Teramind Starter

Features Guide

Version 1.6 (27 NOV 2023)

TERAMIND

Table of Contents

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

3   Monitoring and Detection Capabilities

Teramind 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.

🔒 **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.

ℹ️ 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?**
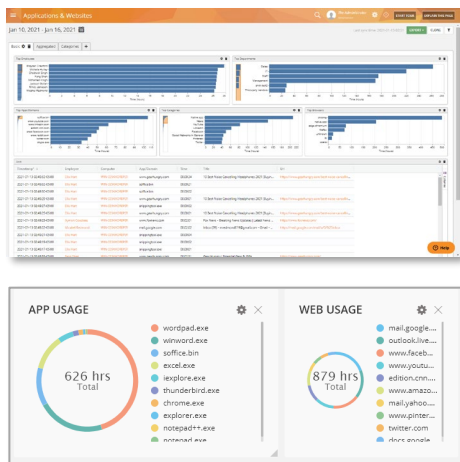
- You can view the timestamp, employee, computer, process/URL, usage duration, idle time, active time, app/webpage, title, etc.
- View top employees, departments, app/domain, categories, browsers, security categories, reputations, classification timeline (e.g. productive vs. unproductive), etc.
- Automatically 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.

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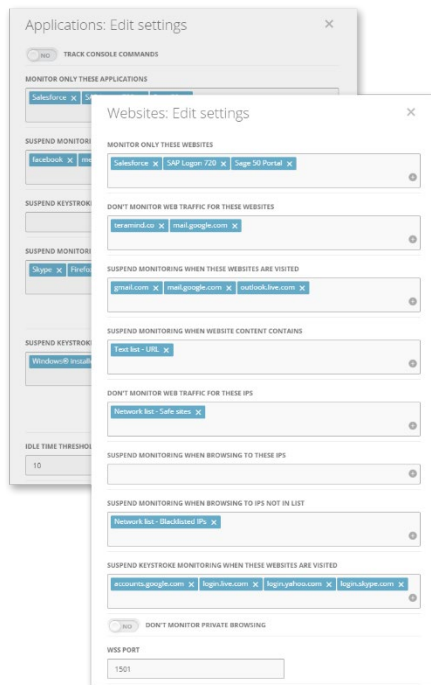
- Track all websites and applications and console commands. Or, you can configure the settings to monitor only select apps/websites.
- Monitor browser plugins and extensions.
- Suspend monitoring of keystrokes logging for certain applications/websites.
- Dynamically blackout screen recording when certain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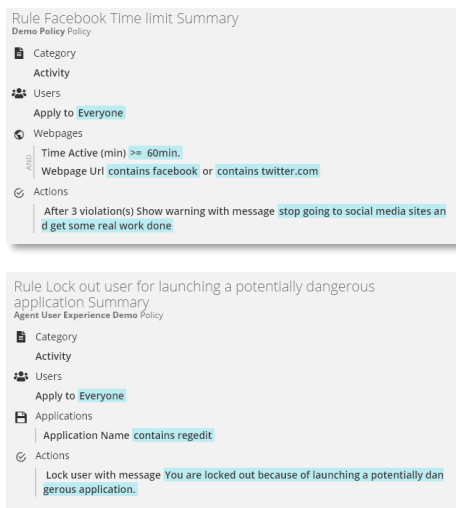- Control the tracking of application idle time.

What rule and alert triggers can I use with this activity?
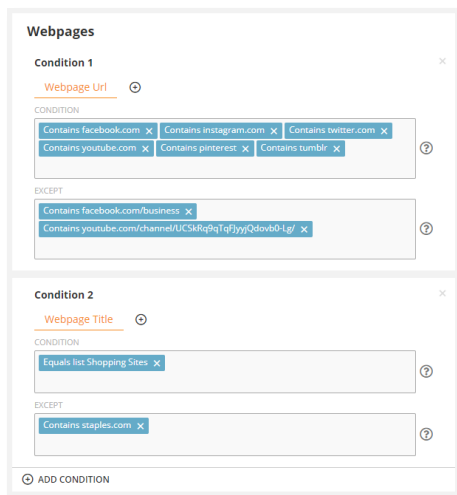
- On Teramind Starter, you can create Activity-based rules for the Websites and Browsers.
- For the Webpages, you can use the Webpage Title, URL, and Query Arguments (URL variables) as inputs for the rule conditions.
- For the Applications, you can use the Application Name, Application Caption, Time Active, Time Idle, Focus Time, etc., and detect if it's launched from a CLI (Command Line Interface).
- 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?

