Kriptone

ENTERPRISE CYBERSECURITY INSIDER THREAT SOFTWARE COMPARISON

To help you better understand how Kriptone® compares to alternatives on the market, we've created a detailed comparison of user activity monitoring software. In particular, we've compared tools that rely on user session video recording as the main security data format. In addition to general information, you can find a feature-by-feature competitor comparison in the table below.

LICENSING AND PRICING

Licensing and Pricing	kriptone	observe it	Veriato	TERAMIND
Floating endpoint licenses	✓	–	–	–
Free database support	✓	–	–	✓
Commercial database support	✓	✓	✓	–
Non-persistent VDI monitoring	✓	–	–	–
Total cost of ownership	$	$$$	$$	$$

There are several popular licensing schemes for insider threat software: per-user, per-session, per-host, a fixed infrastructure fee, and combinations thereof.

The most common licensing schemes for insider threat solutions are based only on the number of hosts, making the pricing transparent and helping you optimize costs. Products with complicated multi-factor licensing may sometimes have hidden costs as well as additional features included by default.

Another useful option is support for floating endpoint licenses, allowing you to reassign licenses between endpoints. This is especially useful if you have a lot of virtual machines to monitor. While Kriptone includes this option for both physical and virtual machines, you'll find it hard to quickly reassign licenses for ObserveIT and Veriato.

Note that in November 2019, ObserveIT was acquired by Proofpoint, a cybersecurity company. ObserveIT previously operated under a permanent licensing paradigm, but Proofpoint has now changed it to a yearly subscription model. For this reason, many current and potential ObserveIT customers have started looking for ObserveIT competitors and alternatives such as Kriptone.

MONITORED PLATFORMS

Feature	kriptone	observe it	Veriato	TERAMIND
Monitored Platforms				
Windows XP / Server 2003	✓	–	–	✓
Windows Vista through Windows 10 / Server 2019	✓	✓	✓	✓
Linux / Unix (Telnet and Console sessions)	✓	✓	–	–
X Window sessions	✓	–	–	–

Determine what endpoints and platforms you need to surveil when choosing activity monitoring software. Keep in mind that you might need a wider choice of platforms as your company grows.

All the solutions we've compared support Windows. Kriptone and ObserveIT also monitor sessions on Linux/Unix systems. Kriptone is the only product supporting X Window session monitoring, which allows you to monitor Ubuntu Amazon Linux Workspaces.

Another important challenge is monitoring virtual environments like Citrix, Microsoft Hyper-V, and VMware Horizon. Functionality for monitoring these environments should be identical to that for monitoring physical endpoints. For virtual desktop environments, it's best to use monitoring solutions that support floating licenses for native endpoints, as virtual machines are created more frequently than physical ones.

As well as floating endpoint licenses, Kriptone delivers a client ready to be added to the golden image and automates license provisioning via the license pool. Whenever any virtual machine instance is shut down, the license is released and returns to the pool. Therefore, to audit VMware or Citrix desktop environments, you only need the number of Kriptone Workstation licenses corresponding to the maximum number of simultaneously active virtual desktops. Also, Kriptone floating licenses support non-persistent VDI monitoring.

At the same time, Kriptone delivers comprehensive functionality to monitor and audit published application sessions. Teramind and ObserveIT also support published application infrastructures.

DEPLOYMENT & MANAGEMENT

Feature	kriptone	observe it	Veriato	TERAMIND
Deployment & Management				
Deployment model	On-premises	On-premises	On-premises	SaaS and on-premises
Easy deployment	✓	–	–	✓
Remote installation/uninstallation of clients	✓	–	✓	–
Management via web console	✓	✓	–	✓
Centralized endpoint client updates	✓	–	–	✓
System health monitoring	✓	✓	–	–
Easy on-premises maintenance	✓	✓	✓	–
Database cleanup	✓	✓	✓	✓
History archiving	✓	✓	–	–

A Software as a Service (SaaS) solution is fast to deploy and available on any platform and device. Teramind provides its service primarily according to the SaaS model. They also offer user activity monitoring and data loss prevention solutions on the AWS platform according to the Platform as a Service (PaaS) model.

