Teramind Third Party Vendor Management

Third party vendor monitoring, threat detection and data loss prevention in a single platform

TERAMIND

www.teramind.co

The risk of third-party vendor access

Third party vendors, partners, consultants and outsourced contractors often have privileged access to a company's internal systems through root or domain administration rights. As privileged insiders, they can change system configuration, steal company data as well as sabotage critical infrastructure. Even with no malicious intent, an external vendor is a major security liability. There are also strict regulatory requirements for some industries like banking, healthcare etc. where vendor monitoring is mandatory to ensure privacy and protection while data is transferred or processed between two parties.

For these reasons, an organization should setup a security perimeter when giving access to external vendors and contractors. It then needs a way to continuously monitor all vendor activity to ensure they conform to the company's security policy and rules. Some compliance regulations also require organizations to keep a detailed record of any security, privacy or data breach incidents caused by a third-party.

Teramind Third Party Vendor Management: activity monitoring, threat detection and data loss prevention in a single platform

With features like user activity monitoring, privileged user management, advanced authentication and access control, remote user monitoring and support for virtualization services, Teramind offers an unrivaled platform to monitor, control and protect third party vendors to ensure access is only granted to systems needed, decrease the chances of accidental mistakes that can damage system settings, and help improve IT safety measures. In addition, Teramind helps you meet many regulatory compliance requirements as it relates to third party vendor management with its extensive user activity monitoring, data exfiltration protection, audit, reporting and forensics capabilities.

Teramind Third Party Vendor Management: Features at a glance

Real-time employee activity monitoring:
Monitor all vendor activity covering 12+ system objects, like: web pages, apps, emails, files, IMs, social media, keystrokes, clipboard, searches, printing and even on-screen content (OCR) in real-time.

Authentication and access control:
Identity based authentication and segregated access control prevent unauthorized access and sharing of sensitive systems and data by a third-party.

Intelligent policy and rules engine:
Create monitoring profiles for individual vendor or groups. Configure rules for dangerous vendor behaviors like abnormal login, privilege escalation etc. with hundreds of pre-built rules or create your own with an intuitive, visual Policy and Rules Editor. Automatically warn, block or take control on detection of any rule violations or anomalies.

Audit and Forensics:
seamless real-time streaming of a vendor's screen and an extensive visual history of all actions. Immutable logs and reports provide a vast collection of investigation data in case of an incident.

Vendor risk management:
Identify high risk vendors, policies and system components on a dedicated risk dashboard. Sophisticated risk scoring helps identify and focus on areas of vulnerabilities.

Productivity & SLA:
Built-in productivity tools let you establish a continuous feedback loop with your vendor network. Refine and adjust your organizational workflow through tracking contract schedules, projects, budget and engagement rate to improve vendor SLA and QA.

Compliance management:
Conform with various compliance requirements in respect to third party monitoring. For example: implementing audit trails (GDPR), limiting unauthorized login (ISO 27001), prevent unencrypted file transfers (PCI DSS), reporting, and more.

Third party vendors: A weak link in cyber security chain

3rd-Party Incidents Are a Reality for Many Companies

In a 2016 global survey of 170 companies, Deloitte found that 87% have experienced an incident with a 3rd-party. Source: Deloitte.

87% **Suffered a Disruptive 3rd-Party Incident**

3rd-Party Vendors Have Access to Critical Systems

3rd-parties have to access many VPNs, networks, and platforms confirmed by 75% of organization leaders. Source: SOHA.

75% **Agree Third-Parties Have Access to Critical Systems**

Organizations Spend Millions on 3rd-Party Breaches

On average, organizations spend $10+ million responding to 3rd-party breaches each year. Source: Riskonnect.

Avg. $10M+ **Spent on 3rd-Party Breaches by Organizations**

Many Companies Lack 3rd-Party Security Standards

In a global survey of companies, PwC found that only 52% have security standards in place for 3rd-parties. Source: PwC.

Only 52% **of Organizations Consider 3rd-Party Security a Priority**

How third party vendors cause security risks

The ability to access system preferences allows external vendors to steal company data as well as damage IT infrastructure. There are several ways a vendor can compromise your system and data. A few scenarios in which external vendors potentially pose risks are as follows:

 **Malware infection**	Opening a corrupted email or visiting a website with malware that can infect an organization's system.
 **Access elevation**	A vendor attempting to bypass security clearances and gain additional access by running foreign programs.
 **Database access**	Attempting to log in to database servers during off-hours or after the completion of a project.
 **Data exfiltration**	A vendor abusing access within a system to view confidential customer and employee records.
 **Cloud security**	Any access to cloud-based storage services, which can lead to confidential information being transferred out of the system.
 **Steganography**	Utilizing screen-capturing software to share confidential files and security information with unauthorized sources outside the organization.

