# Protecting Your Business Applications Against Insider Threats

Business applications now represent the core intellectual property and operational workflows of most modern enterprises. It's therefore more critical than ever to protect them from the full range of possible threats. While most organizations put significant effort and investment into protecting applications from external threats, insider threats are often less of a focus.

**Despite the growing cost and frequency of insider risks, 88% of organizations devoted less than 10% of their IT security budget to insider risk management (8.2% on average).[1]**

1 "Cost of Insider Risks Global Report, 2023," Ponemon Institute

Insider threats can take many forms, including some that do not originate from malicious intent. In fact, most incidents involving insider threats are due to negligence rather than bad actors inside the organization.

**The purpose of this paper is to:**

1. Identify the full range of insider threats.
2. Explore how existing security approaches leave critical gaps in this increasingly important area.
3. Illustrate how application detection and response (ADR) can play a pivotal role in your efforts to stop both known and unknown insider threats.

# Types of insider threats

When most people hear the term insider threat, they often think of a malicious employee abusing their access to sensitive systems and data. This can lead to complacency since most organizations are predisposed to trust their employees and, as a result, place greater focus on external threats.

**The problem is that insider threats can take many forms, and many of them are not the result of explicit malice by an insider. Consider the following possible types of insider threats:**

**In a recent study, 55% of insider threats were the result of negligence or mistakes as opposed to malice.[2]**

2 "Cost of Insider Risks Global Report, 2023," Ponemon Institute

### Malicious Insider

A malicious insider is someone who intentionally uses their access to company data and systems to harm the organization. They may be motivated by financial gain, revenge, or a desire to sabotage the organization.

### Negligent Insider

A negligent insider is someone who unintentionally compromises company data and systems due to carelessness or negligence. They are generally unaware of the security risks associated with their actions, or they may simply not care.

### Misdirected

A misdirected insider is someone who is exploited by an attacker to compromise company data and systems. Examples include users who are tricked into clicking on a phishing link or opening a malicious attachment or users who are coerced into revealing sensitive information through social engineering.

### Compromised Insider

A compromised insider is someone whose account has been compromised by an attacker. Account takeovers can occur in a variety of ways, including phishing, malware, and social engineering. Once an attacker has compromised an insider's account, they can use it to access company data and systems.

You'll notice that only one of the above insider threat types is the result of actual malice. This illustrates how the term insider threats can be somewhat misleading, since most insider risks are, in fact, attack vectors for external threat actors. For this reason, it's critical to treat insider threats with the same urgency as more obvious external threats when prioritizing information security activities and investments.

# Limitations of traditional security approaches

Most enterprises have already made many investments in tools that play a role in securing application usage. While many of these do provide significant value, they generally lack the application awareness necessary to detect insider threats effectively. The following examples illustrate this:

### Identity and Access Management (IAM)

Strengths

- Granular control over application access based on identity and role.
- Standardized use of multi-factor authentication (MFA) to reduce the risk of account takeover.
- Baseline logging, alerting, and reporting for certain types of known bad behavior.

Weaknesses

- Implicitly trusts that an authenticated user is legitimate.
- Limited ability to stop common MFA bypass techniques like session hijacking, leveraging of pre-generated tokens, and clickjacking to turn off MFA.
- Logging, reporting, and alerting lack context about application usage details.

### Web Application and API Protection (WAAP)

Strengths

- Capable of providing inline detection and mitigation for application-level threats.

Weaknesses

- Highly dependent on static rules, which are time-consuming to create and manage and rarely comprehensive.
- High false positive rates lead to reluctance to use inline blocking rules.

### Data Loss Prevention (DLP)

Strengths

- Reduces the risk of data exfiltration as the result of user negligence or error.

Weaknesses

- Easily circumvented by motivated insiders.
- Many insider threats have objectives other than data exfiltration.
- Highly dependent on static rules.

### User and Entity Behavior Analytics (UEBA)

Strengths

- Detects anomalies in users' broad infrastructure usage, including some types of insider threats.

Weaknesses

- Limited, if any, content about specific applications and business processes.
- Dependence on rules for many aspects of threat detection, limiting the ability to detect unknown threats.
- Long deployments (6-9 months) and continuous and laborious maintenance.
- High frequency of false positive alerts.

While each of these technologies can play a partial role in insider threat detection and mitigation, a high percentage of insider threats will be missed by approaches that:

1. Rely on static rules that can't detect novel threats.
2. Lack the necessary awareness of specific application functionality and business processes to catch more than very basic anomalies.

# ADR fills the insider threat gap

**ADR is an emerging category of application security capabilities that are uniquely suited to the detection of all types of insider threats.**

**An ADR platform:**

Analyzes user journeys by trusted and authenticated identities.

