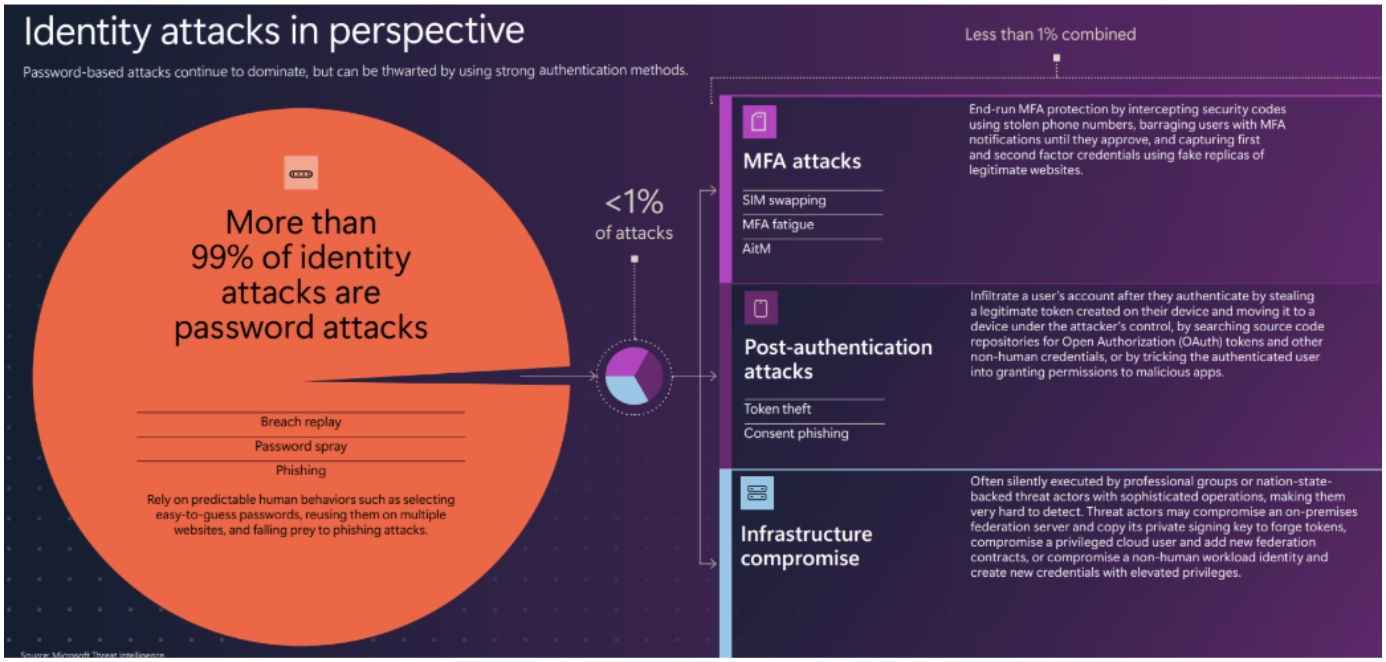
suresystems

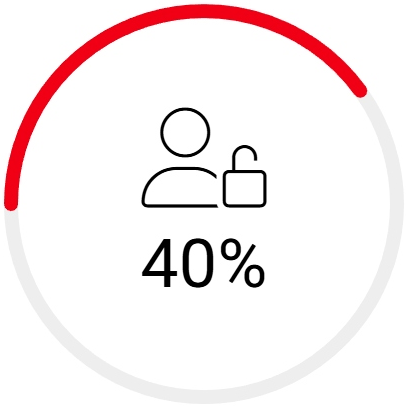
MFA Adoption in Microsoft 365

Executive Summary:

- **99% of identity attacks are password attacks**
- **Business Impact:** Compromised accounts can lead to data theft, financial loss, and reputational damage.
- **Real-World Example: U**nitedHealth Group confirmed a ransomware attack that compromised the private data of over 100 million individuals. Attackers used stolen credentials to access a service lacking multifactor authentication, exfiltrated data, and deployed ransomware, underscoring the critical need for MFA in protecting sensitive information.



Findings from your Tenant:



Users without MFA

22
Users without MFA

1
Users with weak MFA

5
Users Being Excluded from MFA Enforced Policies

Active Licensed User without MFA

No data found

Global Admins without MFA

Display Name	Email	Days Since Login
Bruce Banner	bbanner@tminus365.com	673

Policies Enforcing MFA

MFA is enforced for all users
Conditional Access Policy found that enables MFA for all users.

MFA is enforced for Azure Management
Conditional Access Policy found that enables MFA for Azure Management.

MFA shall be required to enroll devices to Azure AD
A conditional access policy is either missing or misconfigured.

MFA is enforced on accounts with highly privileged roles
Conditional Access Policy found that is enforcing MFA for admins.

