

Features Guide

Version 1.6 (27 NOV 2023)



Table of Contents

1	Teran	nind Starter Features Overview	3
2	Featu	res Comparison	4
3	Monit	oring and Detection Capabilities	5
	3.1	Applications & Websites	5
	3.2	Browser Plugins	7
	3.3	Instant Messaging	8
	3.4	Social Media	9
	3.5	Searches	11
	3.6	Registry	12
	3.7	OS State	13
	3.8	Remote Control	13
	3.9	Activity Blocking	13
4	User E	Behavior Analytics	14
	4.1	Insider Threat Detection	14
	4.2	Abusive Behavior	14
	4.3	Malicious Behavior	15
5	Work	force Productivity	16
	5.1	Productivity Analysis & Reporting	16
	5.2	Time Tracking	16
	5.3	Template-Based Scheduling	17
	5.4	Workflow Automation	17
6	Policy	and Rules Management	18
	6.1	Policy Manager	18
	6.2	Visual Rule Editor	18
	6.3	Out-of-the-Box Rule Templates	19
7	Role-B	Based Access Control (RBAC)	20
	7.1	Standardized Account Roles and Profiles	20
	7.2	Access Control Dashboard	20
8	Third-	Party Integrations	21
	8.1	SIEM / Threat Analytics Solutions	21
	8.2	Project Management & Ticketing Solutions	21
	8.3	Active Directory	21
	8.4	Single Sign On (SSO)	21
9	Deplo	yment	22
	9.1	Supported Platforms	22
	9.2	Hosting Options	22
	9.3	Support	22

1 Teramind Starter Features Overview

Teramind Starter is Teramind's entry-level employee monitoring solution. It is built on top of Teramind's award-winning UAM and DLP platform and includes powerful features such as real-time activity tracking, video capture, and playback, and a set of productivity optimization tools. While it packs a punch in terms of functionality, it is designed to be super affordable for budget-sensitive start-ups and small businesses looking for entry-level employee monitoring, user session recording, and process optimization capabilities.

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 apps 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, Profession Services, Customizations
User Activity Monitoring				
Web pages & applications	\checkmark	√	√	√
OCR		√	√	\checkmark
Remote control	\checkmark	√	√	\checkmark
Email		√	√	\checkmark
Console commands		√	1	√
File transfers		1	1	1
Network		1	1	1
Instant messaging	\checkmark	√	√	1
Social media activity	1	√	1	1
Online meetings	•	√	1	1
Geolocation		√	√ √	√
			√ √	√
Camera usage		1		
Keystrokes		√	1	1
Clipboard (copy and paste)			1	1
Searches	\checkmark	√	\checkmark	\checkmark
Printing		√	\checkmark	\checkmark
Browser plugins	\checkmark	\checkmark	\checkmark	√
Registry	\checkmark	\checkmark	\checkmark	√
OS state	\checkmark	√	√	\checkmark
Custom website field capture				1
Custom app field capture				√
Data Loss Prevention				•
Data discovery & classifications			√	√
Define content-based rules			1	1
Define file operation-based rules			√ √	√
-			· · · · · · · · · · · · · · · · · · ·	
Prevent malicious or negligent data exfiltration			V	1
Document and data fingerprinting			1	1
Regulatory compliance including HIPAA, GDPR, etc.			√	√
User Behavior Analytics		-		
nsider threat detection	\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	√	1	√
Template based scheduling	1	1	1	1
nteractive productivity reporting	1	√	1	1
Policy and Rules Management			•	•
Policy manager	√	√	1	√
/isual rule editor			↓ ↓	√ √
	V	√ /		
Regular expression support		1	1	1
Dut-of-the box rule templates		√	√	√
Activity blocking + 7 other rule actions	Limited	\checkmark	√	√
Audit & Forensics				
/ideo recording of all user activity	\checkmark	\checkmark	\checkmark	\checkmark
Audio recording	\checkmark	√	\checkmark	√
OCR of screen content, OCR search, OCR rules		\checkmark	\checkmark	√
Option to record only during violation		√	\checkmark	√
ull text search of activities and meta-data		√	√	\checkmark
Professional Services				
Tailored deployment assistance				√
Custom reporting configuration				√
Custom behavior rules configuration				√
Custom third-party integrations				√
wailability in AWS GovCloud				√
Availability in Azure Government				1
Interprise SLA				√
On-Premise and Private Cloud Deployment		-		-
nstallation assistance	\checkmark	\checkmark	\checkmark	\checkmark
24x7 follow-the-sun support	\checkmark	√	\checkmark	\checkmark
Subscription includes software updates	\checkmark	√	\checkmark	√
Norry-Free Cloud Hosting				
No servers needed	√	√	√	√
Ve set up and host for you	1	1	1	1
Secure, Tier 3 data center	J			√
	•	1	1	1

