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 ITM is a modern SaaS solution with a dual purpose. It takes a people-centric approach to protect your sensitive data from insider threats and data loss at the endpoint and it provides you with deep visibility into user activities.

With a lightweight agent, Proofpoint ITM is built upon the Proofpoint Information and Cloud Security platform. It combines context across content, behavior and threats. And the visibility and analysis it provides can help your security teams understand user intent before, during and after an event. With such comprehensive and timely insights, you can quickly detect and prevent insider-led data breaches.

Gain Visibility and Context Into User Activity

Proofpoint ITM lets you see data movement and user interactions. And it shows how sensitive content, apps, endpoints and servers are being accessed. By being able to view the entire spectrum of user activity and data movement, you can understand the full context around user-driven incidents. With ITM, you have the flexibility to monitor everyday and risky users with a single, lightweight endpoint agent.

Figure 1: A people-centric approach to investigate insider violations.

Proofpoint ITM lets you build watchlists that you can use to monitor risky users. These watchlists can be based on criteria like user's role and 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 as well as other human resources and legal factors.

Detect and Prevent Risky User Behavior In Real Time

With Proofpoint ITM, you can quickly build customized detection rules and tailor them 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 attributes like user, data, app, endpoint, sensitivity of content, geography and others.

Proofpoint ITM includes out-of-the-box libraries of alerts. These are easy set to up and they afford faster time to value. The alerts keep you quickly apprised of risky data movement and interactions on the endpoint. The libraries include a wide range of risky insider threat behavior, such as unauthorized access, careless behavior, identity theft and others.

Proofpoint ITM identifies sensitive data in motion, when it is most at risk. It scans content in motion and reads data classification labels like those from Microsoft Information Protection. Based on a lightweight endpoint agent, Proofpoint ITM's content scanning is on-demand and is based on specific triggers. This approach can keep your users productive without compromising security.

Proofpoint ITM also actively blocks data leakage in real time. You can prevent users from engaging in out-of-policy interaction with sensitive data. These activities can include web upload or download, copy to USB, cloud share sync and document open. You can set up end-user justifications. When enabled, users will be asked to explain why they need to access sensitive data. This helps to educate them of their risky behavior.

Accelerate Incident Response

Proofpoint ITM offers a centralized view of incident status and history. A unified console provides intuitive visualizations to help you monitor activity, correlate alerts and manage investigations. It also helps you to spot threats and coordinate incident response. This multichannel visibility in one place can help you improve your incident response. And 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 proactively for risky activity specific to your organization or in response to new risks. You can adapt one of the out-of-the-box threat exploration templates or you can build your own.

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

Proofpoint ITM is built on the microservices-driven Proofpoint Information and Cloud Security platform. It gathers telemetry from endpoints, email and cloud. Webhooks into the platform make it easy for your SIEM and SOAR tools to ingest ITM alerts, so you can identify and triage incidents faster.

Achieve Rapid Time To Value

Proofpoint ITM is developed for scale, analytics, security, privacy and extensibility. It reduces setup time and cost on the backend. And it simplifies ongoing management for your security teams with unified policy orchestration as well as alert 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 situation.

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**.