

03. Cloud Break-Glass Security Checklist

Reclaiming Root Ownership of M365, Entra ID, Azure, AWS, and DNS Registrars

1. MICROSOFT 365 & ENTRA ID TENANT RECLAMATION PROTOCOL

Step 1.1 - Audit Granular Delegated Admin Privileges (GDAP): Navigate to Microsoft 365 Admin Center -> Settings -> Partner relationships. Document every active partner relationship and revoke Global Administrator or Privileged Role Administrator delegations held by the outgoing MSP.

Step 1.2 - Audit Enterprise Applications & Service Principals: In Entra ID -> Enterprise Applications, inspect all third-party OAuth apps registered by the MSP (e.g., CIPP, Liongard, ITGlue sync, ConnectWise, Datto SaaS). Disable or delete service principals belonging to the outgoing MSP's multi-tenant management tools at cutover.

Step 1.3 - Conditional Access Exclusions Audit: Inspect all Conditional Access policies for excluded IP ranges (frequently used by MSPs to bypass MFA from their office or offshore SOC). Remove MSP static IPs from Named Locations.

2. ON-PREMISES ACTIVE DIRECTORY, HYPERVISORS & NETWORK PERIMETER

Step 2.1 - Domain Admin & KRBtgt Rotation: Remove all `msp\_\*` or vendor service accounts from Domain Admins, Enterprise Admins, and Schema Admins. Rotate the `krbtgt` account password twice (separated by 12 hours) to invalidate any Golden Ticket Kerberos persistence.

Step 2.2 - RMM Agent Eradication: Outgoing RMM agents (ConnectWise Automate/ScreenConnect, Datto RMM, NinjaOne, Kaseya VSA) run as `NT AUTHORITY\SYSTEM`. Verify complete removal of both the primary RMM service and secondary remote-control binaries (`ScreenConnect.ClientService.exe`).