Rule Facebook Time limit Summary
Demo Policy Policy
📄 Category
   Activity
👥 Users
   Apply to Everyone
🌐 Webpages
   Time Active (min) >= 60min.
   Webpage Url contains facebook or contains twitter.com
⊗ Actions
   After 3 violation(s) Show warning with message stop going to social media sites and get some real work done

Rule Lock out user for launching a potentially dangerous application Summary
Agent User Experience Demo Policy
📄 Category
   Activity
👥 Users
   Apply to Everyone
📁 Applications
   Application Name contains regedit
⊗ Actions
   Lock user with message You are locked out because of launching a potentially dangerous application.

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

3.2   Browser Plugins
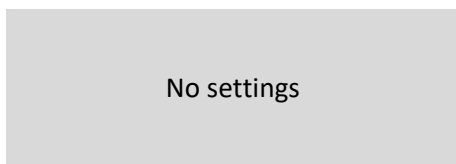
What report can I access for this activity?

No dedicated report
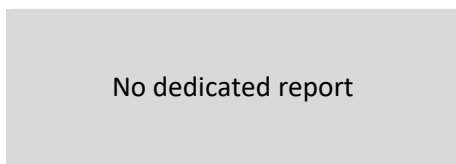
- Browser Plugins activities can be monitored under the Applications & Websites and other related BI reports (e.g. the Web File Events report shows details for all the uploads/downloads done through the browser).

### What monitoring & tracking controls do I have?

No settings

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

What rule and alert triggers can I use with this activity?
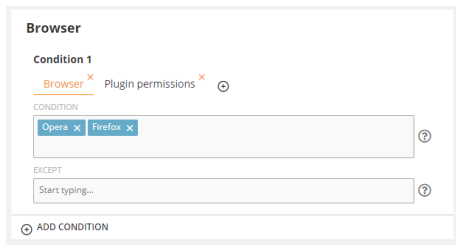
- On Teramind DLP, you can create Activity-based rules for the Browser Plugins.
- You can detect specific browser name (e.g. Chrome), plugin name, and plugin permission (i.e. Proxy VPN, Requests, User Data) as inputs for the rule conditions.
- You can use Warn, Block, Notify actions.

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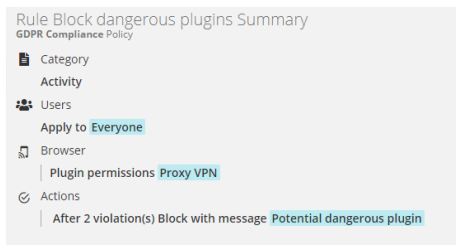
- Restrict use of certain browsers, e.g. old version of Internet Explorer.
- Block dangerous browser plugins and extensions to reduce the risk of malware infection or prevent a plugin from utilizing certain permissions such as the ability to access critical proxy settings or user data.

What are some useful resources for this feature?

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

3.3   Instant Messaging

What report can I access for this activity?

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

**What monitoring & tracking controls do I have?**
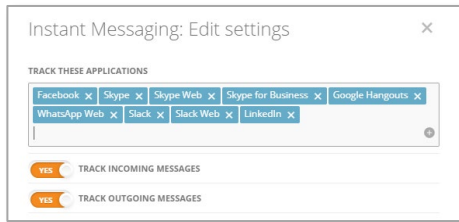
- You can select which messages to capture, incoming/outgoing, or both.
- You can specify which IM clients will be captured. Teramind supports popular clients, such as WhatsApp, Facebook Messenger, LinkedIn, Skype, Slack, Google Hangout, and Microsoft Team - both desktop and web versions.

