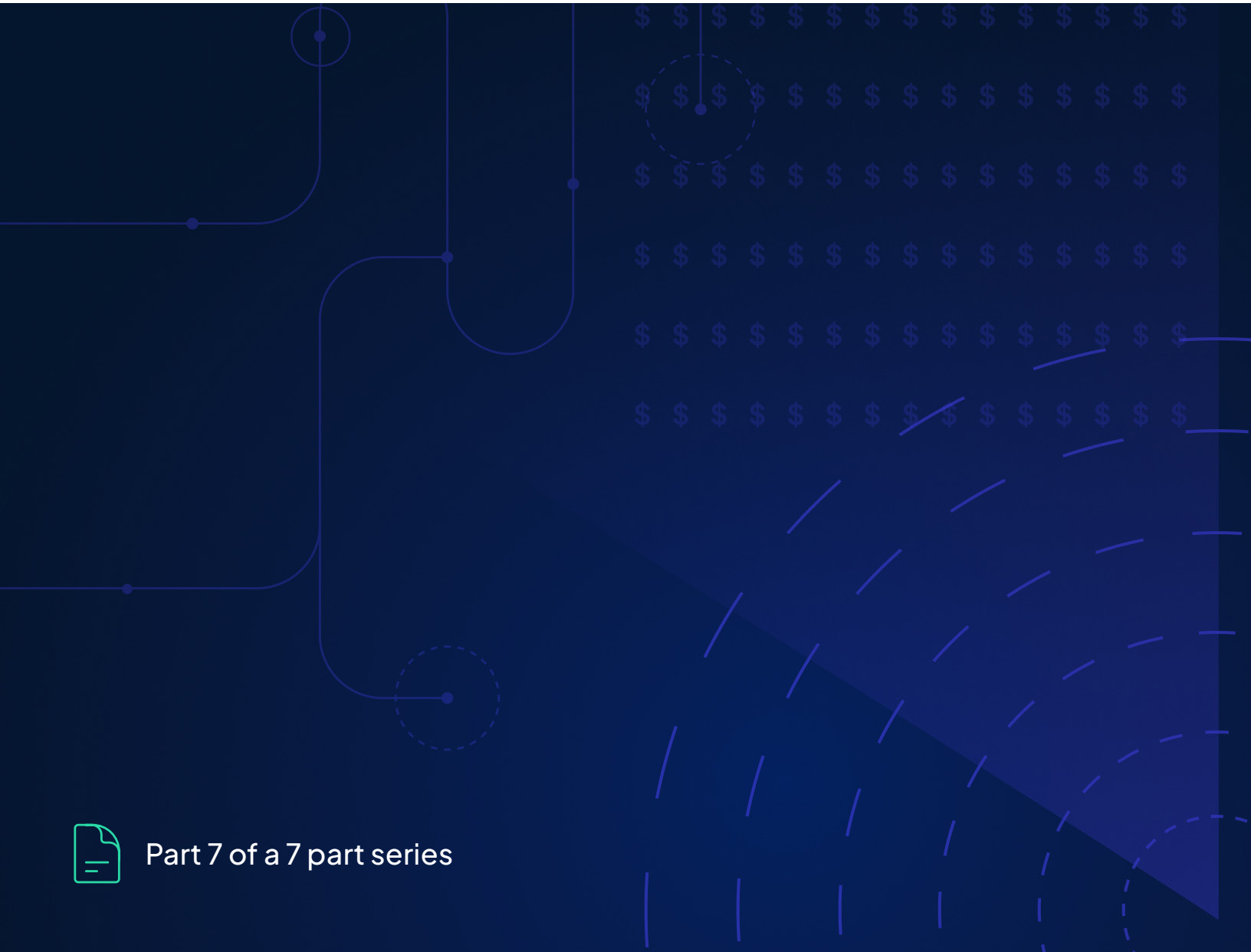
digital hands®

The $13 Billion Question:

How Can MDR Help Mitigate the Growing Account Takeover Threat?



Part 7 of a 7 part series

Table of Contents

Account takeover (ATO) — a cyberattack for the purpose of gaining full, unauthorized access to an account — is one of the oldest tricks in threat actors' playbook. But this tactic has been evolving in recent years.

