Microsoft 365 Insider Risk Management

Quickly identify insider risks and protect your company’s most sensitive information.
More than 60% of insider threat incidents were the result of a careless employee.

SOURCE: GARTNER 2020 MARKET GUIDE FOR INSIDER RISK MANAGEMENT

How can you identify and manage internal risks?

Your most trusted employees can also represent grave security risks.

Emotional stressors and other factors can lead to distraction and carelessness, which can lead to data leakage or loss.
Emotional stressors can also lead a trusted employee to become an inside threat, which might lead to data theft or sabotage.

23% of insider threat incidents are considered to be malicious.

SOURCE: GARTNER 2020 MARKET GUIDE FOR INSIDER RISK MANAGEMENT
Intelligent insider risk mitigation begins with signal gathering

A signal is a combination of user activity with a policy trigger.

User accessed confidential files
User copied confidential files to USB drive
User sent confidential files to external email
User posted incendiary communications

USER SIGNALS
Signals can also come from connectors to integrate with Communication Compliance, HR systems, and others. Microsoft 365 Insider Risk Management integrates naturally with both policy and user interactions to capture these signals.
Identify and review hidden patterns

Using Machine Learning, Microsoft 365 Insider Risk Management receives and analyzes millions of signals per day.
Disparate user signals, when analyzed together, can reveal an anomalous and risky pattern of behavior. This can be reported to your IT Security team.

IRM Alert!

- **Employee *****253**
- **Anomalous activity:**
  - Project Jupiter
  - Confidentiality

Employee privacy is protected through pseudonymization in the identification phase.
More serious anomalous behavior can be flagged with higher priority, and can prompt immediate investigation.
Investigations and actions are enabled by analysis of user history

During an investigation, IT Security can view a timeline of past signals to identify a user's patterns of behavior.

Timeline:
Employee *****253
Sentiment analysis in the Communication Compliance module can provide valuable context to quickly identify and dismiss false positives.

Flagged term found: "kill"

"You really killed that big talk today! Great job!!"

Timeline:
Employee *****253

Sentiment analysis: Positive
Investigation and analysis of user signals, including sentiment analysis in Communications Compliance, can also reveal troubling incidents, such as harassment or bullying.

**Timeline:**
Employee *****995

Flagged term found: "kill"

"I'm so mad I could kill somebody!"

Sentiment analysis: **Negative**
Handle outcomes collaboratively through integrated workflows

Imminent risks can be immediately escalated by IT Security to HR or Legal for follow-up.
Follow-up on escalated cases is determined by each company's legal and security policies.
Outcomes for less serious behavior can also be routed back to employees without involving disciplinary actions.
Learn more about Microsoft 365 Insider Risk Management at aka.ms/insiderriskblog