KuppingerCole Report

EXECUTIVE VIEW

by Alexei Balaganski | September 2018

ObserveIT Insider Threat Management

ObserveIT Insider Threat Management is a platform that combines the functionality of traditional User Behavior Analytics (UBA) and Data Loss Prevention (DLP) products in a lightweight and streamlined solution for detecting and mitigating various insider threats.

by **Alexei Balaganski**
ab@kuppingercole.com
September 2018

Content

Related Research

Executive View: ObserveIT User Activity Monitoring – 71258

Advisory Note: Real-Time Security Intelligence – 71033

Advisory Note: Understanding and Countering Ransomware – 70282

Leadership Compass: Privilege Management – 72330

1 Introduction

ObserveIT is a privately held software vendor based in Boston, MA in the United States. Originally, the company was founded in 2006 by Israeli entrepreneurs with the initial focus on remote privileged user monitoring, which was gradually expanded to cover other types of sensitive users as well: third-party vendors, contractors as well as own administrators and business users. In 2014, after an investment round, ObserveIT has established its US headquarters. Currently, the company is serving more than 1700 customers from over 80 countries, primarily in the financial, healthcare, telecommunications, manufacturing and retail markets.

The company's Visual Endpoint Recording technology utilizes lightweight software agents that allow monitoring and capturing a wide range of details from user sessions across multiple platforms. The solution collects this data centrally and offers its users a wide range of analytics, alerting and reporting functions. KuppingerCole has reviewed the company's user activity monitoring solution in 2015 and our verdict back then was that ObserveIT provided an exceptionally strong session monitoring technology, but its advanced analytics capabilities were not on par with other players in this market. Three years later, however, the market has changed dramatically, and the ObserveIT's portfolio has evolved to address these changes.

Under the pressure of the continued Digital Transformation, many companies are undergoing significant changes that affect their organizational structures and business processes. Constant adoption of new technologies and platforms has led to a massive increase in the complexity of their IT infrastructures. Sensitive corporate data that used to be stored in closely guarded on-premises silos is now spread across multiple clouds. New business models and communications channels dictate the need to provide access to the corporate data, systems, and applications to numerous new users from around the world.

The very notion of a privileged user has changed as well: it is no longer the system administrators that can pose the biggest risk to your company – in fact, every business user that has access to sensitive corporate data can, either inadvertently or with a malicious intent, cause substantial damage to your business by leaking confidential information, disrupting access to a critical system or simply draining your bank account. The most privileged users in that regard are the CEO or CFO, and the number of new cyber attacks targeting them specifically is on the rise, but a threat can come from any level, and knowing what each user is doing at any moment is becoming the most critical part of a sensible cybersecurity strategy.

In the recent years, the market has responded by offering a multitude of specialized User Behavior Analytics (UBA) solutions that usually operate by collecting security events from various sources - network traffic, endpoint monitoring or applications logs - and then utilizing machine learning algorithms to look for anomalies and suspicious activities in them. However, just detecting a statistical anomaly is not enough to understand the exact nature of the incident – an alert raised by a standalone UBA solution must be investigated by a security analyst, who will then have to decide how to deal with it. This decision will unavoidably be a reactive one, responding to a threat long after it has been detected. Automated remediation powered by a fuzzy AI logic alone may not an option for many companies.

ObserveIT offers an alternative approach towards insider threat detection: instead of anomaly detection, the company focuses on academic research of commonly seen indicators of insider threats, creating rulesets to identify them and designing an automated threat mitigation platform that implements flexible prevention methods. At first, this approach may appear similar to a traditional signature-based antivirus pitted against a modern EDR solution, however one should take into account the sheer breadth and granularity of context information the company's technology can collect from endpoints as well as its ability to apply mitigation directly on those endpoints (for example, block access to a USB drive when an attempt to copy sensitive files is detected). In a sense, ObserveIT Insider Threat Management platform combines the functionality of a traditional user behavior analytics solution and a data loss prevention product, but without the limited mitigation capabilities of the former and complexity and high maintenance of the latter.

2 Product Description

ObserveIT 7.5 (the latest version of the product at the time of this review) is an integrated solution for capturing details of user activities from endpoints, collecting all this data on a central application server and identifying commonly seen indicators of insider threats in it. To achieve this, lightweight software agents must be deployed on each monitored endpoint or at least on a file server. ObserveIT provides support for Windows, MacOS and Linux platforms, as well as for other Unix varieties and popular virtualization platforms. Agent deployment is simple and silent and can be performed using existing device management tools.

As opposed to traditional session monitoring solutions, this agent-based approach allows capturing not just a video recording of a session, but a detailed log of various activities: applications and processes, access to files and folders, URLs opened in browsers, key presses, print jobs, USB drives, etc. In addition, ObserveIT supports database access auditing by capturing SQL queries executed by database administrators. The amount of actual data that's being transferred is still quite low, so there is no impact on the workstation performance. More important are the potential privacy implications of such invasive monitoring, so the product allows administrators to define flexible capture policies that define which data is captured and when. For example, instead of continuous video recording, it may be configured to start only after a suspicious event was detected.

Application Server is the component responsible for communicating with agents, collecting the data, distributing policy updates, monitoring system health and generating reports. An external database (MS SQL Server) is required for data storage. Although the application server is scalable and has low resource requirements, there is, unfortunately, no support for highly available or distributed deployments, which can make large-scale deployments somewhat challenging.

The application server is also responsible for applying the real-time user activity analytics to the collected data. The company has made a conscious design decision not to implement the popular machine learning-based anomaly detection, focusing instead on rule-based threat detection powered by an extensive library of commonly seen insider threat indicators. ObserveIT is working with a research team at the Carnegie Mellon University to maintain and expand this library. Currently, several hundreds of insider threat rules grouped into 25 risk categories are shipped with the product, and new ones can be added quickly and easily.