ATO is especially prevalent in identity theft and financial fraud schemes — in 2023, it was the most common fraud type experienced by U.S. organizations (32%). Industries like finance and e-commerce are among the most targeted. But businesses of all types are at risk because cybercriminals are also leveraging ATO as a launching pad for other malicious activities targeting organizations, like launching ransomware, malware, or business email compromise (BEC) attacks. And they're increasingly bypassing common defenses like multi-factor authentication (MFA) through techniques like session hijacking (using stolen cookies or tokens).

Why Every CISO and SOC Should Care about Account Takeover

Account takeover has a hefty price tag both for organizations and their customers. This cybercrime cost U.S. consumers in 2023 $13 billion, up from $11 billion in 2022. And for organizations, BEC attacks alone (which often employ ATO) cost organizations $2.7 billion in 2022 — 80 times more than ransomware — according to FBI's latest available data.

These are just some of the compelling reasons this threat should be on every security team's radar:

- 83% of surveyed security professionals say their organization has experienced at least one ATO attack in the past year (nearly half experienced more than five). Same respondents identified ATO as the greatest concern for their organization (67%), ahead of ransomware and phishing.
- Some security researchers observed a 24% year-over-year increase in ATO attack rates in Q2 of 2024, following on the heels of a 324% increase in Q2 of 2023.
- ATO is tightly intertwined with phishing and credential compromise. For instance, one survey found that 79% of ATO attacks started with phishing that harvested employee credentials.
- These attacks are not only costly and disruptive to operations but can also erode customer and employee trust. For instance, 80% of consumers say they would stop shopping on a site where they've fallen a victim of account takeover.

The impact to organizations ranges from sensitive data exposure to credential compromise that could lead to follow-on attacks like ransomware. The proliferation of apps increases the risk tremendously, and malicious actors are targeting anything from collaboration apps to social media accounts. One example is the 2021 attack on Electronic Arts, which started with ATO of a Slack account using stolen cookies — and resulted in loss of intellectual property data.

How an ATO Attack May Unfold

The adversaries use a variety of tactics, techniques, and procedures through several stages of the attack. **Here is a plausible scenario of the attack lifecycle:**

STEP 1

Data collection

Bad actors obtain compromised credentials from the dark web, where criminal markets teem with logins stolen from various data breaches. Let's say attackers purchase credential pairs that were exposed in a major breach of a retail site, and plan to use them for credential stuffing attacks on other platforms.

STEP 2

Automated testing

The bad actors use bots to test the stolen credentials across multiple platforms, knowing that many people tend to reuse passwords. (One recent survey found that on average, individuals reuse passwords across four different accounts.) In our scenario, the automated tools test hundreds of thousands of the procured email/password pairs on various financial and ecommerce sites.

STEP 3

Exploitation

Once account takeover is successful, the attackers can carry out a slew of malicious actions, such as making unauthorized purchases, draining accounts, and changing access and recovery details to lock out legitimate account owners. In our example, they gain access to an online banking account and initiate fraudulent wire transfers.

How to Combat Account Takeover with Managed Detection and Response

MDR can help contain ATO attacks to limit their impact, spread, and severity. **Here's what the MDR ATO playbook may look like, using a combination of automated tools and human experts:**

1. Detection

The MDR'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 communication patterns to identify anomalies such as:**

- Attempted logins from unusual geos or IP addresses
- Brute-force login attempts or high volumes of failed logins
- Anomalous behavior like high-value transactions initiated by an account
- Activity from unusual countries
- Auto-forwarding emails to external addresses

2. Automation

The platform's automated workflows flag and temporarily lock accounts suspected of compromise and block the suspicious IP address.

3. Investigation

MDR's analysts investigate flagged accounts to confirm whether activity is malicious or legitimate —analyzing log patterns, transaction data, and session details, as well as checking if the affected credentials are linked to known breaches. They also provide recommendations tailored to the customer's needs, such as enforcing password resets or implementing account recovery best practices.

4. Action

Analysts initiate a password reset and enforce MFA for the affected account or reuse MFA tokens for potentially comprised accounts. They provide guidance to the organization on enhancing password policies and educating users on credential hygiene.

Benefits of MDR Beyond ATO Defense

MDR offers much more than defense against the threat of account takeover.

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?

Get your MDR Buyer's Guide to understand key evaluation criteria and the 8 must-ask questions before you buy.

Download Now