3 Monitoring and Detection Capabilities

Teramind Starter monitors user activity for the essential system objects like Applications, Website, Social Media, Instant Messengers, etc. in real-time, for Windows, Mac, Virtual PCs, and Terminal Servers. You can track as much or as little as you want based on your organization's needs and alleviate any privacy concerns.

Ľ /	

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.

You can create behavioral rules based on the user activities and work schedules and receive real-time alerts and notifications when any rule is violated. Additionally, you can prevent malicious or accidental threats with pre-emptive actions such as warning a user or blocking an action.



Teramind Starter has limited activity monitoring and rule creation capabilities. Upgrade to Teramind UAM or Teramind DLP for full activity monitoring and powerful rules support.

3.1 Applications & Websites

What report can I access for this activity?



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

etc. and LDAP groups/attributes (if integrated with Active Directory).

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

MONITOR ONLY THESE	APPLICATIONS	
Salesforce x SA		
	Websites: Edit settings ×	
USPEND MONITORI	MONITOR ONLY THESE WEBSITES	
facebook x me	Selesforce × SAP Logon 720 × Sege 50 Portal ×	
USPEND KEYSTROK	DON'T MONITOR WEB TRAFFIC FOR THESE WEBSITES	
	teramind.co 🗙 mail.google.com 🗴	
USPEND MONITORI	G	Þ
Skype x Firefor	SUSPEND MONITORING WHEN THESE WEBSITES ARE VISITED	
	gmail.com x mail.google.com x outlook.live.com x	>
	SUSPEND MONITORING WHEN WEBSITE CONTENT CONTAINS	
USPEND KEYSTROKI	Text list - URL X	>
	DON'T MONITOR WEB TRAFFIC FOR THESE IPS	
	Network list - Safe sites X	>
DLE TIME THRESHOL	SUSPEND MONITORING WHEN BROWSING TO THESE IPS	
10	G	>
	SUSPEND MONITORING WHEN BROWSING TO IPS NOT IN LIST	
	Network list - Bladdisted IPs x	
	0	3
	SUSPEND KEYSTROKE MONITORING WHEN THESE WEBSITES ARE VISITED	
	accounts.google.com χ login.live.com χ login.yahou.com χ login.skype.com χ	

What monitoring & tracking controls do I have?

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

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

Webpages	- 1
Condition 1	×
Webpage Url	- 1
CONDITION	
Contains facebook.com x Contains instagram.com x Contains twitter.com x Contains youtube.com x Contains pinterest x Contains tumblr x	?
EXCEPT	
Contains facebook.com/business × Contains youtube.com/channel/UCSBRq9qTqFJyygQdovb014g/ ×	0
Condition 2	×
Webpage Title 💿	- 1
CONDITION	
Equals list Shopping Sites 🗙	0
EXCEPT	
Contains staples.com X	3
) ADD CONDITION	- 1

- On Teramind Starter, you can create Activitybased 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).
- For the Browser Plugin, you can use the Plugin Name, Browser (i.e. IE, Firefox), Plugin Permission (i.e. Proxy VPN, Requests, User Data) as inputs for the rule conditions.

 You can use all the available rule Actions, such as: Warn, Block, Notify, Lock Out User, Record Video, Execute Windows Command, etc., and additionally a Redirect action for webpages.