What rule and alert triggers can I use with this activity?
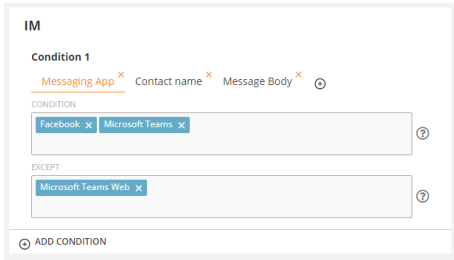
- On Teramind Starter, you can create Activity-based rules for Instant Messaging.
- You can use the Message Body, Message Direction, Messaging Application, and Contact Name as inputs for the rule conditions.
- You can use the Warn, Block, and Notify actions.

What are some sample rules using this feature?
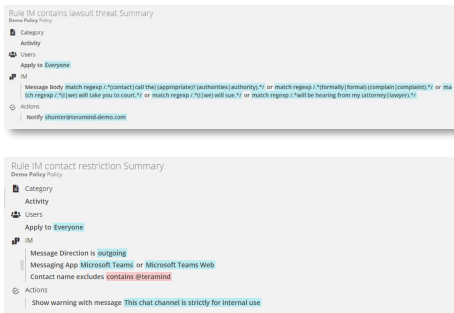
- Restrict messages to/from select contacts.
- Detect if a user is in contact with suspicious people or criminal groups.
- Monitor support chat conversations to improve the quality of customer service and SLA.
- Get notified if the chat body contains specific keywords or sensitive phrases such as lawsuit threats, angry sentiments, sexual harassment, etc.

What are some useful resources for this feature?

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

3.4 Social Media

What report can I access for this activity?
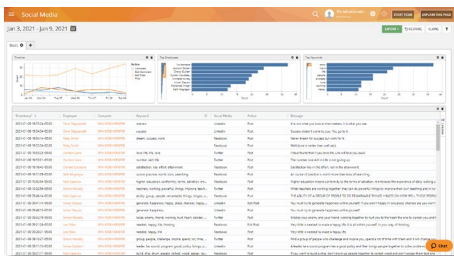
- View the source and action (post, comment, etc.) for the users' social media activities.
- View timeline (shows no. actions for a post, comment, edit post, etc.), top employees (by no. of social media activities), and top keywords, etc.
- See if any attachments are being shared.
- Aggregate or compare activities such as post vs. comments, Facebook vs. Twitter, etc.
- View the actual message.

- Filter the report by the employee, department, computer, platform, etc. and LDAP groups/attributes (if integrated with Active Directory).
- Print or export the reports as PDF/CSV files.
- Schedule regular report delivery to email addresses.
- View video records of the activities by date/time.
- Add real-time widgets on the BI reports.

What monitoring & tracking controls do I have?
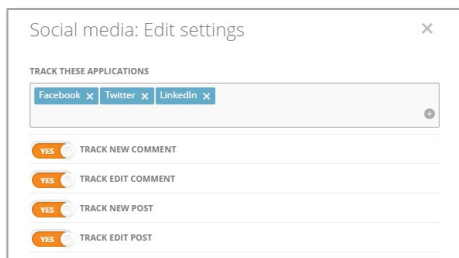
- You can specify which social media platforms to track. Teramind supports the most popular social media platforms, such as Facebook, Twitter, LinkedIn, etc.
- You can track New Comment, Edit Comment, New Post, and Edit Post activities in those applications.