However, on-premises deployment is associated with fewer security risks. On-premises deployment provides these benefits to Kriptone clients:

- A one-time license for Kriptone includes system installation and configuration.
- Kriptone can be deployed on a dedicated server or in a client's personal cloud.
- Cloud storage resources are estimated by the deployment team according to business needs.
- Clients retain complete control over data protection and data access.
- Highly sensitive information remains confidential.
- Kriptone ensures compliance with industry and government regulations.

Some reviewers point out that ObserveIT and Veriato are hard to deploy by yourself. You may also face scalability issues with large deployments, as these products impact server performance. Customers of Kriptone, on the other hand, praise the detailed technical documentation and easy deployment process along with the many automated maintenance tasks.

BASIC RECORDING AND INCIDENT RESPONSE FUNCTIONALITY

Feature	kriptone	observe it	Veriato	TERAMIND
Basic Recording and Incident Response Functionality				
Video replay of every session	✓	✓	✓	✓
Audio recording	✓	–	–	–
Real-time playback of live sessions	✓	✓	✓	✓
Multi-monitor recording	✓	✓	✓	✓
Real-time alerts	✓	✓	✓	✓
User behavior analytics and risk scoring	✓	✓	✓	✓
Multi-tenancy	✓	–	–	–
Privileged account management	✓	–	–	✓
USB device alerting and blocking	✓	–	–	–
Mass storage device control	✓	–	–	✓
Kill process on alert / block user on alert	✓	✓	✓	✓
User blocking	✓	✓	–	✓

Recording is a key functionality of any user monitoring software. Almost all employee monitoring solutions are equipped with real-time alerting functionality: the software notifies a security officer if something suspicious is happening. Kriptone and Teramind also allow security officers to kill this activity and block the user and allow for recording audio in addition to the usual video logs.

Storing records requires plenty of disk space or cloud storage space. To use this space effectively, monitoring platforms use various compression techniques. Kriptone provides two options: to save records with the original screen resolution or compress them. Kriptone's compression algorithms allow for saving the master image and its deltas, thus reducing the amount of required disk space. Additionally, all screenshots are encrypted with a session key and the data structure of records is optimized to ensure fast insertion and deletion of records with any number of active sessions.

ObserveIT divides a user's screen into nine parts and stores those records independently. This approach allows ObserveIT not to duplicate parts of records. For instance, when user activity is located in one part of the screen, there's no need to record the rest of it. On the other hand, this system makes it hard to delete, transfer, or archive data because many records may refer to a single screenshot.

Veriato compresses screen records and stores them in a default format. Teramind saves video streams, compresses them, and changes the screen resolution.

Multi-tenancy is a useful feature for managed service providers who take care of cybersecurity for their clients. It's also useful for organizations with offices in different locations. The Kriptone multi-tenant deployment mode ensures that several independent tenants can operate in one environment.

Kriptone's alert system includes an Artificial Intelligence (AI) module that detects abnormal user activity and possible account compromise by establishing baseline user behavior and monitoring behavior in real time. For instance, this module can create a baseline of a user's work hours and notify a security officer in case of user activity at an abnormal time.

ObserveIT employs user behavior analytics to gather statistics for the main dashboard. It provides a security officer with information on risk scores and user behavior trends over periods of time, but it doesn't notify of suspicious trends.

Veriato offers user behavior analytics and risk scoring functionality to analyze regular user actions, establish a baseline of safe behavior, and notify designated personnel of dubious activity. But keep in mind that Veriato offers this functionality as standalone software that requires an additional license.

Veriato also uses AI to analyze employee correspondence and daily activities for sentiment-based threat detection.

