
Fact or Fiction:
Which Cybersecurity Tools Really Address Insider Threat?
observe it

Fact or Fiction: Which Cybersecurity Tools Really Address Insider Threat?

Contrary to the hopes and dreams of cybersecurity professionals everywhere, there is no "magic fix" for the insider threat problem, which can cost an organization upwards of **$8.76 million on average**, over a 12-month period.

Much like establishing and managing your personal health, Insider Threat Management takes a bit more work to be truly successful.

Addressing insider threats requires a more holistic and strategic approach, with a concentrated focus on the people, process, and technology that can help an organization: set (and understand) cybersecurity policy expectations, deliver visibility into potentially risky activity, and enforce policies in a consistent and transparent manner. For example, key components of an effective Insider Threat Management strategy should involve assembling a dedicated insider threat team, evaluating risk, and creating a business plan and processes.

With that said, choosing the right Insider Threat Management technology can help cybersecurity teams get the visibility they need to effectively detect, investigate, and prevent potential insider threat incidents.

These tools should help teams:

Enforce cybersecurity policy

Detect anomalous or risky user activity

Coach cybersecurity best-practices

Monitor system, file, and data access (for employees, and third-party vendors)

Rapidly investigate potential insider threat incidents with user session data

Safeguard user privacy with data anonymization

In recent years, usage of tools such as Data Loss Prevention (DLP), Privileged Access Management (PAM), User Activity Monitoring (UAM), Secure Information and Event Management Systems (SIEM), and User Behavior Analytics (UBA) software, among many others, have become common for security teams. Despite these robust technologies, major blind spots still remain–particularly when it comes to Insider Threat Management. Let's take a closer look at the strengths and weaknesses of five popular cybersecurity solutions that claim to address insider threats...

Data Loss Prevention (DLP)

For years, Data Loss Prevention (DLP) software has been the first line of defense against files and data illegitimately leaving an organization's control. It accomplishes this through classification and tracking of individual files – not through how a file (or data) is leveraged by users.

Despite this fact, some DLP software vendors claim to help manage insider threats, which is a user activity-based problem. **And therein lies the problem with DLP as an Insider Threat Management tool: data doesn't move itself. People move data!**

What DLP Promises

DLP software is typically set up by an organization to detect data use policy violations, and prevent data loss (i.e., "data leaks").

The implementation involves an extensive data discovery and classification process established to find, categorize, and understand sensitive data. These settings must be managed on an ongoing basis as needs change, requiring teams to fine-tune their policy rules to ensure that the sources and definitions around sensitive data are properly updated.

DLP software is intended to address data loss across multiple channels, including:

- Email
- Endpoint
- Web
- Network
- Cloud

The Reality of DLP

While DLP tools sound great in theory, most real-world implementations have severe limitations.

First, setting up data classifications and applying them to policy can be difficult and time consuming. (And not all teams have the bandwidth or resources to do it properly!) The initial setup is often laborious, with plenty of room for error in terms of tracking all of the possible sources for data exfiltration, manipulation, and misuse. As time goes on, maintaining these classifications and rules can be equally challenging.

For example, some users may know DLP is in place and take steps to get around the policy, find holes, or utilize cloud technology or external devices that aren't being monitored by the system. In the case of the infamous Edward Snowden insider threat incident, Snowden knew he was being monitored on the job, but used CDs to download and exfiltrate data (which were not being watched by the DLP software).

On the opposite end of the spectrum, DLP systems have the potential to be disruptive to business, impeding the productivity of C-suite executives and their employees by slowing down the performance of their systems, and force them to jump through hoops just to complete work.

If the required technologies are constantly reported and blocked for inaccurate policy violations, it can be difficult and frustrating to maintain productivity in the organization. In addition, relying on end-users to properly tag documents may lead to incorrect assessment or tagging, or intentional mis-tagging of documents to maintain authorized use freedom, defeating the purpose of the DLP tool. DLP agents (software residing on the endpoint) have been proven to dramatically slow down systems, frustrating users, and in some cases forcing them to discover workarounds that may include using unauthorized devices to complete work.

