INSIDER THREAT SOLUTION BUYER'S GUIDE

How to measure and evaluate the complex landscape of insider threat solutions and build an effective insider threat program that enhances the whole enterprise.

INTRODUCTION

IDENTIFYING AND CONFRONTING THE INSIDER THREAT

Every day, organizations struggle to develop an effective approach to fighting insider threats. In this world of rapid innovation and distributed enterprises, there is a seemingly infinite number of variables and risk factors to account for within an organization. And even for those who believe they have a comprehensive insider threat defense established, changes in technology and public discourse are forcing a complete reexamination of their security strategies.

Introducing another layer of complexity is the fact that 'insider threats' are actually a much broader category than many people realize. And while it may sound obvious, the first step in effectively detecting and mitigating these types of threats is fully understanding them.

They can be broken down into three distinct types:

- **Malicious Insiders** - These are the "traditional" insider threat as most people define them. These are users who intentionally hurt the organization, whether that be through data theft or by sabotage.
- **Negligent Insiders** - These are employees that unintentionally put security at risk. While often overlooked, these threats are actually the most common - driving more than 60% of insider-related security incidents.
- **Credential Thieves** - These are outside infiltrators that enter the organization through a user account. While these are technically external threats, they're doing damage from within the organization and catching them is a matter of understanding insider user behavior.

Once security teams recognize the diverse, widely varied nature of insider threats, the challenges of creating an effective insider threat management strategy quickly snap into focus. After all, it's easy -- or at least, easier -- to develop a protection plan against one highly specific type of scenario, such as the stereotypical rogue employee in a black hoodie stealing IP from a darkened office building. That task becomes more complicated if the stereotypical insider may actually be a naive employee accidentally downloading malware from a phishing email and letting an outside infiltrator into the network, or a disgruntled user quietly renaming and downloading files over a personal mobile hotspot to take to a competitor.

Many tools claim to "solve" the insider threat problem. But, what insider threats are they referring to? Do they really have the necessary capabilities to protect your data?

Compounding these challenges is a complex and ever-changing landscape of vendors - fraught with ambiguous or unsubstantiated claims, false promises, and misinformation. Many tools claim to "solve" the insider threat problem. But, what insider threats are they referring to? Do they really have the necessary capabilities to protect your data? And what do you have to sacrifice in order to do so?

KEY REQUIREMENTS

While buyers searching for an insider threat solution need to be wary, it is entirely possible to build an insider threat defense that's just as advanced as the technology, people, and data it needs to protect. The key is choosing a purpose-built solution, developed from the ground up with a specific goal in mind: shining a light on insider threats.

In order to find a purpose-built solution, however, there must be a clear understanding of the elements that comprise one. The answer lies in these five keystones:

VISIBILITY

In order to find and mitigate insider threats, security teams need to have the ability to quickly see potential red flags as they arise. This requires complete visibility into what is happening across an entire organization at any given moment. And because all users are equally capable of putting a business at risk, the same level of visibility can and should be consistently applied - regardless of role, location, or designation of privilege.

All users are capable of putting the organization at risk, so an effective insider threat program begins with enterprise-wide, real-time visibility.

Furthermore, real-time visibility is no longer optional. Specific industries are being forced to learn this now -- financial services organizations, for example, now must contend with real-time messaging systems like SWIFT -- but it's something that all industries will need to integrate into their security strategies.

QUESTIONS TO ASK:

- ***What will I be able to see? How quickly will I be able to get answers to questions like:***
    - ***Who touched a given file in the last 24 hours?***
    - ***How many files have left the organization in the last 24 hours? And how did they get out?***
    - ***Which individuals are logging into system admin accounts?***
    - ***What files have recent 'joiners' brought into my system?***

  Purpose-built solutions should be able to provide answers to these types of questions quickly, and provide necessary context around them.

- ***Where does this solution pull its data from?*** - The only way to understand what exactly you'll have visibility into is to understand where exactly the solution is pulling data from - whether it be other systems and log file repositories, or directly from the endpoint or user.

- ***What type of data does this solution collect?*** - Some insider threat solutions collect metadata, some collect content data (like screenshots or keylogging), some collect log data, and some don't collect any data at all. In order to catch insider threats, a solution needs to be collecting user behavior data from the endpoint.

- *Does this solution provide visibility both on and off of the corporate network?* Nearly every modern workplace has some degree of remote workforce, which means that your visibility can't just stop once a company laptop leaves your headquarters.