Additional Recording Features

Feature	kriptone	observe it	Veriato	TERAMIND
Additional recording features:				
Keylogging	✓	✓	✓	✓
Clipboard	✓	✓	✓	✓
Index by active window title	✓	✓	✓	✓
Index by active application name	✓	✓	✓	✓
Host name	✓	✓	✓	✓
User name	✓	✓	✓	✓
Date/time	✓	✓	✓	✓
Visited URLs	✓	✓	✓	✓
IP associated with host	✓	✓	–	✓
IP of remote desktop	✓	✓	–	–
Logging all USB device connections	✓	–	–	–
File activity monitoring	✓	✓	✓	✓
Logging USB mass storage connections	✓	✓	✓	–
Magnifier option (zoom screenshot regions)	✓	✓	–	✓

In order to thoroughly monitor user activity, you need more than a video of the session. Additional data helps you understand the context and search more effectively. If an insider attack has already happened, this data allows you to investigate the scope of the breach, the tools used, and the parties involved.

Advanced user monitoring solutions like Kriptone perform keylogging, record clipboard contents, and log details of active processes and applications, web activities, and device connections. They

also record in-depth network details upon connecting to a host. While differing in the user activity details — and especially in the network connection details — they provide, ObserveIT, Veriato, Kriptone, and Teramind all support file activity monitoring.

Searching, Reporting, and Exporting

Feature	kriptone	observe it	Veriato	TERAMIND
Searching, Reporting, and Exporting				
Search by metadata	✓	✓	✓	✓
Scheduled and ad-hoc reports	✓	✓	✓	–
Interactive system dashboards	✓	✓	✓	✓
Save sessions in encrypted format (forensic)	✓	–	–	–
Export screenshots to external formats	✓	✓	✓	✓
Put your company name on reports and notifications	✓	–	–	–

Recording lots of metadata is only part of the insider threat prevention process. To effectively prevent threats, you need to be able to search within collected data. It's hard to find a single event, especially if you don't know when it happened and your company employs thousands of people. That's why all top monitoring solutions allow you to search by any recorded parameter.

Accumulated data can also be used for generating reports. Usually, activity monitoring software can create various scheduled and ad-hoc reports. Kriptone allows you to customize emails and reports with your company's name and logo.

Finally, monitoring information can be used for investigations and forensic activities. Kriptone, ObserveIT, Veriato, and Teramind export recorded data in an encrypted tamper-proof format that may be used for forensic purposes.

Access Management

Feature	kriptone	observe it	Veriato	TERAMIND
Access Management				
Secondary authentication to identify users of shared accounts	✓	✓	✓	✓ (cloud-based system)
Access request functionality	✓	–	–	–
One-time passwords	✓	–	–	–
Multi-factor authentication	✓	–	–	–
Time-based user access restrictions	✓	–	–	–
Privileged account and session management (PASM)	✓	–	–	–
Password sharing	✓	–	–	–

Recording lots of metadata is only part of the insider threat prevention process. To effectively prevent threats, you need to be able to search within collected data. It's hard to find a single event, especially if you don't know when it happened and your company employs thousands of people. That's why all top monitoring solutions allow you to search by any recorded parameter.

Accumulated data can also be used for generating reports. Usually, activity monitoring software can create various scheduled and ad-hoc reports. Kriptone allows you to customize emails and reports with your company's name and logo.

Finally, monitoring information can be used for investigations and forensic activities. Kriptone, ObserveIT, Veriato, and Teramind export recorded data in an encrypted tamper-proof format that may be used for forensic purposes.

Solution Work and Security

Feature	kriptone	observe it	Veriato	TERAMIND
Solution Work and Security				
Watchdog mechanism	✓	✓	✓	✓
Driver-level uninstall protection	✓	–	–	–
Centralized endpoint client updates	✓	–	–	✓
Audit trail for system users	✓	✓	✓	✓
SIEM system integration	✓	✓	✓	✓
Ticketing system integration	✓	✓	–	–

Employee monitoring software should be easy to use, protected, and compatible with the other security solutions a company uses. This is especially important for large enterprises that build custom security systems using several compatible solutions.

Recording and storing data requires a lot of disk space. If your company has thousands of employees, you may end up with terabytes of surveillance records each week. An insider attack can go unseen for months, so it's a common requirement to preserve data for a considerable amount of time. This may be a problem with some solutions, such as Veriato, that use a lot of resources for data storage, thereby impacting server performance.