What are some sample rules using this feature?



- Restrict access to non-whitelisted/unauthorized applications or websites but allow managers to override if needed.
- Detect and block when a dangerous application (e.g. Windows Registry Editor) is launched.
- Warn users when spending excessive time on social media or entertainment sites such as YouTube.
- Find out potential turnover by checking if employees are searching on job sites. Get notified if the time spent on such sites exceeds a threshold.

What are some useful resources for this feature?

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

3.2 Browser Plugins

What report can I access for this activity?

No dedicated report

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

What monitoring & tracking controls do I have?

No settings

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

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

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

What are some sample rules using this feature?



- On Teramind DLP, you can create Activity-based rules for the Browser Plugins.
- You can detect specific browser name (e.g. Chrome), plugin name, and plugin permission (i.e. Proxy VPN, Requests, User Data) as inputs for the rule conditions.
- You can use Warn, Block, Notify actions.
- Restrict use of certain browsers, e.g. old version of Internet Explorer.
- Block dangerous browser plugins and extensions to reduce the risk of malware infection or prevent a plugin from utilizing certain permissions such as the ability to access critical proxy settings or user data.

What are some useful resources for this feature?

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

3.3 Instant Messaging

What report can I access for this activity?



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

What monitoring & tracking controls do I have?



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

Condition 1	
Messaging App [×] Contact name [×] Message Body [×] ⊕	
ONDITION	
Facebook 🗙 Microsoft Teams 🗙	0
XCEPT	
Microsoft Teams Web 🗙	0

What are some sample rules using this feature?

****	Padicy Policy
	negory
1	ctivity
۵. ۱	980
1	pply to Everyone
P I	
	Message Body match regexp /*(contact)call the) (appropriate)? (authorities (authority).*/ or match regexp /*(formally)(formal)(complain);*/ or match regexp /*(i) we) will take you to court.*/ or match regexp /*(i) we) will tak
01	
	Notify shunter@teramind-demo.com
łu	e IM contact restriction Summary
Derr	Peliky Policy Category
Derr	JRANG HALY Cotegory Authly
Derr	Alfang Nalay Category Activity Ubers
Derr	JRANG HALY Cotegory Authly
Derr B	Alfang Nalay Category Activity Ubers
Derr B	Anlang Yang Catagory Atability Soers George Catagory of Designed
Derr B	Alley holo Catagory Activity Open Apply to Engone M
Derr B	Anlang Noto, Catagory Activity Users Ma Ma Managar Direction is soutgoing
Den E	Anlay holoy Catagory Activity Joans Apply to Expression Monsager Lapp Anlay Expression Teams or Microsoft Teams Web

What are some useful resources for this feature?

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

3.4 Social Media

What report can I access for this activity?

