

Microsoft 365 Insider Risk Management

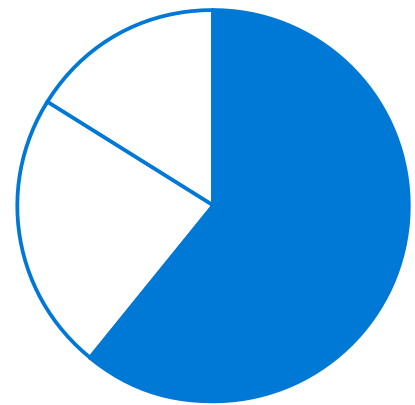
Quickly identify insider risks and protect your company's most sensitive information.



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.



More than 60% of insider threat incidents were the result of a careless employee.

SOURCE: GARTNER 2020 MARKET GUIDE FOR INSIDER RISK MANAGEMENT



Start

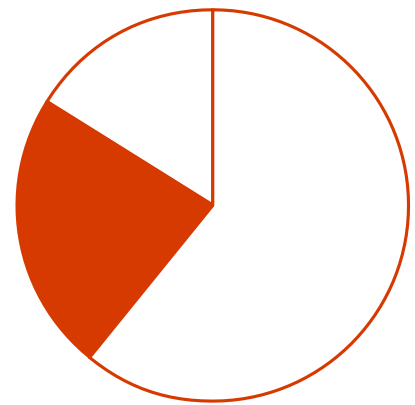
Signal Gathering

Identify

Investigate

Take Action

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



Start

Signal Gathering

Identify

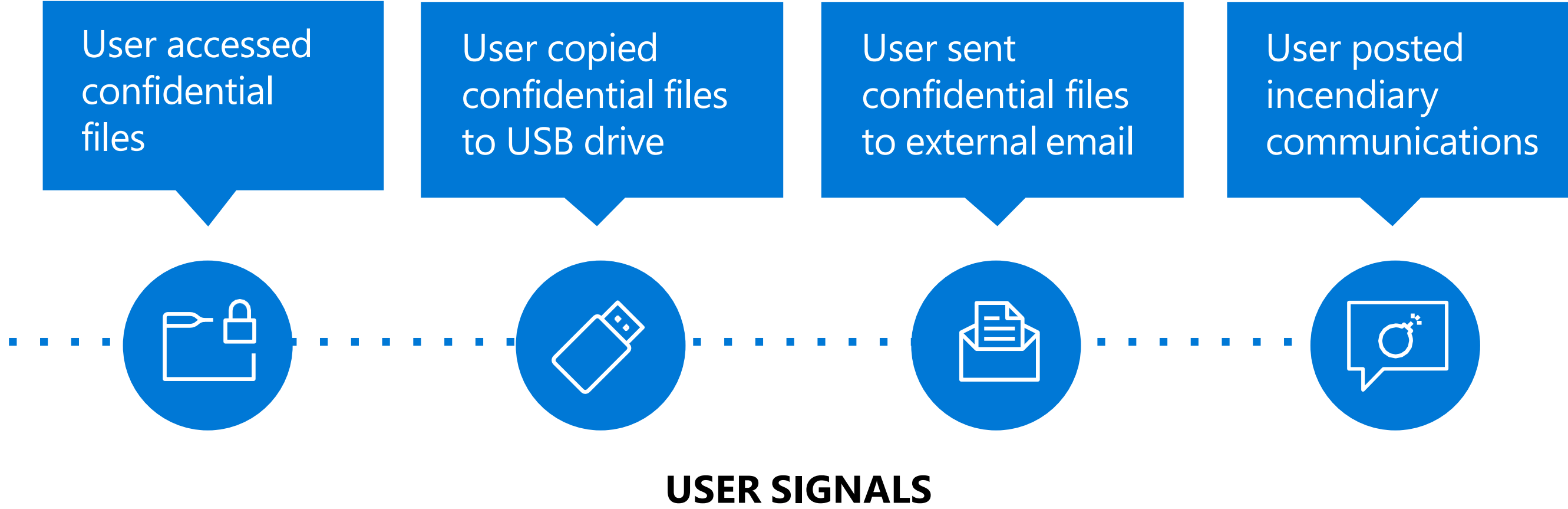
Investigate

Take Action



Intelligent insider risk mitigation begins with signal gathering

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



Start

Signal Gathering

Identify

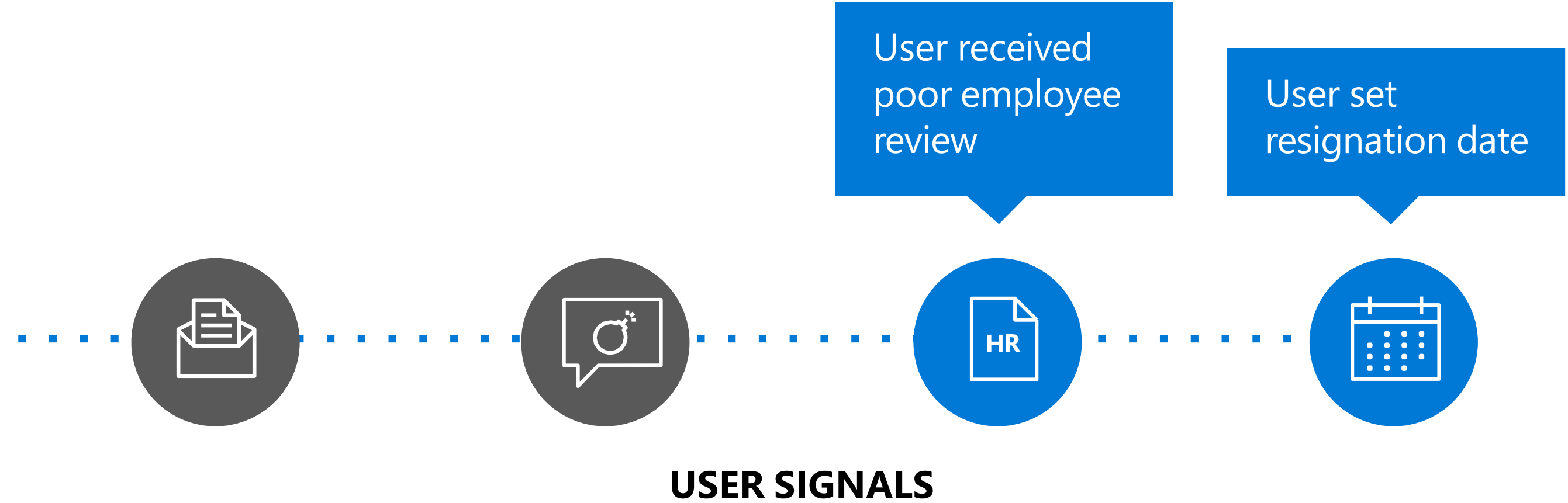
Investigate

Take Action



Signals can also come from connectors to Communication Compliance, HR systems and others.

Microsoft 365 Insider Risk Management integrates naturally with both policy and user interactions to capture these signals.



