Proofpoint Insider Threat Management

Take a people-centric approach to managing insider threats

Key Benefits

- Detect risky insider activity and prevent data loss from the endpoint
- Accelerate response to insider threats and data loss incidents
- Keep users productive and secure with a lightweight endpoint agent
- Speed time to value with a highly scalable SaaS deployment built on a modern cloud platform

Proofpoint Insider Threat Management is a people-centric SaaS solution that helps you protect sensitive data from insider threats and data loss at the endpoint. It combines context across content, behavior and threats to provide you with deep visibility into user activities.

Proofpoint Insider Threat Management (ITM) helps security teams tackle the challenges of detecting and preventing insider threats. It can streamline their responses to insider-led incidents and provide insights that help prevent further damage. The solution correlates user activity and sensitive data movement, enabling your teams to identify user risk, detect insider-led data breaches and accelerate investigations. It is built on the Information Protection and Cloud Security platform and belongs to the Information Protection family of products.

Gain Visibility and Context Into User Activity

Proofpoint ITM helps you understand the full context around user-driven incidents. Everyday users are low risk, so you might only need to monitor their interactions with data. However, you should monitor high-risk users more deeply—for example, executives or employees leaving the company—by also collecting information about their behavior, or user activity. Proofpoint ITM lets you monitor both everyday and risky users with a single, lightweight endpoint agent.

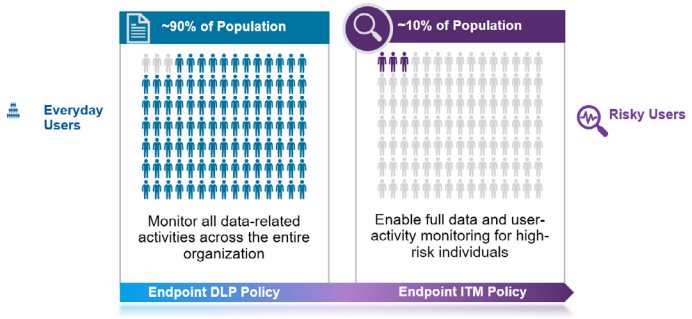

Figure 1: Monitor both everyday and risky users with a single lightweight agent.

Proofpoint ITM lets you build watch lists to monitor risky users. The lists can be based on criteria like a user's role and the data they interact with. They can also be based on the user's vulnerability to phishing and other social engineering factors. And they can take into account changes in employment status or other human resources and legal factors.

Detect and Prevent Risky User Behavior In Real Time

Proofpoint ITM lets you quickly build custom detection rules. You can tailor these rules to your policies for data loss, acceptable use and insider threats. The rules engine is flexible. It lets you optimize alerts for your environment based on user, data, app, endpoint, sensitivity of content, location and more.

Proofpoint ITM includes out-of-the-box libraries of alerts. They are easy to set up and provide fast time to value. They keep you apprised of risky data movement and interactions on the endpoint. This kind of activity can include things like unauthorized access, data exfiltration and use of unapproved software.

Proofpoint ITM identifies sensitive data in motion. This is when the data is most at risk. It scans the content. It also reads classification labels like those from Microsoft Information Protection. Scanning is done on-demand. It is activated on specific triggers. This keeps the endpoint engine lightweight. And it keeps your users productive without compromising security.

Proofpoint ITM blocks data leakage in real time. You can prevent users from engaging in out-of-policy interactions with sensitive data. These can include web upload, copy to USB, copy to cloud, sync folder and print. You can set up end-user justifications as well. When enabled, these notifications ask your users to explain why they need access to the data and capture their response for the security team.

Accelerate Incident Response

Proofpoint ITM offers a centralized view of incident status and history. Its unified console helps you to monitor activity, correlate alerts and manage investigations. This kind of visibility can help you to spot threats and coordinate an effective response. Alerts can be tagged and categorized to improve collaboration with other security analysts.

Proofpoint ITM includes powerful search and filter features to help you hunt for threats. With custom data explorations, you can search for risky activity specific to your organization or in response to new risks. You can adapt an out-of-the-box threat exploration template or you can build your own.

A user timeline details what happened before, during and after an alert. This gives you context into the who, what, where and when of the incident. You can also capture screenshots of the user's activity. This can help inform investigations with clear and irrefutable evidence.

Proofpoint ITM gathers telemetry from endpoints. Webhooks into the platform make it easy for your SIEM and SOAR tools to ingest ITM alerts. This way you can identify and triage incidents faster.

Achieve Rapid Time To Value

As a SaaS-based application, Proofpoint ITM is designed for scale, analytics, security, privacy and extensibility. It reduces setup time and cost on the back end. And it simplifies ongoing security management for your security teams with unified policy orchestration as well as endpoint and access management. It can be configured to meet all of your security privileges and administration needs. You can deploy fine-grained security and access policies to support data privacy and create workflows that fit your business needs.

LEARN MORE

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

ABOUT PROOFPOINT

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including 75 percent of the Fortune 100, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at **www.proofpoint.com**.