

Insider risk management, employee monitoring and productivity optimization powered by user behavior analytics

Since 2014, over 10,000 organizations around the world have trusted Teramind to provide insider threat management, data loss prevention, and business process engineering through behavioral user data. By harnessing behavior analytics, our award-winning platform has helped enterprises in finance, retail, manufacturing, energy, technology, healthcare, and government optimize their workforce and protect their businesses.

## Privacy-First Monitoring

Teramind is dedicated to the privacy of our customers and their users.

The image displays two screenshots of the Teramind monitoring settings interface. The left screenshot shows the 'Monitoring settings' dashboard with a search bar and a table of monitoring profiles. The right screenshot shows the 'Websites: Edit settings' dialog box with various monitoring options.

MONITORING PROFILES	OPTIONS	WHO IS MONITORED	ACTIONS
California Employees	[Icons]	3 employees are monitored No groups are monitored	[Icons]
Default settings	[Icons]	52 employees are monitored No groups are monitored	[Icons]
Default with Keystrokes	[Icons]	No employees are monitored No groups are monitored	[Icons]

WHAT TO MONITOR	TRACKING TIME	SETTINGS
<input checked="" type="checkbox"/> SCREEN	<input checked="" type="radio"/> ALWAYS	Mode: color. Message during remote control (blank = no message): Remote control activated. Maximum frames per second: 1. Allow remote control. Live screen scaling: 100%. OCR languages: English. Delete history after (days): 5
<input checked="" type="checkbox"/> AUDIO	<input checked="" type="radio"/> ALWAYS	Bitrate: 16000. Automatic level adjustment
<input checked="" type="checkbox"/> APPLICATIONS	<input checked="" type="radio"/> ALWAYS	Track console commands. Idle time threshold (minutes): 10. Track window titles
<input checked="" type="checkbox"/> WEBSITES	<input checked="" type="radio"/> ALWAYS	wss port: 1501. Monitor keystrokes for password fields
<input checked="" type="checkbox"/> EMAILS	<input checked="" type="radio"/> ALWAYS	Capture incoming. Capture outgoing. Capture email content. Capture Outlook Meetings. Save outgoing attachments. Save incoming attachments. Ignore events older than (days): 0. Capture emails through: Desktop Outlook
<input checked="" type="checkbox"/> FILE TRANSFERS	<input checked="" type="radio"/> ALWAYS	Track network files. Track external drives. Track file sync with cloud services. Track operation "copy". Track operation "upload". TXT files. DOC(x) files. XLS(x) files. PPT files. ZIP files. PDF files. Track Network Documents. Track External Documents
<input checked="" type="checkbox"/> PRINTED DOCS	<input checked="" type="radio"/> ALWAYS	Maximum capture document size (pages): 50. Printer tracking account password: *****. Printer tracking account user: demo@teramind.co. Capture actual document
<input checked="" type="checkbox"/> KEYSTROKES	<input checked="" type="radio"/> ALWAYS	Track clipboard
<input checked="" type="checkbox"/> INSTANT MESSAGING	<input checked="" type="radio"/> ALWAYS	Track incoming messages. Track outgoing messages. Track these applications: Facebook, Skype Web, Skype, Google Hangouts, WhatsApp Web, Slack, Slack Web, LinkedIn, Microsoft Teams Web, Microsoft Teams, Skype for Business
<input checked="" type="checkbox"/> SOCIAL MEDIA	<input checked="" type="radio"/> ALWAYS	Track new comment. Track edit comment. Track new post. Track edit post. Track these applications: Facebook, Twitter, LinkedIn
<input checked="" type="checkbox"/> NETWORK	<input checked="" type="radio"/> ALWAYS	SSL. Track network connections
<input checked="" type="checkbox"/> OFFLINE RECORDING	<input checked="" type="radio"/> ALWAYS	Offline recording's buffer length (hrs): 24
<input checked="" type="checkbox"/> OS STATE	<input checked="" type="radio"/> ALWAYS	Lock. Sleep. Screensaver
<input checked="" type="checkbox"/> ONLINE MEETINGS	<input checked="" type="radio"/> ALWAYS	Track these applications: Zoom, RingCentral, AirCall, 8x8, Microsoft Teams, Webex, Bluejeans

**Websites: Edit settings**

MONITOR ONLY THESE WEBSITES  
Text list - List of unapproved websites

DON'T MONITOR WEB TRAFFIC FOR THESE WEBSITES  
Text list - Websites

SUSPEND MONITORING WHEN THESE WEBSITES ARE VISITED  
bankamerica.com x hsb.com x tdcandana.com x rbc.com x

SUSPEND MONITORING WHEN WEBSITE CONTENT CONTAINS  
password x private x personal x

