Teramind UAM

Features Guide

Version 1.7 (26 SEP 2024)



Table of Contents

1	Teran	nind UAM Features Overview	4
2	Featu	res Comparison	5
3	Monit	oring and Detection Capabilities	6
	3.1	Applications & Websites	6
	3.2	Browser Plugins	8
	3.3	Email	9
	3.4	Online Meetings	10
	3.5	Console Commands	11
	3.6	File Events	12
	3.7	Web File Events	14
	3.8	Instant Messaging	14
	3.9	Social Media	16
	3.10	Keystrokes	17
	3.11	Searches	
	3.12	Printing	19
	3.13	Network	20
	3.14	Geolocation	21
	3.15	Camera Usage	22
	3.16	Registry	23
	3.17	OS State	24
	3.18	Remote Control	25
4	User I	Behavior Analytics	26
	4.1	Insider Threat Detection	26
	4.2	Abusive Behavior	26
	4.3	Malicious Behavior	27
	4.4	Dynamic Risk Scoring	27
	4.5	Anomaly Detection	
5	Work	force Productivity	29
	5.1	Productivity Analysis & Reporting	29
	5.2	Time Tracking	29
	5.3	Template-Based Scheduling	
	5.4	Workflow Automation	
6	Policy	and Rules Management	31
	6.1	Policy Manager	
	6.2	Visual Rule Editor	
	6.3	Regular Expression Support	31
	6.4	Out-of-the-Box Rule Templates	
7	Audit	& Forensics	33
	7.1	Real-Time Alerts & Audit Logs	33
	7.2	Video Recording of All User Activity	

	7.3	Audio Recording	. 34
	7.4	Option to Record Only During Violation	. 34
8	Role-B	ased Access Control (RBAC)	.35
	8.1	Standardized Account Roles and Profiles	. 35
	8.2	Access Control Dashboard	. 35
9	Third-I	Party Integrations	.36
	9.1	SIEM / Threat Analytics Solutions	. 36
	9.2	Project Management & Ticketing Solutions	. 36
	9.3	Active Directory	. 36
	9.4	Single Sign On (SSO)	. 37
	9.5	API	. 37
10	Deploy	/ment	.38
	10.1	Supported Platforms	. 38
	10.2	Hosting Options	. 38
	10.3	Support	. 38

1 Teramind UAM Features Overview

Teramind's UAM (User Activity Monitoring) solution comes with everything essential you will need for employee monitoring, third-party/external user monitoring, insider threat detection, and workplace productivity optimization use cases.

Teramind UAM includes all the monitoring reports and built-in features except for the Data Loss Prevention (DLP) capabilities such as content discovery & classification, content-based rules, etc.

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

3 Monitoring and Detection Capabilities

Teramind UAM monitors virtually all user activity for system objects such as Applications, Website, Emails, File Transfers, Social Media, Instant Messengers, etc. 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 KPI 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 UAM, you can create behavioral rules based on user activities and work schedules. Then, receive real-time alerts and notifications when any rule is violated. Using the smart policy and rules engine, you can prevent data breaches and malicious or accidental insider threats with pre-emptive actions such as warning a user, blocking an action, or taking control over their computers at any time.

3.1 Applications & Websites



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

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

What monitoring & tracking controls do I have?

NO TRACK COM	NSOLE COMMANDS	
NITOR ONLY THESE	APPLICATIONS	
Salesforce X S4		
	Websites: Edit settings	×
JSPEND MONITORI	MONITOR ONLY THESE WEBSITES	
lacebook 🗙 me	Salesforce x SAP Logon 720 x Sage 50 Portal x	
		0
SPEND KEYSTROK	DON'T MONITOR WEB TRAFFIC FOR THESE WEBSITES	
	teramind.co 🗙 mail.google.com 🗙	
JSPEND MONITORI		0
Skype x Firefo:	SUSPEND MONITORING WHEN THESE WEBSITES ARE VISITED	
	gmail.com X mail.google.com X outlook.live.com X	0
USPEND KEYSTROK	SUSPEND MONITORING WHEN WEBSITE CONTENT CONTAINS	
Windows® installe	Text list - URL X	0
	DON'T MONITOR WEB TRAFFIC FOR THESE IPS	
	Network list - Safe sites X	
		0
LE 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	
	accounts.google.com X login.ive.com X login.yahoo.com X login.skype.com	
		0
	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.

	×
Webpage Url 💿	
ONDITION	
Contains facebook.com x Contains instagram.com x Contains twit Contains youtube.com x Contains pinterest x Contains tumblr x	ter.com X
(CEPT	
Contains facebook.com/business X Contains youtube.com/channel/UCStRq9qTqFJyyjQdovb0-1g/ X	0
ondition 2	×
Webpage Title ④	
ONDITION Equals list Shapping Sites X	(?)
КСЕРТ	

- On Teramind UAM, you can create Activity-based rules for the Websites and Browsers.
- 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), or detect specific version of the OS.
- 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,

What are some sample rules using this feature?



3.2 Browser Plugins

What report can I access for this activity?



No settings

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

more information.

•



Condition 1	
Browser [×] Plugin permissions [×] ⊕	
CONDITION	
Opera 🗙 Firefox 🗙	0
XCEPT	
Start typing	3

What are some sample rules using this feature?

- On Teramind UAM, you can create Activity-based ٠ 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.

Execute Windows Command, etc., and additionally a Redirect action for webpages.

- 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.

Browser Plugin activities can be monitored under

the Applications & Websites and other related BI

reports (e.g. the Web File Events report shows details for all the uploads/downloads done through

	le Block dangerous plugins Summary R Compliance Policy
Ľ	Category
	Activity
***	Users
	Apply to Everyone
5	Browser
	Plugin permissions Proxy VPN
\otimes	Actions
	After 2 violation(s) Block with message Potential dangerous plugin

3.3 Email

What report can I access for this activity?



What monitoring & tracking controls do I have?

Emails: Edit settings	×
YES CAPTURE INCOMING	
YES CAPTURE OUTGOING	
YES SAVE ATTACHMENTS	
YES CAPTURE EMAIL CONTENT	
GNORE ATTACHMENTS WITH FILENAMES MATCHING (REGEX)	
CAPTURE EMAILS THROUGH	
Desktop Outlook X Outlook Web Access X Gmail X Yahoo Mail X Outlook.com X	
	0

- 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.
- 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.
- 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.

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?



3.4 Online Meetings

What report can I access for this activity?

an 3, 2021 - Ja	n 9, 2021 🛅					Employees & Depts • Computers • Ø
suerone -	omployee	Computer	Duration	Application	Direction	Participants
021-01-08-03-48 B e			0.00:08	Zoom	incoming	Tia Sanders, +1
021-01-08 03:48 🖦	Tia Sanders	WN-0356H	0.00108	200m	Outgoing	Ta Sanders, Woharred Kingh, jgollan
021-01-08-03-48 B	Mohamed Rogh	WIN 035404-	0.00-08	200M	incoming	Tia Sanders. +1
021-01-08-03-38 B	jackson Gollan	WN 0356H	0.00.06	20011	ncoming	Tia Sanders, +1
021-01-05 03:37 🗰	Tia Sandersi	WIN-035494_	0.01.01	Zoom	Outgoing	Tia Sanders. jgollan
021-01-07 09:43 🗰	Kate Sparrow	WN-035894	0.00.05	Zoom	Outgoing	Kate Sparrow
021-01-07 00:20 B	Leo Stiles	WIN-035491	0.00.04	Zoom	incoming	Leo Stries. Kate Sparrow
021-01-07 09:20 #	Kate Sparrow	WIN-035401_	0.00.25	Zoom	Outgoing	Kate Sparrow
021-01-07 09:00	Kate Sparrow	WIN-035404	0.0213	Zoom	Outgoing	Kate Sparrow
021-01-07 02:23 🗰	Thomas Cook	WIN-005404_	0.00.25	Zoom	incoming	Tia Sanderz, +1
021-01-07 02:23 🗰	jackson Gollan	WIN-035404	0.00.25	Zoom	incoming	Tia Sanders, +1
021-01-07 02:22 🗰	Mohamed Koogh	WIN-025404_	0.0013	Zoom	incoming	Tia Sanders, +1
021-01-07 03:23 🗰	Tia Sanders	WIN-035404	0.00.26	Zoom	Outgoing	Tia Sanders, topok, Mohamed Krogh, jgollan
021-01-07-03:111 🗰	Tia Sanders	WIN-035404	0.01.28	Zoom	Outgoing	Tia Sanders
1221-01-06-13-58 B		WN-0356H	0.00.04	200m	Outgoing	Leo Stiles

What monitoring & tracking controls do I have?

