Optimize Your Microsoft Entra ID Controls

Reach

Find and Fix Misconfigurations and Activated Unused Security Capabilities

Microsoft Entra ID and Conditional Access

Microsoft Microsoft Entra ID enables organizations to enforce secure authentication, manage user identities, and apply contextual access controls to ensure only authorized users and trusted devices can access corporate resources. Entra ID provides the identity layer for Microsoft 365, Azure services, and third-party SaaS applications. Conditional Access is a key component of Microsoft Entra ID, evaluating user identity, device state, location, and risk signals. It then enforces controls such as requiring MFA, compliant joined device, blocking access, or phishing-resistant MFA.

Key Capabilities

Identity Protection to detect risky sign-ins, identify compromised accounts, and respond to suspicious authentications

Conditional Access policies to enforce context-aware access controls based on user identity, device posture, and risk signals

Single sign-on (SSO) across cloud and enterprise applications to streamline access while maintaining centralized identity control

Multi-factor authentication (MFA) to strengthen authentication security and reduce the risk of credential-based attacks

The Configuration Challenge

Microsoft Entra ID and Conditional Access offer powerful access control capabilities, but misconfigurations or incomplete deployments can weaken identity security. Over time, configurations can drift from security baselines, leaving organizations exposed. Why does this happen? Security teams are stretched thin, managing hundreds of controls while trying to keep up with newly released capabilities. Sometimes other teams change controls without security visibility. The result is configuration drift, hidden misconfigurations, and valuable protections left unused.

Common Misconfigurations

Conditional Access policies may not be set to fully enforce device compliance or location-based access restrictions.

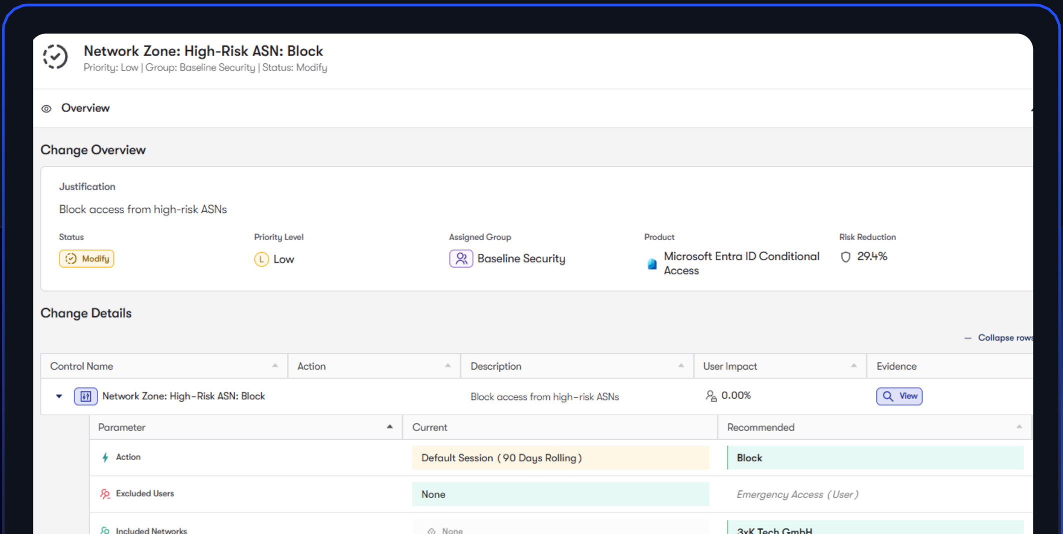
Users, groups, or applications may be excluded from policies, unintentionally weakening access protections.

Multi-factor authentication may only be required for certain users or applications, leaving other access paths less protected.

Risk-based policies that respond to suspicious sign-ins or compromised accounts may not be enabled or fully configured.

Reach Supercharges Microsoft Entra ID and Conditional Access

Reach connects to Microsoft Entra ID to analyze identity security configurations, with particular focus on Conditional Access policies, authentication controls, and identity risk protections. By continuously evaluating how identity policies are implemented, Reach identifies misconfigurations and policy gaps that weaken identity security posture, prioritizes fixes, activates unused capabilities, and guides the security team through remediation.



Network Zone: High-Risk ASN: Block

Priority: Low | Group: Baseline Security | Status: Modify

Change Overview

Justification

Block access from high-risk ASNs

Status	Priority Level	Assigned Group	Product	Risk Reduction
Modify	Low	Baseline Security	Microsoft Entra ID Conditional Access	29.4%

Change Details

Control Name	Action	Description	User Impact	Evidence
Network Zone: High-Risk ASN: Block		Block access from high-risk ASNs	0.00%	View

Parameter	Current	Recommended
Action	Default Session (90 Days Rolling)	Block
Excluded Users	None	*Emergency Access (User)*
Included Networks	None	3xK Tech GmbH

Conditional Access policy coverage and enforcement logic

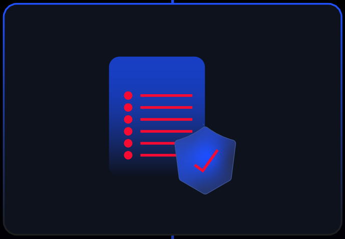
Reach analyzes Conditional Access policies and identifies gaps in policy coverage, missing enforcement conditions, or applications and user groups not protected by policies. This allows organizations to ensure all authentication paths are protected by strong identity-based access controls.

Multi-factor authentication enforcement

Reach analyzes Conditional Access authentication requirements and identifies users, applications, or sign-in scenarios where MFA is not enforced or inconsistently applied so that organizations can reduce the risk of credential compromise and unauthorized account access.

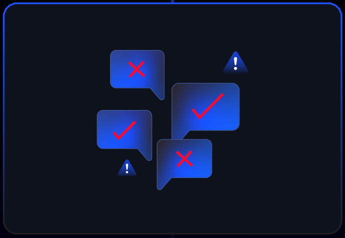
Policy exclusions, exceptions, and bypass conditions

Reach analyzes Conditional Access policy exclusions and identifies overly broad exclusions for users, service accounts, or applications that bypass security controls so that organizations can prevent attackers from exploiting unprotected authentication paths.



Risk-based Conditional Access and identity protection policies

Reach analyzes risk-based access controls and identifies missing or underutilized identity protection policies that respond to risky sign-ins or compromised accounts so that organizations can automatically block or challenge suspicious authentication activity.



Device compliance and device trust requirements

Reach analyzes device conditions and identifies policies that do not enforce device compliance, hybrid join status, or trusted device requirements so that organizations can ensure only secure and managed devices can access sensitive applications.

Reach + Microsoft Entra ID
and Conditional Access

Together, Microsoft Entra ID and Reach help organizations ensure their identity platform remains properly configured, consistently enforced, and aligned with Zero Trust security principles. By optimizing Microsoft Entra ID configurations, organizations achieve stronger identity-based access controls, reduced risk of credential-based attacks and continuous validation of identity security posture.

Learn More reach.security/connect | Webpage | Demo Video