Teramind Third Party Vendor Management use cases

IT Services

Industry Challenge	IT services businesses, MSPs and hosting providers often need to monitor vendor activity in the company servers to enforce SLA and process billing. Another aspect of IT services is that, employees of third party professional services can access your organizational databases, configure servers and often setup IT security systems. They should be treated with same vigor as your other privileged employees and scrutinized for all their activity.
Teramind Solution	With Teramind's activity monitoring solution, it's possible to quickly see (and prove) exactly who worked on the servers, when, for how long and what they did to ensure security and process accurate billing and SLAs. In addition, Teramind supports ISO 27001 compliance that further ensures an organization's overall IT security measures are covered with a single solution.

Healthcare

Industry Challenge	Health Insurance Portability and Accountability Act (HIPAA) is designed to facilitate efficient flow of the healthcare data and protect patient's Personally Identifiable Information (PII), Personal Health Information (PHI) and Electronic Health Record (EHR) from fraud, theft or other misuse. HIPAA covered organizations must protect these data not just from their employees but ensure any contractors or Business Associates (BAs) has systems in place to comply with the regulation. There are even specific Administrative, Security and Technical Rules for such addressable implementation specifications.
Teramind Solution	Teramind helps healthcare organizations conform with ongoing privacy and security requirements of HIPAA regulated PII, PHI and EHR data from both internal and external users. With Teramind, you can create security profiles for vendors allowing or restricting access to patient records on a need to know basis. Granular activity monitoring of all system objects like files, networks, websites, apps, emails etc. helps enforce privacy policy. Use instant alerts and audit trail to meet the HIPAA security review and reporting requirements.

Financial Services

Industry Challenge	Banks and other financial institutions often outsource operational functions to contractors or use third parties to offer value added services. An increasing number of banks are also outsourcing core banking operations (i.e. accessing demand deposit accounts through bankcards) to third party vendors. This creates a new avenue of threats for both the banks and their customers. Regulations and laws are enacted to make sure banks held their vendors accountable for their activities. For example, Federal Financial Institutions Examination Council (FFIEC) recently released the Cybersecurity Assessment Tool that states, "Financial institutions must understand the complex nature of arrangements with outside parties and ensure adequate due diligence for the engagement of the relationships and ongoing monitoring."
Teramind Solution	With Teramind's activity monitoring solution, it's possible to quickly see (and prove) exactly who worked on the servers, when, for how long and what they did to ensure security and process accurate billing and SLAs. Teramind helps banks and financial institutions uncover potential cybersecurity weaknesses in their online banking system and develop threat intelligence with behavioral and content-based analysis of secure financial data. With continuous monitoring, a bank can prevent bad practices by its vendors and if necessary, conduct detailed file search to make sure vendors are using the right forms, following the agreement and addressing customer request on a prompt and responsive manner. Teramind supports standards like FFIEC and SOX, so financial institution can rest assured that their third party vendor management conforms to financial regulations.

Retail / E-Commerce

Industry Challenge	Retails and e-commerce merchants and any business processing payment information must comply with PCI DSS. This entails stringent information security requirements for the merchants and their vendors while processing credit card transactions or dealing with customer data. For example, it's on you, as a merchant to ensure that third party service providers (TPSPs)/vendors you do business with are also following the compliance protocol. You should be able to list each vendor your company does business with, confirm what services they provide, and make sure that each provider listed is compliant with the PCI DSS on an ongoing basis.
Teramind Solution	The simplest way to ensure PCI DSS compliance and proper auditing is to add third party vendors into your existing (preferably Cloud-based) monitoring and auditing system so that you both have a common, transparent, end-to-end auditing system. Teramind has several deployment options including a Cloud solution. It's PCI DSS compliant and implements key security requirements for third party vendors and external users like: financial data (PFI, PII) identification, unique IDs, layered access control, 2FA etc. for both local and network resources.