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

- On Teramind UAM, you can create Activity-based rules for the Emails.
- 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.
- Prevent attaching files from a certain location(s) such as local, network, or Cloud drives.
- Restrict sending work emails from personal email accounts.
- Prevent sending of attachments to non-business addresses.
- Detect if a competitor is contacting your employees or vice versa.
- Get notified if a user is sending emails with large attachments.

- 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 the 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.

Start typing	?
ADD CONDITION	

Applications

Condition 1

	ule test Summary ∎Policy
	Category
	Activity
-23	Users
	Apply to Everyone
B	Applications
	Time Active (min) >= 60min.
	Application Name contains aircall
S	Actions
	Record Smin before and Smin after violation

3.5 Console Commands

What report can I access for this activity?

1, 2021 - Jan 1	6. 2021 🛤						and and the second s	
	ĮT,			11		1 *		
e-vana-iox			And Description of the last	179	2419	141		3 III
11103208-008			Party age for the second	1000	10000	unnit.		£ 10
CONTRACTOR			manifest and strength	and a	10127			
ALCORDON DO			And and the owner of the same		-		1	
11.11.11.11.11.11.11.11			And provid Accord	and a	-	Inflators		
0.1884.08			IncluSement-Incluse		8100	amenda		
			sale-frequences	-	1000			
ROOMERCO.			Adultation of Section	-	Ave. A			
10110-0000111-0100			manufacture and second		101010			
HO TELEVISION			handbarrant derivation	makey	2010/07	(Friday)		
0.000200			State Designed Services		1004	and the second		
- ex-0-0000			participation and second			104		
			and a descent descent	124	1000	insurance of		
				-		-		
			termidulation advance.	-	leves.	100		
NO-THREE CO.			photosen anno	-	1010.1		0	Dat
121.010.000			manufacture and	14/64	1011.08	-		
COMN Jun 30	Tama Compu Comm	r Loya Iter WIN-03 and TERAM		4-035KH	ORSPE	l\$: "C:\Users\tl	çal AppDatal Local iyahoomessenger lap	Î
		om 00:00:01						11
Jun 30	Tama	r Loya						
-	Compu	ter WIN-03	5KHOR8PEI					
	Comm	and TERAM	IIND-DEMO\WIP	1-035KH	ORSPE	\$: "C:\Users\tl	oya\AppData\Local\yahoomessenger\ap	
	Durati	on 00:00:00						. 11
		r Loya						11
Jun 30	Tama							

What monitoring & tracking controls do I have?

Applications: Edit settings	×	
NO TRACK CONSOLE COMMANDS		

- 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.
- Record the session if a user spending more than the allotted time for a meeting.
- 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.

- 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.

ndition 1		
Application Name × Launched from	ıcu [×] ⊕	
NO	YES	0

What are some sample rules using this feature?

Ru Den	le Preventing running of network sniffers from the console Summary ¹⁰ Policy Policy
B	Category
	Activity
4	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.

3.6 File Events

What report can I access for this activity?



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

What monitoring & tracking controls do I have?

File transfers: Edit settings	×
C SETTINGS ADDITIONAL SETTINGS	
WHAT TO TRACK	
YES TRACK LOCAL FILES	
YES TRACK NETWORK FILES	
YES TRACK LOCAL DOCUMENTS	
YES TRACK NETWORK DOCUMENTS	
YES TRACK EXTERNAL DOCUMENTS	
YES TRACK CD/DVD BURNING	
YES TRACK EXTERNAL DRIVES	
YES TRACK FILE SYNC WITH CLOUD SERVICES	
FILE TYPES TO TRACK	
YES TXT FILES	
YES DOC(X) FILES	
YES XLS(X) FILES	
YES PPT FILES	
YES ZIP FILES	
YES PDF FILES	
FILE EXTENSIONS LIST TO TRACK	
.odm 🗙 .gdoc 🗙 .gsheet 🗙	
	0
TRACK DOWNLOADS AND UPLOADS FROM THESE APPLICATIONS	
Google Drive X OneDrive X Dropbox X Box X	
	0
DO NOT MONITOR THESE LOCATIONS	
windows X	
	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?

reral	Start by defining the general rule settings	Rule tit Summary Berry Palay Poly
dis ons Ownges seved	Create a New Rule or Load a Template Te	Contrary Activy Unes Apply to Bergene Enum Inn Inn Inn Inn
	Rule Cotogory Statistics in the contact Acting Acting Means the Rouce with their to observe its inverses	
	Types of Activities washads APPOLATIONS washingtoogs	
	PALES 00 PRIALS 00 PRI DE	
	PERTING 100 MEPACORDAG 100	

What are some sample rules using this feature?



- On Teramind UAM, you can create Activity-based rules for the File Transfers.
- 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.
- Detect/block access to sensitive files.
- 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.

3.7 Web File Events

What report can I access for this activity?

6.00	and the second					File Events
					5.2021 🛅	10: 2021 - Jan 16
	A A Submann	Second .				and a second
			there is a		-	
		And the second s	21-			-
	-	Conception of the local division of the loca	· Anna			
		And Address of Address	8.04			-
the car one are the three		4 44 44 44	1.1	20.00	ALC: AN	1 1 1 1 1 1
264	- I CONTRACTOR INCOMENTATION			10.0 0.00 000	Acr. 574	14.4 0.4
	the family first the second se	-	10000	Traipater	- Dellaw	
and an implication of a failure and an and	Date Description/	Close in the distant in the manifesters.	Online 1			XCOMBLE CH
and produces of the American Street, 197	Intra Characteriante aphra	Cust regimenteroofpetagementel	10			10-01-0-1000
in d'an baptinisme & ababas, statu ya	Loss Constitution	Current of Institute Institution	(mer			ner-space-ook
and a section with a section of the section of the	The Characteristics	Commencement of the local data	**			100-00 (100-00)
in all and heap of inclusion. A scheduler, onlines of a	Court Countries and	Charter of a company of a last of the	140			CONDERED OF
fail and a substantial shadow and again and	with Characterization	Country of an annual property of	***			CLASS O DIRECTOR
and an impriming the statement and an	Core Description (Control of the Antiperson	Com			ROTHING THE
for antennetic thermore relation	The Course of the	Closed of the second standing to provide the	-			10.05 (1 kinet) (1 cp. c)
and a state of the	This Challenbergham	Constant a destill around abacian	114			Pro-110212 (1977)
and participation of the participation of the participation	mathemanica.	Disarta and a state of the state of the				
	mis Commission	Custom installation and	***			ROTHERON
		Coal and an other has been store	Code:			to an A house so at
in all gas happing in the station of the set						NO-ROLLING CO.
		Could be in the lot of second second				
inalga kapi ni mik shaha ni ang	The Constantion		ine.			
na ing kapitalan kalalan sa na n	1710 (Aussilianskov Door Daardinaster		iner Tate			
land ya kapanalan kabalan sana ya Maga baga sa sa da atalam sa kasa sa Inad ya kapanalan kabalan sa kasa ya	in the Association Statements Statements	Contrast de la chief particularies				P-0-12022-04
inalization internalization of an and a second	Pris Operation See The Statement	Construction optimized by particular to an Construction optimized by the type optimized	Tall			10111111100 10101111100 10101111100 1010111100
	Pris Operation See The Statement	Contractor and a set of program in Contractor and Contractor and Contractor	y nation and the second			0-0-12022-09 0-0-12022-09

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

What monitoring & tracking controls do I have?

