Proofpoint Insider Threat Management

People-Centric Insider Threat Management for the Modern Enterprise

KEY BENEFITS

- Detect risky insider activity and prevent data loss from the endpoint
- Simplify response to insider threat and data loss incidents
- Accelerate time to value with highly scalable SaaS deployment powered by modern cloud-native backend
- Keep users productive with a lightweight endpoint agent

KEY ITM USE CASES

- Identify user risk
- Protect from data loss from the endpoint
- Accelerate response to user-caused incidents
- Grow insider threat programmes

Proofpoint Insider Threat Management (ITM) takes a people-centric approach to protect your organisation against data loss, malicious acts and brand damage involving insiders. We defend you against authorised users acting maliciously, negligently or unknowingly. And we correlate user activity and data movement to protect you from insider-led data breaches. Plus, we detect risky behaviour in real-time to give you easy to understand evidence of wrongdoing.

Detect and Prevent Risky Behaviour in Real-Time

With ITM, you can correlate risky behaviour across applications, files, desktops, servers and virtualised environments as it happens. This occurs when the user is behind them and not just after an incident has occurred. Our real-time visibility gives you powerful new ways to correlate, detect and resolve insider threat incidents.

Crowdsourced, real-world threat scenarios

You can detect risky behaviour in real-time. This includes:

- Data exfiltration
- Risky lateral data movement
- Privilege abuse
- Application misuse
- Unauthorised access
- Risky accidental actions

With our Boolean logic-based rules builder, you easily create rules and triggers tailored to your environment. You can start with out-of-the-box threat scenarios and change existing ones. Or you can create them from scratch. Our wide-ranging insider threat rules draw on the collective knowledge of Carnegie Mellon's CERT Division, NITTF, NIST and our customers.

Point-and-click threat hunting

Threat hunting isn't just about external threats. With ITM, you can identify insiders taking needless or malicious risks. Our point-and-click interface makes it easy to proactively explore and search for anomalous behaviour.

With simplified point-and-click hunting, you can:

- Review risky behaviours and activities tailored to your environment
- Use intelligent groupings to filter out thousands of activities that aren't relevant—and focus on the ones that are
- Contextualise anomalous behaviour through timeline and screenshot-based evidence

Data classification support

We integrate with Microsoft Information Protection (MIP). Our ITM agent reads sensitivity labels in real time as the user interacts with the file. You can set detection and prevention rules based on the file MIP sensitivity label, file origin, file type and file destination.

Data loss prevention

ITM can prevent sensitive data exfiltration through common endpoint channels. That includes USB-connected devices such as local sync folders, network-attached storage, flash drives, multimedia devices and phones. It even works when the user is offline.

You can manage USB-based activities by user, groups and hosts as follows:

- Block data writing to USB
- Safelist some USB devices
- Block files that match filename patterns
- Block file types
- Block file sources
- Enforce global prevention rules

The Proofpoint Enterprise DLP suite can extend protection to email and cloud apps.

Accelerate Incident Response

Many organisations undertake insider threat initiatives in the wake of a security event. And most of them find that the generic workflows of their existing security tools don't work with insider threats. Insider data is sensitive and requires a higher degree of collaboration with non-cybersecurity teams.

Immediate context and irrefutable evidence

Our workflows are tailor-made for user-driven events. You can search through security events with keywords and filters across all the collected metadata and screenshots. In other words, you don't need to learn a whole new query language. You can save the filters for proactive threat hunting or for future reference in an investigation.

As you identify critical events and alerts related to investigations, you can tag and categorise them. When you need to share evidence, you can find the relevant events and alerts through those tags. And you export them into common file formats, such as a PDF. These reports include screenshot evidence and associated context of who, what, where and when. This is much easier to manage for cybersecurity and easier to understand by HR, legal, compliance teams and investigators alike.

Advantages of ITM Architecture

Our cloud-based architecture is built for scale, ease of use, security and extensibility. It uses our industry-leading lightweight endpoint agents to collect activity data. You get powerful, app-agnostic visibility into what the user does on their system without hindering their work.

Pure SaaS Deployment

Proofpoint Endpoint DLP is a modern SaaS platform built for scale, analytics, security, privacy and extensibility. This reduces setup time and cost on the backend. And it simplifies ongoing management for security administrators across the organisation. This means instantaneous visibility on data activity.

Two problems, one lightweight solution

Endpoint DLP and Insider Threat Management use a single, common, lightweight agent and a modern SaaS architecture. When used together, Endpoint DLP protects from data loss risks among everyday users. And ITM extends that protection to all risky behaviour by malicious and higher risk users.

LEARN MORE

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