INTELLIGENCE

"Intelligence" can be a vague and overused term in the cybersecurity world, but it has a very specific and important meaning: the powerful combination of context, knowledge, and flexibility. And an intelligence-driven approach to insider threat management means decisions are made based on actionable insights, not just a high volume of data.

Insider threats can come in so many different forms. Security teams cannot afford to be paralyzed by information or bogged down in manual analysis. They need to quickly know what slips through the cracks. They need to know exactly where their most vulnerable data is, and how users interact with it. And most importantly, they need to be able to understand these things without picking through an overwhelming amount of data.

QUESTIONS TO ASK

- *Is this a rules-based or analytics-based solution?* - Insider threats are, by definition, human -- and human behavior is too intricate to be boiled down to a series of written rules or policies. Analytics are necessary to understand and detect anomalies in events and behav,iors. In order to be most effective, a tool needs to be smart enough to truly learn what's normal or abnormal, and adapt as needed (which means that it needs to employ some form of machine learning).

- *Does this solution understand and provide context around an activity / event?* - Context is critical, both when it comes to triaging alerts and when it comes to forensic investigations. This means a solution needs to offer human-readable, easily accessible context that answers the important questions: the "who," "what," "where," "when," and "how."

- *Does this solution prioritize alerts? On what basis?* - Analysts aren't able to fight threats if they're buried beneath noise. Alerts should be answers, not a continuous loop of false positives. It's critical to understand what a solution does in order to cut down on noise and enable swift action.

SCALABILITY

If there's one thing that continually proves itself to be true, it's that there is no single type of "high-risk" user. Any insider has the ability - intentionally or unintentionally - to put an organization at risk. So, an effective insider threat tool must be scalable enough to be deployed enterprise-wide and fully function across the company's environment. If it significantly impacts network performance, or hinders user productivity in such a way that it is constantly being disabled or worked around, then the tool isn't really protecting the user or the organization.

QUESTIONS TO ASK:

- ***Can this tool be deployed across the entire organization? What is the impact on a network? On user productivity?*** - The only truly scalable solutions are those that have a near-zero impact on network, system and user performance. Be wary of tools that generate excessive amounts of data, as the heavy footprint associated with that kind of data collection is likely to hinder scalability and usability. The same goes for tools that advise you to only deploy to selected users or disable core features in order to make enterprise-wide scalability manageable.

- ***How many people does managing this solution require? Will it require additional dedicated manpower?*** **-** A sustainable solution needs to have a high enough signal-to-noise ratio that it doesn't require excessive man hours to manage alerts or tuning. Your chosen solution should be tailored to the available staff and expertise you have on hand, instead of requiring you to hire additional team members.

- ***Is this solution able to support / adapt to cloud environments?*** - In order to support today's most forward-thinking organizations, a tool needs to be capable of adapting to modern security architectures and frameworks – which means it need to clearly demonstrate flexibility, agility, and the ability to support automation requirements.

- ***Does it provide performance metrics?*** - This should go without saying, but numbers speak louder than any sales pitch.

AGILITY

Modern threats move quickly, so organizations need to be able to pivot just as quickly if they hope to keep up. This also means that security measures - and insider threat tools - need to be agile enough to adapt to changing priorities and conditions if they hope to be effective.

It's only realistic to expect that any solution or tool - especially one that is analytics-based - will require some time to tune and customize. But, being stuck in an endless loop of tuning and configuration means that tool isn't providing enough value or delivering return on investment.

Modern threats move quickly. Organizations need the ability to pivot just as easily, and understand activity in real-time.

QUESTIONS TO ASK:

- ***Does this solution require tuning before it starts to show value? If so, how much?*** - While it's inevitable that some tools require some degree of tuning before they provide actionable insights, find out exactly how long that tuning will take and what value you'll see -- if any -- in the interim. Look for a tool that provides value while it continuously tunes, instead of one that traps you in a perpetual tuning cycle.

- ***Is this solution capable of learning or self-tuning, or does it rely completely on manual tuning?*** **-** For a solution to generate continued value, it needs to incorporate advanced analytics and machine learning capabilities, which in turn make it capable of self-tuning. If it relies only on known and available information, without seeking out additional context or intelligence, there will inevitably be things that fall through the cracks.

- ***How frequently is data uploaded and processed? How long does it take for an alert to process after an activity?*** - Some products only upload data a few times a day, meaning that visibility and alerts are far from real time. And in some cases, analytics may take hours to run, which means alerts and insights are always far behind the activity or event that occurred. Modern enterprises need a solution that processes data in real-time or, near real-time, in order to proactively defend against threats.

