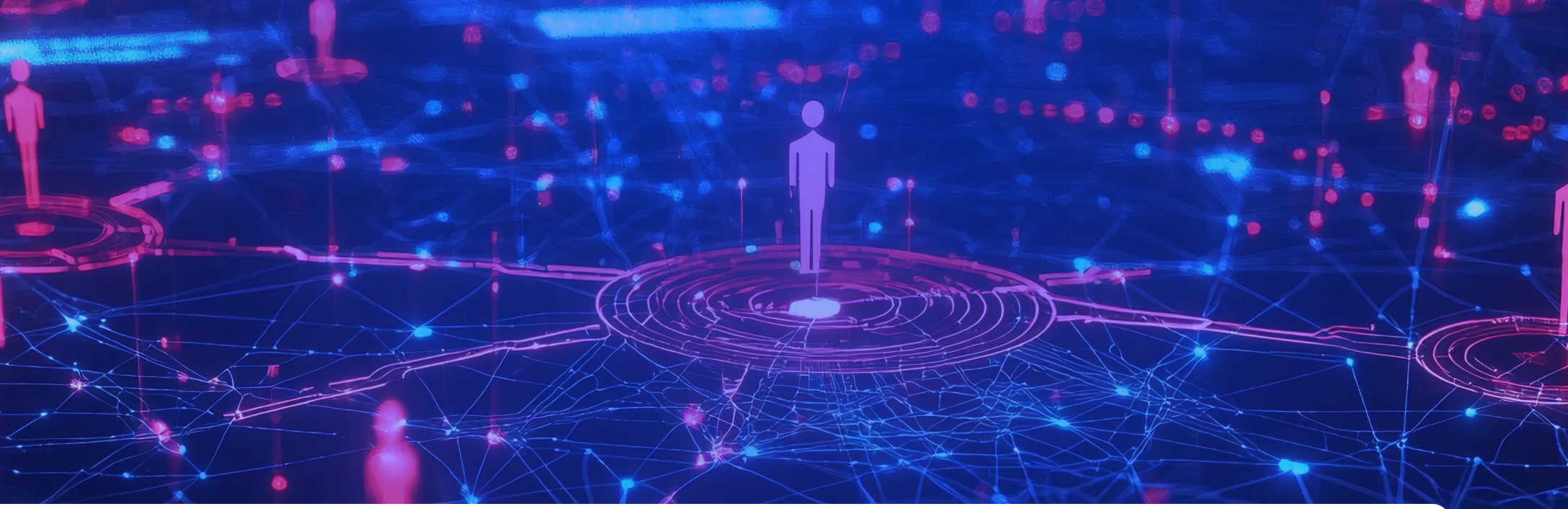
digital hands®

The Threat Within:

How MDR Mitigates Insider Risks to Your Business

Part 3 of a 7 part series

Table of Contents



Human risk is one of the biggest risks any organization faces, and much of it stems from insider threat. Insiders are individuals who have authorized access to your organization's IT infrastructure, network, systems, or data. This can be anyone internal like employees, interns, and independent contractors, or third parties like your trusted vendors and suppliers. **Insider threats can be grouped into four main categories:**

- **Unintentional insider threat** — includes carelessness, negligence, or honest mistakes, such as clicking on a phishing link or inadvertently sharing sensitive data with an unauthorized party. Based on our detections, this is the most common insider threat scenario.
- **Compromised insiders** — individuals whose credentials or other identity data has been exposed, whether due to a breach, malware infection, or phishing.
- **Malicious insiders** — individuals who are acting intentionally to disrupt the organization, attack IT systems, or gain unauthorized access to data.
- **Trusted partners** — vendors, suppliers, consultants, and outsourced support staff who have access to your IT infrastructure or resources and are putting you at risk by acting either maliciously or inadvertently.

The motivations behind intentional insider behavior are broad and may include:

- Espionage, Sabotage, Theft, Violence or disruption

Often, the primary driver behind malicious behavior is financial gain, but it could also be personal in nature, such as retaliation by a disgruntled employee. Nonmalicious behavior can be as simple as employees taking confidential documents when leaving the organization because they want to have a competitive advantage in their next role — they're not trying to hurt your organization intentionally.

Why every CISO and SOC should care about insider threats

Insider threats are nothing new, but they're on the rise. Nearly half of surveyed IT and cybersecurity professionals say their organization has experienced more frequent insider attacks in the past 12 months. More than half of them had six or more insider incidents.

These attacks can be very costly and difficult to detect. Since the access to systems and data originates from a trusted user with legitimate access, insider threats often bypass traditional defenses. And what makes insiders especially harmful is that they often have privileged access to your most sensitive resources.