Start

Signal Gathering

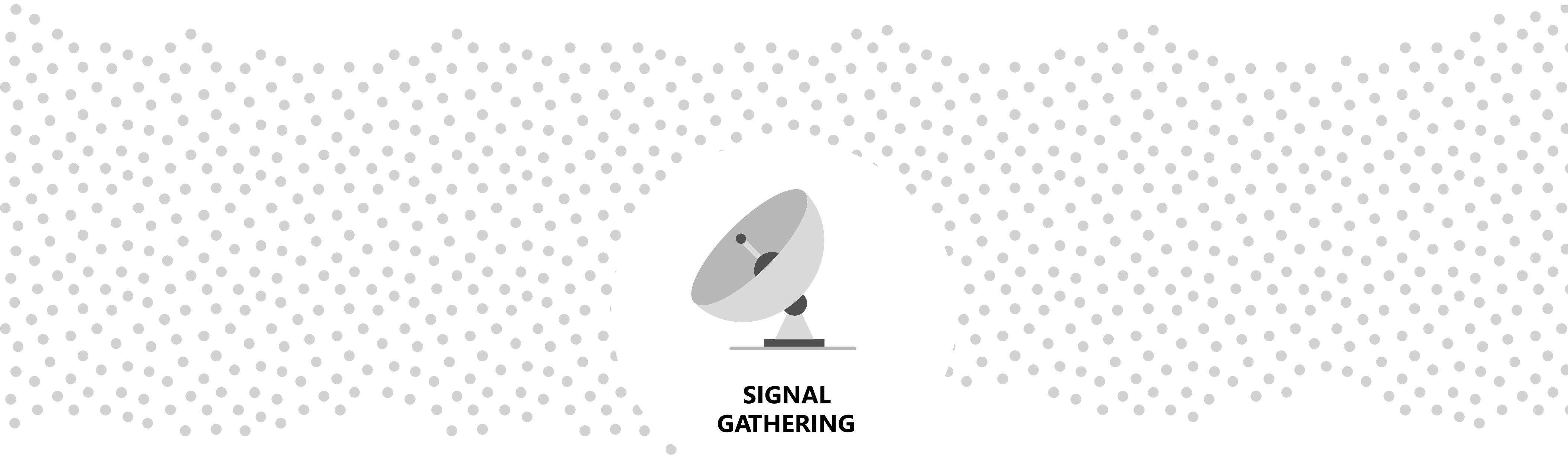
Identify

Investigate

Take Action

Identify and review hidden patterns

Using Machine Learning, Microsoft 365 Insider Risk Management receives and analyzes millions of signals per day.