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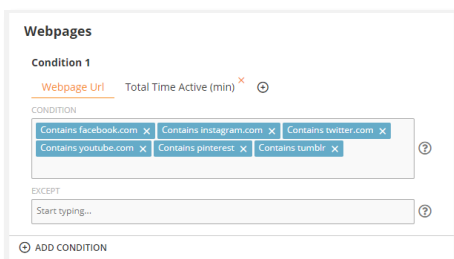
- Social Media does not have a dedicated rules category. However, you can create rules to monitoring social media sites using the Activity-based rules using the Webpages category. You can also create Content-based rules for social media. For example, using the Files category with a Content-based rule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

## What are some sample rules using this feature?
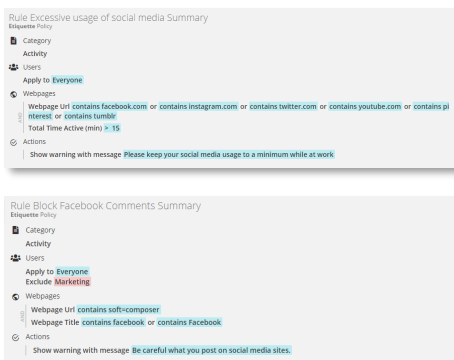
- Warn employees about excessive use of social media that might hamper productivity.
- Block posting of comments on certain social media sites such as Facebook but make an exception for the Marketing department.
- Monitor your corporate social channels. Get notified when any updates, posts, or comments are made on your social media accounts.
- Block uploading / downloading of files to/from social media sites.

What are some useful resources for this feature?

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

3.5   Searches

**What report can I access for this activity?**
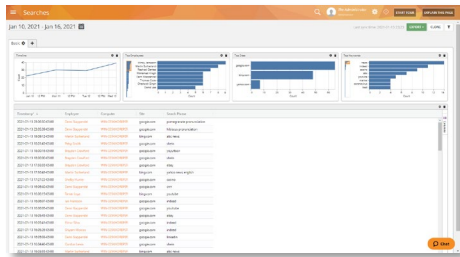
- View all the search phrases by timestamp, site, employee, department, computer, etc.
- Compare or group searches by timeline, top searches by employees, sites, keywords, etc.
- Search for activities or filter the report by the employee, department, computer, etc.
- Print or export the reports as PDF/CSV 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?**
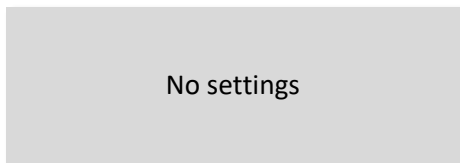
No settings

- 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 Applications & Websites for more information.

What rule and alert triggers can I use with this activity?
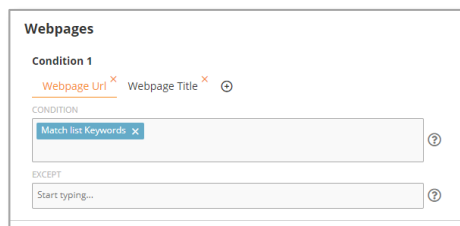
- You cannot create any Search-based rules directly. However, in Teramind Starter, you can create Activity-based rules and use the *Website URL* and *Website Title* conditions to detect a search engine and the term(s) a user is searching for.

**What are some sample rules using this feature?**
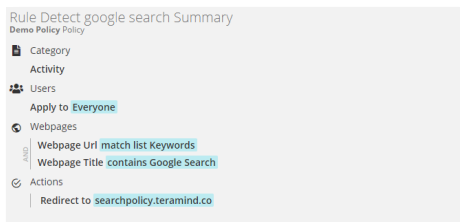
- Use the Websites rules to detect when an employee searches for certain keywords.
- Redirect to another URL when a certain search engine is detected. For example, redirect all searches from Bing to Google.

What are some useful resources for this feature?

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

3.6   Registry
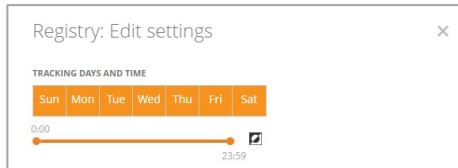
**What report can I access for this activity?**

No dedicated report
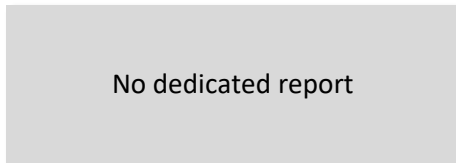
- Registry changes aren't tracked on a dedicated report but you can view rule violation incidents related to the registry on the Behavior Alerts report.