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> monitoring and tracking controls for more information.

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

Condition 1	
File operation Download URL ×	
CONDITION	
Download x	3
EXCEPT	
Start typing	3

What are some sample rules using this feature?



- Web File Events do not have dedicated rule triggers. However, you can use the Files category and use Activity-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.

3.8 Instant Messaging

et 1	, 2023 - Oct 31,	2023 🗖								6000F* (\$10000	6394 🗾
	0 8 i And										
	EUNE		0	οTX	TOP EMPLOYEES		0.01×	HOURLY			0 e T
	4			in state			Enter Street	eters.		1.1	Ĩ
	٨				-			1			
-	Mar. 201. 2012	fill but said the	64 N								
	INATIONS					-					
		Territory' 1	Denter Dester	line and	lace week(0) be	Destructions Desk 1	timege The Local Sector	Dates in	having Maleren	Dagate discheren	
	Uniting Exclusion	firmary' i	Denter		increased in the		linge	Balance B			
1	Water in the second sec	Trentany' 1 2014-10 Charlo-Land	Denter Gegeleg	in the	manutaCEEE has manutaCEEE has	Owia 1	kinage Trick an alkalenee	Distances Incluyed			0.01
1	INVESTIGATIONS University Restriction University Teams	Developery' A 2014 - N. P. Status - Andre 2014 - N. P. Salas - Andre	Dente Deping Landing	Linches Linches	interview (USE) free interview (USE) free and interview (USE)	Owin 1 Owin 1	Neuge This is an attachment That	Distances Incluyed	Incriting Disaboreties 0 1 0		
es 1	Uniting Exclusion United States United States United States Stoppi Chill	Tennery' 1 301-10 K Cardonadi 301-10 K Cardonadi 301-10 K Cardonadi	Denter Depter Depter	Linclose Linclose Robert Lin	insertia (2011) he insertia (2011) he insertia (2011) he insertia (2011) herita (2011)	Decis V Decis V Andrear Deci	Marge This is a stationed but	italowa watiopi bio spotopi	Incriting Disaboreties 0 1 0		
es 1	Invite Instante Unreal Tore Unreal Tore Unreal Tore Dogs Chil Dogs Chil	Terreturg" 3 2014 0 N Talitz-Addi 2014 0 N Talitz-Addi 2014 0 N Talitz-Addi 2014 0 N Talitz-Addi 2014 0 N Talitz-Addi	Denter Depring Depring Depring	March 100 March 100 March 100 March 100	acceleration of the second card	Des 1 Des 1 Adres De Adres De	khoope Tris is an addateered Tris anti- Passe-Deci Tris Plachmett	italowa watiopi bio spotopi	Incriting Disaboreties 0 1 0		

- 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.

Instant Messaging: Edit settings ×

- TRACK THESE APPLICATIONS TRACK INCOMING MESSAGES VES C TRACK OUTGOING MESSAGES
- 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 Team - both desktop and web versions.

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

Condition 1	
Messaging App [×] Contact name [×] Message Body [×] ⊕	
CONDITION	
Facebook 🗙 Microsoft Teams 🗙	0
EXCEPT	
Microsoft Teams Web 🗙	0
	Ŭ

What are some sample rules using this feature?



You can use the Message Body, Message • Direction, Messaging Application, and Contact

rules for Instant Messaging.

On Teramind UAM, you can create Activity-based

- 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,
- Restrict messages to/from select contacts.

Execute Windows Command, etc.

- 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 monitoring & tracking controls do I have?

3.9 Social Media

What report can I access for this activity?

1, 2021 - Jan 9, 3	2021 💼				BOOMT DIMINI LOG T
		1.1 NO.1			•• Teleparte •••
		Restances of the second		<u>_</u>	
					they .
CONTRACTOR OF THE CASE		naim.	Leader	Test	No. which dependent that matters, 10 a shad process.
01-01-01 TRONOM DATE		100.000	Letade	Red	harama damar'i samaria para, fao pario h
COLUMN TRANSPORT		street, surraw, well-	Testoria .	inst.	Second seat for accounted with facility
0.0101000000			Pauli suf.	Post	that upon a belier three-real card.
01-02-04 10-02-03-03		lane, His He, have	Turker 1	Test	Trace from that if you is a the Life atting you had.
		manifest and, the	1.04	101	The number and data to the end group up
0.00 (0.16 (0.16 (0.16 (0.16		satisfaction, See, effort) attainments	Texture	Real	Established Sector Menuficet, nucleo Herandoloments
0.01.01.01.00.00.00		overage which were and the	Restrick	Port	in oursed package worth in particular of particing
10.010-010-010-010-0		higher relation conformity large adjustice area	Testinol	Peak	Higher education researcion beneficial to increase at advances. In endocument the respectives and delay loading a
10.01 (0.010)		texture, working provertial things, improve teach-	luine .	inst.	When trackets are volving together, they can als powerful thing to improve their own backling and in fur
		alify you, page worked to proper pr	Testinol	Red	THE ABLETE OF A DROP OF REPAIL TO GO REAARAHEE THINGS INFORE OF HOR ABLE THOSE PROFY.
		press heplan hep-land hem-hem-	Links	Tain Dyan	The most type generate happings within prevail. If you are in happy in marping, thereas any prevaints
10.00		generatio, hoppings	Letada	Part	Too much by to generate tappings within yourself.
			Turner	ited (Index your energy and your bland, sorting together to horryou to the base the area to electer you and C
		maniful heppy Bit theory	Reading A.		
		mailed, heavy IN, Dentry mailed, heavy IN	Testing (Red .	They find a second second a ready the contract of the second
				Near Rote	They Mile & sampled to realize a barry Mil. Real suppose physically development input you, good a real of time with their and it will develop also
		control largery the	Testing 1		They belle is considering realize a fragmy life,

What monitoring & tracking controls do I have?

RACK THESE APPLICATIONS	
Facebook X Twitter X LinkedIn X	٥
YES 🚺 TRACK NEW COMMENT	
YES 🕥 TRACK EDIT COMMENT	
YES O TRACK NEW POST	
YES TRACK EDIT POST	

- 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.
- 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?

webpage Url Total Time Activ	ve (min) × 🔿	
ONDITION		
Contains facebook.com X Contains Contains youtube.com X Contains p		r.com X
XCEPT		
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.