Privileged Access Management (PAM)

The role of Privileged Access Management (PAM) software is to understand who has access to specific systems and applications at any given time. PAM software accomplishes this by provisioning and deprovisioning user identities, using password vaulting and access management for critical systems and applications.

What PAM Promises

PAM software is focused on privileged users, or people with high-level credentials to servers, applications, and other areas of an organization's private networks.

Oftentimes a PAM software solution will include the following components:

Password Vaulting

These systems can be used to generate temporary credentials to a system, without the end-user being required to memorize lengthy, complex passwords. Vaulting helps to prevent individual passwords from being easily discovered or cracked.

Session Management

PAM software can help track individual user sessions, to visually ensure that their actions are well within an organization's cybersecurity policy.

Access Management

An access manager can act as a point of entry to a system or network, where a user can request access to perform tasks. Super admins (a.k.a. Privileged Users) can control who has access to specific areas of a system or network.

The Reality of PAM

Unfortunately, many PAM solutions inaccurately or imprecisely define privileged users, which can lead to increased risk. For example, they may define sysadmins and executives as the sole owners of privileged access when, in fact, there are many more people who are responsible for (or are capable of) handling sensitive data. These people may include third-party contractors and vendors, as well as employees.

The primary challenge with privileged access management, however, is that users tend to acquire (and require) increased access privileges over time, and these increases need to be periodically assessed. Of course, that requires additional time and resources to accomplish, making this issue a significant problem for organizations.

Organizations need to regularly evaluate access requirements and issues by employing the principle of least privilege (in other words, only granting access employees need, for the exact time period they need it)– that way, there's less margin for error when it comes to detecting potential insider threats.

User Activity Monitoring (UAM)

User activity monitoring (UAM) tools are user-centric rather than data-centric. Unlike DLP solutions that manage data activity, UAM does not limit or reject any action. Instead, user behavior is monitored for policy compliance, and suspicious trends are extracted and analyzed on a case-by-case basis.

What UAM Promises

UAM software looks at what users are doing on any given endpoint, helping cybersecurity teams answer questions such as:

- How are users working with files?
- Are they moving files or folders?
- What are the user's application privileges?
- Do users have access (or are they granting access) to files they shouldn't?

UAM also provides the cybersecurity team or investigator with the ability to understand the context of an incident through session recordings and visual capture.

For example, a typical insider threat behavior of a user who is about to exfiltrate data is moving files around systems, or assigning different names to a file or folder and moving it around the system or local machine. UAM can help create a forensic evidence trail for suspicious user behavior, helping the cybersecurity team identify exactly how the insider threat was violating policy.

The Reality of UAM

One downside to UAM is its primary focus on the endpoint versus network-level data, which can exclude certain types of insider threats. For example, some sophisticated insider threat attacks use methods including DNS tunneling to encode and exfiltrate data over a network – and may remain undetected by endpoint-only security solutions.

Another known downside involves UAM tools' relatively reactive approach to identifying insider threats after the user activity has already occurred. Organizations must detect and prevent insider threat incidents before they become a big, costly problem.

User Behavior Analytics (UBA)

Many organizations that look to set up an Insider Threat Management program for the first time (remember: holistic approach including people, process, and technology) believe that **understanding user behavior is the key to discovering intent**. This makes the predictive nature of User Behavior Analytics (UBA) tools particularly appealing, because they promise to identify potential insider threats or problems before they happen, based on previous behaviors.

In other words, UBA, like UAM software, promises to be useful for detecting user behaviors thought to be outside the norm of an organization's cybersecurity policies.

What UBA Promises

UBA technologies use machine learning to group users together to try to find outliers, helping cybersecurity teams create a list of users to monitor.

This technology brings in log data sets from endpoints, networks, hosts, and cloud environments, and often works by leveraging a SIEM data store, as opposed to direct telemetry. Since UBA uses machine learning, it is not tied to the data (or data activity) itself or the value of the data like a DLP solution.