What monitoring & tracking controls do I have?

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

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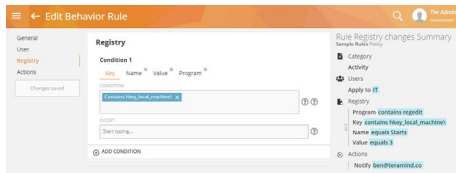
- You can detect changes to registry keys, names, values and programs.
- You can use the Notification, Block, Lock Out User, Warn, Set User's Active Task, Record Video and Command Actions with the Registry.

What are some sample rules using this feature?

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

What are some useful resources for this feature?

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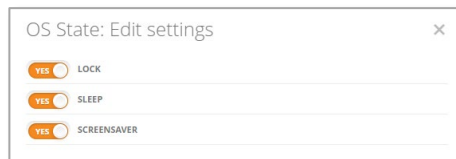- Rules Guide: Activity Rules > Registry

3.7   OS State

**What report can I access for this activity?**

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

What monitoring & tracking controls do I have?

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

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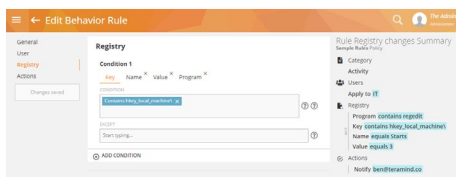
- You cannot use any rules directly with the OS State. However, you can monitor idle time with the Agent Schedule-based rules. You can also use the Lock Out action with some rules to lock out the user's computer (Windows only).

What are some useful resources for this feature?

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

3.8   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 Audit & Forensics 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.

> **i** 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

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: [Teramind: Insider Threat Prevention](#)

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
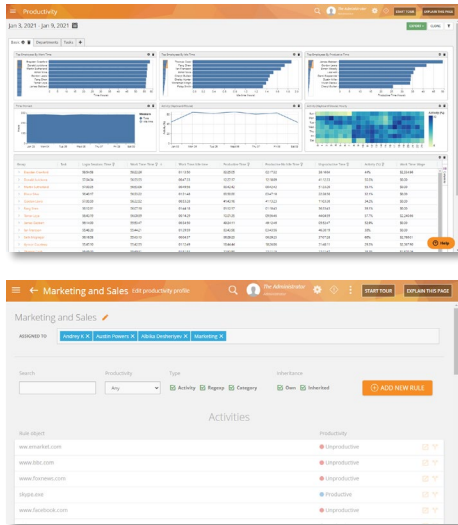
- Productivity reports allow you to track productive, unproductive, active, and idle time and performance KPIs for employees and departments.
- Classify apps/websites as productive, unproductive or into custom categories.
- Identify top employees by Work Time, Idle Time, Productive Time, Session Time, 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.

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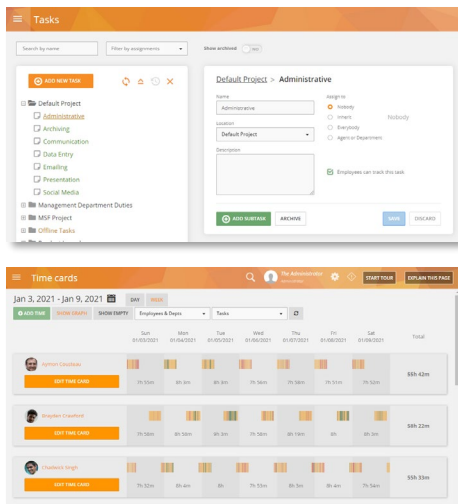
- Automatically assign tasks to employees and track time based on their activity or let them manage their clock-in.
- Comes with Time Tracker, Employee Cost, Task Cost, Time Records, and Time Card reports.
- Add missing time entries and notes such as PTO/time off, accruals, etc. for auditing and compliance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

