

INSIDER THREAT MANAGEMENT.

The riskiest actor in your environment might already have valid credentials, legitimate access, and no reason to raise an alarm — **because they're an employee, not an outsider**. Insider threat management turns access and behavior signals into early warning before damage is done.

- BEHAVIORAL ANALYTICS
- ACCESS ANOMALY DETECTION
- OFFBOARDING CONTROLS
- EXFILTRATION MONITORING

01 THE MECHANISM

Behavioral Baselining
Establishing what **normal access and data-handling patterns** look like for each role, so deviations stand out.

Anomaly Detection
Flagging unusual data movement, access timing, or volume **against a user's established baseline**.

Case Investigation
Escalating flagged behavior through a **structured, evidence-based review** before any action is taken.

02 THE FLOW

The Monitoring Cycle ONGOING

1

User activity across email, file systems, and applications is **continuously baselined** against role and peer norms.

2

Deviations — large downloads, off-hours access, unusual destinations — **generate a risk-scored alert**.

3

Analysts **triage the alert against context**: recent role change, resignation notice, performance issues.

The Departure Cycle PER EXIT

1

A resignation or termination is **flagged to security** before or at the moment it's announced internally.

2

Monitoring sensitivity **increases automatically during the notice period**, when exfiltration risk peaks.

3

Access is **revoked at the moment of departure**, not on the next scheduled provisioning cycle.

03 CORE PILLARS & COVERAGE

PILLAR	WHAT IT COVERS
Behavioral Analytics	Establishes per-user baselines and flags statistically significant deviations.
Data Loss Prevention	Monitors and blocks unauthorized movement of sensitive data across channels.
Privileged User Monitoring	Applies heightened scrutiny to admins and users with elevated access.
Offboarding & Exit Controls	Tightens monitoring and revokes access around voluntary and involuntary departures.

04 INSIDER RISK APPROACHES COMPARED

SIGNAL	SUFFICIENT ALONE?	WHAT IT MISSES
Trust-Based Access Alone	No	Assumes good intent indefinitely, with no signal when that changes.
Exit Interviews Only	No	Surfaces intent after the person has already left with access intact.
Static Rule-Based Alerts	No	Misses gradual, low-and-slow exfiltration that no single rule catches.
DLP Without Behavioral Context	No	Flags every large file transfer equally, burying real risk in noise.
Combined Insider Threat Program (Analytics + DLP + Case Mgmt)	Yes	Surfaces genuine risk early while reducing false-positive fatigue on the team.

INSIDER THREAT.

BASELINE · DETECT · INVESTIGATE

05 PROGRAM OPERATIONS

Most insider incidents involve legitimate access, not a hacked account. The signal is behavioral, not just technical.

The 30 days around a resignation carry the highest exfiltration risk. Programs that don't flex monitoring there miss the window.

Privacy and legal review must be built into the program, not bolted on after a false accusation.

False positives erode trust in the program faster than missed detections do. Tuning matters as much as coverage.

06 CONTROL MAPPING

NIST SP 800-53 (PM-12)

Insider threat program requirements for federal and enterprise environments.

CERT INSIDER THREAT FRAMEWORK

Carnegie Mellon research-based model for insider risk indicators and controls.

CISA INSIDER THREAT GUIDE

Federal guidance on building a cross-functional insider risk program.

NIST CSF 2.0

Detect function coverage for anomalous activity and unauthorized access.

07 WHAT THIS DOES NOT SOLVE

A first-time actor with no history
Baselines take time to establish; a new hire's **first bad act may not stand out yet.**

Collusion between multiple insiders
Coordinated actors **can each stay within their own individual baseline.**

Legitimate access used for a single act
One authorized action **can cause damage without ever looking anomalous.**

Over-collection without legal guardrails
Monitoring that outpaces privacy and labor law **creates its own liability.**

08 MYTHS VS. REALITY

MYTH "Insider threats are mostly malicious actors."	REALITY Most incidents are negligent or accidental, not intentional sabotage.
MYTH "Background checks solve insider risk."	REALITY Intent and circumstances can change long after a person is hired.
MYTH "Monitoring employees is mostly a legal risk."	REALITY A well-scoped, disclosed program with legal review reduces both risk and liability.
MYTH "DLP tools alone are an insider threat program."	REALITY DLP without behavioral context and case management just generates noise.
MYTH "Only departing employees are the risk."	REALITY Long-tenured staff with accumulated access are often the highest-impact insiders.

09 SPEAK THE PROGRAM — KEY TERMS

INSIDER THREAT

Risk of harm from someone with **authorized access** to an organization's systems or data.

BEHAVIORAL BASELINE

The established pattern of **normal activity** for a user or role, used to detect deviations.

DATA EXFILTRATION

The **unauthorized transfer** of data outside an organization's control.

UEBA

User and Entity Behavior Analytics: technology that **models normal behavior** and flags deviations.

PRIVILEGED USER MONITORING

Enhanced oversight applied to accounts with elevated system access.

CASE MANAGEMENT

The structured, evidence-based process for **investigating flagged alerts.**