Teramind UAM

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

TERAMIND | American Technology Solutions

Effective defense against insider threats: Detection and prevention

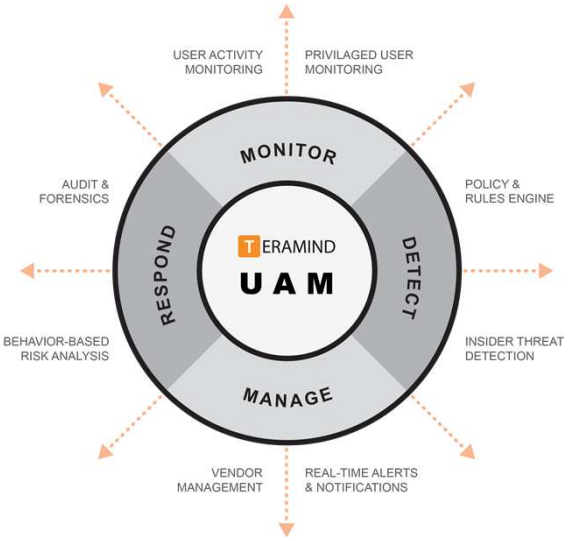
Most organizations have cybersecurity measures in place including antivirus, firewall, intrusion detection to protect infrastructure and IT assets. While these are generally good at defending the organization from external threats, they leave a security hole when it comes to employees and other internal users, third party vendors, contractors and privileged administrators who already have access to an organization's valuable assets and sensitive data.

Whether it is a company's intellectual property, financial records, customer data, PII, PHI or other sensitive material, it only takes one insider to engage in unwanted behavior and expose an organization to risks. In fact, majority of the data breaches in recent years involved weak or exploited employee credentials either by malicious or accidental incident (source). This is where User Activity Monitoring (UAM) can help fill the gap.

Employee monitoring is the process of tracking all activity conducted by an employee while logged into a computer (endpoint). With a employee monitoring solution in place, businesses have the necessary means to keep an eye on their sensitive data and employees so that that they can identify and stop misuses of company data and resources.

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

Teramind UAM goes 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, Teramind UAM captures violation incidents as forensic evidence and take action to alert, stop, block and more.



Teramind UAM can also measures 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, Teramind UAM 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.

Teramind UAM: Features at a glance

Real-time employee activity monitoring:
Teramind monitors all employee activity covering 12+ system objects like: 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. Create monitoring profiles for individual employees, groups or departments.

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. Establish a continuous feedback loop to refine and 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 few examples of Teramind's powerful audit and forensic capabilities. Together they provide a vast collection of investigative data to locate the source of an insider threat with pinpoint accuracy.

Third party vendor management:
Teramind's 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.

Compliance management:
Teramind UAM can be used to 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.

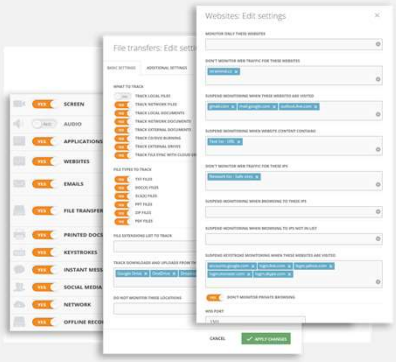
52%	**businesses agree employees are biggest weakness**

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.

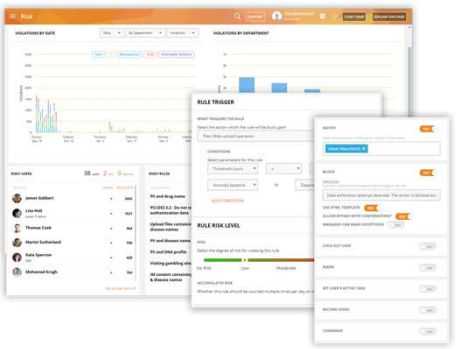
64%	**browse unproductive sites**
85%	**use email for personal tasks**

Teramind UAM delivers immediate business benefits



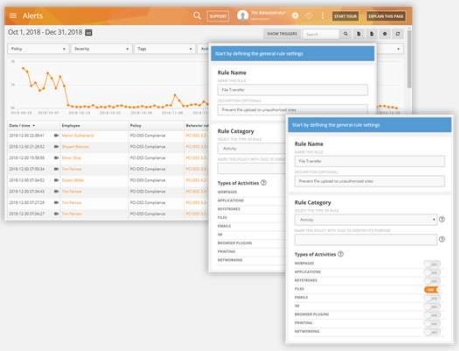
Establish organization-wide visibility and control

Teramind 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.



