KAI

TECHNICAL RESOURCE BLUEPRINT

The Zero Trust Starter Kit:
20 Baseline Conditional Access Policies

A practical, enterprise-grade blueprint for implementing Zero Trust within Microsoft 365. Translate theory into exact Entra ID & Intune configurations without breaking employee workflows.

AUTHOR:
KAI Security Architecture Team

TARGET AUDIENCE:
M365 IT Directors & Security Leaders

SCOPE:
Entra ID & Intune Policies

About This Blueprint

While many vendors treat Zero Trust as abstract theory, this guide translates architecture into the exact 20 Conditional Access (CA) configurations you need to protect Identity, Devices, and Data—maximizing ROI on existing M365 licenses with zero downtime.

The Expected Outcome

By implementing these 20 baseline policies, your organization shifts from a fragile "castle-and-moat" posture to a resilient "Assume Breach" foundation—shutting down common attack vectors and drastically reducing blast radius while maintaining employee trust.

⚠️ The Golden Rule of Deployment

Never deploy these policies in "On" mode immediately. Always deploy in *Report-Only* mode first for at least 14 days to review Entra ID sign-in logs and surface potential compatibility issues before enforcement. **Secure the business, but never break the business.**

The 60-Day Frictionless Deployment Roadmap

IMPLEMENTATION STRATEGY

Rolling out 20 policies simultaneously causes helpdesk overload. Follow our 4-sprint phased deployment plan to telemetry-test each layer before enforcement.

SPRINT 1 (WEEKS 1-2)

The Silent Shield

Action: Deploy Phase 1 (Blocks) in Report-Only for 3 days, then switch to ON. Deploy Phase 2 (Identity) in Report-Only.

Goal: Stop automated bot attacks immediately with zero end-user friction.

SPRINT 2 (WEEKS 3-4)

Identity Enforcement

Action: Switch Phase 2 (Identity) to ON. Deploy Phase 3 (Device Health) in Report-Only mode.

Goal: Secure password vulnerabilities and launch the "Security for Humans" campaign.

SPRINT 3 (WEEKS 5-6)

The Zero Trust Perimeter

Action: Switch Phase 3 (Device Health) to ON. Deploy Phase 4 (Session/Data) in Report-Only mode.

Goal: Enforce that corporate data can only live on healthy, approved devices.

SPRINT 4 (WEEKS 7-8)

Advanced Containment

Action: Switch Phase 4 (Session/Data) to ON.

Goal: Lock down session hijacking and set boundaries for Shadow AI tools.

Phase 1: Closing the Front Door (Block Policies)

6 POLICIES

Shut down outdated, unmanaged, or high-risk entry points to stop automated attacks immediately.

01 Block Legacy Authentication

WHAT IT DOES

Blocks authentication protocols that don't support modern MFA (IMAP, POP3, SMTP, basic auth).

WHY IT MATTERS

Legacy protocols bypass modern security controls. Attackers use compromised passwords against IMAP/POP3 to skip MFA entirely.

02 Block High-Risk Sign-ins

WHAT IT DOES

Integrates with Entra ID Protection to automatically block logins flagged as highly suspicious (anonymous IPs, impossible travel).

WHY IT MATTERS

Stops automated credential-stuffing attacks and botnets in real time before initial foothold.

03 Block Access from High-Risk Countries

WHAT IT DOES

Uses geofencing to deny authentication originating from regions where your company does no legitimate business.

WHY IT MATTERS

Drastically shrinks your global attack surface right at the perimeter.

04 Block Unsupported Device Platforms

WHAT IT DOES

Prevents sign-ins from unmanaged or obsolete OS versions (Linux, ChromeOS, old Windows/Android).

WHY IT MATTERS

Closes gaps that standard compliance policies miss. If your company uses Windows/macOS/iOS/Android, block unapproved OS attempts.

05 Block Device Code Flow

WHAT IT DOES

Disables OAuth device code authentication designed for devices without a web browser (smart TVs).

WHY IT MATTERS

Prevents device code phishing attacks that trick users into authenticating attacker sessions.

06 Block Authentication Transfer

WHAT IT DOES

Blocks QR-code-based authentication transfer mechanisms between devices.

WHY IT MATTERS

Prevents "quishing" (QR phishing) where users scan codes handing over active authenticated sessions to attackers.

Phase 2: Identity & Authentication Protection

6 POLICIES

Enforce strict verification for all users, requiring maximum security for administrative privileges.

07 Require Phishing-Resistant MFA for Admins

WHAT IT DOES

Requires admin accounts to authenticate strictly using FIDO2 keys, passkeys, or Windows Hello for Business.