Profiles expected behavior and creates clusters of typical journeys for users and groups.

Detect instances of anomalous behavior.

Uses threat-scoring techniques to engage response processes when warranted.

User journeys include sequences of activities users perform within and across multiple applications. Using unsupervised machine learning, the ADR platform segments these sequences into "micro personas." By comparing in-progress user journeys against existing micro personas, an ADR platform can detect anomalistic behavior with a high degree of accuracy. In response, high-fidelity alerts can be sent to security orchestration and response (SOAR) workflows to initiate a timely and effective response to insider threats.

## Overcoming the Limitations of UEBA

Earlier attempts have been made to analyze user behavior to detect security threats. The most notable example is UEBA. While UEBA does typically include some behavioral analysis, most solutions remain heavily dependent on pre-defined rules.

**These rules are often:**

1. Too broad, so they produce a high volume of false positives
2. Too narrow, so they fail to detect serious threats.

Rules also very labor-intensive to create and maintain. For these reasons, even the largest and most sophisticated security teams have struggled to realize value from UEBA.

ADR leapfrogs UEBA by completely eliminating the need for security administrators to create and manage rules, while detecting the application-level threats that matter most with a high degree of accuracy.

## ADR business impact

Implementing an ADR platform as part of your security strategy can positively impact your organization's ability to stop insider threats in several critical ways.

### Accelerating time to detection

By improving your security team's ability to detect insider threats that would otherwise escalate into more substantial security incidents, ADR reduces your risk of financial damages and business disruption substantially. This includes novel insider threats that would have been impossible to detect with pre-defined rules. In real-world ADR implementations, it is common to see the mean time to detection for application-level threats drop from months to less than a few hours.

### Reducing false positives

Because ADR has full application context and detects statistical anomalies rather than matches to imperfect, manually created rules, false positive alerts are reduced by orders or magnitude. Simply stated, ADR learns known good behavior and looks for outliers rather than using rules to watch for known bad activities. This prevents alert fatigue and ensures that your security team focuses its limited time and resources on the most important threats. Organizations that deploy ADR often see the number of alerts reduced from hundreds per week to 2 to 3 accurate, high-fidelity alerts per day.

## Expanding application security coverage and consistency

Most organizations have a wide range of business applications, including:

1. Custom applications
2. Commercial and open source software deployed using on-premises servers or cloud instances
3. SaaS applications

ADR can be deployed to all of these variations simultaneously, providing one approach for stopping insider threats across all applications. In contrast, rule-based approaches force security teams to be selective about which applications they focus their security efforts on.

The intelligent and highly automated detection techniques used by ADR platforms can scale up to thousands of applications without manual effort, providing more comprehensive coverage.

## Improving efficiency and inter-departmental collaboration

In addition to being less effective and more prone to false positives, detection rules are very time-consuming for security teams to create and maintain. After all, security teams do not know the business logic of every application and require extensive guidance from business and technical subject matter experts. This is extremely time-consuming and costly. With ADR, security teams spend less time writing rules and more time focusing on high-value activities.

ADR's ability to automatically and accurately model normal behavior for specific applications also simplifies communication between security teams and application developments. Security teams can operate much more independently, as they are less dependent on developers for subject matter expertise about the inner workings of specific applications. This also reduces the time burden on the development team.

**The number of organizations with formal insider risk management programs is expected to rise from 10 percent today to 50 percent by 2025.[3]**

3 "Predicts 2023: Cybersecurity Focuses on the Human Deal," Gartner Inc.

# Start your ADR journey with RevealSecurity

**RevealSecurity pioneered the use of ADR to detect and stop insider threats. Our TrackerIQ solution makes it easy to detect and respond to the abuse and misuse of trusted application identities thanks to the following innovations:**

### User journey analytics

Based on unsupervised machine learning, removes the need to create and maintain rules while enabling organizations to detect zero-day malicious behaviors.

### Individual and peer group analysis

Compares an individual's current user journey to their own past journeys, as well as those of their peer group.

### An application-independent approach

Translates the often cryptic logging terminology of individual applications into understandable and actionable insights, so your security team doesn't need to have in-depth knowledge of each application.

### Cross-application user journey tracking

Creates more robust micro-personas across all of your SaaS, cloud, and on-premise applications, ultimately producing more accurate alerts.

### Rapid data ingestion

Can analyze historical log files overnight and begin producing accurate alerts the very next day.

Reveal security

Contact us today to learn how TrackerIQ can protect all of your custom and third-party applications, including SaaS platforms, from insider threats while reducing the day-to-day burden on your team.

Visit us at: www.reveal.security | General inquiries: info@reveal.security