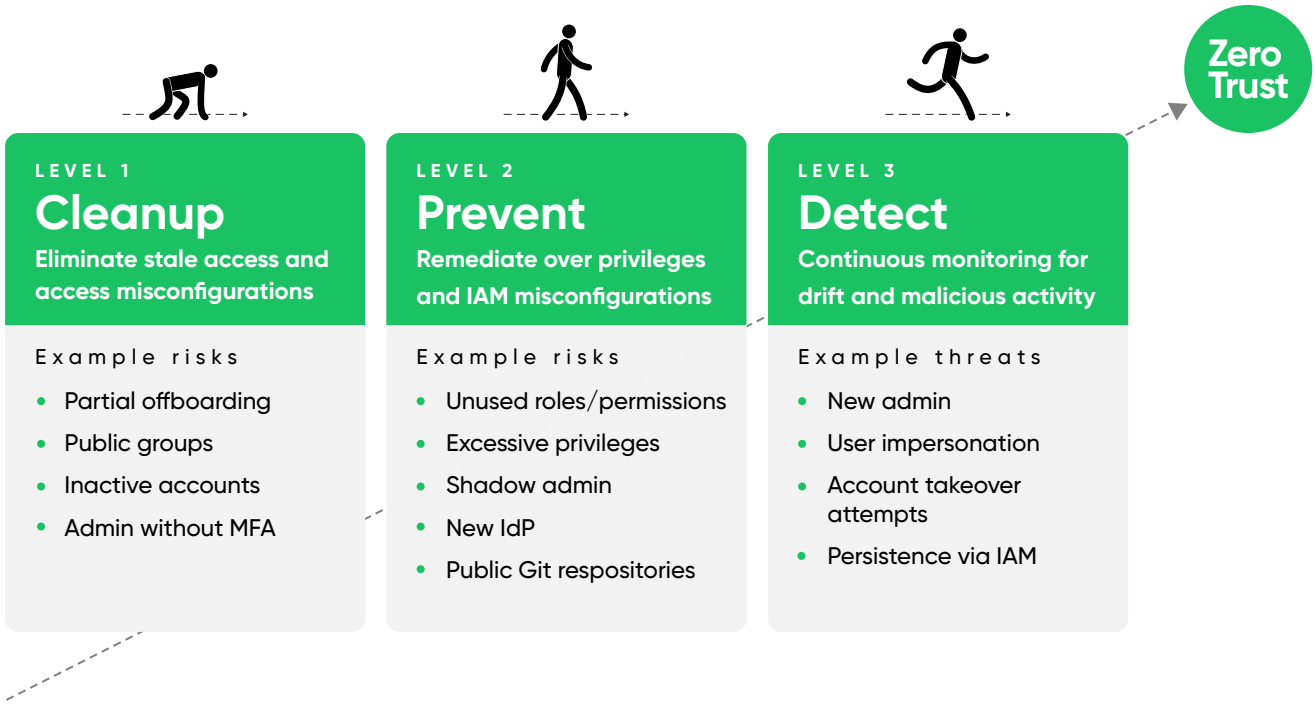
Authomize

Climb the Identity Security Maturity Model on Your Way to Zero Trust

Identity is the new perimeter. In 2022, 84% of identity and security professionals say their organization experienced an identity-related breach. It's not surprising that CISA (Cybersecurity and Infrastructure Security Agency) calls out Identity as a core component of Zero Trust Architecture and the first pillar of the Zero Trust Maturity Model. Authomize's research experts built the Identity Security Maturity Model to help organizations implement the necessary controls for preventing and mitigating most account takeover attacks, and reducing the blast radius of potential threats.



Level 1

Cleanup

Organizations fully understand the risk of stale access and most of them can detect inactive accounts in their primary cloud services and applications. The problem is that secondary and custom applications are not always supported. Stale access that goes unnoticed can be used to attack the organization. In some cases these inactive accounts can save money for the company, for example in the case of SFDC, where seats cost around $1000 each.

You achieved level 1 when you

- Identify and eliminate inactive accounts EVERYWHERE
- Fix partial offboarding
- Ensure MFA is enforced for ALL admins

Level 2

Prevention

Most organizations understand the risks of excessive access in the hands of external and internal attackers and have monitoring solutions in place to review, identify and remediate access privileges. Siloed posture management solutions like CIEM (Cloud Infrastructure Entitlements Management) and SSPM (SaaS Security Posture Management) may miss a few of the access risks that go across applications. For example, the only way to detect and mitigate shadow admins across AWS and Okta is to have complete, granular visibility into both and cross-reference permissions.

You achieved level 2 when you

- Achieve Least Privilege across IaaS, SaaS, and IAM (Identity and access Management) solutions
- Identify and protect exposed assets
- Find and fix IAM misconfigurations that facilitate account takeover and privilege escalations

Level 3

Detection

After achieving a secure state, it is necessary to maintain it by continuously detecting and mitigating active threats. Organizations at this stage are able to detect and stop account takeover attempts, continuously monitor and alert on risky changes across the cloud and IAM infrastructure, and search for events that indicate persistence via the IAM solutions. Being able to prioritize and respond rapidly to the most critical threats is key.

You achieved level 3 when you

- Detect and mitigate Account Takeover across cloud and IAM
- Identify user impersonation and persistent threats in IAM
- Continuously monitor Cloud and IAM to identify and investigate drift

Alignment with IAM Maturity

There are many organizations that are in the midst of implementing IdP/SSO, IGA or PAM solutions and believe they need to wait for these solutions to be fully deployed in order to start monitoring them. Unfortunately malicious actors will not hold off until these projects are complete. IAM solutions hold "the keys to the kingdom" the day identity teams start connecting them to the organization's applications. We recommend implementing identity security controls as part of the adoption of IAM solutions to ensure security and compliance from the get go.

Contact us

About Authomize

Authomize protects organizations from identity-based cyberattacks with the first Identity Threat Detection and Response (ITDR) Platform. Authomize collects and normalizes data of identities, access privileges, assets, and activities from cloud services, applications, and IAM solutions in order to detect, investigate and respond to identity risks and threats. Customers use Authomize to gain visibility of actual access, achieve least privilege across cloud services and applications, secure their IAM infrastructure, and automate compliance and audit preparations.