6	Category	1
-	Activity	I
<u>*</u> :	Users	1
	Apply to Everyone	1
0	Webpages	I
	Webpage Url contains facebook.com or contains instagram.com or contains twitter.com or contains youtube.com or contains pi Interest or contains fumble Total Time Active (mix) > 15	
8	Actions	1
	Show warning with message Please keep your social media usage to a minimum while at work	
Etk	ule Block Facebook Comments Summary	
Etk	ule Block Facebook Comments Summary unite May Conjeny	
Eck B	ule Block Facebook Comments Summany events thought Cotagony Activity	
B	ule Block Facebook Comments Summary week how Conjeny Activity Users	
B	ule Block Facebook Comments Summany events thought Cotagony Activity	
600 60 40	ule Block Facebook Comments Summany event history Cragory Activity J. Ures Apoly to Designate	
604 104 104	ule Block Facebook Comments Summary went how Congeny Active Viens Apple to Response Evolution Marketing	
604 104 104	ule Bick Facebook Comments Summary www.hing Category Active Users Exclose Maintening Webgers	
60 6 0	ule Block Facebook Comments Summary werne how Congeny Activity Users Apple to Despense Exclude Marketing Webgages Webgages	

3.10 Keystrokes

What report can I access for this activity?

Reystrokes			Q D THE OWNER DEVICE
10, 2021 - Jan 1	L 2021 🛅		
	*		
			11 (Marcal 11
	NI 18 1	-	
101.11.11.11.11.01.01.01.01		diamont in the	00.000
101-11-11.11-10-10-00.00		attains	Alter Alter Alter Alter Alter Atter Anter Alter Atter Atter Atter Atter Atter Atter
10x 25 11 [] 10 al (0)		artists 1	and the protection of a performance destination and the second hour may decrease - decreases and that have how
DO DO HEARING		- articles	concentration of the lattice has well to choose experience for the lattice former for the descent of the second states
SCHOOL IN DOMINICASE		wheeld	Statistic and Tarra an an internet, there proved in the same of the same of the same spectra frequency of the same of the same of the
an o nava e ca		-	The second Link Constant of California Constant Constant Constant Constant Constant Constant Constant Constant
210124208			
D-0-1242-08 D-0-1242-08		-	taken har all the approximate poor and of the Net Barliel, or Balance
		-	navez ha a di te appetet angan a di di K. Na appete or Balagar Kalana na dapatete haring senara ng canana gibangan dangan da basang ata kina mingan a te m
			service at the approximation of the No Bardel or Matter In Advances and an experimental service as converse of datasets from the Advances and Lances and and Lances and Advances for the advances and an experimental consequent and approximate that is determined and the Advances of the Advances and an experimental service and advances for the Advances of the Advances of the Advances of the Advances in Advances in Advances for the Advances of the Advances of the Advances of the Advances of the Advances of the Advances of the Advances of the Advances of the Advances of the Advances of the Advances of the Advances of the Advances of the Advances of the Advances of the Advances of the Advances of the Advances of the
		[]]]	men de la la sectión españa da la XIV. Na gede de la basari en la se de la sectión de la Basaria de la desarrol de la sectión de la Basaria de la sectión de la
			service at the approximation of the No Bardel or Matter In Advances and an experimental service as converse of datasets from the Advances and Lances and and Lances and Advances for the advances and an experimental consequent and approximate that is determined and the Advances of the Advances and an experimental service and advances for the Advances of the Advances of the Advances of the Advances in Advances in Advances for the Advances of the Advances of the Advances of the Advances of the Advances of the Advances of the Advances of the Advances of the Advances of the Advances of the Advances of the Advances of the Advances of the Advances of the Advances of the Advances of the Advances of the Advances of the
			Insertion to approximate and an Additional Hospital
			Another and a second part of each Another and another and a second part of each Another and Anoth
			Insertion to approximate and an Additional Hospital

What monitoring & tracking controls do I have?

Keystrokes: Edit settings	×
YES TRACK CLIPBOARD	

- 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 / downloading of files to/from social media sites.
- 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.
- 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>.



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

ondition 1	
Text Typed 💿	
ONDITION	
Contains <prtsc> X Contains <shift+prtsc> X</shift+prtsc></prtsc>	3
KCEPT	
Start typing	?

What are some sample rules using this feature?

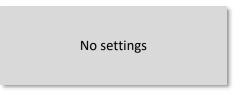
Rul	le Screenshot taken Summary no Palicy Policy	
6	Category	
	Activity	
4	Users	
	Apply to Everyone	
ń	Keystrokes	
	Text Typed contains <prtsc> or contains <shift+prtsc></shift+prtsc></prtsc>	
8	Actions	
	Block	

3.11 Searches

What report can I access for this activity?



- On Teramind UAM, you can create Activity-based rules for the Keystrokes.
- You can use Text Typed or Word 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.
- 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.
- View all the search phrases by timestamp, site, employee, department, computer, etc.
- Compare or group searches by timeline, top searches by employees, sites, keywords, etc.
- Filter the report by the employee, department, computer, platform, etc. and LDAP groups/attributes (if integrated with Active Directory).
- Print or export the reports as PDF/CSV files.
- Schedule regular report delivery to email addresses.
- View video records of the activities by date/time.
- Add real-time widgets on the BI reports.



What monitoring & tracking controls do I have?

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

Condition 1	
Webpage Url [×] Webpage Title [×] ⊕	
CONDITION	
Match list Keywords 🗙	0
XCEPT	
Start typing	(?)

What are some sample rules using this feature?

1	Category	
	Activity	
. :	Users	
	Apply to Everyone	
9	Webpages	
	Webpage Url match list Keywords	
	Webpage Title contains Google Search	
3	Actions	
	Redirect to searchpolicy.teramind.co	

3.12 Printing

What report can I access for this activity?

Printing						Q 👔 Tor association 🗢 🔿 Enter Yook 🛛 BRANCY HEIRON
0, 2021 - Jan 1	s. 2021 🛅					Last que time 2021 dt 10.2100 EPOET + 0.040 T
artes			· ·			•• ••
				and last		
				rate:		
				1.1.0		
			10			
ALC: 100 B		14.11 1.11 M			0.4.4.	H
	Indust	Computer			Page Cast	
Contraction of the second seco	The land	and Management	Manual And To HW	Contract	- None - Lage	
COLUMN DA			Annual Post of Post	The same data and the		E
ALC: NOTICE AND			Manual Rist In 201	designed hand (Maximum Last		-
			Manual Res & WY	Description of		
			Manual Inte To 201	When having had only		
410.0004.000			Manual Red To FDF	Metalizada Lat		
			Managed Read To PEP	Managing part 2 and		
			Manual Red Script Manual Inst Script	Mentaling-date Load Inserve Redenant Coald		
			Manual Red 1,409 Manual Inst 1,409 Manual Red 1,409	Mentingster Lait Instructioner Cost R. Managemeil Materials - M		
			Marcardt Rock To HEP Marcardt Rock To HEP Marcardt Rock To HEP Marcardt Rock To HEP	Methologian Lab Inserv Balance Golt Ritherapered Autochter - Sci The Berlinse Cenning Realphore obj	1 1 2 1 2 1 1	
			Manual Red & PDF Manual Red & PDF Manual Red & PDF Manual Red & PDF Rance Dating Ray Red	Metering stars Last Insura Talance Cost R. Managament Materials - 54 The face Tosta Canoning Padaphone and Setting 1	1 1 2 1 2 5 1 1 1 1 1 1	
			Manageh Rock To HEP Manageh Rock To HEP Manageh Rock To HEP Manageh Rock To HEP Remote Deality Res. Rock Remote Deality Res. Rock	Menting per Last Inner Samerican Rithergenet Addrition - 54 The last Sameling Readjoint and United 1 Loning 1	1 1 2 1 2 1 3 2 3 3 3 4 3 4 3 4 3 4 3 4 3 4 3 4 3 4 3 4	
			Housek Rocks 1979 Housek Rocks 1979 Housek Rocks 1979 Housek Rocks 1979 Rocks Dathy Roc Net Rocks Dathy Roc Net Rocks Dathy Roc Net	Metalogue Lait Inner Inner Cat Mangemet University of Selation and University Advances United Towards Learnes T	1 1 2 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
			Manageh Read Sy HEP Manageh Read Sy HEP	Mantergan Lait Issuer Jannen Gait Kittergenet Apterten - sid Ter Bei Taus Zouting Halpformach Umber 1 Intera 1 wittigs objecting phra. 2000 Adjancet Alleren Steame Jannen järe et ei emergik.	1 1 2 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
			Manageh Read Sy HEP Manageh Read Sy HEP Manageh Read Sy HEP Manageh Read Sy HEP Reader Databage Read Manageh Read Sy HEP Manageh Read Sy HEP Manageh Read Sy HEP Manageh Read Sy HEP	Meeting year Last Inner Universität Kollengisere Universität United 1 Universität Universität Universität Universität Universität Universität Universität Universität Universität	1 1 2 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
			Marandi Kata Sy HP Marandi Kata Sy HP	Mentingues Lait Isour Annue Cuit The Benne Cuit The Benne Cuit States Lainting Nadjone and Utility 1 Lemma 1 Lemma 1 Annue Jossen phan- Nation Appartation Africana benner a Scatter phan Nation 7 data pageweb their deal Appartations (L) Fragment Present Disarde Strategies (L)	1 1 2 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	