						and a state of the
, 2021 - Jan 9, 1	1021 🗃					LANSING SALENDS C.ONS 1
0 +						
		A.A. Delation			a labora	
		Ada Distance	_	_		
-		 And Andrew Andre		<u>.</u>	thus	
					Insp	
0.00101010101		1000	Departure .	Aut	his not offer one has a then rester	bhafeanam Sie
		1000	limete .	24	from peer constructs for a	
C-0130/14/001		Peer, scient work	Textures .	7.0	Terrer dream for ancient by which he	
C-M MILLARD			Texture .	2.4	Webling it lates for and unit	
C 10 10 10 10 10 10		10.10.10.00	lume .	ing.	Description of the local data in the	utilization had
0.0616100-0000		surface set the	furner .	Aut	The same one difficulty user pr	apa.
100100-001		whitehas has effect attaining	factors	714	Sectodor to in the start sector.	N allannett.
C-010108-0101		many product worth they precise	Restore	Aut	An our to Parallel a solution of	ten bes sheet (11)
		type about a starty term about en-	feedees	764	Type elastic renauctions.	to the terms of selation. It is to make the experiment of data to dary a
0.01000000000		hadres noting socals may income such.	former .	Post.	The such as a surface up the	Periah Reserved integral terms for an integral to be
					THE ABUTY OF A GROUP OF MORE	
0-08-00289-0908						
		phone happens had place have had	press.	includ.	The first to be private teachers	when yourself in you and in the processing of the second
			pression.	anna Au		the purch is a series of the purch in property during any series
0-10-0009-010 0-10-0404-010 0-10-0404-010 0-10-0404-010		phrase features feats place dense, feats -			No. And Tyle provide tagginess	the purch is a series of the purch in property during any series
0-0 0004-000 0-0 0444-000 0-0 04774-000 0-0 04774-000 0-0 04674-000		priese fagnes has per dens here,	preds.	Ref	No. 1.1 (21) preside happings Kinkerplan premy and your hand	etha pusht futu antifatty in tocards during an accord etha pusht
C - N COM-ON C - N SAC4-CM C - N SC - CA		private happing has plot dense has a private happing task start, there raising had had cande	Longs.	Rol Rol	No. 1.1 (21) preside happings Kinkerplan premy and your hand	while purched if your and it happy in programs, channes are you winn while provide instrump forgether to hard you for the hand the sime to caracter you and t with the at white yourself in your way of thereing
		privates fragment many prior division many, in privates fragments tasks arrange, literal metrogickult frant sämler - manies, rappy Electronicy	Danda Sellar Rankasi	Red Tel: Tel: Red	The field type private trajectory Kilden can avery ord part hand May 2016 a method to make a trajec May 2016 a method to make a trajec	while purched if your and it happy in programs, channes are you winn while provide instrump forgether to hard you for the hand the sime to caracter you and t with the at white yourself in your way of thereing

- 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.
- On Teramind Starter, you can create Activitybased rules for Instant Messaging.
- You can use the Message Body, Message Direction, Messaging Application, and Contact Name as inputs for the rule conditions.
- You can use the Warn, Block, and Notify actions.
- Restrict messages to/from select contacts.
- Detect if a user is in contact with suspicious people or criminal groups.
- Monitor support chat conversations to improve the quality of customer service and SLA.
- Get notified if the chat body contains specific keywords or sensitive phrases such as lawsuit threats, angry sentiments, sexual harassment, etc.

- 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.
- Social media: Edit settings × TRACK THESE APPLICATIONS

 Facebook x Twitter x Lankedin x

 TSS TRACK NEW COMMENT

 TSS TRACK NEW POST
 TSS TRACK LEDIT FOST

What monitoring & tracking controls do I have?

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

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

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

ondition 1					
Webpage Url	Total Tim	ie Active (min)	€ ⊙		
ONDITION					
Contains facebook.co	om 🗙 C	ontains instagram	.com 🗙	Contains twitter.com χ	
Contains youtube.co	m 🗙 Ca	ntains pinterest	K Conta	ains tumblr 🗙	?
KCEPT					
Start typing					?

What are some sample rules using this feature?

Rule E:	xcessive usage of social media Summary Policy
Cate	gory
Acth	dty
🕼 User	5
Appl	ly to Everyone
Web	pages
§ nte	sbpage Url contains facebook.com or contains instagram.com or contains twitter.com or contains youtube.com or contains pl terest or contains tumbir I Time Active minit > 15
😪 Actio	
	ow warning with message Please keep your social media usage to a minimum while at work
Sh	
Rule E	Block Facebook Comments Summary
Rule E	Bock Facebook Comments Summary Jakey eeyy
Rule E Etiquette	Policy
Rule E Etiquette Cat Act	Pelay esory Way
Rule E Etiquette Act App	Pelay esory Way
Rule E Etiquette Act App	- Shany
Rule E Etiquetto Act Act Exc Q We	- Shany
Rule E Etiquette Act App Exc Q Wel	Jamiy
Rule E Etiquette Act App Exc Q Wel	shany 980y Wity 5) to Exervise Marketing Organi Foregage This contains soft-composer respage This contains facebook or contains facebook

What are some useful resources for this feature?

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

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. 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.

3.5 Searches

What report can I access for this activity?