- ***What happens if our organization needs to change priorities or focus?*** Be wary of products that require lengthy re-tuning if you choose to re-prioritize. Most security teams will inevitably need to adjust threat criteria, so your chosen solution should allow you to change priorities (such as alert criteria) quickly and easily.

PRIVACY

Employee privacy has become a topic of increased interest and scrutiny for both governments and enterprises - and should be given strong consideration when building an insider threat program. Here's why:

Increasing Regulations: Organizations in the EU - as well as any doing business there - must comply with the requirements of the General Data Protection Regulation (GDPR) legislation. Other countries have even stricter privacy laws that dictate what kinds of information organizations can collect about their users and employees, how they can use it, and how they can store it. With digital privacy becoming such a high-profile conversation topic, it's impossible to believe that there won't be more legislation on the way.

Public Opinion: In the last year, highly-public discussions about data and privacy have sprung up seemingly everywhere - largely stemming from news (and controversy) surrounding Facebook and similar technology providers. In general, people are more aware and have stronger opinions about how their behavior is collected and used.

In a survey conducted in conjunction with Harris Poll, we found that most people - 64% - do believe that it is acceptable for organizations to monitor user activity... but only if that monitoring is conducted with transparency.

Company Culture: Creating a culture of intense surveillance and treating every employee as a subject of distrust is likely to seriously hurt employee morale. And it can backfire in very tangible ways that go beyond moral responsibility.

QUESTIONS TO ASK:

- ***Does this solution have core privacy-conscious features and capabilities?*** - A sophisticated insider threat solution should take advantage of privacy-related innovation such as data anonymization, which can keep a user's identity hidden and behavioral data protected until suspicious activity is detected. These capabilities not only help alleviate employee privacy concerns, but also provide a layer of protection at a time when behavioral data is increasingly considered sensitive, personally identifiable information.
- ***Does this tool provide the ability to anonymize data?*** - Anonymization is a mandatory requirement for global organizations because it helps with compliance on GDPR and other privacy laws. Outside of GDPR, it can also reduce liability and put employee morale at ease. Specifically, look for a solution that anonymizes data from the server, not within the UI, and that allows for de-anonymization by only a strictly-controlled set of keyholders.
- ***Can this tool be deployed in a GDPR compliant manner? Would that entail any special changes to the functionality or deployment?*** - Any company that does business in the EU must select tools that can be deployed in a GDPR-compliant manner. This means the tool must have been constructed with a core focus on the principles of 'Privacy by Design' or 'Data Protection by Design and by Default.' Any tool that requires extensive changes in order to be deployed under GDPR is a risk and potential red flag.

The same poll revealed that 70% of employees would consider leaving their jobs if they found out that their employer was monitoring them without their knowledge or consent.

INSIDER THREAT SOLUTION LANDSCAPE

A variety of solution categories aim to solve the insider threat problem. This is a general overview of the strengths, weaknesses, and prime considerations of what are considered to be the most prominent ones.

***Note: The information included below is meant to reflect the majority within these categories, and specific products within each can certainly deviate from the generalizations.*

SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

SIEM tools collect and aggregate log data from existing IT infrastructure - including security controls, systems, and applications - for analysis. Their intention is to provide visibility into what's happening within the organization by utilizing data already being produced, and then applying a variety of methods to draw insights out of that data.

VISIBILITY 🟡

- Because SIEM tools acquire and ingest data from other data sources, the degree of visibility provided can vary significantly based on what types of data are available.
- Most support nearly all commonly-used log sources, while some support integrations to draw from a more complete set of data sources or the ability to collect additional event data via agent deployment.

INTELLIGENCE 🟠

- SIEM tools employ a rule-based model - relying on human analysts to guide them on how to parse, process, and alert on data, as well as for examination and analysis.
- Because these tools rely on static correlation to identify insider threats, most are unable to detect unknown threats, complex attacks, or lateral movement.
- Some - often branded "next-gen SIEM" - do offer more advanced analytics, threat intelligence, or reporting capabilities to improve tool performance and accuracy. But, most SIEM solutions rely on the addition of UEBA to derive the insights needed to detect insider threats.

SCALABILITY 🟠

- Legacy SIEM tools typically require a significant initial investment in hardware and in resources / expertise.
- Because many use a volume or event-based pricing model, this means ongoing costs may increase as the amount of data ingested or aggregated increases - though some new tools hitting the market do offer unlimited or user-based pricing models.