WHY IT MATTERS

Standard push notifications can be phished via AiTM proxies. Phishing-resistant credentials are domain-bound.

08 Require Phishing-Resistant MFA for Break-Glass Accounts

WHAT IT DOES

Dedicated policy forcing emergency accounts to use hardware FIDO2 keys.

WHY IT MATTERS

Ensures emergency admin accounts remain protected even if standard policies fail.

09 Require MFA for Azure & Admin Portals

WHAT IT DOES

Mandatory MFA prompt whenever accessing administrative interfaces (Azure Portal, M365 Admin Center).

WHY IT MATTERS

Locks down the core control plane of your cloud infrastructure.

10 Require Strong MFA for All Users

WHAT IT DOES

Requires modern MFA for every user, explicitly excluding weak methods like SMS and voice calls.

WHY IT MATTERS

SMS can be SIM-swapped or intercepted. Closing legacy MFA options secures all user endpoints.

11 Require MFA & Password Reset for Risky Users

WHAT IT DOES

Automatically flags accounts with dark-web leaked credentials, requiring MFA + mandatory password reset.

WHY IT MATTERS

Instantly neutralizes compromised credential leaks.

12 Require TAP for Security Info & Device Registration

WHAT IT DOES

Forces Temporary Access Pass (TAP) or fresh MFA when registering new auth methods or Intune devices.

WHY IT MATTERS

Prevents an attacker with temporary password access from registering rogue devices.

Phase 3: Device Health & Access Control

3 POLICIES

Ensure that devices attempting to access corporate data meet strict security standards.

13 Require Compliant Device (Desktops & Laptops)

WHAT IT DOES

Blocks M365 access from computers not enrolled in Intune and marked compliant (or Entra-joined).

WHY IT MATTERS

Primary security perimeter gate. Personal devices cannot touch company data unless fully managed.

14 Require App Protection & Approved Apps (Mobile BYOD)

WHAT IT DOES

Forces mobile access exclusively through approved apps protected by Intune App Protection Policies (MAM).

WHY IT MATTERS

Protects corporate data on personal mobile devices without full device enrollment or touching personal photos.

15 Block Mobile Browser Access

WHAT IT DOES

Denies mobile web browsers (Safari, Chrome) from accessing M365 cloud apps.

WHY IT MATTERS

Closes BYOD loopholes, preventing users from downloading corporate files to unmanaged phone storage.

Phase 4: Session Controls & Data Protection

5 POLICIES

Limit the lifespan and usability of authenticated sessions to minimize data exfiltration and AI risk.

16 Windows Token Protection

WHAT IT DOES

Cryptographically binds authentication tokens to the specific Windows device that requested them.

WHY IT MATTERS

Stops token theft attacks. Stolen memory tokens become instantly useless on any other machine.

17 Sign-In Frequency & Session Lifetime Limits

WHAT IT DOES

Sets time limits on active user sessions before re-authentication is required.

WHY IT MATTERS

Limits the blast radius of a stolen session token.

18 Block Persistent Browser Sessions

WHAT IT DOES

Disables persistent browser sign-in states across session closes.

WHY IT MATTERS

Stops subsequent users on shared or public computers from opening employee sessions.

19 Block Downloads via Conditional Access App Control

WHAT IT DOES

Routes browser sessions through Defender for Cloud Apps to allow web viewing while blocking local file downloads.

WHY IT MATTERS

Enables safe web document viewing without saving corporate files to unmanaged hard drives.

20 Block Unsanctioned Generative AI & Web Leaks

WHAT IT DOES

Integrates CA with Defender for Cloud Apps to block navigation to consumer AI tools and restrict copy-pasting corporate text into external forms.

WHY IT MATTERS

Prevents employees from inadvertently pasting proprietary code, PII, or strategy into public AI models.

Security for Humans: Change Management Guidelines

USER ADOPTION

1. **Explain the "Why"**
   Don't just send an IT memo dictating rules. Host a brief company town hall framing changes around protecting employee hard work and personal data.

2. **Ditch 40-Page Manuals**
   Provide 1-page visual cheat sheets for setting up Authenticator or enrolling a new device.

3. **30-Day Nudge Campaign**
   Drip out weekly security tips in Slack/Teams to slowly build a security-first culture without overwhelming staff.

4. **Safe Space Feedback Loop**
   In Report-Only mode, proactively reach out to users who trigger a block so their setup is fixed before enforcement.

Need Help Implementing This Architecture?

Deploying these 20 policies is the foundation of a resilient business. Let's talk about how to implement these exact policies with zero workflow disruption.

Book a 15-Minute Strategy Call →