaj di disene en anglesti dise se comens	
	Apreni Sourie Apreni Sourie Apreni Sourie Apreni Sourie Apreni Sourie Apreni Sourie	n on Used n on Used n on Used n on Used n on Used n or Used n or Used	1111	Instande Publické Instande Instande Utstande	1993 James Capture Cont 1993 David Al Document 1993 David Al Document 1993 David Al Document	in automore enteringinal see	ang naanga ba soo/ditaan ang naanga ba soo/ditaan angka hanandi dari disoo ar		
	Apreni Sourie Apreni Sourie Apreni Sourie Apreni Sourie Apreni Sourie Apreni Sourie Apreni Sourie	n on Used n on Used		Posternak Posternak Posternak Posternak Posternak	1993) Server Captors Cord Note: Faceful Processo Note: Faceful Processo Note: Faceful Processo Note: Faceful Processo Sealing Salt Table Tory of	in spiniter opgenginden. 1999: The of May (Second down age 1999: The of May (Second down age 1999: The of May (Second down age) 1999: Netlerk Decondoce Second (Sec	ang naanga ba soo/ditaan ang naanga ba soo/ditaan angka hanandi dari disoo ar		
	Apreni Sourie Apreni Sourie Apreni Sourie Apreni Sourie Apreni Sourie Apreni Sourie	a a Dool a a Dool		Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule Protectule	1933 Seven Captors Con 1968 Searched Sevenes 1968 Searched Sevenes 1968 Searched Sevenes Institute Searched Sevenes Institute Section 2003	in spinister ongengenden. 1999 - Der of Mystewart denne ger 1999 - Der of Mystewart denne ger 1999 - Der of Mystewart denne geför 1997 - Der of Mystewart (Der of Mystewart) 1997 - Der of Mystewart (Der of Mystewart) 1997 - Der of Mystewart	ang naanga ba soo/ditaan ang naanga ba soo/ditaan angka hanandi dari disoo ar		
	Apreni Sourie Apreni Sourie Apreni Sourie Apreni Sourie Apreni Sourie Apreni Sourie Apreni Sourie	a a 10000		Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Political Politi	1993 Januar Saylan Suri 1993 Bastini Dosmo 1993 Bastini Dosmo 1993 Bastini Dosmo India Bastini Dosmo 1997 Bastini Dos	in spinister ongengenden. 1999 - Der of Mystewart denne ger 1999 - Der of Mystewart denne ger 1999 - Der of Mystewart denne geför 1997 - Der of Mystewart (Der of Mystewart) 1997 - Der of Mystewart (Der of Mystewart) 1997 - Der of Mystewart	teng managa ka seci/i tang teng managa ka seci/i tang angkahan tituk dan seci rituk teng teng teng teng teng teng rituk teng teng teng teng teng teng teng teng		40170 40170 40170
	Aprenis Course Aprenis Course Aprenis Course Aprenis Course Aprenis Course Aprenis Course Aprenis Course Aprenis Course Aprenis Course	a a 10000		Roberts Descent Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Robert	1933 Januari Saytura Suri 1960 Basarika Goussen 1960 Basarika Goussen 1960 Basarika Goussen 1960 Basarika Goussen 1960 Basarika Angli 1990 Basarika Angli 1990 Basarika Angli 1990 Basarika Angli	In a scholar wagengind an in that for a fang Jonach down yn inter for a fang Jonach down yn inter fan a fang Jonach down yn tau fan down fang Jonach yn ar yn 10.746 Alfred Barrige 100.746 Alfr	teng managa ka seci/i tang teng managa ka seci/i tang angkahan tituk dan seci rituk teng teng teng teng teng teng rituk teng teng teng teng teng teng teng teng		
	Apres Scott Apres Scott	a a 10000 a a 10000		Roberts Descent Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Roberts Robert	1933 Januar System Carl Note Constant Constant Note Constant Constant Sector Sector Constant Sector Sector Sector Sector Sector Sector Sector Sector Sector Sector Sector Sector Sector Sector Sector	In a scholar wagengind an in that for a fang Jonach down yn inter for a fang Jonach down yn inter fan a fang Jonach down yn tau fan down fang Jonach yn ar yn 10.746 Alfred Barrige 100.746 Alfr	teng managa ka seci/i tang teng managa ka seci/i tang angkahan tituk dan seci rituk teng teng teng teng teng teng rituk teng teng teng teng teng teng teng teng		

- 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 <u>Video Recording of All User Activity</u> 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 highspeed OCR search in the captured recordings. See the <u>OCR</u> section above for more information on how the OCR feature works.