Some implications to think about:

- ✓ The insider threat is widespread and growing — 83% of surveyed organizations have experienced insider attacks in the past 12 months, compared to 60% the previous year.
- ✓ The annual cost of insider threats is growing as well — the annual estimate was $17.4 million in 2024, compared to $16.2 million in 2023.
- ✓ Data breaches caused by malicious insiders are the costliest — they average $4.99 million per incident, compared to $4.88 million across the board.
- ✓ Insiders are among the top sources of data loss events — 42% of surveyed CISOs attribute data loss to negligent or careless employees, 36% to malicious or criminal insiders, and 33% to compromised employees.

There have been numerous high-profile cybersecurity incidents due to insiders over the years. Here are some noteworthy ones:

Apple: Software engineers took confidential information about a chip technology to a startup competitor who poached them. Apple said it spent billions of dollars on researching the technology over a decade.

Disney: Attackers obtained more than 1 terabyte's worth of company data, including employee PII, after breaching an employee's Slack account. The employee had downloaded an AI app from GitHub that turned out to be malware, which gave the hackers access to his password manager containing credentials and session cookies. Disney was hit with a class-action suit as a result.

Cash App

Cash App: A disgruntled former employee downloaded sensitive information affecting as many as 8.2 million customers, accessing the data after leaving the company.

Dallas Police Department: A reckless IT employee who didn't have proper training erased millions of files — 7.5 terabytes' worth — containing evidence and investigations.

How an insider attack may unfold

Malicious insiders could harm your organization in a variety of ways, such as intentionally leaking sensitive data, infecting systems with malware, or disrupting the network. But nonmalicious or compromised insiders can equally inflict damage by being inadvertent participants in an attack, and you're more likely to experience these unintentional actions than malicious attacks.

STEP 1

Accessing data with a legitimate account

The attack begins when a malicious insider or an outsider leveraging the identity of a compromised user gains access to sensitive data, applications, or systems using a legitimate person's credentials. From there, the actor could escalate privileges, access unauthorized information or systems, execute malware, or perform other actions undetected. If the attacker uses a privileged user's credentials, the risk is even higher since privileged users typically have access to more sensitive systems or data.

STEP 2

Exfiltrating the data

The malicious actor moves laterally across the environment, exfiltrating sensitive data through file transfers, unauthorized cloud storage, personal email accounts, or removable media. The attacker remains undetected by mirroring expected user behavior and operating within normal workflows.

STEP 3

Exploiting the data

The stolen data may be sold on the dark web, shared with competitors, used for extortion, or weaponized to disrupt business operations. Additionally, nation-state actors and cybercriminals often use compromised insiders as a foothold for deeper infiltration, leading to long-term security risks beyond a single breach.

How to combat insider threats with managed detection and response services

Insider threats, whether malicious or unintentional, are difficult to detect because these users are logging into your systems with legitimate credentials. However, MDR can look for indicators of compromise and help contain these attacks to limit their impact, spread, and severity.

An MDR provider uses a combination of technologies and people to identify anomalies across multiple technologies and enable rapid containment like automating account lockdowns and privilege restrictions to minimize damage. Your MDR partner also leverages human expertise to understand the root cause of the incident and how to prevent similar attacks in the future.

Here's what the playbook may look like, using a combination of automated tools and human experts:

1. Detection

The MDR vendor's detection platform sees across multiple technologies. This breadth and depth across systems allows it to detect abnormal behaviors that single point systems may miss due to the lack of curated threat intelligence and AI capabilities. The platform monitors for anomalies, such as:

- **Unusual access patterns** — including large data transfers, off-hours activity, or access to files unrelated to job roles.
- **Unusual behavior** — rapid file deletions or uploads, privilege escalations, unusual login geolocations, mass emails being sent, or unusual requests or conversations.

2. Automation

Automated workflows in the MDR platform immediately disable the suspicious accounts or limit their access and further exploitation and contain the compromise. The platform also alerts the security team to investigate unusual behaviors in real-time. Automated actions may include:

- Disabling the compromised or suspicious account
- Resetting passwords for that account
- Performing custom actions based on the customer's environment

3. Human expertise

MDR analysts investigate flagged activities to validate whether the behavior is malicious or benign. They use context, such as recent role changes or employee grievances, to assess risk and recommend mitigation steps to the customer. The analysts also review all other activity for the compromised or suspicious identity across the entire customer environment.

Benefits of MDR Beyond Insider Threats

MDR offers much more than defense against insiders.

Your MDR partner can augment your in-house SOC or security team, enabling them to:

- ✓ See more — faster — to protect your environment holistically.
- ✓ Get higher-fidelity alerts and integrated, enriched telemetry.
- ✓ Improve operational efficiency while allowing you to automate your workflows based on your risk appetite.
- ✓ Decrease response time with automated containment and expert-led investigations, reducing the window of opportunity for the adversary.

Buyer's Guide

Not sure where to start?

Learn how to use the right mix of machines and humans for an MDR solution customized to your environment and needs.

Download Now