ThreatLocker® eBook

THREATLOCKER®

How to secure Microsoft 365

A guide to practical recommendations for hardening your Microsoft 365 environment.

How to secure Microsoft 365

Stay ahead of threat actors with this concise eBook on fortifying Microsoft 365. Discover key security configurations to protect your data, assets, and trust against growing threats.

Here are the top strategies you can deploy to harden your Microsoft 365 environment.

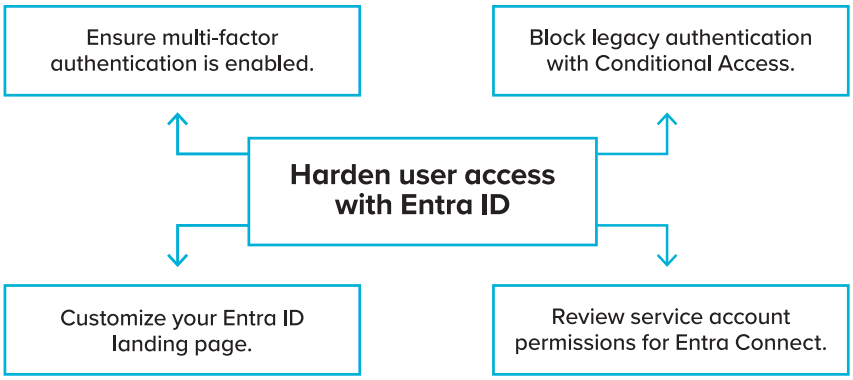
1. Harden user access with Entra ID

Strengthen user access security in Entra ID by following these best practices:

- Block legacy authentication with Conditional Access.
  - Organizations blocking legacy authentication see 67% fewer compromises.
- Review service account permissions for Entra Connect.
  - Avoid express installations and use least privileges for service accounts to prevent over-permissioning. Treat the connector's host like a domain controller to guard AD objects from unauthorized modifications or compromise.
- Customize your Entra ID landing page.
  - Many phishing attacks are not targeted—using your company logo can reduce the efficacy of these attacks because they would not have your logo present on a login page.
- Ensure multi-factor authentication is enabled.
  - Security defaults enforce MFA for tenants created after October 22, 2019.
  - From October 15, 2024, MFA is required for all admin accounts in the Azure portal, Entra, and Intune admin centers.

Why it matters:

Securing user access is a simple, powerful way to boost your organization's security posture.



TIP

ThreatLocker® Tip: "ThreatLocker® Suggested Policies" in Configuration Manager, Application Control, and Elevation Control manage and simplify some of these tasks, providing additional security measures in one central location.

For more information on setting up user access control security, check out this article from Microsoft.

2. Microsoft 365 Apps admin center customization policies

Microsoft offers over 2000 customizable policies for Office Apps. Microsoft's "Security Baseline" covers 137 of these. Policies are not configured by default, but doing so prevents Microsoft 365 apps from being used as an attack vector. A few examples of these policies include:

- Automation security for macro enabled files
- Always open untrusted database files in protected view
- VBA macro notification settings
- Force file extension to match file type
- Always prevent untrusted Microsoft query files from opening
- Require application add-ins are signed by a trusted publisher
- Set default file block behavior

Why it matters:

Security Baseline policies help protect against known vulnerabilities and exploitable features in Microsoft Office apps.

TIP

ThreatLocker® Tip: ThreatLocker® Application Control enables you to choose what applications are allowed to run, while ThreatLocker® Ringfencing™ limits the actions and access of those applications.

3. Cloud Update

The Cloud Update setting in the Microsoft 365 Apps admin center enables administrators to allow workstations to update their apps to the specified version. This feature enables update waves to minimize network congestion, supports rollbacks, and allows update channels to be customized for specific user groups and devices.

Why it matters:

Enabling the Cloud Update feature will allow for patching and version control of Microsoft 365 apps.

TIP

ThreatLocker® Tip: ThreatLocker® maintains thousands of built-in applications, including the Microsoft 365 apps, to ensure a seamless update process.