This approach is somewhat similar to the way traditional signature-based antivirus products used to work. However, the company claims that pattern-based solutions are too noisy and may produce too many alerts that must be investigated by security experts before a mitigation action can be applied. A rule-based solution, on the other hand, will only raise an alert when a known malicious activity is detected, and an appropriate response action can be performed automatically. Given the company's focus on preventing sensitive data exfiltration, this decision actually makes sense, but it's still worth stressing that the solution will not detect "zero-day anomalies" that are not yet included in the library of known threats.

The solution's web-based dashboard is the central interface for viewing the detected insider threats, investigating details of user activities and generating analytical and compliance reports. The dashboard provides an overview of the organization's most risky users and their activities. The rich metadata that's collected by the system allows security teams to reconstruct the most minute details of every user session and present their full activity log along with the video recording. Since access to such sensitive data may lead to potential privacy violations (especially in countries with strong regulations like GDPR), the dashboard provides a number of privacy-enhancing features such as configurable data anonymization, access control and a global "session privacy lock" to ensure compliance. Furthermore, integration with an existing Active Directory ensures that only authorized administrators can access the session captures. Finally, all administrative activities within the system leave an audit trail as well.

Out of the box, ObserveIT provides over 300 Insider Threat Rules that identify various malicious activities like data exfiltration attempts, usage of unapproved applications, unauthorized privilege escalation and so on. The system can also proactively recognize configuration problems that may lead to malicious actions in the future. For each supported rule, a notification policy can be set up that defines what the system should do when the rule is triggered. Supported actions range from simple email notifications or sending events to an external log management or SIEM tool to automated mitigation actions: for example, the endpoint agent can initiate session video recording, show a warning message to the user, block a command execution or completely lock the user out. A REST API for custom integrations with 3rd party tools is supported as well.

Recently, ObserveIT has added the *File Diary* feature to the dashboard, which offers an alternative, data-centric view of the user activities. Here administrators can track what's happening to sensitive files as they are moved around, renamed, opened and edited, or, for example, uploaded to a cloud service. Each activity is attributed to a corresponding user, and both user-centric and document-centric tracking is supported. Unfortunately, the system does not yet support file hash capture, so potentially, it may confuse two documents with the same name or vice versa; hash capturing is planned for a future release.

For incident investigation, the dashboard provides comprehensive full-text search capabilities for all captured activities, giving administrators full visibility into all aspects of every session and helping them quickly pinpoint the specific actions that led to a policy violation. There is a basic support for investigation workflows so that multiple experts can work on the same incident, collaborating with comments and other findings. For more advanced usage, integration with popular IT ticketing systems is supported. In fact, integration with ticketing systems goes beyond investigation: users that want to access a sensitive resource may be required to provide a valid ticket number to ensure that they have appropriate authorization.

ObserveIT's reporting capabilities are quite rich as well. The solution provides a library of preconfigured report templates, as well as a possibility to create customized reports for various aspects: from detected threats and user activities to application usage and trend analysis to compliance audits and executive summaries. Built-in privacy protection ensures that the solution remains compliant with such frameworks as HIPAA and GDPR. Overall, even with the broad range of sensitive metadata collected from user sessions, ObserveIT can guarantee that its usage adheres to the strictest compliance regulations in every industry while helping to detect compliance violations much quicker than traditional tools.

3 Strengths and Challenges

ObserveIT Insider Threat Management is a platform that combines the functionality of traditional User Behavior Analytics (UBA) and Data Loss Prevention (DLP) products in a lightweight and streamlined solution for detecting and mitigating various insider threats, which is easy to deploy and difficult to bypass. The company's detection technology based on a curated library of known insider threat indicators offers a strong contrast to most other UBA solutions on the market, which utilize statistical methods to detect anomalies in user behavior. This design choice has both clear advantages (much lower "noise level", a broad range of automated mitigation actions) and obvious drawbacks (the solution will not detect a "zero-day anomaly" not known to the ObserveIT researchers yet). The latter is to a certain extent offset by the amount of context data collected by the system as opposed to more traditional network-based products.

In the end, the ObserveIT Insider Threat Management platform can be recommended for evaluation to any company looking for a modern, easy and low-maintenance alternative to an outdated traditional DLP solution, especially to those without a strong internal IT security team.

Strengths	Challenges
● A unique approach based on a curated library of known insider threat indicators ● A broad range of supported device platforms, massive amounts of context data captured by agents ● Data-centric view of user activities tracks document movements across the enterprise ● Easy deployment, low maintenance, no training period required ● Comprehensive privacy controls built-in	● Requires agent deployment on every monitored workstation or server ● By design, does not detect anomalies unknown to the company researchers ● No file hash capture yet; can limit DLP functionality

4 Copyright

The Future of Information Security – Today

KuppingerCole supports IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst company, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global Analyst Company headquartered in Europe focusing on Information Security and Identity and Access Management (IAM). KuppingerCole stands for expertise, thought leadership, outstanding practical relevance, and a vendor-neutral view on the information security market segments, covering all relevant aspects like: Identity and Access Management (IAM), Governance & Auditing Tools, Cloud and Virtualization Security, Information Protection, Mobile as well as Software Security, System and Network Security, Security Monitoring, Analytics & Reporting, Governance, and Organization & Policies.

For further information, please contact **clients@kuppingercole.com**

KuppingerCole Analysts AG
Wilhelmstraße 20-22
65185 Wiesbaden | Germany

Phone +49 (211) 23 70 77 – 0
Fax +49 (211) 23 70 77 – 11
www.kuppingercole.com