• You cannot create any Search-based rules directly. However, in Teramind UAM 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.

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

What monitoring & tracking controls do I have?

Printed docs: Edit settings	×
PRINTER TRACKING ACCOUNT USER	
demo@teramind.co	
PRINTER TRACKING ACCOUNT PASSWORD	
VES CAPTURE ACTUAL DOCUMENT	
MAXIMUM CAPTURE DOCUMENT SIZE (PAGES)	
50	
EXCLUDED PRINTER NAME (REGEXP)	
	©

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

rinting	
Condition 1	×
Printer name [×] Number of pages [×] ⊕	
CONDITION	
Contains HP_Color ×	(?)
EXCEPT	
Start typing	?

What are some sample rules using this feature?

Ru	le Print restrictions Summary •• Pelicy Policy	
В	Category	
	Activity	
\simeq	Users	
	Apply to Everyone	
Ģ	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	
8	Actions	
	After 2 violation(s) Show warning with message Please consider using the HP BW printers for large print jobs.	

3.13 Network

	work Monito	ring (Clonec	i)					* • •	START TOUR
Nov 1, 202	23 - Nov 30, 20	23 🗃		Lat. yes 1	Pre 2023-11-16.0	as prove	• Datstolt BSNt +A	0.017 0.016	о 🖊 т
Basic 0	+								
OUTGOIN sees citole- selars citole- selars citole- selars citole- ty		0 0	No arrestor	Ster Territori Stepar Advisor Metter - Scillar Internet 2020 Metter			CONNECTION BY PROCE antiquitante antiquitante antiquitante No		toris and manage and home and home and
maslill	a 20,300 40,300 Connections	101W 17	unitedija	alinji (Barnah) U	attara (4.00)		a 20,000 40,000 E 20,000 40,00 Carmadan	·	informe nationen mationel/en] an antana
PLAIN GRI	D								0 T ×
	umpt +	Department	Employee	Computer	Test	Destinution lg		Protocal	Serti
8 2923-0	1-15 1217/40-0408	No Oepartment	John Simmore	Amven2003	Debuik seik	239,255,255,2	50 1000	10	700
	0-15121741-0488	No Department	John Simmone	www.ee/2003	Default tesk	21436272.13		UDP	1826
	1-15 121730-0400	No Oepartment	John Simmone	ATTV042003	Debuilt telik	1052525	53	10	70
1 884	0-15121740-0488	No Organizment	John Simmore	Amagen(111)	Default tesk	10.52.52.58	483	104	1093
	1-15121740-0400	No Cepartment	John Simmone	wmware(203	Debuit telk	21658292.0		UDP	640
	0-11020348-0498	Na Department	several devices to hollow	ded cap to hollow	Debuilt Sells	108.177.726.1		UDP	24
	111020144-0400	No Oepartment	served divide dealerap-107/50 hv	deletap-to/tollev	Default tell	21658293.19		UDP	24
	0.11 62/01/40-04/00	Na Department	several distance of the low	desking-till film	Debuil tea	188.774.98.7	40	UDP	72
	11 520144-0408	No Oepurtment	served divide dealerapie 745 divi	deleting-to7507v	Default tell	1122173683		UDP	24
	0-11 62/01/40-04/08	Na Department	several distance of their	And up to highly	Debuil tea	1122013981		UDP	45
1 2023-		ing only a search			CALIFORNIA STATE			0.04	

- Specify which printer account will be used for printers that require a 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.
- On Teramind UAM, 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.

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

• Add a real-time *Network Usage* widget on the dashboard.

What monitoring & tracking controls do I have?

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	
	0
TRACK ONLY THESE PORTS	
	0
DO NOT TRACK THESE PORTS	
	0
TRACK PROCESSES	

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

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

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

Rule PCLDSS 1.3.4 - Unauthorized traffic from cardholder environment Summary Rest deviation many Company Anting Wins Note websited Note with the meante host exclude match 1925/86.80% or match 1980.83% Officing Restrict host exclude match 1925/86.80% or match 1980.83% Officing Restrict host exclude match 1925/86.80% or match 1980.83% Officing Restrict host exclude match 1925/86.80% or match 1980.83% Officing Restrict host exclude match 1925/86.80% or match 1980.83% Officing Restrict host exclude match 1926/86.80% or match 1980.83% Window match 1920 Restrict host sit host allowed per PCI055.13.84 and the match 1980.83% Restrict host match 1920 Restrict host match 1921 Restrict host fields fields and dema.com Restrict host match 1923.33% Restrict host match 1923.34% Restrict host match 1923.34% Restrict host host host defining per PC 055.23, and host hyperbasoddeteramind-dema.com </tbod

What are some sample rules using this feature?

3.14 Geolocation

- On Teramind UAM, you can create Activity-based rules for the Network.
- You can use the Application Name, Remote Host and Port, Bytes Sent and Received, 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).
- Implement geo-fencing, for example, restrict access to your EU server from US users.
- Get notified when abnormal network activity (i.e. sudden spike in network traffic) is detected which might indicate an intrusion.

	19, 2023 🛱						araanaa miinaanaa kaasaa gaaraa kaasa kaasaa 🔹 🚺
0 +							
						0.01	0.01
							and the second state of the second seco
	and the state of t	construction of	indexes.	Scienti.	(618.89		
and income of	and the state	const have	fair francess	el+thi	(clashe		
Sugar Special	and in the second second	control former	fair/amount	seal.	10.0840	-man F	
And Persons in	and in case of the	- main larger	in terms	64.04 M	101844	-10.004	the second se
integ Theor	or other day	unet Leve	Section and	(0.001)	10,000	10000	The second se
	and in case of the	unit form	Sections	(0.48)1	10,000	-10.000	
		const three	54700068	10100	10,000		And a second
Include Section 1.		const thread	54700000	214810	10.00	100000	A second s
in an	and included	const laws	inforcer.	615254	10404		
and i have	and included	const laws	la facer	1442.00	10.000		Come Contract of the Contract
Circle and	also in the second second	man here	la familia	1414/1	1112.00	-0.00	
Station Sugar	all Cliniches	men here	the frances	11.18.49	11144	-122.00	and the second se
Appartment.	and the state of the	construction.	Technology.	(6242)	(1)(1)	-10120	22 March 1997 Contraction of the second
Rosen Carriel	distanting to a	construction of	7470000	104(2)	(1)(2)	-1272.01	
			1010000	14104	17.02.00	-12.52	
					11.15.00		

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

What monitoring & tracking controls do I have?