SCORECARD:

🟡 **Visibility**

🟠 **Intelligence**

🟠 **Scalability**

🟠 **Agility**

🟡 **Privacy**

LEGEND:

🔴 *Does not fulfill requirement*

🟠 *Mostly does not fulfill requirement*

🟡 *Partially fulfills requirement*

🟢 *Mostly fulfills requirement*

🟢 *Fully fulfills requirement*

- This also means that, due to budget restraints, some organizations are forced to limit their use of the tool or are prohibited from expanding visibility as more potentially valuable data sources become available.

AGILITY 🟠

- SIEM tools, in general, do process data and fire alerts in near real time - but there may be a latency period because they are working to reverse engineer insights from existing data.
- There is typically a need for significant analyst resources or manpower for ongoing maintenance, notably updating written rules and manual tuning.
- SIEM solutions collect data that tends to be prohibitively noisy, meaning that teams often need to sink many man hours into weeding out false positives.

PRIVACY 🟡

- Because SIEM tools primarily leverage existing data sources versus collect data themselves, the amount of personal or sensitive information is dependent on what is contained within those log files / data sources.
- Most SIEM tools do not currently offer a mechanism to mask or anonymize personal or sensitive data.

USER BEHAVIOR ANALYTICS / USER & ENTITY BEHAVIOR ANALYTICS (UBA / UEBA)

UBA / UEBA solutions apply behavioral analytics to IT infrastructure data being generated and aggregated. Often deployed to strengthen existing SIEM solutions, these tools aim to draw more adaptive conclusions about human behavior to pinpoint potential insider threats.

VISIBILITY 🟠

- Because UBA / UEBA tools ingest and analyze existing system data, their level of visibility is dependent on the quality and amount of behavioral data made available to them.

INTELLIGENCE 🟢

- UBA / UEBA tools have played a critical role in acknowledging that human behavior is fluid and pioneering the application of machine learning and analytics to provide insights into user behavior.
- These tools apply behavioral models, analytics and machine learning algorithms to establish a baseline of normal user and/or machine behavior and detect abnormalities.

SCORECARD:

🟠 **Visibility**

🟢 **Intelligence**

🟠 **Scalability**

🟡 **Agility**

🟡 **Privacy**

SCALABILITY 🟠

- UBA / UEBA tools - like SIEM - rely on system logs that typically generate a staggering amount of data and leave a heavy footprint that's likely to hinder network performance.
- As these tools increasingly get wrapped into more complete solutions like "next-gen SIEM" tools, leading industry analyst firms predict that the standalone UEBA market may be on the cusp of disappearance.

AGILITY 🟡

- Many UBA / UEBA tools require a significant amount of time for deployment and tuning - meaning it may take weeks or months to establish baselines and begin to see value, and any re-tuning needed is likely to be resource-intensive.
- They also use risk-scoring, versus strictly transactional alerts, to attempt to minimize the number of false positives and noise generated.

PRIVACY 🟡

- UBA / UEBA tools were largely built on the premise that system data could be used to understand user behavior without having to monitor excessively or invade privacy.
- In building a comprehensive risk profile, however, they may include sensitive or identifying information - such as identity and employment data; IT activity, violations and access logs; and phone, email, or chat records - without a mechanism to mask or anonymize that information.

ENDPOINT DATA LOSS PREVENTION (DLP)

Endpoint Data Loss Prevention tools (or DLP) are the iron chain of the insider threat prevention landscape. Endpoint DLP largely intends to fight data theft by controlling how users interact with machines and data - blocking avenues of exfiltration, stopping employees from doing things like accessing certain files, using certain methods of file sharing, and utilizing certain applications.

VISIBILITY 🔴

- Endpoint DLP solutions aim to provide control rather than visibility, with the goal of stopping specific activities or events from happening. What is allowed or disallowed is usually managed through a set of written rules.
- These tools typically need to be paired with an additional form of visibility that's able to see both on and off network activity in order to comprise a truly effective solution.

SCORECARD:

🔴 **Visibility**

🟠 **Intelligence**

🔴 **Scalability**

🟠 **Agility**

🔴 **Privacy**

INTELLIGENCE 🟠

- Endpoint DLP tools decide what is allowed or disallowed through a set of manually-defined, written rules - which are not guaranteed to catch every type of data theft.

SCALABILITY 🔴

- Endpoint DLP tools require a huge amount of configuration and management in order to develop and maintain the number of rules needed to stop risky behavior or activities.