4. Configure tenant-wide settings for Exchange, SharePoint and Teams

These tenant-wide settings help enforce stricter access controls and data protection measures, reducing risks of unauthorized access and data breaches. Focus on the following:

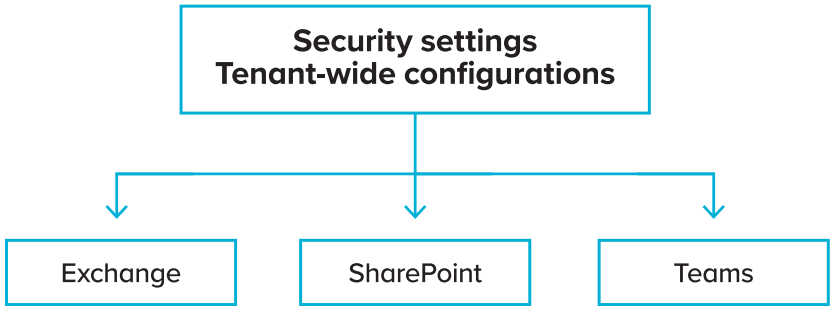
- Exchange security configurations.
  - Set alert policies to notify about certificate expirations and email forwarding by new users or domains.
  - Enforce encryption, require mailbox passwords, and block certain device types via mobile access policies.

- SharePoint security configurations.
  - Restrict access from non-domain joined or non-compliant devices, specified network locations, and applications that don't use modern authentication.
  - Limit external sharing to approved groups and domains or disable it entirely.

- Teams security configurations.
  - Use an approval process alongside permission policies for third-party apps in the Teams admin center to block or limit app installations. This is needed because third-party apps can pose significant risks if they contain malicious code.
  - Enable end-to-end encryption for calls and meetings to meet compliance and prevent interception risks.

Why it matters:

Default settings for Exchange, SharePoint, and Teams often prioritize usability over security, potentially leaving systems exposed to vulnerabilities and cyber threats.



TIP

ThreatLocker® Tip: ThreatLocker® Cloud Detect policies provide visibility into actions taken within SharePoint and Exchange.

In addition, adding mail flow rules in Exchange Online boosts protection with an additional security layer. For more info, see this article.

5. Protect and encrypt sensitive data

Protect your data from breaches caused by unauthorized access, cyberattacks, or human error with these Microsoft features:

- Use Microsoft Purview Information Protection (formerly Microsoft Information Protection) to protect your information. Learn more about the feature in this article.
- Deploy Exchange, Teams, SharePoint, and OneDrive security features through the admin security center, including:
  - Anti-malware protection, anti-phishing protection, and anti-spam protection
  - Safe links and attachments
  - Threat trackers, threat explorers, and attack simulators

Why it matters:

Encrypting and protecting your data reduces the likelihood of successful cyberattacks.

TIP

ThreatLocker® Tip: Add layers to data protection by leveraging ThreatLocker® Storage Control, Application Allowlisting, Ringfencing™, and Configuration Manager.

Explore specific settings for Microsoft's Purview compliance portal in this article.

6. Enable Conditional Access

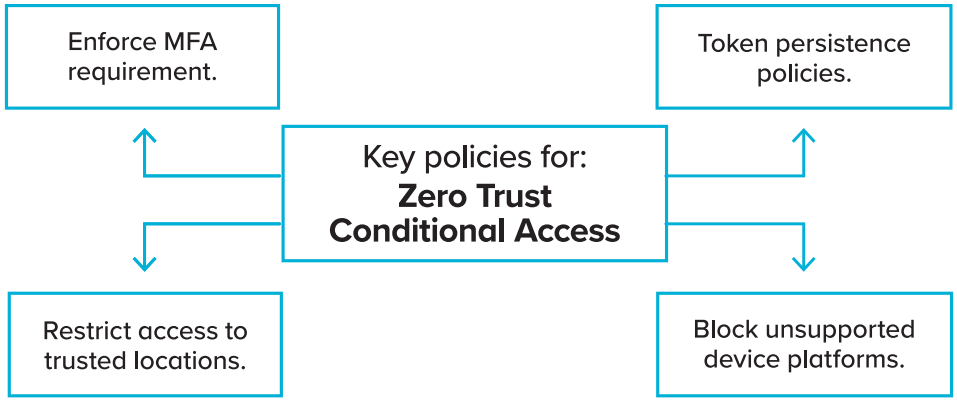
Conditional Access policies leverage user and device identity to enforce access control decisions. While security defaults provide basic protection, Conditional Access introduces Zero Trust principles to your Microsoft 365 environment when carefully planned. Consider these strategies:

- Token persistence policies.
  - Disable token persistence for all accounts—or just admin accounts—signing in from non-compliant devices. Combine this with a revocation policy for accounts flagged with suspicious activity to reduce the risk of token theft.
- Block unsupported device platforms.
  - Minimize attack surface by blocking unsupported platforms. Pair with device authentication or MFA controls for added security.
- Restrict access to trusted locations.
  - Limit account access to trusted locations, reducing risk from compromised credentials.

- Enforce MFA requirements.
    - Configure session controls to require MFA on every login, for sign-ins outside of trusted locations, and when sign-ins are flagged as high risk.

