proofpoint.

DATA SHEET

# Proofpoint Communications Insights for Insider Threat Management

## Human risk insights for proactive detection

### Key benefits

- Identify early warning signs before harmful actions occur
- Gain holistic visibility into user intent and behaviour
- Accelerate decision-making with AI-generated summaries and contextual insights
- Intervene early to prevent further damage and guide appropriate action
- Protect employee privacy by surfacing high-fidelity alerts without exposing full communications

## Insider threats start with intent

Insider threats rarely begin with action; they begin with intent. Yet most insider risk programmes rely mainly on behavioural signals. They detect policy violations only after risky activity has occurred. However, critical warning signs—such as resentment, coercion, grievances or malicious intent—often surface first in everyday workplace communications. These include email, messaging and collaboration platforms.

Without visibility into communications signals, security teams lack the full context needed to stay ahead of insider risk. The result is delayed detection and reactive investigations. Teams miss opportunities to intervene before sensitive data is exposed or damage has been done to systems and networks.

## Why Communications Insights for ITM

Proofpoint Communications Insights for Insider Threat Management provides further context for user intent by analysing workplace communications for indicators of malicious or risky behaviour. By fusing insights into communications with user activity at the endpoint, the solution helps insider risk teams detect potential threats earlier. Importantly, teams can understand not just what users are doing, but what they might be thinking or planning.

Holistic insight into motive and action enables faster, more proactive intervention before damage occurs. The result is a more mature insider risk programme that reduces exposure, improves response time and supports compliance.

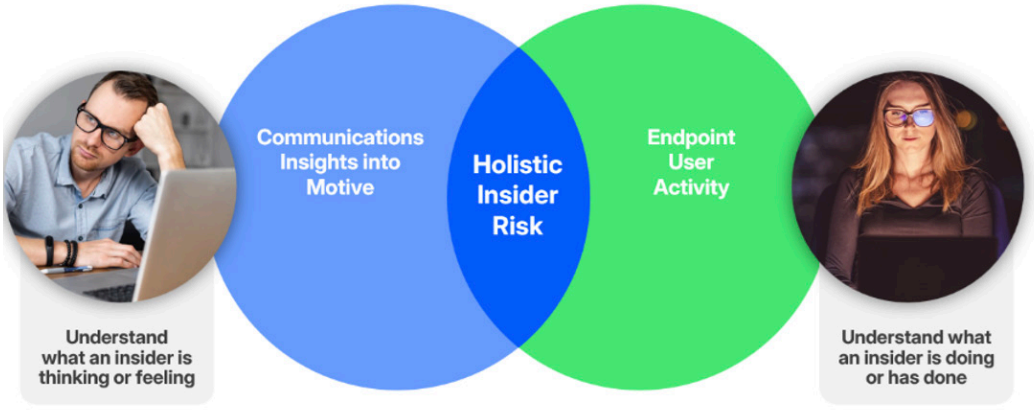


**Figure 1**: Communications Insights for ITM combines insights into user communications and endpoint user activity.

## How Communications Insights for ITM works

Communications Insights for ITM can monitor user communications in Microsoft 365 and Google Workspace. Microsoft 365 monitoring includes Copilot, Mail, OneDrive, SharePoint, Teams and Viva Engage. Google Workspace monitoring includes email, voice, SMS, call recordings and Google Chat.

AI-driven risk analysis of user communications identifies indicators aligned to the Insider Threat Matrix™, an open, public industry framework for detecting and preventing insider threats. This analysis identifies user sentiment, including nuanced states such as resentment, disgruntlement or coercion. AI analysis of user communications is supported for over 100 languages and dialects.

When Communications Insights for ITM identifies user communications as risky, it sends an alert to the Data Security Workbench, the unified console in Proofpoint Insider Threat Management. From there, security analysts can review AI-generated summaries that highlight potentially concerning intentions. Analysts can see entire user conversations only when necessary. This ensures controlled access to sensitive data and user privacy.

The solution retains user communications for 90 days.

## Proactive insider risk detection

Communications Insights for ITM enables security teams to move from reactive investigations to proactive insider threat detection. It unifies motive and behaviour in a single, actionable view of risk.

Combining AI-driven communications analysis with endpoint telemetry from ITM gives security teams insight into user intent and behaviour. More in-depth context drives faster, more confident investigations. Enhanced detection capabilities protect employee privacy.

With Communications Insights for ITM, you can enable proactive insider risk detection with:

- **Early risk identification** — Gain visibility of user intent through continuous capture and intelligent analysis of workplace communications. Detect potential threats earlier and more precisely.
- **Insights into the 'why'** — Understand why risk is occurring by adding human context and intent to technical signals.
- **Shorter investigation times** — Through visibility of communications signals and endpoint behaviour, gain further context for faster investigations.
- **Enhanced detection** — Free security analysts from reviewing unintended communications. Shift the focus to high-fidelity alerts, reducing operational burden.
- **Privacy controls** — Maintain user privacy by surfacing only risks as alerts, not entire user communications.

proofpoint.



**DISCOVER THE PROOFPOINT PLATFORM →**