AGILITY 🟠

- Endpoint DLP tools also tend to require significant, manual re-tuning - again due to the sheer number of rules that need to be managed and consistently updated.

PRIVACY 🔴

- Because Endpoint DLP tools read the contents of files, websites, and emails in order to determine if an activity is allowed based on rules and policies, they may see and/or capture personal, confidential information.
- Some more advanced versions enable policies or rules to be set based on what network a user is connected to - such as corporate versus home.

EMPLOYEE / USER ACTIVITY MONITORING (UAM)

Employee or user activity monitoring (UAM) software does exactly what it claims: it tracks employee behavior, usually via an endpoint agent. These tools typically capture data such as screenshots, video, and keylogs to monitor user activity and will often include a rule-based alerting system.

VISIBILITY 🟢

- Employee monitoring tools claim to stop insider threats by being an "all seeing eye", providing complete visibility that then provides security and assurance that employees are not jeopardizing the organization.

INTELLIGENCE 🟠

- Analysis methods vary from tool to tool, but most employee monitoring solutions alert based on a series of predefined rules.
- Rules produce an excessive amount of information or alerts as a result - which require manual triage / analysis by already-stretched security analysts and teams.

SCALABILITY 🔴

- Because employee monitoring tools collect such heavy data, their endpoint agents have significant performance impact - leading many organizations to only deploy them over a small number of high risk users.

SCORECARD:

🟢 **Visibility**

🟠 **Intelligence**

🔴 **Scalability**

🔴 **Agility**

🔴 **Privacy**

AGILITY 🔴

- Rules produce an excessive amount of information and alerts, which require time-consuming manual triage and analysis by already-stretched security analysts.

PRIVACY 🔴

- Traditional employee monitoring tools are not consistent with a privacy-first approach, and are nearly un-deployable in countries that have strict privacy laws (such as the EU countries, with the advent of GDPR).
- Videos, screenshots and keylogging are invasive measures that are impossible to anonymize. Not only do these measures make it difficult to adhere to privacy regulations, they also can have a negative effect on employee culture.

ENTERPRISE USER INTELLIGENCE

Enterprise User Intelligence (EUI) delivers privacy-conscious endpoint visibility, enriched with contextual understanding and powered by advanced analytics - with a core, specific focus on protecting organizations against insider threats.

SCORECARD:

- 🟢 **Visibility**
- 🟢 **Intelligence**
- 🟡 **Scalability**
- 🟡 **Agility**
- 🟢 **Privacy**

VISIBILITY 🟢

- EUI delivers real-time visibility into all user activities and behaviors, directly from the endpoint.

INTELLIGENCE 🟢

- EUI generates a baseline understanding of 'normal' behavior for each individual user - which is then used to more quickly and accurately detect anomalies.
- When advanced analytics are combined with machine learning models, it becomes possible to measure a user's behavior against a variety of conditions to proactively alert on potentially suspicious behavior. Correlating seemingly unrelated behaviors also makes it possible to catch complex threats like credential theft.

SCALABILITY 🟡

- EUI records extremely lightweight user behavior metadata directly from the endpoint, so there's minimal impact to network performance and user productivity.

AGILITY 🟡

- Because EUI tools apply a contextual understanding to behaviors and events, alerts are analyzed, prioritized, and delivered near real-time - so security teams are receiving actionable intelligence, rather than excessive alerts or false positives.

- User behavior data is parsed through advanced behavioral models, which minimizes the need for manual fine-tuning and speeds time-to-value.

PRIVACY ●

- The most advanced EUI tools include anonymization capabilities that can be used to strip data of all identifying user information at the point

CONCLUSION

With investments in intelligent, behavior-based solutions - that prioritize actionable visibility, scalability, agility, and privacy - organizations can stop insider threats while enabling their greatest assets (their employees) to remain their greatest assets. Security does not need to come at the expense of users or the rest of the organization. And it's entirely possible to build an insider threat program, from the ground up, to support the business as a whole... not stifle it.

LEARN MORE ABOUT DTEX AND ENTERPRISE USER INTELLIGENCE

Dtex's Enterprise User Intelligence Platform is purpose-built to provide intelligent, scalable, real-time, and privacy-conscious user insights. Dtex provides the visibility that you need in order to catch insider threats, utilizes machine learning to pinpoint critical insights, and prioritizes answers with alert stacking and intuitive risk scoring.

Learn more at www.dtexsystems.com.