Microsoft Security

Microsoft Entra Conditional Access

Enforce granular access controls with real-time adaptive policies.

Protect your applications, data, network, and infrastructure from threats inside and outside your organization—based on Zero Trust principles—with fine-tuned policies that examine user, device, and network context, as well as real-time risk signals, before granting access.

Protect identities and secure access to resources

Real-time session monitoring and access revocation

Actionable security insights and recommendations

Flexible policy testing with report-only mode

Enhanced protection for critical operations

Key Benefits of Conditional Access

Enhanced security beyond passwords
Consider historical behavior, network conditions, threat signals, device health, and other real-time factors before giving authenticated users access to apps and resources.

Streamlined access management
Design granular access policies, then let the system determine when to allow, block, or limit access based on real-time user context, device, location, and session risk information.

Context-based restrictions on user activity
Prevent insider mistakes or misuse by restricting activity based on user role, device compliance, or other factors, such as whether the user's trying to access a trusted app or a non-compliant website.

User-friendly sign-in experience
Minimize productivity interruptions by only prompting for multifactor authentication (MFA) when risk conditions reach a high enough threshold.

Built on Zero Trust principles
Verify users explicitly by requiring MFA when necessary, enforce least privilege access using granular controls, and assume breach by blocking or limiting access when risk conditions are high.

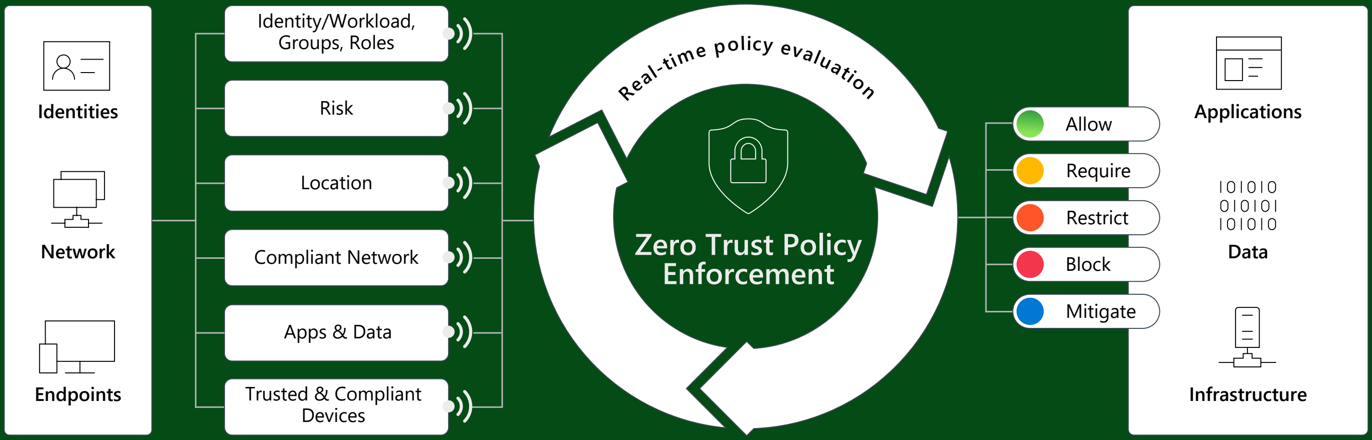
A universal conditional access policy engine

Microsoft Entra Conditional Access works across third-party tools and Microsoft security products—including Microsoft Entra, Microsoft Defender for Cloud Apps, Microsoft Intune, and Microsoft Purview—to enforce granular access controls.

Microsoft-managed Conditional Access policies

To provide secure defaults, Microsoft automatically deploys baseline Conditional Access policies that protect tenants based on risk signals, licensing, and usage. These include policies that enforce MFA for high-risk scenarios. The policies deploy in report-only mode, which means Conditional Access will log the policy results without enforcing them. Once they appear in your tenant, you have 90 days to review, customize, or disable the policies before Microsoft turns them on automatically.

How Conditional Access works



Granular Conditional Access policies that instantaneously adapt to real-time conditions are essential for any Zero Trust security strategy. When a user or workload authenticates their identity, for example, with a username and password, Conditional Access uses machine learning to analyze real-time data signals and assess the user's behavior, location, state of device, application being accessed, and sign-in risk score.

Conditional Access then enforces policies, evaluating which policy rules apply to determine whether to allow, limit, or block access, require stronger authentication, force a password reset, or continuously monitor access.

For more information, visit aka.ms/ConditionalAccess