movate

Outsmart rising insider threats with

AI-FIRST ENTERPRISE CYBERSECURITY GOVERNANCE

Insider risk governance: We will examine key research stats, the shifting tides, how these risks have evolved over the years and Movate's response in today's AI era.

83% of companies **reported insider attacks in 2024**, and CISOs are increasingly concerned about mushrooming threats in 2025. However, insider threats are more visible, complex, and strategically executed than ever before. They now take on a top priority at the cross-functional governance level.

LET'S LOOK AT SOME KEY STATS.

Employee misuse of AI tools: Over **4%** of GenAI prompts and 20% of uploaded files **exposed sensitive corporate data** in Q2 2025.
- AXIOS

Only **14–15%** of organizations **report having the talent** they need to meet cybersecurity objectives.
- WEF

93% of respondents say **insider threats are as complex** or more challenging to detect than external cyberattacks.
- Cybersecurity Insiders

In 2025, up to **4.8 Mn roles remained unfilled**, leaving many organizations without the necessary support.
- Techopedia

KEY FINDINGS

from the 2025 Insider Risk Report point out that insider threats have outpaced defenses, employee behavioural signals remain underutilized, lack of predictive analytics, risk amplification due to AI tools among other barriers such as...

- **71%** Inadequate tools
- **69%** Tight budgets
- **58%** Privacy concerns

The **WEAKEST LINK** in enterprise defense

- Internal misuse
- Compromised credentials
- Human behavior

WHAT HAS SHIFTED NOW?

The TERMINOLOGY
"Insider threat" (implying malicious intent) has evolved to "insider risk" (including negligence, mistakes, or burnout).

The APPROACH
From reactive investigations to continuous, risk-based governance.

The TOOLS
From rule-based alerts to AI-driven, privacy-conscious platforms.

A CHRONOLOGY OF DEVELOPMENTS

2010s & earlier

Known as "insider threats", focused mostly on malicious employees or spies.

Security teams used perimeter defenses, access controls, and audit logs.

2010 – 2019

Growing awareness of data breaches caused by insiders (e.g., Snowden, Equifax data breach).

Rise of Data Loss Prevention (DLP) and User Activity Monitoring (UAM) tools.

Still reactive and siloed; limited context or behavioral understanding.

2020 – 2024

Cloud adoption, hybrid work, and BYOD made insider risk more complex.

Insider risk expanded to include negligence, accidents, and third-party risks.

AI/ML and behavior analytics started enabling more proactive detection.

Privacy and ethics became central to insider risk programs.

Shift from "threat hunting" to risk governance involving legal, HR, IT, and compliance.

2025 & beyond

Insider risk is now seen as a strategic business risk, not just a technical one.

AI-powered platforms, context-aware risk scoring, and cross-functional governance are mainstream.

Focus has shifted toward early detection, mitigation, and culture of trust + accountability.

Insider risk is not a new concept in 2025, but how organizations understand, detect, and manage it has significantly evolved in recent years.

AN **AI-POWERED INSIDER RISK PLATFORM**

brings intelligence, context, and automation to insider threat management — making it more proactive, accurate, and scalable.

Use cases in action include:

- **Spotting** a phishing victim who is unintentionally leaking credentials.
- **Preventing** accidental leaks from over-sharing via collaboration tools.
- **Identifying** a contract employee misusing credentials to access customer data.
- **Proactively identifying** a departing employee leaking trade secrets.

Insider risks are more complex to detect than external threats because insiders often have authorized access, which makes their behavior appear 'normal' at a surface level.

Addressing this rising threat requires a new governance model, supported by an experienced and certified Managed Security Services Provider.

movate x Anzenna

The next-generation AI-powered insider risk platform signals a significant stride in addressing pressing concerns for enterprise security leaders in today's AI era.

Addressing this rising threat requires a new governance model. **Movate is a certified MSSP** for Anzenna, delivering 24/7 detection, response, and insider risk governance as a fully managed service.

Current typical state of affairs	AI-powered value from an MSSP
Siloed	Generative AI and LLMs to detect and prioritize insider threats.
Reactive	Context-aware precision.
Dependent	Autonomous or semi-autonomous responses.
Agent-based setups & slow performance	No need for endpoint agents.
Erodes user trust	

The **Movate-Anzenna partnership** is redefining insider risk governance in the AI era.

OUTSMART THE INSIDER THREATS

Movate's **Digital Infrastructure Services** brings in cybersecurity depth and operational rigor to help CISOs operationalize trust and take meaningful action in real time.

- **Reduced operational complexity**
- **AI-enabled governance frameworks**
- **Seamless transition from reactive controls to proactive state**
- **Swift time-to-value**

At a large educational institution, Anzenna's platform accelerated threat resolution by 40%, eliminated 228 risky applications via automated remediation, and secured a 20% increase in cybersecurity budget justification without expanding headcount.

INSIDER RISK REMEDIATION AS A SERVICE

Benefit from simplicity, scale and intelligence, not more tools.

Movate-Anzenna partnership offers a first-of-its-kind model tailored to how modern enterprises consume security: integrated, contextual, and outcome-driven.

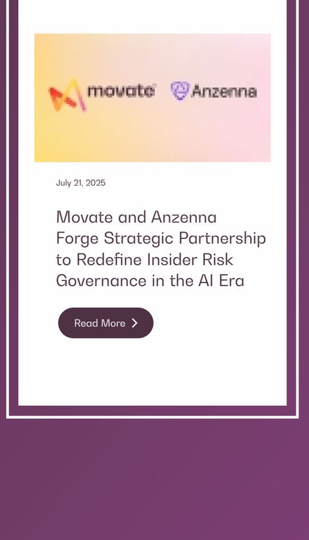
Learn how to integrate the lightweight agentless platform in your SOC.

Act now to identify & mitigate threats.

Contact us

Additional information:

Press release on the Movate-Anzenna partnership



Blog:

AI-powered insider threat protection: smarter, faster, safer

movate

For more information, please send a mail to **info@movate.com** or visit **www.movate.com**