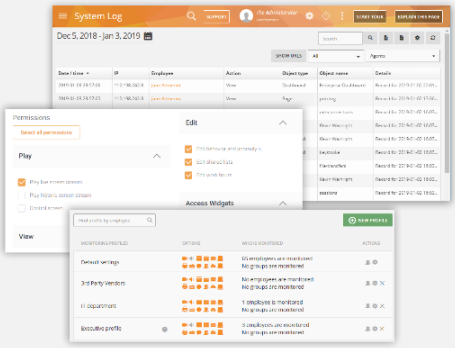
GDPR / Privacy Data Protection

Industry Challenge	Since May 2018, any organization handling EU citizens' personal data has to comply with the GDPR law. Known as the Controller, these organizations also have to ensure the GDPR compliance for its Processors. A Processor is someone following instructions from the data controller to collect/process the personal data (PII), in other words a third party vendor. Any controlling organization employing a third party vendor to process EU citizens' personal data, will be responsible for their GDPR compliance.
Teramind Solution	Third-party vendor management, access control and contractual oversight is required to make sure a GDPR Controller has implemented the right accountability procedures for its Processor(s). Teramind can ensure your third party is processing privacy data only in the context it is required to be processed. Additionally, the software can be configured with restricted feature sets allowing for further privacy of EU customers. Extensive reporting and forensic capability help you fulfill GDPR's record keeping and breach reporting requirements.

Telecom

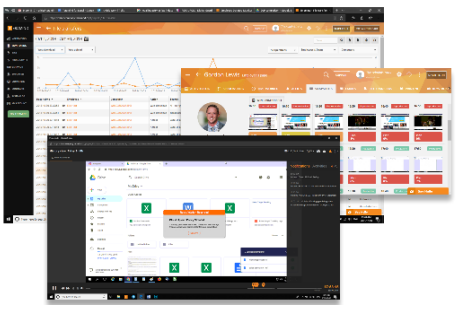
Industry Challenge	Telecommunications is a fundamental backbone in today's world. Like utilities and other critical infrastructures, it touches everyone including people, businesses and government. This is why telecom operators and ISPs are often the primary target of cybercriminals. And these criminals are getting desperate. According to a telecom threat intelligent report by Kaspersky, cybercriminals are recruiting insiders including contractors and vendors to gain access to telecommunications networks and subscriber data. They blackmail the targeted insiders forcing them to handover credentials or distribute spear-phishing attacks on the criminal's behalf.
Teramind Solution	With Teramind's privileged user monitoring and intelligent behavioral analysis, telecom providers can look out for compromised vendors who show abnormal signs, like: attempting to bypass security clearances and gain additional access, attempt to change system component etc. Moreover, Teramind's granular activity monitoring and data loss prevention solution is designed for high-grade security standards like NERC-CIP, NIST-FISMA, ISO 27001 for critical infrastructure providers like telecom and utilities.

Teramind Third Party Vendor Management Delivers Immediate Business Benefits



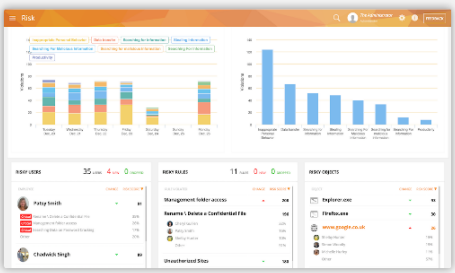
Authentication and Access Control

Identity based authentication and segregated access control prevents unauthorized access or sharing of confidential data outside your organization. You can setup an access account for each vendor that is going to need authorized clearance and easily track what each vendor is doing at any given time. Create profiles for regular, privileged and contract/external users and then define what information and system resources each profile can access.



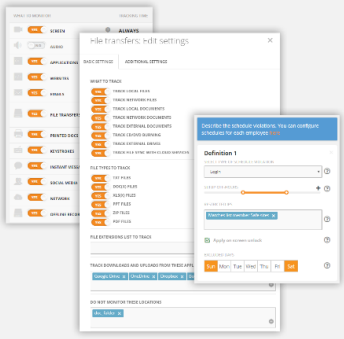
Session Recording and Playback

Live view and history playback provide seamless real-time streaming of third party vendor activity through the dashboard as well as an extensive visual history of all actions taken for both on-site and remote vendors. All actions can also be searched via metadata, regular expression and natural language. Recordings can be tagged by time and date highlighting any alerts and notification.