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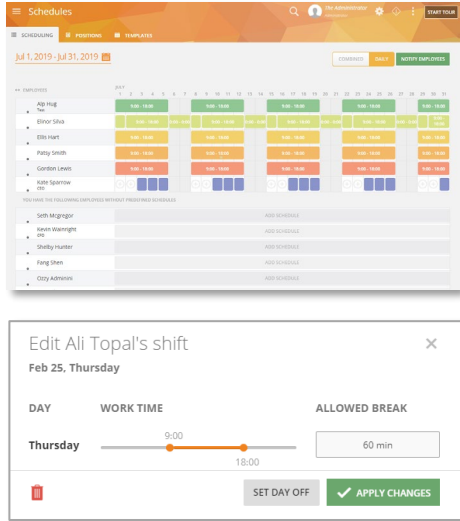
- Create daily and weekly schedules for your employees and contractors.
- Notify employees about their schedule changes automatically.
- Configure worktime, launch breaks, days off, etc.
- See who is late, stays overtime, or leaves early.
- Prevent users from using their computers or access certain apps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

5.4 Workflow Automation
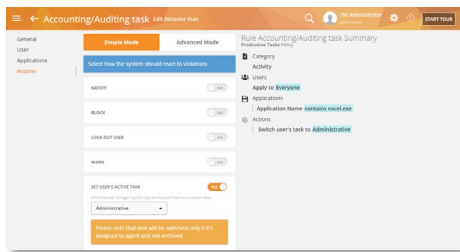
- Create productivity rules. For example, if an employee is idle for longer than a certain time, send them a warning automatically.
- Train new staff or provide job shadowing support using the Remote Control feature. Develop training materials, demo, tutorials, etc. using the Screen and Audio recording 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
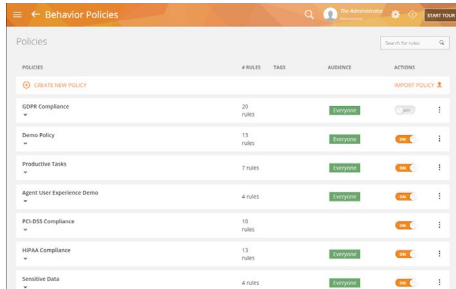
Policies help you organize similar rules together or apply a set of rules to some particular users. For example, you can have all your HR-specific rules such as 'Preventing email harassment', 'Limiting social media use' etc. under the 'Business Etiquette' policy.

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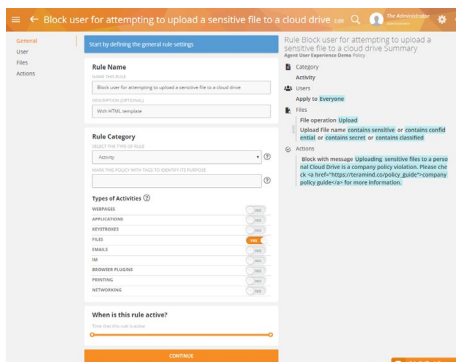
The Rules Editor is an intuitive, visual editor where you can create even complex rules easily without going through multiple screens or coding.

- 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
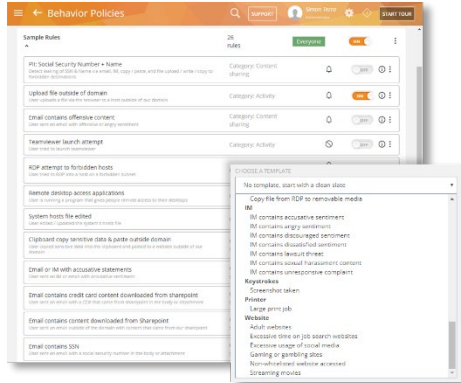
- Teramind Starter comes with hundreds of pre-defined policies and rules. For example, block email containing sensitive keywords, stop the uploading of a confidential document, detect screen capture, prevent the use of external drives, etc.
- Pre-packaged sample rules ready for use.

