Optimize Your Microsoft Defender for O365 Controls

Reach

Find and Fix Misconfigurations and Activated Unused Security Capabilities

Microsoft Defender for Office 365

Microsoft Defender for Office 365 protects organizations from phishing, malware, and other threats delivered through Microsoft 365 services such as Exchange Online, SharePoint, and OneDrive. The platform analyzes email messages, attachments, and URLs to detect malicious activity and prevent users from interacting with harmful content. It also provides investigation and response capabilities to help security teams detect and remediate threats across collaboration environments.

The Configuration Challenge

Microsoft Defender for Office 365 provides many layers of protection, but over time, configurations can drift from security baselines, leaving organizations exposed to phishing and malware threats. 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.

Key Capabilities

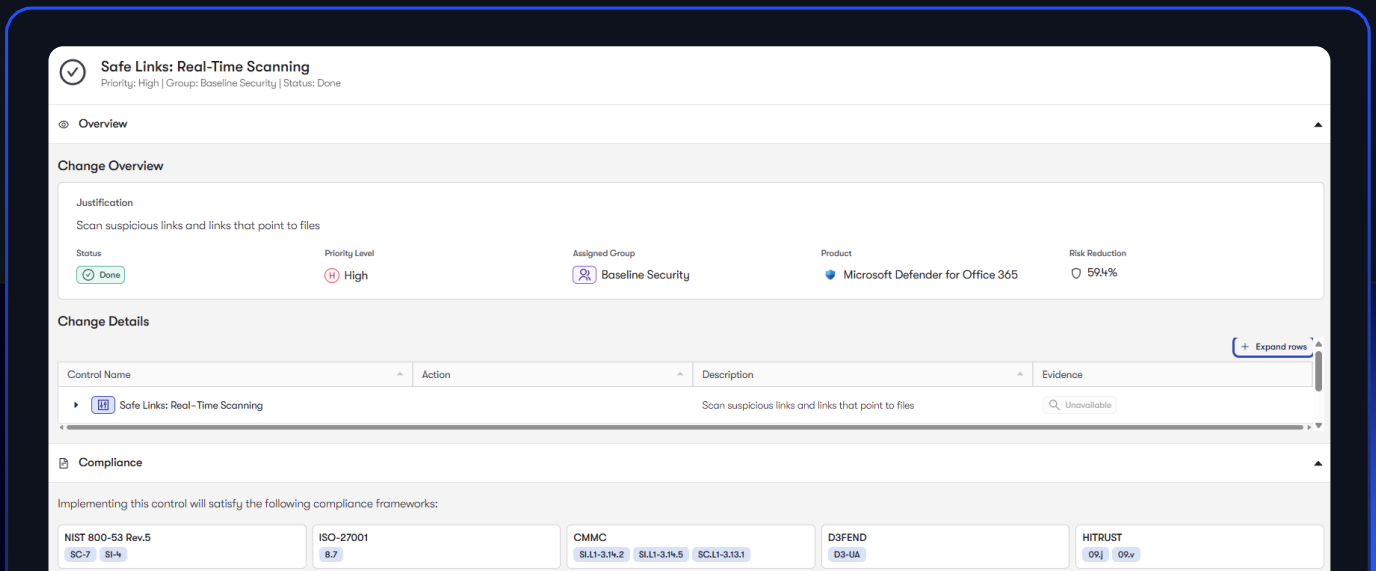
- **Anti-phishing protection** to detect impersonation and credential harvesting attacks
- **Safe Links** to protect users from malicious URLs, phishing and other attacks
- **Safe Attachments** to analyze email attachments in sandbox environments
- **Threat detection** across collaboration tools such as SharePoint, OneDrive, and Teams

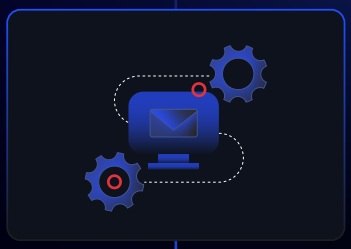
Common Misconfigurations

- **Advanced anti-phishing protections** may not be fully configured for high-value users or domains.
- **Safe Links or Safe Attachments** protections may not be enabled for all users or policies.
- **Inconsistent email security policies** may result in uneven protection levels across the organization.
- **Overly permissive allow lists** may permit malicious senders, domains, or URLs to evade inspection.

Reach Supercharges Your Microsoft Defender for Office 365 Deployment

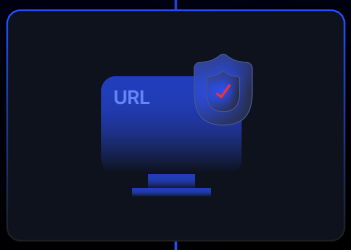
Reach connects to Microsoft Defender for Office 365 to analyze email security policies, phishing protections, and collaboration security configurations. Reach develops a genius-level understanding of how your Microsoft tooling is being used (and misused), and then automatically identifies and remediates misconfigurations, activates unused capabilities, stops configuration drift, and validates over time that security posture remains strong.





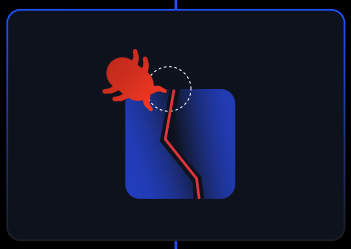
Anti-phishing protection policies and impersonation protection settings

Reach analyzes anti-phishing configurations and identifies missing impersonation protection, incomplete domain protection policies, or insufficient coverage for high-value users so that organizations can reduce the risk of phishing attacks and business email compromise.



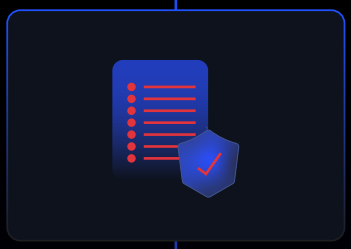
Safe Links policy enforcement and URL protection settings

Reach analyzes Safe Links configurations and identifies disabled URL rewriting, incomplete policy coverage, or user groups not protected by Safe Links policies so that organizations can prevent users from accessing malicious phishing or malware-hosting websites.



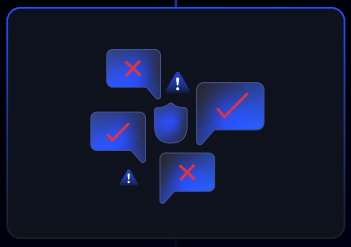
Safe Attachments sandboxing and malware protection policies

Reach analyzes attachment scanning and sandboxing configurations and identifies policies where attachment protection is disabled, inconsistently applied, or configured in monitoring mode so that organizations can block malicious attachments before they reach user inboxes.



Allow lists, bypass rules, and policy exceptions

Reach analyzes allow lists and policy exceptions and identifies overly permissive sender or domain allowances that bypass inspection so that organizations can prevent attackers from exploiting trusted sender policies to deliver malicious email.



Threat protection coverage for collaboration platforms

Reach analyzes protection settings for SharePoint, OneDrive, and Teams and identifies incomplete threat protection policies or gaps in file and link scanning so that organizations can extend threat protection across the full Microsoft 365 collaboration environment.

Reach + Microsoft Defender For O365

Together, Microsoft Defender for Office 365 and Reach help organizations ensure their email and collaboration security controls remain properly configured and consistently enforced. By optimizing Microsoft Defender for Office 365 controls, organizations strengthen protection against phishing, malware, and email-based attacks. Stronger protection against malicious links and attachments, improved security across collaboration platforms, and continuous validation of email security posture ensures strong protection against evolving threats.

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