Start

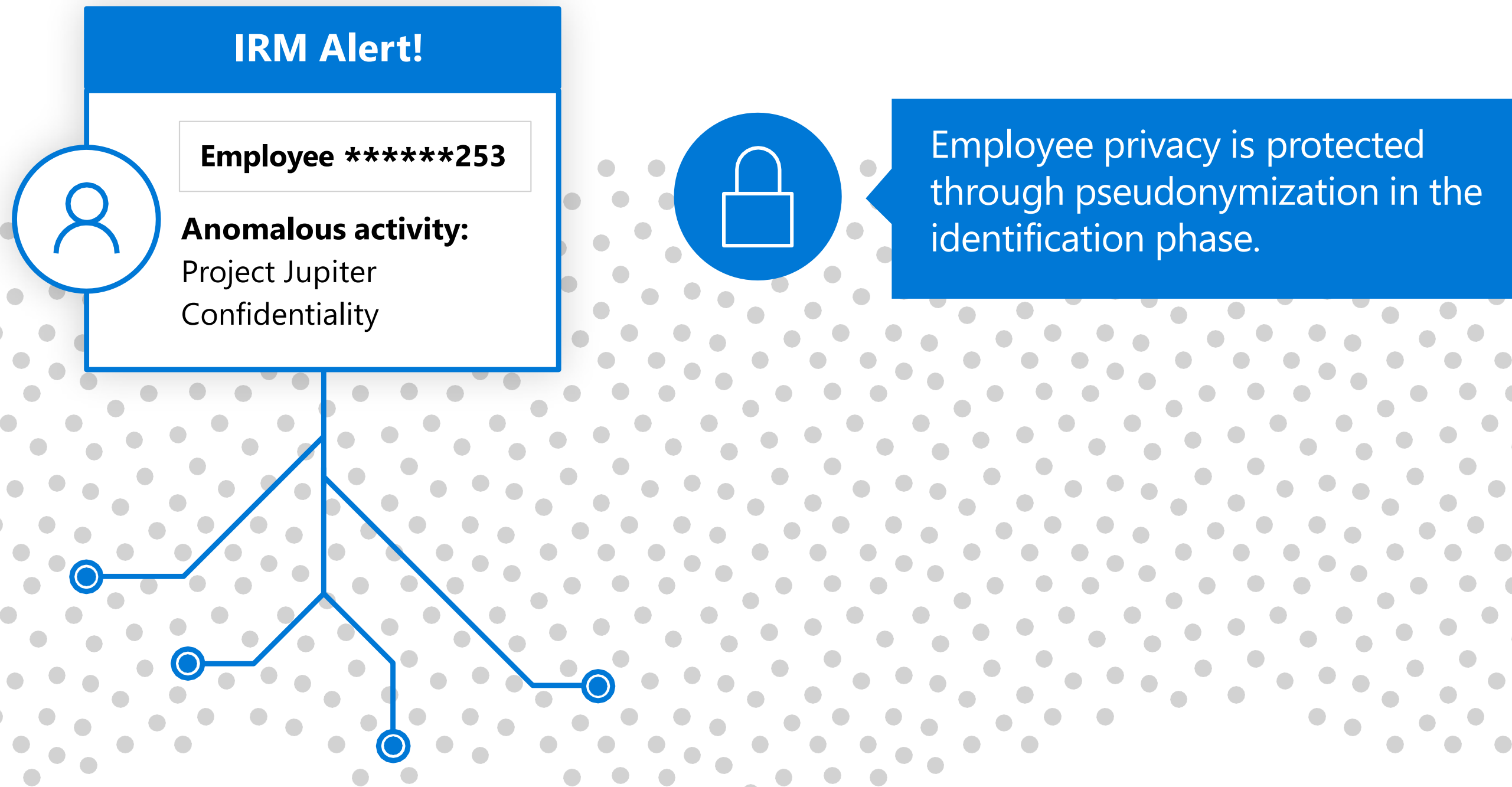
Signal Gathering

Identify

Investigate

Take Action

Disparate user signals, when analyzed together, can reveal an anomalous and risky pattern of behavior. This can be reported to your IT Security team.



Start

Signal Gathering

Identify

Investigate

Take Action

More serious anomalous behavior can be flagged with higher priority, and can prompt immediate investigation.



Start

Signal Gathering

Identify

Investigate

Take Action



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

The timeline visualization consists of three white boxes arranged horizontally, each containing three rows of data. Each row has an icon on the left and horizontal lines representing text on the right. The icons are: a folder with a lock, a USB drive, and a document. The third box has a blue circle with a white clipboard icon in the first row, indicating an action taken. Below the boxes is a blue horizontal line with three circular markers corresponding to the boxes.

Start

Signal Gathering

Identify

Investigate

Take Action



Sentiment analysis in the Communication Compliance module can provide valuable context to quickly identify and dismiss false positives.

Timeline:
Employee *****253

Flagged term found: "kill"

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

Sentiment analysis: **Positive**

Start

Signal Gathering

Identify

Investigate

Take Action



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**