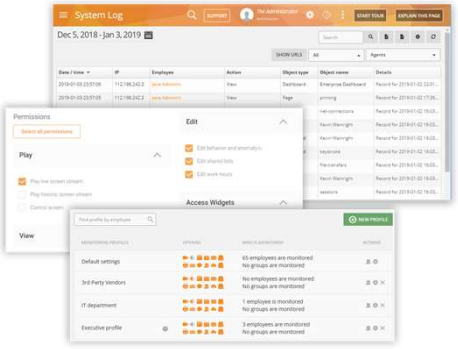
Protect your sensitive data and resources

Take a look at Teramind DLP if you need a dedicated data loss prevention solution. However, Teramind UAM 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

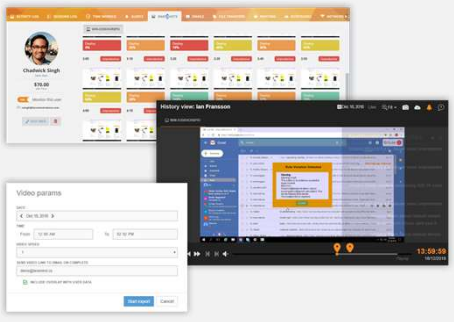
Use the workforce productivity tools to track active vs inactive time, late shifts, long breaks etc. Design etiquette rules to limit unproductive behavior. For example, set a time limit on social media usage or restrict access to gambling sites.

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

Teramind 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.



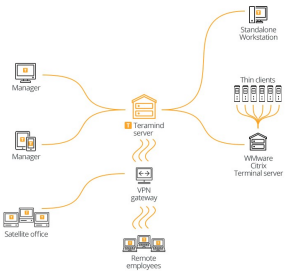
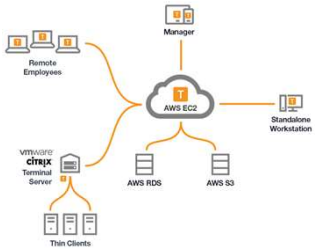
Reduce organizational risk and protect yourself with proof

Take action against a malicious employee backed by solid proof. On Teramind, 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 2008 & Up	VMware Horizon	Mac OSX

Flexible deployment 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.

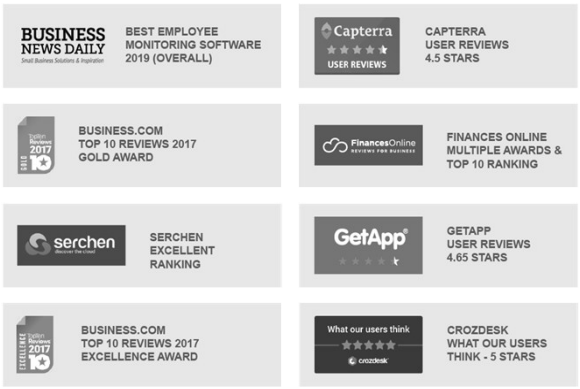
About Teramind

Founded in 2014, Teramind is a leading, global provider of employee and user activity monitoring, user behavior analytics, insider threat detection, forensics and data loss prevention solutions.

Over 2,000 organizations in finance, retail, manufacturing, energy, technology, healthcare and government verticals across the globe trust Teramind's award-winning platform to detect, record, and prevent malicious user behavior in addition to helping teams drive productivity and efficiency.

Teramind is headquartered in Miami, Florida, with sales and support operations around the world.

Teramind is Ranked #1 by:



www.americantechnology.com

sales@americantechnology.com

1-800-955-5790

Live Demo

www.teramind.co/sim