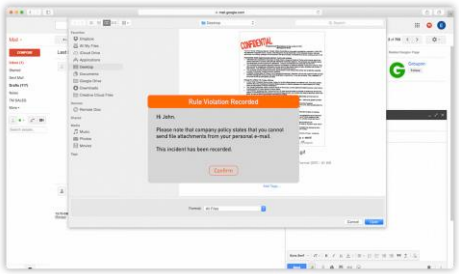
Vendor Vulnerability and Risk Analysis

Teramind has a dedicated Risk dashboard where the supervisor can conduct organization-wide risk assessment. Risk can be profiled by vendors, departments responsible for the vendor or by system objects accessed by the vendor. Reports can be derived by severity of risks or by how many times security violations occurred. Unique Risk Scores helps you identify high-risk vendors or policies so that plans can be developed for treating the risks.



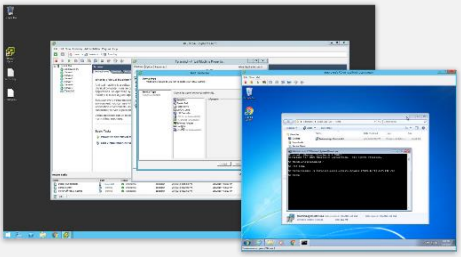
Enterprise-Wide Monitoring and Tracking

Teramind has a dedicated Risk dashboard where the supervisor can conduct organization-wide risk assessment. Risk can be profiled by vendors, departments responsible for the vendor or by system objects accessed by the vendor. Reports can be derived by severity of risks or by how many times security violations occurred. Unique Risk Scores helps you identify high-risk vendors or policies so that plans can be developed for treating the risks.



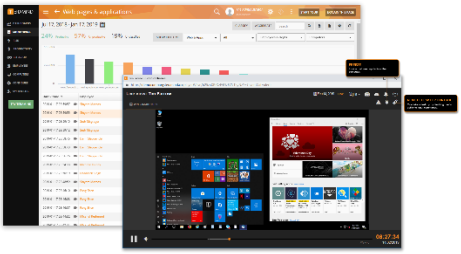
Document tracking

Monitor the interactions between third-party vendors and your data including reports on: who accesses data, when the data is accessed, any changes, abnormal activity or any attempts made to alter the data. The document tracking ability can be configured to fit your policies. Some examples of the possibilities with document tracking are: documents transferred to emails as an attachment, USB, Dropbox, Google Drive, documents printed etc. The goal of document tracking is to supply organizations with a view into what interactions vendors are making with your data.



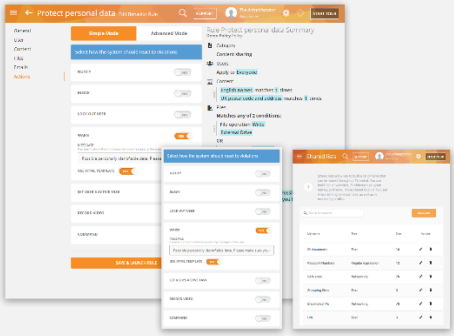
Security sandbox

Teramind allows you to create virtual servers on Windows, VMware Horizon etc. Utilizing this capability, you can for example, setup a Terminal Server for your vendors and install the Teramind Agent on it. Vendors can then login to the server using RDP keeping out of your internal network and repositories. At the same time, you can record vendor activates separately, restrict access or take control of the server in case of an incident keeping rest of your business immune to disruption.



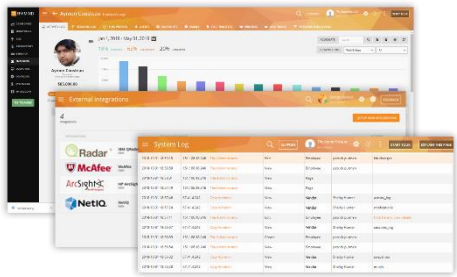
Remote desktop control

Remote contractors and vendors can enjoy the simplicity of tracking their project and time with Teramind with the click of a mouse. Once the Teramind agent is started, all actions and data are recorded. You can take control of an external vendor's desktop control and access at the first sign of malicious activity to eliminate threats of all kinds.



