Optimize Your Microsoft Teams Controls

Reach

Find and Fix Misconfigurations and Activated Unused Security Capabilities

Microsoft Teams

Microsoft Teams is a collaboration platform used for messaging, meetings, sensitive file sharing, and application integration across organizations. It enables employees, partners, and external collaborators to communicate and work together in real time through chat, video meetings, and shared workspaces.

The Configuration Challenge

Although Microsoft Teams is not a security product, it introduces a significant attack surface if settings are misconfigured or poorly governed. Because Teams sits at the center of communication and collaboration workflows, attackers like to exploit it for social engineering, phishing, and identity abuse inside trusted communication channels.

Key Capabilities

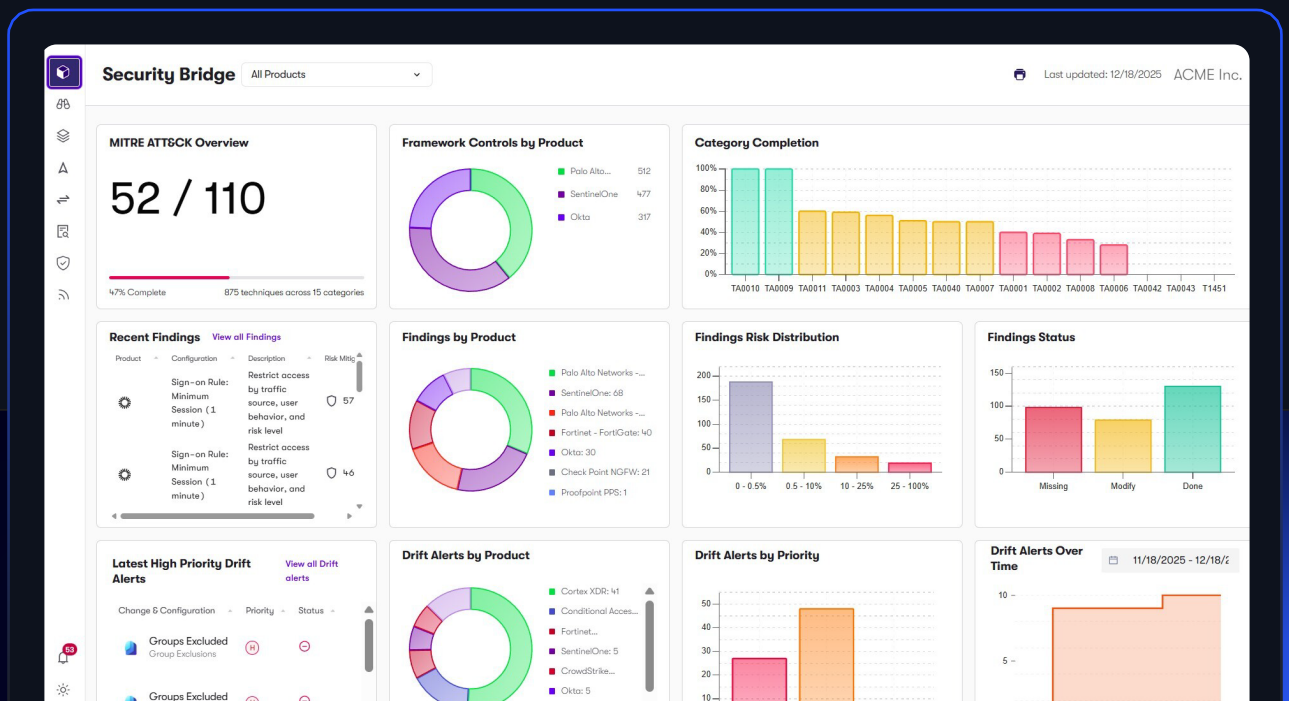
- Persistent team and channel messaging
- Video meetings and voice collaboration
- File sharing through SharePoint and OneDrive integration
- External collaboration with partners, vendors, and guests

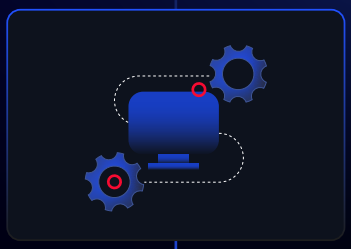
Common Misconfigurations

- Unauthorized or overly permissive external access settings
- Anonymous meeting access and lobby bypass risks
- Unmanaged guest and external account exposure
- Trust boundary and policy misconfigurations that increase lateral social engineering risk

Reach Supercharges Security for Microsoft Teams

Reach connects to Microsoft Teams to analyze collaboration settings, access policies, and trust boundary configurations that impact security posture. By evaluating these configurations against security best practices and frameworks such as the CISA Secure Cloud Business Applications (SCuBA) Secure Configuration Baseline, Reach identifies exposures that increase the risk of social engineering or unauthorized access within collaboration environments.



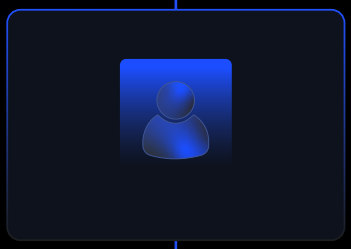


External access and federation configuration policies

Reach analyzes external communication settings and identifies overly permissive federation policies, unrestricted domain access, or external messaging allowances so that organizations can reduce exposure to social engineering attacks originating from external accounts.

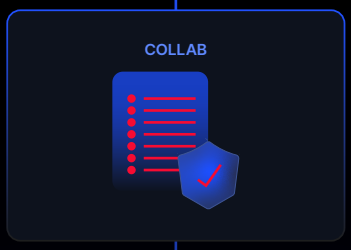
Meeting access settings and anonymous participant policies

Reach analyzes meeting configuration settings and identifies policies that allow anonymous meeting participation or bypass lobby controls so that organizations can prevent unauthorized participants from joining meetings or impersonating trusted users.



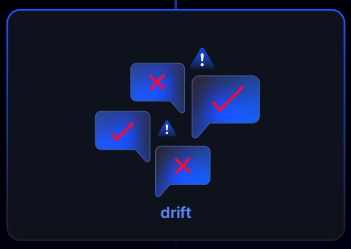
Guest access policies and external account governance

Reach analyzes guest account and external user policies and identifies unmanaged guest access, excessive permissions, or exposure created by external accounts so that organizations can reduce the risk of unauthorized data access and insider-style threats from external collaborators.



Trust boundary and collaboration policy configurations

Reach analyzes collaboration policies governing how internal and external users interact and identifies trust boundary misconfigurations or overly permissive collaboration settings so that organizations can limit lateral social engineering opportunities within trusted communication channels.



Configuration drift across collaboration settings

Reach analyzes changes to external access, meeting policies, guest permissions, and collaboration controls and identifies configuration drift that weakens security posture so that organizations can ensure Teams configurations remain aligned with intended security policies over time.

Reach + Teams

Together, Microsoft Teams and Reach help organizations ensure collaboration environments remain secure, well-governed, and resilient against social engineering attacks within trusted communication channels. Organizations can achieve reduced social engineering exposure, improved control over external and guest access, and continuous assurance of collaboration security posture.

Learn More reach.security/connect | **Webpage**