0.2021 - Jan 1	anos #1						
2021-3011	5, 2021						210100 0000 000
+							
alas -		• • 100	where .		0.8 Teller	# # Subject	
			Terre Annual Annual Const Annual Const Annua				Ow1
			-				
21-01-13 28-06 80-0148			poptore	property previation			i i
96-15 D B B B 6-15-15			popton	Missi providen			
0101010000000			Emprove.	and were			
100-010010-010			pophore	sheta			
21-21-13 telefore-child			peptor	yesher			
Industry in additional			pophore	view			
BORD 010			poptore	100			
Increase in the second			tepos	price and eighty			
			pageare	8679			
21010310060-010			pepase	-			
INCOMENDATION CONTRACTOR			bisport.	padde			
01-01-10 10:0001 40:00			pepeox	reat			
			popula	yearder			
			pegnam	stay			
			popular	indeed			
0-0-11 10040-048 0-0-11 10040-048				cana			
01011110000000							
0.0.1110044-048			presson	inate.			
0-0-111004-040 0-0-111004-040 0-0-111004-040							0

- 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.
- Search for activities or filter the report by the employee, department, computer, etc.
- Print or export the reports as PDF/CSV files.
- Schedule regular report delivery to email addresses.
- View video records of the activities by date/time.
- Add real-time widgets on the BI reports.

What monitoring & tracking controls do I have?



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

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

•

for.

Condition 1	
Webpage Url [×] Webpage Title [×] ⊕	
CONDITION	
Match list Keywords 🗙	3
XCEPT	
	(?)

What are some sample rules using this feature?

- Rule Detect google search Summary

 Demo Pality Policy

 Category

 Activity

 Users

 Apply to Everyone

 Webpages

 Webpage UII match list Keywords

 Webpage Title contains Google Search

 Actions

 Redirect to searchpolicy.teramind.co
- Use the Websites rules to detect when an

You cannot create any Search-based rules

directly. However, in Teramind Starter, 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

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

What are some useful resources for this feature?

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

3.6 Registry

What report can I access for this activity?



What monitoring & tracking controls do I have?

Registry: Edit settings								
RACKI	NG DAYS	AND T	IME					

- 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.

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

General User Registry Actions Overges saved	Registry Condition 1 Kay Natace ^X Value ^X Program ^X Concross Foreseast large long transformed and the X	© (1)	Rule Registry changes Summary Sengeh Rais Rais Park Activity Sumary Rais Rais Apply to IT Registry Program Contains regardit
	Start tiping	Ø	Key contains Noey_local_machine\ Name equals Starts Value equals 3
	⊙ ADD CONDITION		Actions Notify ben@teramind.co

What are some sample rules using this feature?

	e Registry changes Summary ple Rules ^p olicy	
Ē	Category	
	Activity	
2	Users	
	Apply to IT	
R	Registry	
	Program contains regedit	
	Key contains hkey_local_machine\	
ar	Name equals Starts	
	Value equals 3	
8	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.

What are some useful resources for this feature?

- User Guide: <u>Monitoring Settings > Registry Settings</u>
- Rules Guide: <u>Activity Rules > Registry</u>

3.7 OS State

What report can I access for this activity?

elect action								Licenses I	n use: 53 / 5	100
Lock	15 Not deleted		-	ters Employee	Denn	riments •				0
Unlock Delete							۹			
Restore		Depart	ment	Last login time		Last login from	Status	Monitore	27A	
Enable Monitoria Disable Monitori				2020-08-05 16	15:39	WIN-035KHOREPEI	Locked	No	No	
Bulk edit	dteramind-demo.com	Arick1		Online		win-035khor8ter	Active	Yes	No	
8en Th., ben	Oteramind.co	my de	partment				Active	No	No	
Bob Pine bob	rick@teramind-demo.com	Staff		2022-01-04 15	24:13	WIN-035KHORSPER	Active	765	No	
Brayde. bon	wford@teramind-demo.com	arick-b	1982	2022-08-27 23	100:17	win-035khorðter	Active	Yes	No	
Cather cath	erine@teramind.co						Active	Yes	No	
Chadw csin	gh@teramind-demo.com	Sales		Online		win-035khor@ter	Active	Yes	No	
Cheryl cgu	len@teramind-demo.com	Staff		Online		wn-o35khor8ter	Active	1965	NO	

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

What monitoring & tracking controls do I have?