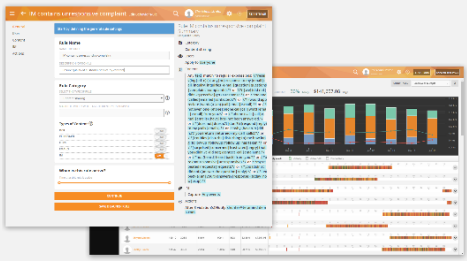
Powerful policy and rules editor

Define what constitutes dangerous or harmful activity such as unscheduled and/or unauthorized changes to system configuration, and creation of backdoor accounts. The system will then automatically detect when a vendor violates the rules. Sophisticated anomaly engine can even automatically identify vendor activity outside the normal behavior. Warn/notify/lock-out the vendor or take remote-control of their system in case of a malicious or harmful incident.



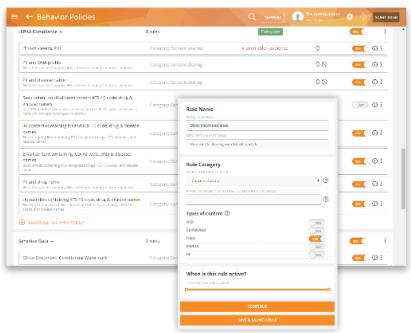
Integrated threat management

Attain full knowledge of which vendors are accessing systems and network resources with in-depth activity reports. Receive real-time alerts for high-risk vendor behavior. Session logs, anomaly and risk analysis, incident reports make your findings and observations tasks easier by identifying where sensitive data is stored, who accessed it and how. Finally, event triggers and logs from Teramind can be send to SIEM and other analytics tools for a holistic threat management system.



Ensure quality of service

Built-in productivity tools let you establish a continuous feedback loop with your vendor network. Refine and adjust your organizational workflow through tracking contract schedules, projects, budget and engagement rate to improve vendor SLA. If your vendors handle customer care services, you can monitor their performance and quality and if necessary, conduct detailed investigation to make sure vendors are using the right forms, following the agreement and addressing customer request on a prompt and responsive manner.



Compliance management

Many organizations are required to follow several regulatory, cybersecurity, administrative and privacy standards that includes vendors accountability and liability protection. Teramind has built-in support for many of these compliance standards including HIPAA, GDPR, PCI DSS, ISO 27001 etc. and can be adapted to support evolving compliance requirements with its powerful Policy & Rules editor and various monitoring and reporting capabilities.

Supported on all major platforms

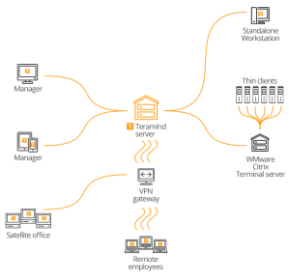
Windows 7 & Up	Citrix XenApp® & XenDesk®	Windows Server 2012 & Up	VMware Horizon	Mac OSX

Flexible deployment options

Cloud

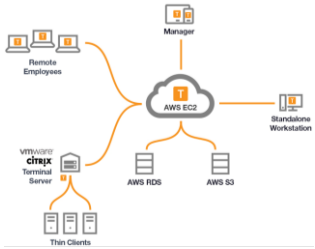
No server maintenance, only install Teramind Agents on the machines you want to monitor and set up your users, policies and rules and let us take care of the rest.

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.

Easy 3-step process

1 Install

Deploy the Teramind Revealed or Stealth Agent on the desktop and servers you want to monitor.

2 Configure

Create policies and rules and setup monitoring profiles for your third party vendors and contractors.

3 Sit-back

Watch Teramind automatically enforce the rules, provide real-time alerts and blocks malicious activity.

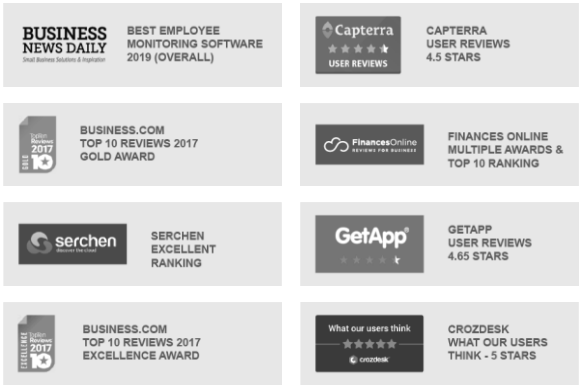
About Teramind

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:



Live Demo

www.teramind.co/sim

www.teramind.co

hello@teramind.co

+1-212-603-9617