DON'T MONITOR WEB TRAFFIC FOR THESE IPS

MONITOR WEB TRAFFIC ONLY FOR THESE IPS

SUSPEND MONITORING WHEN BROWSING TO THESE IPS

SUSPEND MONITORING WHEN BROWSING TO IPS NOT IN LIST

SUSPEND KEYSTROKE MONITORING WHEN THESE WEBSITES ARE VISITED  
accounts.google.com x login.live.com x login.yahoo.com x login.monster.com x login.skype.com x

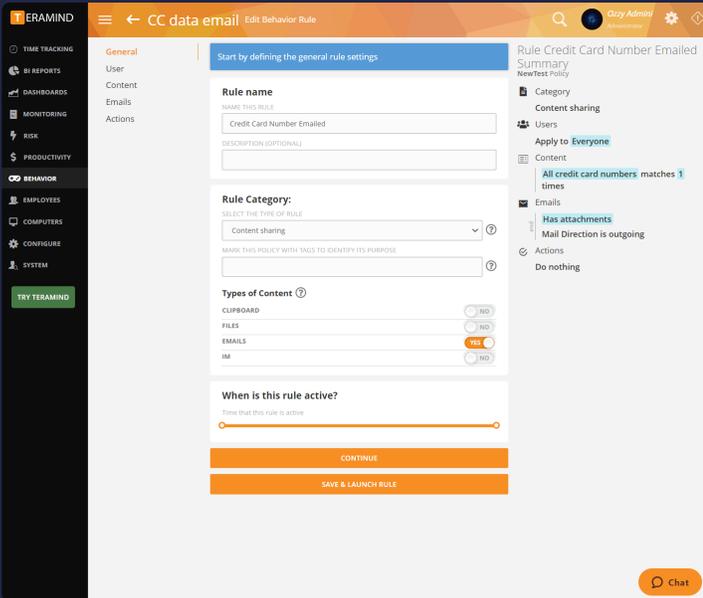
NO DON'T MONITOR PRIVATE BROWSING

YES MONITOR KEYSTROKES FOR PASSWORD FIELDS

### Monitoring Limits

Use Teramind's monitoring limits to restrict what the agent records

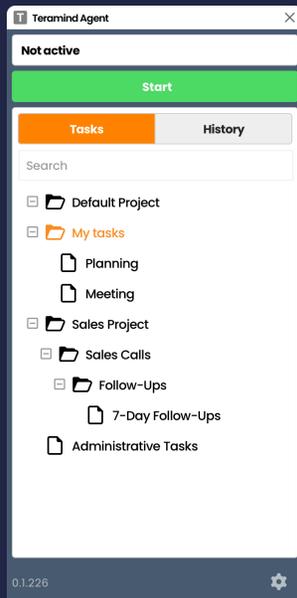
- Limit session recordings to only record rule violations and the surrounding activity
- Disable recording for personal websites and apps like banking or messaging apps
- Black out user PII, PHI, or PFI when it appears on-screen during session recording
- Set monitoring schedules so off-the-clock activity like lunch breaks aren't recorded



## Customer Data Protections

Teramind's rules and policies provide an added layer of security to customer data protection

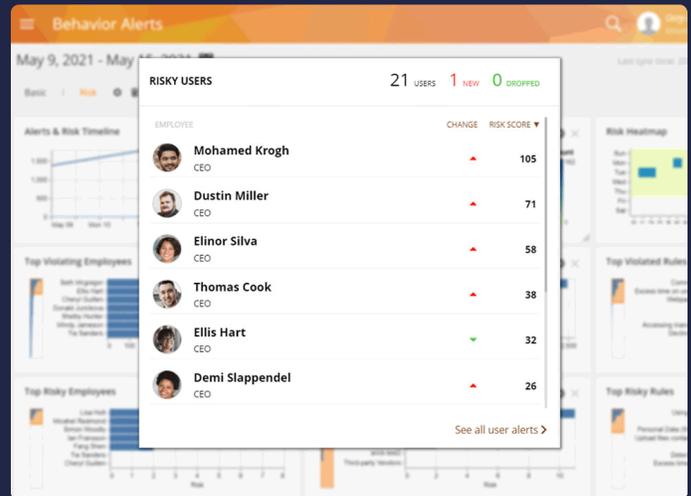
- Customize rules and alerts to protect against malicious customer data usage
- Find out when customer privacy data is transferred, copied, or edited
- Restrict access to customer data to only those who need it



## Teramind Revealed Agent

Get complete monitoring transparency using Teramind's Revealed Agent

- Allow users to toggle their monitoring on and off at will
- Satisfy data collection consent laws like GDPR
- Give users the ability to select what tasks they're working on
- Track user activity rather than the machine. Perfect for remote work or BYOD



## Privileged User Monitoring

Keep track of administrative access and gain oversight of those who can do the most damage

- Customize permission settings and access controls
- Use role-based access controls to limit permissions to monitored employee data
- Segment access so privileged users have limited capabilities
- Limit viewing and retrieval of monitored employee data to restrict data distribution

Contact [sales@teramind.co](mailto:sales@teramind.co) for a 1:1 demo