OS State: Edit settings	×
YES SLEEP	
SCREENSAVER	

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

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

Seneral Jser	Registry		Rule Registry changes Summary Sample Bales Policy
egistry ctions	Condition 1 Key Name [×] Value [×] Program [×]		Category Activity
Changes saved	Constitution Marg, book, machinet, 1X	•	Apply to IT Registry Program contains regedit
	Start tiping	Ø	Key contains hkey_local_machine\ Name equals Starts Value equals 3
	ADD CONDITION		Actions Notify ben@teramind.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).

What are some useful resources for this feature?

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

3.8 Remote Control

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

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

3.9 Activity Blocking

Teramind Starter only supports the Warn, Block, Notify actions and a Redirect action for webpages. For other Actions (Lock Out User, Record Video, Execute Command, etc.), you will need to upgrade to Teramind UAM or Teramind DLP.

4 User Behavior Analytics

Teramind Starter comes with the essential User & Entity Behavior Analytics (UEBA) features to identify and alert you about 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 and regression analysis helps you detect common threats over applications and websites. Additionally, Teramind Starter also comes with workforce optimization and scheduling tools, using which you can measure employee productivity. Use automated rules to enforce company policy and decrease unproductive behavior. Track project costs and eliminate waste for not just regular employees but external consultants, remote employees, and freelance contractors.

Teramind Starter has limited user behavior analytics capabilities. Upgrade to Teramind UAM or Teramind DLP for full UEBA, insider threat detection, and data loss prevention features.

4.1 Insider Threat Detection

i

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

- Establish organization-wide visibility and control for several objects: screen, apps, websites, IMs, and social media.
- 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.
- 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.

What are some useful resources for this feature?

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

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

- 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.
- Using applications or sites that are unproductive or unauthorized.
- Not following corporate etiquette policy, for example, visiting gambling sites.
- Using browser's incognito/private mode.

• Contractor submitting invoices that do not match work hours or task completion status.

4.3 Malicious Behavior

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

- Running network snooper, registry editor, or other dangerous applications.
- Communicating with competitors.
- Sudden change in schedules or work patterns.

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



5.4 Workflow Automation

	Imple Mode	Advanced Mode	Rule Accounting/Auditing task Summary Productive Teaks Policy						
dors Select (ion the system should r	nact to violations	Category Activity						
NOTIFI			Apply to Everyone Apply to Everyone Applications						
BLOCK		(143)	Application Name contains excel.exe						
LOCK	4/7 USER	() N2)	Switch user's task to Administrative						
WARN		<u>()</u> 82							
	IR'S ACTIVE TASK	en 's sant au a cannor volue.							
	inistrative •	and the second second second							

- 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.
- 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 warning when an employee spends too much time on unproductive apps/websites.

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.

Teramind Starter has some limitations in terms of what types of rules you can create. For example, you cannot create any rules for objects like Emails, Files, Networks, etc. Or, use rule Actions such as, Lock Out, Auto Task Assignment, Command Executions, etc. You cannot use features such as Shared List, OCR, or Content-sharing either.

Upgrade to Teramind UAM or Teramind DLP for advanced policy and rules management features.

6.1 Policy Manager

i

E ← Behavior Policies		C De Advainistra	STATT
folicies			Search for rules Q
POLICIES	# RULES TAGS	AUDIENCE	ACTIONS
◎ CREATE NEW POLICY			
GDPR Compliance	20 rules	Everyone	(Jan) I
Demo Policy	13 rules	Everyone	.
Productive Tasks	7 rules	Everyone	
Agent User Experience Demo	4 rules	Everyone	••• •
PCI-DSS Compliance	10 rules		
HIPAA Compliance	13 rules	Everyone	
Sensitive Data	Andes	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 Starter comes with a sample policy with some rules for you to experiment with.

