Buyer's Guide to Insider Threat Management Solutions

This buyer's guide highlights the most important capabilities of an insider threat management (ITM) solution. It sums up what Proofpoint has learned building successful ITM programmes for organisations of all sizes around the globe and across all verticals. It's meant to be a reference guide for readers who are just starting out on their ITM journey or who are updating their existing ITM solution.

Begin with human-centric security

To defend data against insider threats, you need a solution that supports a human-centric security model. A human-centric security model provides complete visibility into users' risky behaviour and how users interact with sensitive data. This ensures you get important context about their intent when something they do seems harmful to the organisation, whether intentionally or unintentionally.

With a solution that takes a human-centric approach, you can quickly understand your insider risk based on behavioural indicators. When these indicators are looked at holistically, over time, and within the context of other activity, they can signal that a user might be causing harm to an organisation and may warrant more investigation to determine the most appropriate response.

Key elements of an ITM solution

If you want to stop insider threats, you need to be able to identify, protect, prevent, and respond to insider-led incidents. It's only when you do all this in a coordinated way with a proactive approach that you decrease your risks of insider threats.

Identify

You need a solution that provides visibility into risky behaviour before an insider threat occurs. You'll want to identify abnormal behavioural patterns based on a baseline. The solution should allow monitoring of risky users, such as users with privileged access, flight risks, departing employees, contractors, executives, and users under investigation. Stressors such as a change in job status (like termination or resignation), company changes (like a merger and acquisition or reorganisation) and concerning behaviours (like disgruntled acts or financial conflict) can also be taken into consideration when identifying risky users.

Each organisation should decide what prevention controls work best for them based on their business objectives, culture, and speed of innovation.

Protect

You will want a solution that helps protect sensitive data and systems with human-centric security controls. Policies and rules should be built with behavioural indicators to help protect against risky behaviour.

Preventing a user from accidentally or intentionally violating security policy with user education, real-time reminders and blocking is important. Not all activities can or should be blocked; it is a best practice that prevention should be balanced with user productivity. Each organisation should decide what prevention controls work best for them based on their business objectives, culture, and speed of innovation.

It is also important for an ITM solution to provide a flexible and easy way to manage access to user data. You'll want a solution that has access controls to ensure security analysts have visibility into data only on a need-to-know basis.

Detect

An ITM solution should provide real-time activities and alerts of user behaviour. Alerts of risky user activity can include:

- Hiding information
- Privilege elevation
- Bypassing security controls
- Data exfiltration
- Downloading unapproved software
- IT sabotage
- Creating a backdoor
- Unauthorised access
- Unacceptable use

When a rule is violated, the solution should capture the who, what, when, and where of a user's activity to provide detailed context and insights into behaviour and intentions. The solution should also capture screenshots to provide irrefutable evidence as part of investigations. It is important that an ITM solution has the flexibility to dynamically respond to risky behaviour and capture screenshots only after an alert is generated, helping to protect user privacy and enabling security analysts to work more efficiently.

Careless users are the leading cause of data loss and insider threats. They can be characterised as having good intentions but making bad decisions. However, their mistakes can have severe consequences.

Respond

It's important to investigate and respond to incidents quickly and efficiently. The longer an insider threat persists, the more damage it can do to your reputation and bottom line. Investigative workflows are critical to track the status of an incident, especially when it needs to be escalated to groups outside of Security like HR, Legal, Compliance and Privacy, which may need to be involved in an investigation. A robust ITM solution should also integrate with a centralised event management system like an SIEM that the security analyst team already works in.

3 Primary use cases

There are three primary types of insider threats. All of them are caused by people. A human-centric ITM solution must address:

- **Careless users.** These are people who are not careful and make mistakes.
- **Malicious users.** These are people who intend to cause harm.
- **Compromised users.** These are people whose credentials have been stolen by an external threat actor.

1: Careless users and common mistakes

Careless users are the leading cause of data loss and insider threats, according to the Proofpoint 2024 Data Loss Landscape report. These users can be characterised as having good intentions but making bad decisions. Often, they just want to get their work done as efficiently as possible. However, their mistakes can have severe consequences, such as business disruption, brand damage, a weakened competitive position, regulatory violations and fines, and lawsuits.

Here are some of the ways these users create risk:

- Sending emails to the wrong person, either with or without attachments
- Sharing sensitive data to GenAI sites
- Visiting phishing sites
- Installing unauthorised software
- Sharing sensitive files and data publicly
- Emailing personally identifiable information (PII) to a personal email account
- Saving sensitive corporate data to personal devices

Malicious users are dangerous because they're in the ideal position to take sensitive data and cause harm to an organisation. They are motivated by personal gain.

Protecting against careless behaviour

An effective ITM solution will detect and prevent risky activities. It will also provide careless users with coaching to help them understand what's wrong with their behaviour so that they can change it.

What to look for:

- **Classification.** Make sure that email, data, and content are consistently monitored both manually and with artificial intelligence (AI) to identify and classify risky users. Once a user is classified as high risk, the system will assign a risk score to protect data accordingly.
- **Monitoring.** The solution should monitor for risky behaviour and activity such as unauthorised application and web use, changing file names and types on sensitive documents, accessing data out the scope of their job, and exfiltrating a high volume of confidential documents. Monitoring high risk groups may identify users who need a deeper level of monitoring.
- **Prevention.** Users should be blocked from exfiltrating sensitive data from the endpoint. That includes misdirected emails with and without attachments, USB, web upload, cloud sync, network share, and print. If they make a mistake, they should receive a contextual warning message in-the-moment, allowing them to remediate and prevent the incident in real-time with no administrator input. When warranted, users can explain why they need access to it. This, in turn, will notify the security team, which can allow or deny that request.
- **Ongoing Education.** Careless users often aren't aware that their behaviour is risky. An ITM solution should provide end user education and training through notifications of risky behaviour and links to corporate policies.