Kriptone uses highly optimized formats to store session recordings and metadata. It also optimizes bandwidth use.

Integration with SIEM and ticketing systems allows you to exchange data inside your security infrastructure. By combining information from these systems, you can trace not only the details of user actions but the reasons for them. All the monitoring solutions we've mentioned integrate with some set of popular SIEM systems, and several also integrate with ticketing systems.

KRIPTONE® VS COMPETITORS

ObserveIT, Veriato, and Teramind are the top user activity monitoring solutions on the market. Let's consider their functionality compared to Kriptone.

ObserveIT

ObserveIT has robust recording functionality and logs a lot of metadata in addition to video. It's equipped with two-layer authentication (credentials and email codes) and secondary authentication for shared logins. Deployment can be somewhat complicated without a product expert.

On the other hand, ObserveIT has limited access management functionality, providing only secondary authentication. Product licensing is a combination of a fixed infrastructure fee and a set of endpoint monitoring licenses. You may have some trouble distributing these licenses between virtual machines, however. Also, it's impossible to update a client offline.

ObserveIT doesn't provide automated or manual incident response tools besides a warning message forcing users to acknowledge their actions.

Note that ObserveIT changed to a yearly subscription model after its acquisition by Proofpoint. Since the acquisition, more and more ObserveIT clients have been choosing Kriptone as a worthy ObserveIT alternative.

Bottom line: Kriptone is a proven alternative to ObserveIT. It provides the same monitoring and alerting functionality while offering robust identity and access management capabilities, device management, and incident response tools. In addition to recording video, audio, and metadata, Kriptone uses a UEBA module to analyze this data and detect suspicious activity. Coupling these features with granular access and identity management, this all-in-one solution ensures full-cycle insider threat management. Kriptone offers a flexible licensing scheme, with floating endpoint licensing and with licensing for the Standard Edition based only on the number of endpoints.

Veriato Cerebral

Veriato Cerebral (formerly Veriato 360) is a solution for monitoring Windows and macOS-based endpoints. With a flexible licensing scheme, it's currently more affordable than ObserveIT.

Veriato provides basic recording functionality with a limited ability to block suspicious activity. What differentiates Veriato from its competitors are a UEBA module and computational linguistic analysis. Veriato identifies disgruntled employees (who are considered potential attackers) by analyzing sentiments in their correspondence and actions. This solution also uses AI to detect indicators of stolen credentials.

With employee monitoring as its main use case, Veriato delivers a number of additional activity-specific reports such as on email monitoring and chat monitoring.

Bottom line: Compared to Veriato, Kriptone supports more platforms (macOS, Linux/Unix, X Window, Citrix, VMware Horizon, Microsoft Hyper-V, and Windows) and is equipped with more

robust access control functionality. Kriptone ensures granular access to critical endpoints using tools such as multi-factor authentication, one-time-passwords, and access requests. Also, Kriptone employs UEBA to detect suspicious user behavior and prevent insider threats.

Teramind

Teramind offers two types of deployment: SaaS and on-premises. However, the SaaS model is the most common. As an on-premises solution, Teramind is deployed as a Linux virtual machine. It provides you with tools for native database management, deployment scaling, permission configuration, etc.

Despite considerable recording, alerting, and incident response tools, Teramind doesn't include identity and access management functionality besides secondary authentication for shared accounts, which is available only for the cloud-based system. Without multi-tenancy and specific scaling capabilities, it may be complicated for managed service providers and those with large infrastructures to deploy Teramind.

Bottom line: Kriptone is a worthy Teramind alternative, as Kriptone is a universal and stable on-premises solution that allows you to record not only Windows but also Linux and virtual endpoints. While on-premises software takes more time to deploy than do SaaS solutions, it brings more benefits in the long run.

Kriptone provides an incident response toolset in addition to monitoring and recording features. It also includes robust identity and access management functionality and is equipped with must-have features for scaling a deployment from a limited pilot to an extra-large hybrid infrastructure.