Employee monitoring, productivity optimization and insider threat detection in a single platform

INDATA

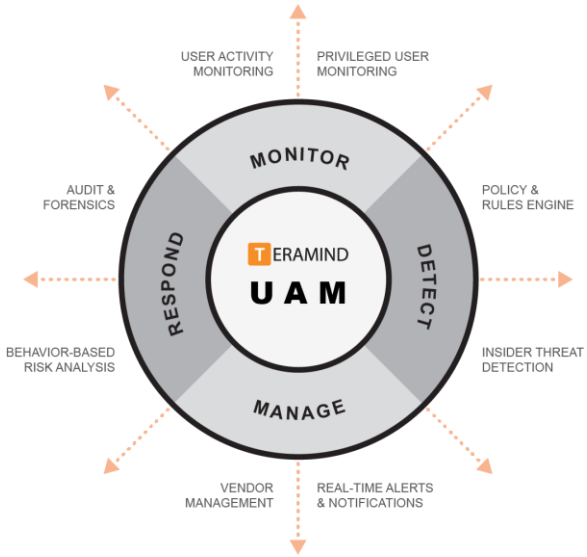
WWW.INDATACONSULTING.COM

(888) 502-3221

Google Cloud Partner

Employee monitoring, productivity optimization and insider threat detection in a single platform

Go beyond the basic employee monitoring and tracking functionality and adds intelligent behavior-based analysis to provide actionable insight and automated responses to employee generated threats. It can monitor employees, third-party vendors, contractors, remote and special/privileged users. With its rules and policies, capture violation incidents as forensic evidence and take action to alert, stop, block and more.



Measure employee productivity, conduct risk analysis, prevent unauthorized data exfiltration and keep track of how employees and third-party vendors access company resources while logged in at work. Finally, in case of a data breach or security incident, provides comprehensive forensic data and session recordings to identify the employees and vendors who have triggered a rule violation along with their activity footprint with pinpoint accuracy.

Why Choose Our Employee Monitoring Solution?

Ranked #1 by users and reviewers on PC Mag, TechRadar, Capterra and others

Intuitive, easy to use dashboard requires no additional resources to use Teramind

Most feature rich solution delivering activity monitoring, threat prevention, time tracking & productivity benefits

Extended functionality by integrating with SIEM, PM and Human Capital Management (HCM) systems.

Built-in access control and privacy settings to conform with GDPR, HIPAA and other compliance laws

Deploy in minutes on Cloud, Private Cloud and On-Premise. Suitable for both SMBs and large enterprises

Features at a glance

Real-time employee activity monitoring:
Monitors all employee activity covering 12+ system objects such as: web pages, applications, email, console commands, file transfers, instant messaging, social media, keystrokes, clipboard, searches, printing and even on-screen content (OCR) in real-time.

User behavior analytics:
Intelligent behavior analysis can detect malicious activity and anomalies that indicate deviation from normal behavioral baseline. Dynamic risk scoring and vulnerability scanning identifies insider activity before they represent a real threat.

Policy and rules engine:
Get started right away with hundreds of pre-built rule templates, activity classification lists and data categories. Create your own policies and rules with an intuitive, visual rule editor. Use natural English, regular expressions and conditions to easily define your requirements.

Built-in productivity optimization:
Define which apps and websites you consider productive and get in-depth reports on how your employees utilize them. Identify the laggards or high performers with active vs. idle time analysis. Adjust your organizational workflow through tracking of schedules, projects and employee engagement rate for overall productivity boost.

Audit and forensics:
Video recording of all employee activity, audio recording, session recording, immutable logs, alerts and optional OCR search are just a few examples of Teramind's powerful audit and forensic capabilities. Locate and stop the source of an insider threat with pinpoint accuracy.

Third party vendor management:
Monitoring features cover third party vendors and remote users who have access to your critical systems. This enables you to control vendor management and third-party SLA and decreases the chances of cyber threats.

Enterprise monitoring
Make it easy to monitor enterprise apps, e.g. SAP, Salesforce, etc. to detect malfeasant activity without requiring complex integration. However, if needed threat events and session logs can be sent to SIEM, threat analytics and PM systems for further analysis.

Compliance management:
Create activity and schedule based rules to support several common compliance requirements like: implementing audit trails (GDPR), limiting unauthorized login (ISO 27001), prevent unencrypted file transfers (PCI DSS) and more.

Industry statistics prove the need for employee monitoring

Colluding Employees are the Sources of Insider Threats

According to the Community Emergency Response Team, the main reasons for insider caused incidents are collusion from employees and third-parties.