2: Malicious users

Malicious users are dangerous because they're in the ideal position to take sensitive data and cause harm to an organisation. What's more, they are motivated by personal gain. Departing employees are one of the riskiest types of insiders but there are several other types.

The major types of malicious insider threats are:

- **Fraud.** This involves deception that causes corporate disruption
- **Sabotage.** This includes damage to a system or destruction of data
- **Theft.** This involves theft of any proprietary information that is valuable to an organisation
- **Espionage.** This involves the selling of valuable data, trade secrets and more to a competitor or adversary

A human-centric system will monitor some users more closely than others. And it will apply tighter security controls to the riskiest users.

What makes malicious insiders such a threat is that they are in a position of trust. As such, they can bide their time and use their privileged access to find valuable data and security weak spots. Plus, companies often create vulnerabilities by allowing employees to access and store data on their personal devices. This just makes it easier for employees to steal sensitive data and cause harm.

Protecting against malicious users

A human-centric system can monitor some users more closely than others. And it will apply tighter security controls to the riskiest users. Also, it will proactively block malicious actions based on risk factors, like when an employee resigns or is terminated.

What to look for:

- **Visibility.** Visibility across data activity and behaviour provides a holistic view and gives you contextualised insights into what a user is doing and their intentions. Telemetry of user interactions with data and systems should be collected – like when they rename a sensitive file or upload it to an unauthorised website or cloud sync folder. If a user downloads unauthorised applications, tampers with security controls, or installs a TOR browser, these risky activities should also be monitored. A contextualised timeline of events will help understand the "who, what, when, where" of user activity and provide insights into what a user was doing before and after an alert.
- **Threat Library.** You want a comprehensive threat library of alerts for the most common insider threat use cases (such as time fraud, data exfiltration, bypassing security controls). This will ensure you can get up and running quickly with rules for the most common behavioural indicators.
- **Investigations.** You want a solution that provides detailed metadata and screenshots of user activities that can provide forensics evidence in investigations. Collaborative workflows are important to manage insider incidents. Since insider investigation involve stakeholders outside of security, such as HR, Legal, Privacy, and Compliance, you will want to share user risk reports in consumable and easy-to-read formats such as PDF reports.
- **Privacy controls.** A robust ITM solution includes features like attribute-based access controls, data masking and anonymisation, and multi-regional data centre support to meet data privacy and residency requirements and eliminate bias in investigations. You want to dynamically and flexibly change a user's monitoring policy in real-time if a user triggers an alert, thereby ensuring user privacy by only capturing screenshots when needed.

3: Compromised users

Compromised users may have their accounts taken over and misused by an external threat actor. Once their accounts are compromised, attackers have insider-level access to your data and systems. What makes compromised users so challenging is that threat actors may be lurking on internal systems for months until they are discovered.

External cyber attackers rely on exploiting human vulnerabilities. Social engineering, and in particular, phishing, is one of the most common ways that attackers lure users. This is no surprise given it has such a high success rate: 71% of organisations experienced a successful phishing attack.

Common phishing techniques include:

- Sending malicious links, malicious attachments and requests for data
- Smishing (SMS phishing)
- Social media phishing
- Telephone oriented attack delivery (TOAD) attack
- Business email compromise (BEC)
- Multi-factor authentication (MFA)

The end goal is the same: external threat actors want access to valuable data and systems to exploit for their benefit and financial gain.

Protecting against compromised users

An effective ITM solution will provide visibility and context to help understand if a user's behaviour is unusual. If a user is prone to clicking on phishing links, for example, you can monitor that risky user for any unusual behaviour. You can also protect data by ensuring that only those who have a need-to-know can see it.

What to look for:

- **Proactive monitoring.** By building and saving custom explorations your teams can regularly search for data exfiltration and risky activities. Very Attacked People (VAPs), who have a history of clicking on malicious links or attachments or interacting with vulnerable apps, can be monitored for unusual behaviour, potentially indicating a compromised user. The same approach can be used for other high-risk groups such as departing employees or users with privileged access. Since it is impossible to identify all risky insiders ahead of time, the ITM solution should be able to dynamically and flexibly change a user's monitoring policy in real-time if a user triggers an alert.
- **Adaptive access controls.** You can apply conditional access rules to data, like safe-listing and/or block-listing countries, networks or high-risk IP addresses. You can also limit sensitive data access to certain privileged users and groups and allow uploads and downloads only to managed devices. With attribute-based access control, you can address privacy requirements.
- **Integrations.** An effective ITM solution will extend your security system, helping provide context. That's because it will be easy to integrate with a variety of tools, including:
  - Security orchestration, automation and response (SOAR)
  - Security information and event management (SIEM)
  - Incident response
  - Ticket management systems
- **Modern architecture.** The benefit of a cloud-native platform is that it can scale for hundreds of thousands of users. An ITM solution should collect telemetry through a lightweight endpoint agent that does not impede user productivity or conflict with other solutions.

Conclusion

Protecting your organisation from insider risk, whether intentional or not, requires an ITM solution that enables a proactive approach. An ITM solution should have visibility into risky behaviour and the ability to dynamically and automatically respond. Given the cross-collaboration to support insider risk initiatives, an ITM solution should enable investigative workflows and gather irrefutable evidence such as screenshots to accelerate investigations. Lastly, an ITM solution should be able to scale with your business, leverage your existing investments, and provide flexible access and privacy controls to ensure compliance. Using an ITM solution with these required capabilities will help ensure your business is protected from insider risk while enabling your security team.

LEARN MORE

For more information, visit **proofpoint.com**.