6.2 Visual Rule Editor



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

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

6.3 Out-of-the-Box Rule Templates

		Contraction of the		-		
ample Rules	26 rules	Everyone	-	1		
PI: Social Security Number + Name Detect likeling of SSI & Memory is email, M, copy / piece, and the upload / write / copy to forsider deconations	Category: Content sharing	۵	(arr)	01	ы.	
Upload file outside of domain User uploads a file via the browser to a best outside of our domain	Category: Activity	٥	Œ	0!		
Email contains offensive content. Daw service and with otherwise or angry services	Category: Content sharing	٥	(arr)	0:		
Teamwiewer laurch attempt User tried to laurch samulouer	Calegory: Activity	0	(Jarr.)	0!		
RDP attempt to forbidden hosts user their to RDP ans a horizon a formation subset)	-	
Remote desktop access applications ther a running a program that gives people remain access to their desteaps	No complate, start with a clean slate Copy file from RDP to removable media					
System hosts file edited loor edited / updated the system them: file	IM contains	accusative sentimer	4			
Clipboard copy sensitive data & parte outside domain dee copet sensitive data no the trybuerd and parted to evelope substate of our remain	IN contains discouraged sentiment IN contains discadified sentiment IN contains leveluit threes					
Email or IM with accusative statements over set as M in extra with resolutive refitment		social harasserent unresponsive comp				
Email contains credit card content downloaded from sharepoint operant on enal with a COI that come than sharepoint in the body is attachment	Screenshot Printer Large print					
Email contains content downloaded from Sharepoint User set on envirousable of the domain with construction same hor nor sharepoint	Website Adult webs	tes				i
Email contains SSN User set on envil with a tocal security number in the body or attachment	Excessive u Gaming or	ne on job search we sage of social media pambling stes				
	Non-whitel	sted website access	d			8

- Teramind Starter 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.
- Pre-packaged sample rules ready for use.

Some of the sample rules require additional features that are not available on Teramind Starter. You will need Teramind UAM or Teramind DLP (for rules that use the *Content sharing* category) to use them.

7 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.

7.1 Standardized Account Roles and Profiles

	level .	anopener.	same of lag young	and on frage	Lordsmoore.					1 2010/10/00		
	L. OR PANING BOLLAN		2010/01/4940	ATTEXNED	212140-0518152		PEOPLE		LANK		-	
	 avign-press 								in		~	
	L AT BRIDE MARK			L dit info La	or Lines							
- Bert	C. bertievrinsis				0							
- 211	· when which is the or	bear .	2020/07/22112	 (FE0-44, N/O		40	encene.		IACK/OR	seamers		HOULDVP HOLE
	· her-digters and dense nee	108										
-	. suragescore				1012-110-0	79-05-0-19	9					
- 240	. inwandaminidensen		2014214555									
GAN	. ununalisamus				PERSONAL PROPERTY.	frative						
- 1006	. regiption in terration	Apr.	1000 (F177 75 Half)				d above in	-				
(18)	Dashboard session			C day set warm	factor of	Crakies			-			
Cam	L S			E instructions					+ 4+ 4.7			
				B thirth by the	tops of Decriment						AL3 PLA	
	 Outro constant 	CONTRACTOR OFFICE AND	1000 1000 00000									
Carro					or services	Terriet						0
- Carl												
		COOR DO THE 7									_	
		VICEASE TATE	Period and an address								OCK	V HPLICENEES

7.2 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.

8 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.

8.1 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.

8.2 Project Management & Ticketing Solutions



8.3 Active Directory



8.4 Single Sign On (SSO)



- 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.
- 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.
- 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.

9 Deployment

9.1 Supported Platforms

	CİTR IX [®]		vm ware [.]	Ú
Windows 8 & Up	Citrix XenApp [®] & XenDesk [®]	Windows Server 2012 & Up	VMware Horizon	macOS 10.14 & Up

9.2 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.

9.3 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