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

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



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

3.15 Camera Usage



- 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?



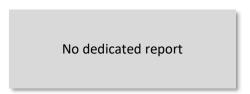
What are some sample rules using this feature?

Rule Campora App Summary camera Hay Category Activity Subset Carene Carene Carene Carene anne contains VMware Virtual USB Video Device or contains Logitech HD Webcam or so Carene application name contains zoom.exe or contains Logitech HD Webcam or so Carene application name contains zoom.exe or contains chrome.exe or contains webex Show warning with message Camera use detected

- 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.

3.16 Registry

What report can I access for this activity?



What monitoring & tracking controls do I have?

- Registry: Edit settings × TRACKING DAYS AND TIME Sun Mon Tue Wed Thu Fri Sat 0:00 23:59
- Registry changes aren't tracked on a dedicated report but you can view rule violation incidents related to the registry on the <u>Behavior Alerts</u> report.
- You can toggle the registry monitoring on/off or set up a monitoring schedule.

neral			Rule Registry changes Summary
er.	Registry		Sample Rules Policy
	Condition 1		Category
ions	Key Name × Value × Program ×		Activity
2013			👛 Users
Changes saved			Apply to IT
	Cerearis Hey, local_machine1_x	00	Registry
		00	Program contains repedit
			Key contains hikey local machines
	Start typing	T	Name equals Starts
			Value equals 3
	ADD CONDITION		G. Actions
			Notify ben@teramind.co

What are some sample rules using this feature?

	e Registry changes Summary I e Rules Policy
Ē	Category
	Activity
2	Users
	Apply to IT
	Registry
	Program contains regedit
and	Key contains hkey_local_machine\
ar	Name equals Starts
	Value equals 3
0	Actions
	Notify ben@teramind.co

- 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.

3.17 OS State

What report can I access for this activity?

electronice						Literary in	use: 53 / 500
task -	The second	· Annual	ora Dagingan	-		1000	
LHILCK Deleter					α.		
Bestare		Department .	Latignme	Last tops from	Toria .	Mantored	24
Enable Monitoring Disable Monitoring	amond diama.com		2020-08-01 16/12-08	-	Lotiest	No.	140
Buk edit.	distance democrat	Aught	Ditte	an USA after	ADR	761	
Berth. berdte	arindus	my-department			A25-8	10	10
Bolton babries	Placament James Jom	The P	2022-01-0415-0415	BUD-22541-CARPER	A2114	790	
Dapite. Israels	ciparantei dans.com	and-test2	2022-06-27 23:00:17	an Ultimeter	1004	100	-
Cather, sphare	edhearend as				A25.0	141	100
Cate, cogd	terative demonstra	Same .	Onice	win-both-britter	ADM	141	74
Cary. quiter	Bacanton Science com	THAT	Ditte	with Differ before	A204	144	144

What monitoring & tracking controls do I have?

- OS State: Edit settings × vec lock vec sleep vec screensaver
- 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.
- You can toggle the monitoring of Lock, Sleep and Screensaver states.

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

seeral seer legistry changes saved	Registry Condisisn 1 Koy Name ^K Value ^K Program ^K Controll Controll	0 0	Rule Registry changes Summary seeps toxics hulp G. Cropsy Activity Apply to ff Registry Program contains regedit. Interpretation services
	Start typing	Ø	Key contains hierg,local_machine\ Name equals Starts Value equals 3 © Actions Notify ben/Rteramind.co

• 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).

3.18 Remote Control

Remote Control 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 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.

4.1 Insider Threat Detection

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

- Establish organization-wide visibility and control for over 12 objects including the screen, 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 and 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 insider incidents and identify what happened, who, and what caused the incidents.
- Risk analysis to identify security gaps & vulnerabilities.

4.2 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 UAM, you can create Activity and Agent Schedule-based rules to detect abusive behaviors easily. For example:

- 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.

4.3 Malicious Behavior

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

- A user trying to hide information in an image.
- Sending out emails with sensitive files to non-corporate emails.
- Unauthorize use of Cloud sharing drives as an attempt to exfiltrate data.
- Sharing embargoed 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.
- Communicating with competitors.
- RDP connection attempts to forbidden hosts or unauthorized use of RDP applications.
- Sudden change in schedules or work patterns.

4.4 Dynamic Risk Scoring

											2 🗢 mere
3, 2021 - Jan 9, 20	121 🗖								ECOR- DAILO	a and	100 B
and the local data											
etta dia Vitatta					Marrie La						
		. 1.00			12222	22		2			
a fina dirugiyante			es brate					(heliniber			
Barter Breiter Breiter Breiter Bewitter	ri,			Annual Contraction				-			
The second secon				Paultin and CO-		<u>-</u>			and a second	~	
Antening Parting Device	~	la.	-	And a second sec		ta.				~	
Deviloe Deviloe	teet i		-	And a second sec		ta.				~	
Deviloe Deviloe	for the second s	in. p	-	And a second sec		ta.				-	
Deviloe Deviloe	for the second s	ina pr 10	a la fa	Bengingen	Company	ka. Itinγ	ha	á.ten	ing	-	- 1
Deviloe Deviloe	No. (1001) J. (201) 1	ant M M A	in the second se	Experience Control of	torgane	ha. Inny Podeta bits	tar	A San Native Data	road	100 100 100	
Deviloe Deviloe	Na Gasti i 1997 191 1	84 94 95 9	n Intervit -	Internet in a constraint of the second secon	to country to country to country	Fe.	tas Instru-	A Tan Natify State. Natify State.	read of the second seco	100 100 100 100 100	
Deviloe Deviloe	Fee First L A 200 1 1 1 1 2 1 2 1 2 1 2 1 2 1	104 34 30 0 0	Instany 2 +	Engineering filler Registration Beginnering Engineering Engineering Engineering Engineering Engineering Engineering Engineering Engineering		Fer Inny Postoria Tato Instoria Tato Postoria Tato	ha hain. hain.	A.500 Nation National National National National National Nationae	Integral	100 100 100 100 100 100	
Deviloe Deviloe	Tea Classifi A Classif A Classifi A Classifi A Classifi A Classifi A Classifi	844 34 30 0 0 0 0	1	Engineering fil an office The part of the second se	torgate and an and an an an and an and an an and an an and an	Fer Inny Postote Tato Postote Tato Postote Tato Postote Tato	hai hai hai hai hai hai hai hai hai hai hai	A.310 1449; 344. 1449; 544. 1449; 544. 1449; 544.	Integral	100 (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	el tragelari el tragelari el tragelari el tragelari el tragelari
Bank series Beneficies Develope 1994	Res 	104 14 10 0 0 0 0 0 0	8 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Register Register Stephenski og som Register Reg	to design of the second	Fai Posturior Talia Posturior Talia Posturior Talia Posturior Talia Posturior Talia	hai Inelm, Inelm, Inelm, Inelm,	A.500 1489; 3ml. 1489; 5ml. 1489; 5ml. 1489; 5ml.	Integral Integral Integral Integral	100 100 100 100 100 100 100 100 100 100	e i in egoladi el freegoladi el freegoladi el freegoladi el freegoladi el freegoladi
Bank series Beneficies Develope 1994	Rec 6444 384 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3	ни 14 10 0 0 0 0 0 0 0	8 10 - 0 0 0 0 0 0 0 0 10 - 0 0 0 0 0 0 0 10 - 0 0 1	Engineering Segmenting of the Segmenting of the Segmenting of the Engine Views Digen Views Digen Views Digen Views Digen Views Digen Views		Re. Restartion from Distantion from Production from Production from Production from Production from	hai Incline Incline Incline Incline Incline	A.200 1489; 3ml. 1688; 5ml. 1689; 5ml. 1689; 5ml. 1689; 5ml. 1689; 5ml.	Frageri Integri Integri Integri Integri	500 100 100 100 100 100 100 100 100 100	el la agrical el la agrical
Roberts Control History Control And Antonio Description	Ras Finant A 2004 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1	844 94 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	8 8010 0.000000 8010 0.000000 8010 0.000000 8010 0.000000 8010 0.000000 8010 0.000000 8010 0.000000 8010 0.0000000	Engineerin Engineerin	Corport Cor	Re. Rely Productor Twin Distortion Twin Productor Twin Productor Twin Productor Twin Productor Twin Productor Twin	hai hailin, hailin, hailin, hailin, hailin, hailin,	A.200 1499;344. 1499;544. 1499;544. 1499;544. 1499;544. 1499;544.	Ing in an or in the second sec	500 (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	(1)(1): (1)