8.5 Option to Record Only During Violation

Screen: Edit settings	×
NO RECORD ONLY WHEN BEHAVIOR RUL	E WAS VIOLATED
UPDATE SCREEN ON EVENTS ONLY	
RECORD VIDEO	YES
MINUTES BEFORE VIOLATION	MINUTES AFTER VIOLATION
10	5

- 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

exe	REAL PROPERTY AND	eest.	• Merical	dealers a la			1444 (B	2.0		8				
							1 realization				ein i bein			
	 conditioned lists configurations 			20140-03143423	-	ELECTRONIC D	212146-0514	11500	AN DISCORPT		40 104. 24 24	-		
	L. Antibelijaninini L. Sentierinisis	enderen .			1	L dit info 12								*
	, which we have a		54th	2010/07/221125	2	resources			ALT DITORDS	iaca.	TORNE OF	646	1906.0	VER PROFIL
	n horstgersondans	5.047	-1.17	0010-2030411	1		1012-1-10	• [Teaching .					
- 24	. investigation	eranee.		2014214555										
	- universities						10000-004		françes					
(33)	L ragiptonition		Ages.	300.0177.214684					Cyruckens advertised	-				
- Can Can Can	Dashboard		nonta nenara ant	colored and social control of the color		Constraint and Constraint and Constraint and Constraint age to Constraint age to		ľ) barren 1 de seco 1 de seco				
Car								. [Seager-rol					0
Gar			CECHA DIN CHE *	14 Roberts								0.08	J 101	- CHARTER
				1.0		_	-			-	-	-	-	
			Lanes Long Long	Le										

9.2 Access Control Dashboard



- 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.
- 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

		Edit SIEM events	×	
		Chapte events to send		
88729	AND IT OFFICE		Integration: D-La (54)	ng X
		COLO USER LOGS IN	Louis Unbilin operad	
plunk> 📰	Spring States with the beaching the object	(we)	100000000000000000000000000000000000000	
-	· Deservers Press day, Secharater Re	The second second	Die foreit	64
Radar 🖉 🖉	Standards and the former	*** (***) PW# 800940	She Agentiy	-
LogRhythm: 35the	 Porter des Jacob ganier Administration 	000 TENTED	Distant states	
Sam Anton Anon	Aspering -	(CC) (001/40/048	Con 191	Jan.
New Search		AFF 0.5320	Distance	-
secondary and second period	ww.	mi weren overto	Con Science	
Dillowikesind televities		(III) MERINI CURINO	Distantinas	
8449-05 P7549 33000		THE STARLED AND THE DESIGN OF	Gia here Cara a	*
Forse Tendra 1 - Zoon the		CELEVICIA SCAMP IS ()	Ene Monege	
	un chemi internati	CONTRACTORS	Dia Xia-	
traction Hatten	a Ine Bari	TO RANDOWNERS	Constant and the	94.
404730-4020 41947-1	10500 071004435004419 10200000 0017 schronelschroten 10.114 cohranelschroten 10.114 cohra.108 starten	1 400 TOT 00110	Quark Sale Name	100 C 100 C 100 C
a sectore 1	1 2522 27/2014/2014/2014	and a second sec	Concernant Inc.	-
1 mil 1 1 mil 1 1 mil 1		h etc	Qualitizity Salar	*
accell 3 accell 3 accell 3 accell 3			South Arts	1.11
a della 1 a testas 1 a testas 3 a testas 1			214.9-11.1s	*
erpanni 3 ernapant 2 Rei 3		1.1.10 (percenter of a set of approximation and the constraint of the set of the set of the set approximation of the set of the set of the set of the set approximation of the set of the set of the set of the set of the set of the set of the set of the set of the set of the set of the set of the set of the set of the set of the set of the set of the set of the set of the set of the set of the set of the set of the set of th		

- 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)



10.5 API



- 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.
 - 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

	CİTR İX [®]		vm ware [.]	Ú
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

www.teramind.co sales@teramind.co