48.3%	**insider-insider collusion**
16.75%	**insider-outsider collusion**

Employee Privilege Puts Sensitive Data at Risk

According to a survey of 400,000 member online by Cybersecurity Insiders published on The Insider Threat 2018 report.

37%	**excess privilege**
34%	**increased amount of sensitive data**

Employees are a Major Security Concern

Businesses agree employees are their biggest weakness in IT security - according to Kaspersky Lab and B2B International study of over 5,000 businesses.

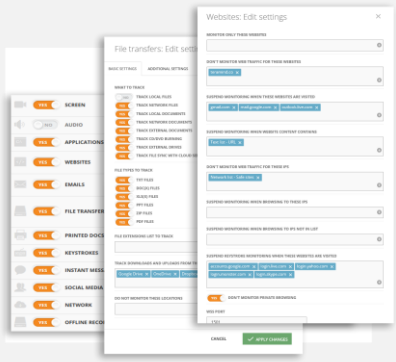
52%	**businesses agree employees are biggest weakness**

Many Employees Spend Unproductive Time at Work

According to FinancesOnline, 64% of employees use non-work related worksites every day and 85% of employees use their email for personal reasons.

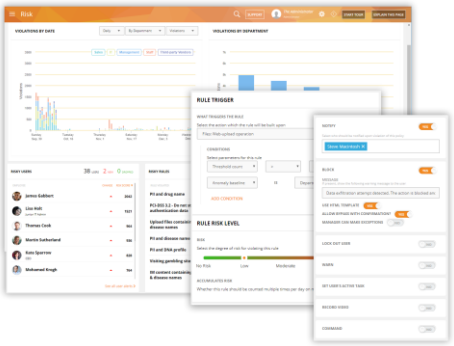
64%	**browse unproductive sites**
85%	**use email for personal tasks**

Deliver immediate business benefits



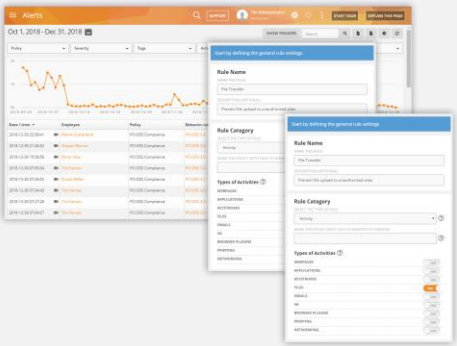
Establish organization-wide visibility and control

Visually records every action that an employee makes for over 12 objects including screen, apps, websites, files, emails, etc. Each object can be configured to take into consideration what needs to be monitored and measured and who has access to the monitored records. You can control which employees or third-party vendors to monitor, how much you want to monitor, when and for how long. This allows for both instant administrative viewing and respect employee privacy requirements as needed.



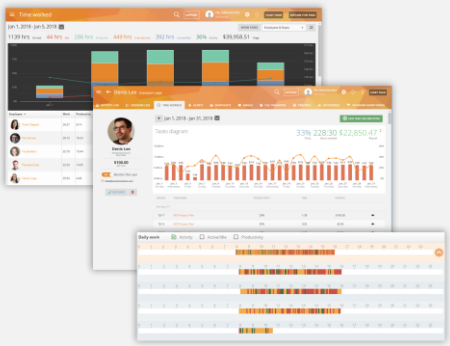
Detect insider threats and vulnerabilities

First, determine what behaviors are high risk i.e. copying files to external drives, using cloud storage to share corporate files, downloading/opening files and attachments from unknown sources etc. Then, apply advanced behavior-based rules to automatically detect when employees violate the rules. Utilize sophisticated anomaly rules to identify employee activity outside the normal behavior. Immediately get notified about harmful employee activity, lock them out from the system or take remote control of their computer before any malicious or fraudulent attempt.



Protect your sensitive data and resources

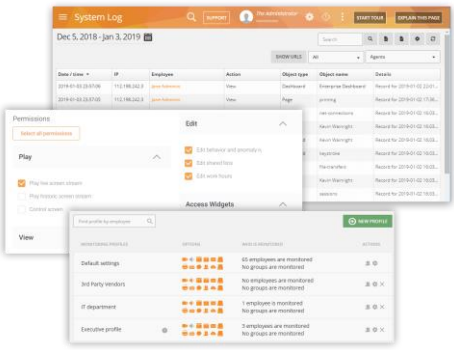
Take a look at DLP, if you need a dedicated data loss prevention solution. However, our basic package comes with some useful data protection features too. For example, you can utilize the Activity and Schedule-based rules to prevent external drive usage, detect unusual or unauthorized network login or files transfers. Or, write rules that react to any observable employee activity like blocking an e-mail from being sent outside the company domain, receive instant notification when certain sensitive document gets printed etc. All these features can help minimize information exfiltration and data leaks by malicious or ignorant employees.