Legacy Authentication shall be blocked
Conditional Access Policy found

Users are enrolled in MFA and covered by a policy
22 users do not have MFA enabled

Recommended Remediation Plan

Immediate Actions (0-30 days)

- Identify all accounts missing MFA
- Enforce MFA for admins and high-risk roles
- Communicate the MFA rollout plan to employees

Short-Term Fixes (30-90 days):

- Enroll all users in MFA using Microsoft Authenticator or other approved methods
- Configure conditional access to require MFA
- Provide user training and support to ease the transition

Long-Term Improvements (90-180 days):

- Monitor and report on MFA compliance quarterly
- Disable Weaker forms of MFA such as Email/SMS
- Enable Phishing Resistant MFA for Admin users.

Proposed Project: MFA Rollout & Enforcement

Project Objectives:

- **Strengthen Identity Security** – Minimize compromised accounts through the added layer of MFA.
- **User Adoption & Compliance** – Ensure a seamless user experience and adherence to regulatory or policy requirements.
- **Best Practices & Governance** – Align with Microsoft's recommended security best practices for identity protection.
- **Visibility & Reporting** – Provide insights into usage, user compliance, and security posture.

Scope of Work

Discovery and Assessment

1. **Environment Review**
   - Identify all user accounts (including shared/service accounts) in Microsoft 365.
   - Assess current authentication methods and password policies.
   - Validate licensing requirements (e.g., Microsoft 365 Business Premium, Office 365 E3/E5, etc.).
2. **Requirements Gathering**
   - Confirm business, security, and compliance needs.
   - Identify any third-party applications or legacy systems that might be impacted by MFA.

Estimated Hours: 4

Project Planning and Kickoff

1. **Project Plan Creation**
   - Develop a project plan and timeline (account grouping, enrollment strategy).

2. **Kickoff Meeting**
   - Present the objectives, project timeline, and stakeholder responsibilities.
   - Outline communication plan and escalation procedures.

Estimated Hours: 2

Configuration and Implementation

1. **MFA Settings in Microsoft Entra**
   - Enable and configure MFA settings within Microsoft Entra (e.g., Conditional Access).
   - Determine the MFA methods (Authenticator app) and any exceptions or exclusions.
2. **Policy Setup & Pilot Group**
   - Define pilot group(s) to test the MFA enrollment process and policy effects.
   - Adjust configurations based on pilot feedback and organizational security needs.

Estimated Hours: 6

User Enrollment and Rollout

1. **Pilot Deployment**
   - Enroll pilot users in MFA to verify user experience and identify potential issues.
   - Document lessons learned for larger rollout.
2. **Phased Rollout**
   - Gradually expand MFA enrollment to additional user groups/departments.
   - Monitor enrollment progress, provide support, and address issues in real time.
3. **Communications**
   - Provide end-user notifications and guidance on how to set up MFA.

Estimated Hours: .5/user

Testing and Validation

1. **Functionality Testing**
   - Validate MFA prompts on various devices (desktop, mobile) and services (web apps, third-party services).
   - Test Conditional Access rules and exceptions.
2. **Reporting & Analytics**
   - Review Entra sign-in logs and MFA usage reports to confirm adoption rates.
   - Check for any anomalies or unauthorized access attempts.
3. **Adjustment & Optimization**
   - Refine MFA policies or user messaging based on test results and feedback.

Estimated Hours: 3

Documentation and Training

1. **User-Facing Documentation**
   - Prepare easy-to-follow guides or quick reference materials for end users.
   - Document FAQs and common issues to reduce help desk burden.
2. **Knowledge Transfer**
   - Provide final documentation on MFA configuration, policies, and best practices.

Estimated Hours: 4

Project Management (Ongoing)

1. **Coordination & Status Updates**
   - Conduct regular status meetings or email updates to key stakeholders.
   - Track project timeline, risks, and issues, and manage escalations.
2. **Resource Management**
   - Assign and manage tasks as needed throughout the project.

Estimated Hours (over project duration): 4
(May be spread out depending on the project length.)

Estimated Hours Summary

Task	Estimated Hours
Discovery & Assessment	4
Project Planning & Kickoff	2
Configuration & Implementation	6
User Enrollment & Rollout	.5/user
Testing & Validation	3
Documentation & Training	4
Project Management (Ongoing)	4

Note: Number of users scoped only for users who aren't enrolled for MFA currently

Assumptions and Constraints

1. **Licensing**: The client has the necessary Microsoft 365 licenses that support MFA and Conditional Access.
2. **Compatible Devices**: End-user devices support the chosen MFA method (e.g., smartphone with Authenticator app).
3. **Stakeholder Availability**: Key stakeholders and user champions are available for timely feedback and testing.
4. **Single Tenant**: Scope is limited to one Microsoft 365 tenant unless otherwise specified.

---

6. Exclusions (Out of Scope)

- Advanced security measures beyond standard MFA setup (e.g., advanced identity protection or third-party MFA solutions).
- Remediation of issues unrelated to MFA (e.g., upgrading legacy systems, domain migrations).
- Significant custom integrations with non-Microsoft tools (unless specified).

---

7. Pricing

- **Professional Services**: Based on the estimated hours above, delivered on a Time & Materials (T&M) or fixed-fee basis.
- **Travel & Expenses**: Billed separately at cost, if onsite assistance is required.