Chose time period for	thresholds	
Choose the period of time for threshold cal	ulations	
Daily	•	?
Configure action thre	shold	
Configure action three Sequence of actions	shold O	

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.

RULE TRIGGER					
WHAT TRISGERS THE RULE					
Select the action which the rule will be built up	on				
Webpages					•
CONDITIONS					
Select parameters for this rule					
Anomaly baseline	Ψ.	15	Department		• *
Time (%)	۲			10	×
ADD CONDITION					
RULE RISK LEVEL					
RISK					
Select the degree of risk for violating this rule					
Since an approximation in a single state					
No Risk Low		Modera	Ce .	High	Critical
ACCUMULATES RISK					
Whether this rule should be counted multiple	times per day on mi	ultiple violations			(111)
					_

4.5 Anomaly Detection

≡ Anoma	ly rules				۹	The Administrate	*) [SART TOUR
2 fuiet							⊙ ∧∞	ANONO	LYRULE
FILTER RULES	τ	RULES	CONDITIONS			APPLIES TO	ACTIO	15	
Input the name of	(rule	Webpages Anomalies	Webpages Time (%) >	- 7		All employees	1	0	×
Add employees	or departments	File upload anomaly	Files: Web- Threshold	upload operatio I count > 3	m	All employees	1	0	×
CONDITIONS									
Conditiontype	0								
								-	_
019-07-22 11:02:52	Mohamed Krogh		Webpages Anamalies	Neacton	Used beime.com	46.8% of time. Company Average	1 i 2.2%, Depar	Creent 2.2	10g+112.5%
19-07-2211-0252			Webpages Anomalies	Neaction	Used excellent 30	4% of time. Department average	n is 1.0%. User a	o eraga is	8.8%
019-07-02 11-00-53	Ton Farmer		Weigages Anamalies	Neactory	Used www.fames	wi.com 14.0% of time. User avec	ge 15 0.2%		
				No ection		cem 54.3% of time. Department			

Create Anomaly Rule		×
	USE TEMPLATE	
TEMPLATE TO USE		Ŧ
By Type Applications Application usage anomaly Emails		Â

Assign Risks to Behavioral Baselines:

With the Anomaly Rules, you can assign dynamic risks to anomalous behaviors based on time and baseline compared at the user, departmental, or organizational 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):

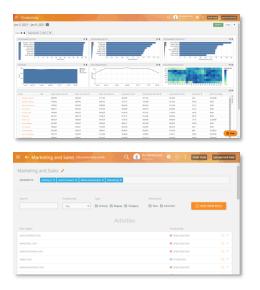
Anomaly Rules are special types of rules available on Teramind UAM and Teramind DLP. They allow you to identify anomalies in user behavior or application activities by utilizing behavioral baselines. An anomaly rule also allows you to assign risk levels to user behaviors and create notification actions 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 UAM comes with many anomaly rule templates for Applications, Emails, Files, Instant Messages, Networks, Printers, etc. Using the templates, you can start creating sophisticated anomaly rules in no time.

5 Workforce Productivity

5.1 Productivity Analysis & Reporting



5.2 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 period.
- Import projects and tasks from PM solutions such as Zendesk, JIRA, etc.

5.3 Template-Based Scheduling



Feb 25, Thursday DAY WORK TIME ALLOWED BREAK Thursday 9:00 18:00 SET DAY OFF

5.4 Workflow Automation

	Simple Mode	Advanced Mode	Rule Accounting/Auditing task Summary Reductor Tests Pulsy
bcations	Select how the system should	rant to violations	B Category Activity
	SCOPY	() ()	Apply to Everyone Apply to Everyone Apply an Everyone
	8000	000	Application Name contains excellance
	LOCK CUT LINER	(160	Switch user's task to Administrative
	-	(76)	
	BET UNDER SAUTHAT FAIR.	(11)	
	Administrativa •	-	
	Process outer that facility will be an open to open and roll a	i Official i Official	
HAT TRIGG	ERS THE RULE	e built unon	
HAT TRIGG		e built upon	v
HAT TRIGG	ERS THE RULE ction which the rule will b Productivity	e built upon	×
HAT TRIGG elect the ac Activity: F	ERS THE RULE ction which the rule will b Productivity	e built upon	~
HAT TRIGG elect the ac Activity: F CONDI Select	ERS THE RULE ction which the rule will b Productivity TIONS	e built upon	V Department V
Activity: F CONDI Select	ERS THE RULE ction which the rule will b Productivity TIONS parameters for this rule		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 an 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.

6 Policy and Rules Management

The core of Teramind is its policy and rules engine which can automatically detect malicious, inadvertent, or accidental threats. You can get started right away with hundreds of pre-built rule templates and activity classification lists. 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.

6.1 Policy Manager

			Search for rules Q
POLICIES	# RULES 7A65	AUDIENCE	ACTIONS
CREATE NEW POLICY			IMPORT POLICY 1
SDPR Compliance	20 rules	Everyone	()#1) I
Demo Policy v	13 rules	Everyone	• •
Productive Tasks	7 rules	Everyone	••• •
Agent User Experience Demo V	4 rules	Everyone	•••
PCI-DSS-Compliance	10 rules		.
HEPAA Compliance	13 rules	Everyone	.
Sensitive Data	4 miles	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 UAM comes with a sample policy with some rules for you to experiment with.

6.3 Regular Expression Support

Regular expression match	• ?
PECIEV VALUE	

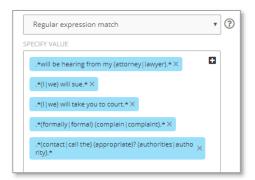
The Rules Editor is an intuitive, visual editor where you can create even complex rules easily without going through multiple screens or coding.

- 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 UAM 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.

6.2 Visual Rule Editor



6.4 Out-of-the-Box Rule Templates

• Celsularia Policies 0 memoria 0 memoria • Sector Varianza Martina 0 memoria 0 memoria • Method Policies 0 memoria 0 memoria • Method Policies 0 0 memoria 0 0 • Method Policies 0 0 0 memoria • Method Policies 0 0 0 0 0 0 0 0

• You can also detect sensitive words or phrases such as harassment or angry sentiment in emails.