The Reality of UBA

While the concepts of machine learning and artificial intelligence are hot and buzzworthy, these technologies are not yet advanced enough to accurately detect and ultimately prevent insider threat incidents from occurring.

They are also incapable of providing any action outside of an alert when an insider threat risk has been detected, making it difficult to stop further damage.

Security Information and Event Management System (SIEM)

Security Information and Event Management Systems (SIEMs) are typically the heart of any Secure Operations Center (SOC). These tools are used for everything from log ingestion and log archiving, to the de-facto regulatory system for certification and audit controls in a compliance program.

Some SIEMs are set up with event-based alerting, and are used as the primary technology for acting on potential cybersecurity threats within a SOC.

What SIEMs Promise

In some cases, SIEMs are used to reveal similar data to user behavior analytics (UBA) tools, but require extensive rule sets and tuning in order to get comparable information – involving a time-consuming setup process.

If cybersecurity teams are willing to make this significant up-front investment, SIEMs can provide a lot of value to an organization, particularly based on analysis of the sheer volume of log data that's being ingested from sources across the organization.

The Reality of SIEMs

With that said, the reality is that monitoring for insider threats can be difficult with a SIEM, as log data access is usually more focused on forensics, than real-time "in-the-moment" user activity.

Another downside is that SIEMs are typically focused on spotting external threats, not insider threats. These tools are deployed at the edge of a network, which means they usually aren't taking in log data from employee applications, databases, and more. As such, it can take a lot of manual work to set up a SIEM system that's purpose-built for insider threats, and log ingestion is a fairly extensive process.

Effective Insider Threat Management

Whether caused unintentionally or maliciously, **insider threat incidents can cost organizations an average of $8.76 million per incident, per year**, according to independent research performed by The Ponemon Institute. As such, selecting the right Insider Threat Management solution is critical.

When evaluating technologies to detect and minimize insider threat risks, consider these three critical building blocks:

Detection
(User Activity Monitoring, Third-Party User Activity Monitoring, File Activity Monitoring)

Investigation
(Rich Metadata, Video Session Recordings)

Prevention
(Real-time Alerting, User Coaching)

It is important to note that the cybersecurity tools previously mentioned that claim to help teams manage insider threats are capable of some of these highlighted elements, but not all of them.

ObserveIT is the only true Insider Threat Management solution capable of providing teams with a comprehensive method of detecting, investigating, and preventing insider threat incidents, whether they are of accidental or malicious intent. ObserveIT also fits into a more holistic and comprehensive strategy for effective Insider Threat Management, which focuses on a solid balance of People, Process, and Technology to combat potential threats.

People

- Insider threat detection and prevention is a team sport. Ensure the right groups and stakeholders are involved in your secure operations center.
- Limit user access to non-essential data, or attempt to limit the duration of time privileged users can access the information needed to complete a task.
- Look for **leading behavioral indicators** to uncover a potentially malicious insider threat.

Process

- Evaluate your organization's risk and develop a dedicated insider threat function in your organization, especially if your data is particularly sensitive or valuable.
- Establish consistent, repeatable processes that are fair to all employees, using technology to enable and support these processes.
- Invest in training for users, empowering them in areas such as secure data handling, security awareness, and vigilance.

Technology

- Consider the performance impact, as well as ease of management, deployment, stability, and flexibility of any insider threat solution.
- Choose a solution that can scale with the organization as it grows.
- Keep in mind a vendor's expertise on insider threat vs. external detection and prevention.
- Determine if your solution gives you visibility into what your users are doing, particularly privileged users.

ObserveIT helps organizations leverage both user and file activity data, as well as robust analytics, to detect, investigate, and prevent insider threats.

As a result, organizations can save time and money, and – perhaps most importantly – preserve their reputation by avoiding cybersecurity incidents.

To learn more, **try it free** today.

https://www.observeit.com/

observe it