The diagram shows a horizontal timeline with three stages. The first two stages are represented by white boxes with yellow shield icons containing a white exclamation mark. The third stage is represented by a larger white box with a red speech bubble icon containing a white exclamation mark. To the right of the timeline, there is a vertical list of icons: a folder with a lock, a speech bubble with a camera, a calendar, and a clipboard with a checkmark. A red line with three circular markers runs along the bottom of the timeline.

Start

Signal Gathering

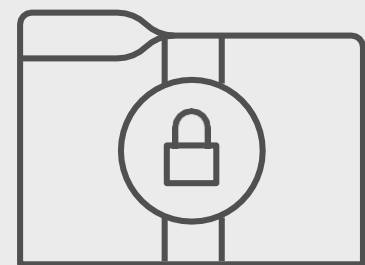
Identify

Investigate

Take Action

Handle outcomes collaboratively through integrated workflows

Imminent risks can be immediately escalated by IT Security to HR or Legal for follow-up.



Create case and escalate to HR



Start

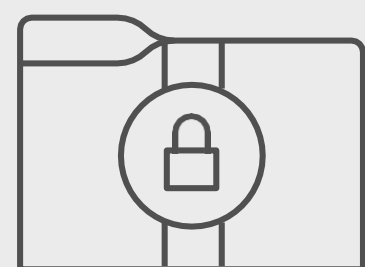
Signal Gathering

Identify

Investigate

Take Action

Follow-up on escalated cases is determined by each company's legal and security policies.



New Priority Case:

Employee
17232995



Start

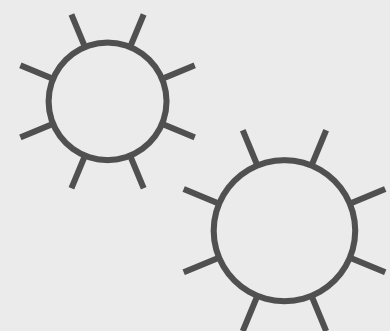
Signal Gathering

Identify

Investigate

Take Action

Outcomes for less serious behavior can also be routed back to employees without involving disciplinary actions.



**Configure
Automated
Policy
Guidance**



Start

Signal Gathering

Identify

Investigate

Take Action

Learn more about Microsoft 365 Insider Risk Management at
aka.ms/insiderriskblog

