Checklist: Prevent Brute Force Attacks in Microsoft 365 Tenants

Brute-force attacks are increasingly more targeted, persistent, and successful. In 2024, Microsoft 365 saw over 30 billion password-based attacks per month. High-profile incidents like the Midnight Blizzard campaign show how easily attackers exploit outdated protocols, over-permissioned accounts, and lack of visibility.

This checklist is designed for IT and security admins who want to move beyond reactive defenses and take concrete, prioritized steps to secure their Microsoft 365 environment against brute-force attacks.

Immediate Actions				
Action Item	**Assigned to**	**Due Date**	**Notes**	✔
ENABLE AUDIT LOGGING				
Turn on audit logs if not already enabled				
Review for frequent failed logins, unusual geographies, or new admin role assignments				
Use tools like Microsoft Sentinel or Azure Monitor to automate alerts				
DISABLE LEGACY AUTHENTICATION PROTOCOLS				
Identify users accessing via IMAP, POP, or SMTP				
Block legacy auth with Conditional Access				
Transition users to modern authentication				
RESTRICT POWERSHELL ACCESS				
Limit PowerShell to approved admins via Conditional Access				
Require MFA or passwordless for PowerShell sessions				
Monitor usage via logging and review regularly				
BLOCK ANONYMOUS OR HIGH-RISK IPS				
Use Conditional Access to deny access from risky geographies or anonymizers				
Require MFA for privileged roles				
Allow access only from compliant, trusted devices				
Test policies with Report-Only Mode before rollout				

Medium-Term Actions				
Action Item	**Assigned to**	**Due Date**	**Notes**	
MONITOR FOR INDICATORS OF COMPROMISE (IOCS)				
Watch for login attempts from flagged IPs (e.g., 158.58.173[.]40)				
Audit anonymous access and impersonation roles				
Use Entra ID Sign-In Logs and Defender for Identity for detection				
ENFORCE STRONG PASSWORD AND SESSION POLICIES				
Set secure password rules and account lockout settings				
Configure session timeouts (e.g., 8h for Admin Center)				
Shorten timeouts for sensitive areas using Conditional Access				
REDUCE ADMIN PRIVILEGES				
Audit all admin roles and trim unnecessary ones				
Apply least privilege principle				
Use RBAC to grant scoped access				
Use CoreView's Admin Permissions Scanner if available				

Advanced Actions				
Action Item	**Assigned to**	**Due Date**	**Notes**	
REFINE CONDITIONAL ACCESS POLICIES				
Require MFA or passwordless auth for all sensitive roles				
Block access from countries where you don't operate				
Allow only compliant, corporate devices				
DEPLOY AUTOMATED THREAT RESPONSE				
Use Microsoft Defender or Azure Sentinel for real-time detection				
Automate session revocation, password resets, and IP blocks				
MONITOR APP PERMISSIONS				
Audit all third-party apps and review permission scopes				
Revoke access for unused or overly permissive apps				

Want to go deeper? Take the next step with these resources:

- **Benchmark your environment with the CIS Baselines:**
  Compare your Microsoft 365 setup—including Entra, Intune, and Exchange—against industry-backed best practices. Download the CIS Baselines
- **See how attackers actually get in:**
  The Anatomy of a Microsoft 365 Attack breaks down how threats like Midnight Blizzard bypass weak spots and persist undetected. Explore the attack blueprint
- **Build long-term resilience, not just reactive defenses:**
  Use the Cyber Resilience Maturity Model to assess your readiness across entry points, privilege escalation, and recovery. Get the maturity model

CoreView builds cyber resilience into Microsoft 365 by detecting risky configurations, locking down excessive permissions, and keeping your environment recoverable. From blocking legacy protocols and overprivileged roles to restoring secure baselines after drift, CoreView helps IT and security teams stay ahead of tenant-level attacks—without relying on manual cleanup. Read more