Boost employee productivity and performance

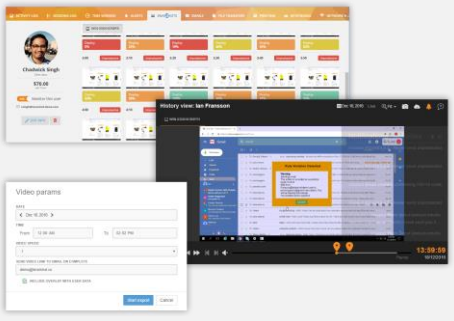
Use the workforce productivity tools to track active vs inactive time, late shifts, long breaks etc. Design etiquette rules to limit unproductive behavior. For example, set a time limit on social media usage or restrict access to gambling sites.

Use intelligent content-based rules to automatically identify clues to customer dissatisfaction (angry sentiments in emails/ customer query in IM chat not answered etc.) and implement processes to provide better service.



Monitor privileged employees and third-party vendors

Allows organizations to stop potential employee-employee or employee-third party collusion attempts. Create profiles for remote, privileged, external vendors and then define what information and system resources each profile can access. Further rules can be set up by behavior policies so that access to sensitive information is segregated by the organization's security policy, or on a need-to-know basis. Rules can also be created to notify the authorities of any suspicious privileged employee and third-party vendor activity, such as unscheduled and/or unauthorized changes to system configuration, creation of backdoor accounts etc.



Reduce organizational risk and protect yourself with proof

Take action against a malicious employee backed by solid proof. You can view detailed reports for all employees including any security incidents and what steps were taken. Instant snapshots, session recordings and history playback features can be used to view employees desktop for audit and evidence gathering purposes. Video and audio recording can be exported and shared with law enforcement authority.

Supported on all major platforms

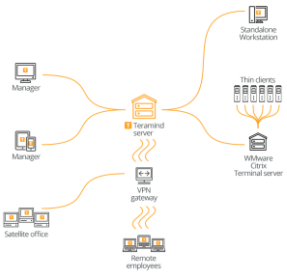
Windows 7 & Up	Citrix XenApp® & XenDesk®	Windows Server 2012 & Up	VMware Horizon	Mac OSX

Flexible deployment options

Cloud

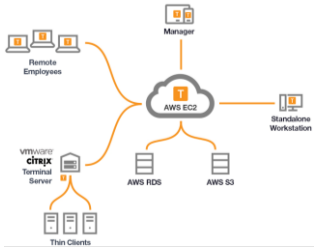
No server maintenance, only install Teramind Agents on the machines you want to monitor and set up your users, policies and rules and let us take care of the rest.

On-Premise



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.

Private Cloud



Use your own secure, scalable private cloud implementation including AWS, Google Cloud, Azure and more.

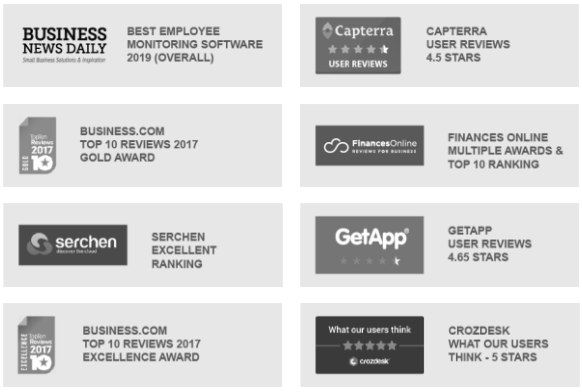
About InData

InData is your Next Gen IT Service Provider. We offer IT advice and solutions that make your business operate at peak performance. Our Managed Services, Infrastructure as a Services, and Cloud Infrastructure are world class.

We design, build, deploy, support, and monitor IT solutions for some of the most distinguished brands in the world. Our Service Team is available to document your requirements and provide customized solutions to meet your business objectives.

We understand the constant challenge to accommodate new staff and infrastructure locally, regionally and globally.

Ranked #1 by:



Google Cloud Partner

INDATA

Call for pricing
(888) 502-3221