Why it matters:

Conditional Access policies allow organizations to granularize access controls to their Microsoft 365 tenant.



TIP

ThreatLocker® Tip: The ThreatLocker® Access Application dynamically adjusts named locations to include the user's IP address for use in Conditional Access policies.

Microsoft also offers a guide with some commonly used Conditional Access policies in this article.

7. Configure Identity Governance and External Identities

Entra ID's Identity Governance and External Identity configurations help organizations maintain a Zero Trust approach by using least privilege access, identity verification, and offering risk assessment to their tenant. Key features include:

- Access reviews.
    - Provide permissions insights by monitoring administrative and guest user access, business-critical data access, and Azure resource access. With it, administrators can implement an access lifecycle that fits their organizational needs.

- Privileged Identity Management (PIM).
    - Add an approval process to activate roles, enforcement of MFA to activate roles and assign time-bound access to resources with a start and end date to mitigate risk of excessive permissions.

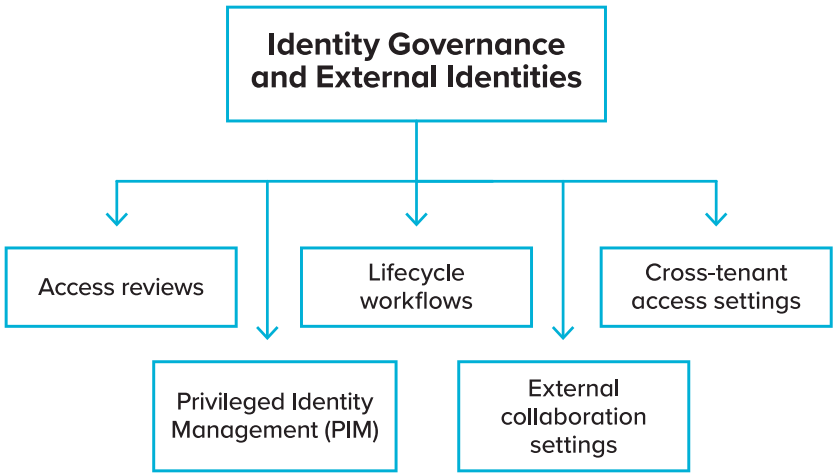
- Lifecycle workflows.
    - Offboard employees in a timely manner, ensure access rights are consistent, automate account creation, role assignment, and access revocation.

- External collaboration settings.
    - Restrict invite settings to control who can invite guests for collaboration on SharePoint and Azure resources as well as adjust access settings for guest and cross-tenant users.

- Cross-tenant access settings.
    - Granularize tenant inbound and outbound access, tenant restrictions for external users and applications as well as trusting external organizations MFA and compliant device claims.

Why it matters:

Configuring Identity Governance and External Collaboration settings ensure only authorized users access sensitive data, provide detailed audit logs of access, and enforce access controls to meet a Zero Trust model by treating identity as a primary security perimeter.



TIP

ThreatLocker® Tip: ThreatLocker® Cloud Detect can alert based off PIM approvals and denials, as well as PIM settings changes.

For an overview of Identity Governance use cases, check out this article.

See an overview of External Identities in this article.

CONCLUSION

Securing Microsoft 365 isn't easy. Protecting your business requires strategies like hardening user access with Entra ID, reducing attack surfaces in Office apps, and encrypting sensitive data.

ThreatLocker® offers Microsoft 365 integrations that keep track of SharePoint activity logs and set alerts for security risks, including leaked credentials, sign-ins from anonymous IP addresses, and more.

Learn more about how ThreatLocker® adds security event monitoring to your cloud and endpoint environments by booking a free demo.

More information on baselines and best practices

Best practices for securely using Microsoft 365—the CIS Microsoft 365 Foundations Benchmark now available | Microsoft Security Blog

Security baseline for Microsoft 365 Apps for enterprise - Microsoft 366 Apps | Microsoft Learn

Granular delegated admin privileges (GDAP) introduction - Partner Center | Microsoft Learn

Manage add-ins in the admin center - Microsoft 365 admin | Microsoft Learn

Microsoft Entra Connect: Accounts and permissions - Microsoft Entra ID | Microsoft Learn

Microsoft Entra ID Governance - Microsoft Entra ID Governance | Microsoft Learn

About ThreatLocker®

ThreatLocker® is a Zero Trust Endpoint Protection Platform that improves enterprise-level server and endpoint security with Zero Trust controls, including: Allowlisting, Ringfencing™, Storage Control, Network Control, ThreatLocker® Detect, Elevation Control, and Configuration Manager.

sales@threatlocker.com

+1-833-292-7732

threatlocker.com