

# Stop Account Takeover and Privilege Escalations

With the agentless Identity Threat Detection and Response (ITDR) platform

## The Challenge

Identities and access privileges are defined across many different systems, each with its own format and logic. Point solutions for identity security are focused on specific siloes and do not provide visibility and threat detection across your IdP/SSO solutions, cloud services, and downstream cloud applications. Recent identity-based attacks like Uber and Okta stress the need for a unified approach to detect and mitigate cross-cloud identity risks and threats.

## The Solution

Authomize's agentless platform seamlessly connects to your entire identity fabric to unify and monitor identity and access data and to detect and mitigate risks and threats. Authomize empowers security teams with unmatched identity visibility and threat intelligence, and helps cut costs with automated remediation and response and automated user access reviews.

## Why Authomize

End-to-end protection from account takeover threats to risky privileged access

Automated remediation and response

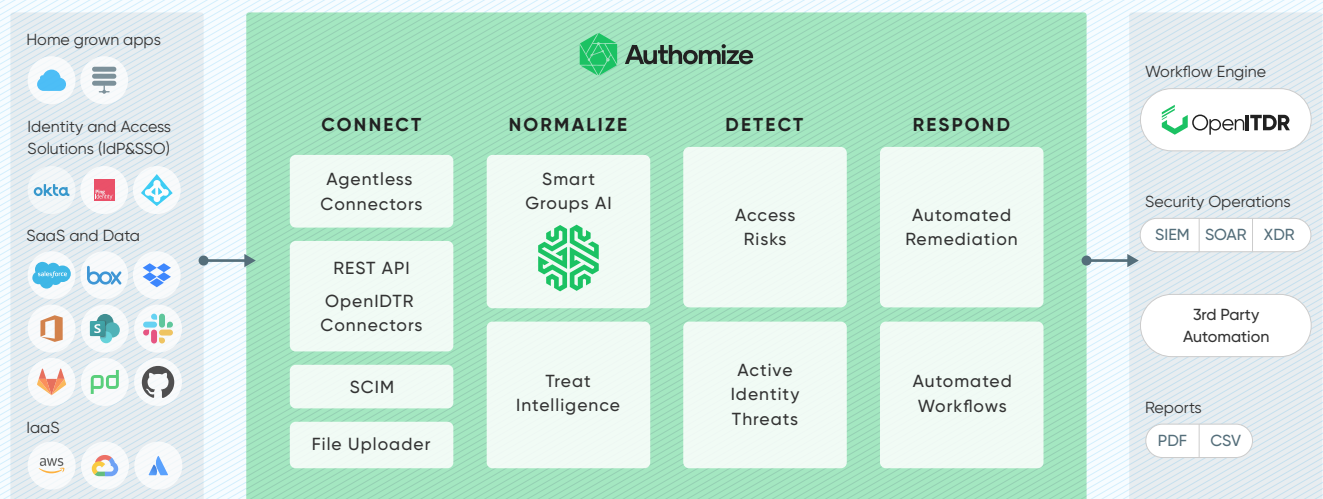
Seamless integration with any IaaS, SaaS, IdP/SSO, and custom applications

Rapid deployment (2-3 days) of an agentless platform

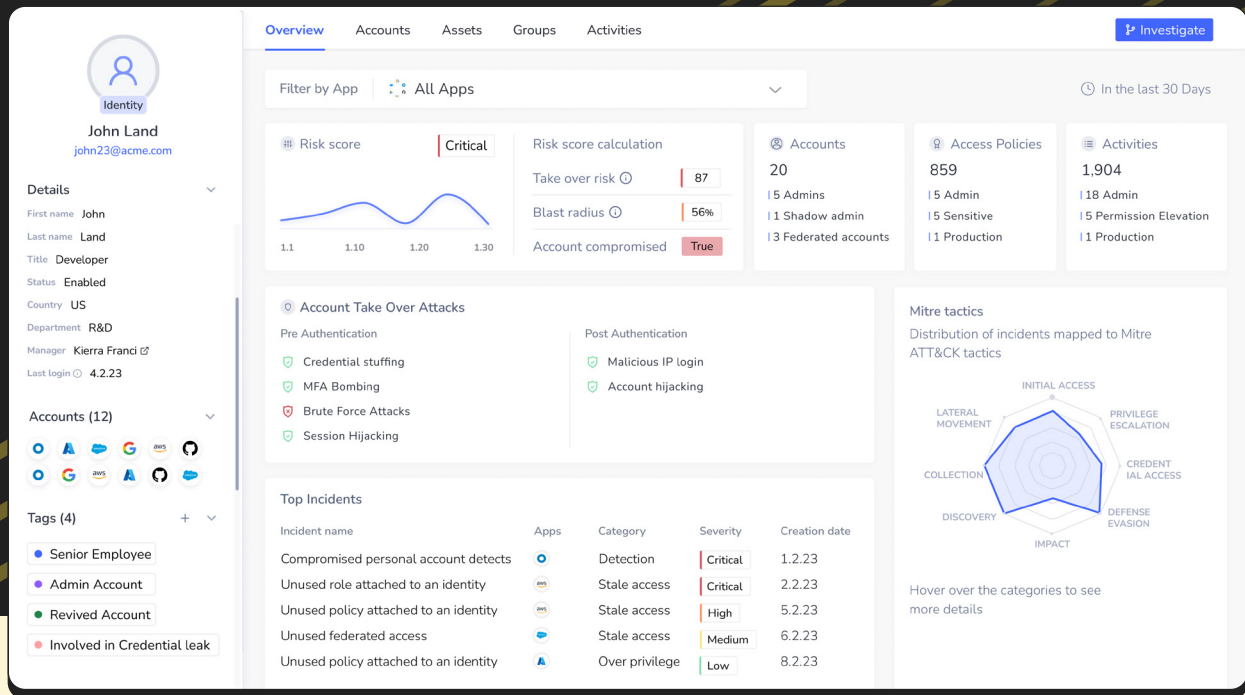
Enriched identity context with threat intelligence and ML-based insights

Unified, granular visibility (to the file permission level) of de facto access

### The Authomize ITDR platform monitors the entire identity fabric



# Holistic, Granular Visibility of Each identity, Account, Asset, Access Privilege, and Activity



"Authomize provides instant visibility and risk reduction across our entire identity and cloud stack, giving us deeper and broader context on the risks in our environment and allowing us to prioritize addressing the issues that matter. It's one of the best security tools I've seen in a long time."

Paul Elli, Head of Information Security | Curebase

## Authomize customers use the solution to

### Detect and Stop Account Takeover

- Detect Compromised Accounts
- Mitigate MFA bombing and misconfigurations
- Prevent exploits in AD, Okta, and other IdP/SSO

### Gain Unified Identity Visibility of De Facto Access

- Accelerate SOC team investigation, prioritization, and response
- Achieve true conditional access with correlation of threat intelligence

### Prevent Privilege Escalations

- Right size permissions across IaaS, SaaS, and IdP/SSO (CIEM)
- Control shadow admins and role chaining
- Detect and protect exposed resources

### Save Time and Costs on Audit Preparation

- Automate remediation and response
- Automate User Access Reviews
- Continuously monitor and fix violations

### Your Data Is Secure With Us



REQUEST A DEMO