- Teramind UAM 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.
- You cannot use any templates or sample rules that use the *Content-sharing* rules on Teramind UAM. You will need Teramind DLP to use those templates/rules.

7 Audit & Forensics

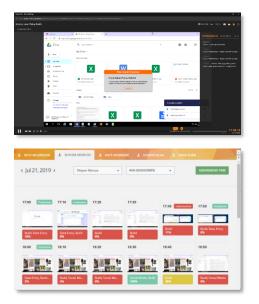
In addition to the monitoring and alert reports, Teramind DLP comes with a Session Player that allows you to access a user's desktop live or view recordings of previous sessions. You can see all the notifications the user received and search for specific information/activity.

7.1 Real-Time Alerts & Audit Logs

3, 2021 - Jan 9, 2021 🛅 R 🕈 🗑 Risk +					EXPORT • CLONE	ŀ
inatra 🛛 🖉						
	 Navy 		0 8	tap Drugstynni	0	
Line 1 the 2 the 3 t	1 2 7 8 5 8 5		Court	Tell Magnage Brayter Countrol Driver Toxics Online Wome Direct Jointon Drive Dom- Drive Dom- Drive Dom- Drive Dom- Driver Dom-		
antilition of Taulot Webb Thub? From Sector						
irrestang" à Erekvee Co	reputer P	oley Rule		Action	Description	Ē
821-01-09-23-58-44-05:00 Mindy Jameson W	N-CONFORMER I	SA Samala	centerit sule	Neth	Service celled an email with Lass	
121-01-09 23 58 28-05:00 Silvers Monros 10	N-CESK-CREPER P	roductive Tesks Data Er	en tesà	Notify SwitchTesk	their the application notegaal.ex	ŝ
821-01-09-23-58-59-05-00 Shiyara Monces 10	N-DISK-OMPER	reductive Tasks Data En		Notify Switchlink	Used the application workpadle	H
			mication task	Notify Switchlask	Used the application slack even	
		roductive Tasks Data br		Notify SwitchTask	Used the application motogradies	
		roductive Tasks Data Dr		Notify Switchlink	Used the application wordpacks	
(302) - Aor 1, 2023 🗃					BOOK THE COU	8 1
rates I to I term	ALC: No					
CONTRACTOR AND CONTRACTORS	the Adams	and the second s			A THE DRIVE CONTRACTOR AND A CONTRACTOR	
CONTRACTOR AND ADDRESS	W 805	away .	Chinese Company, Class To	N AGENTARIA SUBJECT	The second second second second second	
International Address Income Statements	See Block	100	Select of Laboration Plant's	- Andrew & Televise state	1	
contractions and a second second	See Black	too all	Statute Berland		Ten Date: 1000 002 00 00 00 - 0020 07-00	
NUMBER OF STREET	Ser Adap	and the second s			n naga salah da sa salah sa sa	
Includence and an inclusion inclusion	Ser Alley	all the second sec	Advertising the second	to The loss logitudes & Vol	approximition and here you will be a set of the	
CONTRACTOR AND ADDRESS STATES	ter etter	Inclusion and the second second	Venanoweloog	- State & Manager and All	rate Charles becaute the Observer	***
CONTRACTOR AND A REAL REAL REAL	14 Black	and one of the second s			ALTERNO - 201410	
10000-2000-00 200-0 56.0 m 1272-1	teral trade	here				
and the second s	the type					
management and report of the		anaper and				
AND DESCRIPTION OF A DE	ter No	ercolors and an				
4 overts. 8. 2029 - Mog 28. 2023 ₪ 9				- an age and a fill	0 (1) 0 A	-
1440					0	н т
ALTERNATION AND AND ALTERNATION AND ALTERNATION OF A		PER Dashed Recoverie where D have	President Cost in success	-		
	to the test of the	U.See Oales Victor conclusion	anglotan.			
					Andrews 's 'n Allert at an 1514 official for	
Alterative Annalises and the Original						
All IN A VIEW AND ADDRESS OF COMMENT	en traiscon W	ten bastis because they have b	Surface + destrugetores	And opposites and the owner was	Anderson's Artifician and and an analysis	
All Program and All Anno Anno Anno Anno Anno Anno Anno	en transcon M regional de Canacita de M regional de Canacita de Ca	ten bastis because they have b				-
All PATER AND ADDRESS AND ADDRESS ADDR	ni Galera V ni Galera V ni Galera V ni Galera V	1999 Dealthd Decements (City) Travel M 1999 Dealthd Decements (City) Travel M	10: 1000 1 dentropetere) 10: 1000 projector 1000 10: 10: 10: 10: 10: 10: 10: 10: 10: 10:		Anderson's Artifician and and an analysis	1

- 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.

7.2 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.

7.3 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.

7.4 Option to Record Only During Violation

Screen: Edit settings						
NO RECORD ONLY WHEN BEHAVIOR RULE WAS VIOLATED						
UPDATE SCREEN ON EVENTS ONLY						
RECORD VIDEO	YES					
RECORD VIDEO						

- 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.

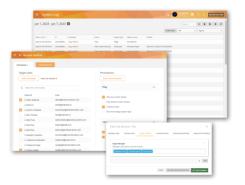
8 Role-Based Access Control (RBAC)

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.

8.1 Standardized Account Roles and Profiles

POR	sisterini for source	• Administra	distance in	- 1 - 1 - 1 - 1	• •	1000 Q			• 0	8				
	una l	1112401-012	service for early		rankes from	configuration of the second se		1000	t Tryn		1000	387975757	d m.	
* Mar.	CONFRONTING BUT LIGHT		2021-00-23 14:34:23	14.1	R16008P0	212146-0314.0	109	10.0	n KORP I		Luke	1.10	194	
e 2016).	antigrepresies										1000	10	- 20	
- AP1	And the growing way to be a set of		2014/01/12/12/2018		Ldit info La	ng Shen								
< derta	benflaraminslag													
- aut.	whether and taken interfaces	54th	2022/06/21 22:11:09	21	resources in to			40.0	incense		Hece/TOE	NEOTTON		1906-01179-2006
- #33.7.	heir digte small dens ner.	108	301312-20100031			1000-1100								
	hatrisigen Low					100217101	1.1							
· Own	low/indfamini-densers		2014521145515											
- CAN	utionatioumou					1000010-002		i pliver.						
< CO.	regispronic transm		20010-0122-0124						above.					
 CLBQ. 	Dashboard session				C Also set times	failed.						*****		
- Dette	S CONTRACTOR OF CONTRACTOR				E instances and						و له الم ا			
					Britanian berter	Name of Decision of						ei sa ang	1992 14.4	
	2 Carpo Presson	socies to reside anti-	Internet and the second second		0									
- Gen .						17 - Party Table								
· 0419.														-
		COOR LINE 1	1.0											
		VICTOR OF THE PARTY	Provide at a state	-									0.050	
				۰.	_	_	-	-	-	-	-	-	-	
		IT P THEY IF ?												
		CONTRACTOR OF T	te:											

8.2 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.

9 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.

9.1 SIEM / Threat Analytics Solutions



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

9.2 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.

9.3 Active Directory

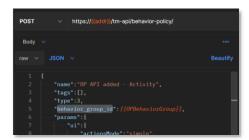


- Built-in integration with Active Directory over LDAP.
- Import users, computers, groups/OUs, attributes.
- Filter reports with attributes and groups.
- Apply rules to OU's and/or groups.
- Remote install using Group Policy (GPO).
- Use Teramind only on a specific group.
- Use your own custom AD sync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

9.4 Single Sign On (SSO)



9.5 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.

10 Deployment

10.1 Supported Platforms



10.2 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.

10.3 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