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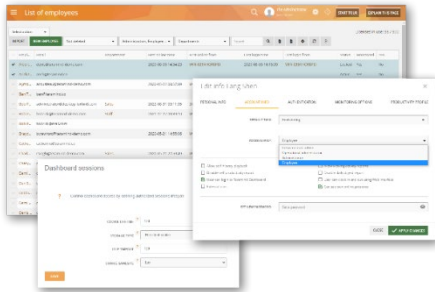
- Use built-in account types such as Admin, Ops Admin, Sys Admin, Employee, Department Managers, etc.
- Control monitoring settings, authentication and productivity profiles of users or groups.
- Enforce password policy, expiry and complexity requirements.
- Enforce session policy, time out, lifespan,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

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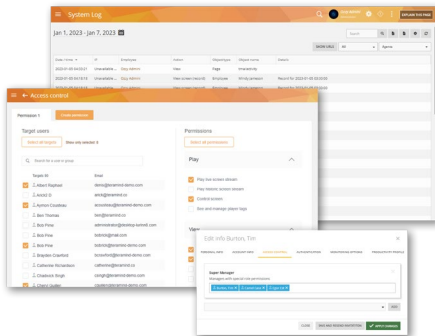
- Implement multi-layered identity authentication, authorization, and access control policies.
- Create access permissions, view and edit controls for privileged users.
- Apply special role permissions to department managers, supervisors, etc.
- Audit admin activities with immutable system logs.

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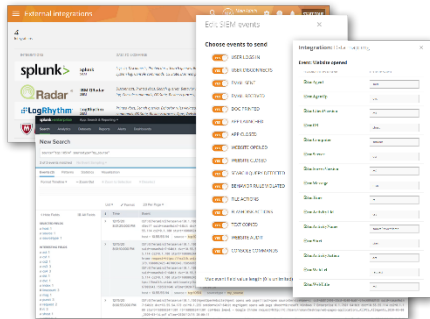
- Built-in integration support for Splunk, HP ArcSight, IBM QRadar, LogRhythm, etc.
- Send real-time event telemetry and meta-data.
- Common Event Format (CEF), Common Information Model (CIM) and JSON formats enable integration with virtually any solution in minutes.
- Customizable field mapping.
- Customized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

## 8.2 Project Management & Ticketing Solutions
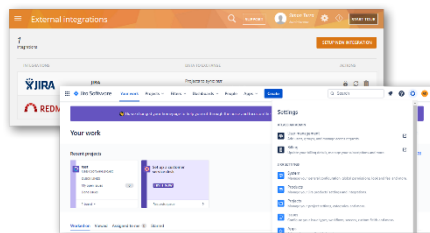
- Built-in integration support for JIRA, Redmine, Zendesk, etc.
- Sync projects, task statuses and test statuses.
- Import time tracking information directly to Teramind.
- Assign users, testers and supervisor roles.
- Customizable field mapping.

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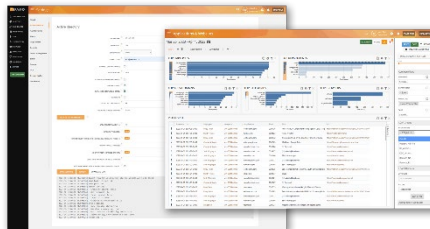
- Built-in integration with Active Directory over LDAP.
- Import users, computers, groups/OUs, attributes.
- Filter reports with attributes and groups.
- Apply rules to OU's and/or groups.
- Remote install using Group Policy (GPO).
- Use Teramind only on a specific group.
- Use your own custom AD sync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

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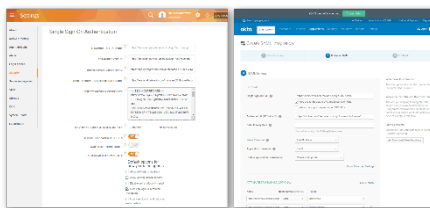
- Authenticate to the Teramind Dashboard using a Single Sign On (SSO) service such as Okta, One Login etc.
- Support for SAML 2.0 protocol, X.509 certificate.
- Auto register new agents and configure default options.

9 Deployment

9.1 Supported Platforms

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