LMNTRIX
BE THE HUNTER | NOT THE PREY

MICROSOFT 365 & INTUNE SECURITY HARDENING GUIDE

Preventing Cloud Management Plane Attacks Practical Implementation Guide for Security Teams Lessons from the Stryker Incident (March 2026)

WHITEPAPER

LMNTRIX USA
19800 MacArthur Blvd,
Suite 850
Irvine, CA 92612
sales@lmntrix.com
888-388-1879

LMNTRIX UK
Kemp House, 152–160
City Road, London,
EC1V 2NX
sales@lmntrix.com
+44.808.164.9442

LMNTRIX INDIA
VR Bengaluru, Level 5, ITPL Main
Rd, Devasandra Industrial Estate,
Bengaluru, Karnataka 560048, India
sales@lmntrix.com
+91-22-49712788

LMNTRIX AUSTRALIA
Level 25, 100 Mount Street,
North Sydney 2060
sales@lmntrix.com
+61.288.805.198

LMNTRIX SINGAPORE
60 Kaki Bukit Place, #05-19,
Eunos TechPark
sales@lmntrix.com
+65-3129-2639

EXECUTIVE SUMMARY

On March 11, 2026, an Iran-linked threat group called Handala—assessed as a front for Void Manticore, an MOIS-affiliated APT—compromised Stryker Corporation's Microsoft 365 tenant and used Microsoft Intune's native remote wipe capability to execute a mass device wipe. Handala claimed the attack destroyed over 200,000 endpoints across 79 countries; the exact scope has not been independently confirmed by Stryker.

The attackers abused the cloud management plane itself—a legitimate MDM feature—to execute a catastrophic wiper attack. Because the attack occurred through legitimate APIs and administrative features, endpoint security tools typically cannot distinguish legitimate management-plane commands from malicious ones.

This guide provides practical, immediately actionable hardening controls for Microsoft 365 and Intune environments. Configuration paths, KQL queries, and PowerShell commands are provided as starting points and should be tested in your environment before production deployment. The goal is simple: make sure this cannot happen to your organization.

> **Practical Note:** *Traditional endpoint-only controls may not reliably detect this type of attack—actions came through authorized cloud management APIs. Organizations must extend detection to identity and cloud admin layers, not just endpoints.*

Contents

CLOUD CONTROL PLANE

In traditional on-premises Active Directory, Domain Admin was the keys to the kingdom. An attacker who compromised a Domain Admin account could push Group Policy to every endpoint, reset any credential, access any resource, and effectively own the enterprise. The modern Microsoft 365 environment has the same power—but it is now distributed across four cloud services, each accessible from anywhere on the internet.

- **Microsoft Intune = Group Policy + SCCM.** Intune manages device configuration, software deployment, compliance enforcement, and—critically—remote wipe. A compromised Intune Administrator can push destructive actions to every managed endpoint, just as a Domain Admin could push a malicious GPO to every domain-joined machine.
- **Microsoft Entra ID = The Domain Controller.** Entra ID is the identity authority for the entire tenant. It controls who can authenticate, what roles they hold, what Conditional Access policies apply, and which federation trusts are honored. Compromising Entra ID is the cloud equivalent of owning the domain controller—every downstream service trusts its assertions.
- **Microsoft Graph API = The Programmatic Admin Console.** Graph API provides programmatic access to virtually every administrative function in M365. An attacker with the right permissions can enumerate users, read mail, modify configurations, and execute device actions—all through authenticated REST calls that look like legitimate admin activity. This is the interface an attacker would use to script tenant-wide destructive actions at scale.
- **OAuth App Registrations = Service Accounts with Delegated Power.** OAuth applications and service principals can hold persistent, non-interactive permissions to device management APIs, mail access, and directory operations. A malicious or compromised app registration with the right consent grants is functionally equivalent to a rogue service account with Domain Admin privileges—except it never needs a password and its access persists until explicitly revoked.

The controls in this guide are designed to protect this cloud control plane with the same rigor that mature organizations once applied to their on-premises Domain Controllers: least privilege, tiered access, approval workflows, continuous monitoring, and the assumption that any single credential can be compromised.

THE FOUR MISCONFIGURATIONS THAT ENABLE TENANT-LEVEL ATTACKS

Most Microsoft tenants that suffer destructive attacks share four common weaknesses. If your organization has all four—and most do—an attacker needs only a single phished admin credential to execute a Stryker-style attack.

Misconfiguration 1: Too Many Accounts Have Device Wipe Permissions

Default Intune roles include destructive permissions (Wipe, Retire, Factory Reset, Delete). Any compromised account with these permissions can script tenant-wide destructive actions through the Graph API, iterating wipe commands across every managed device.

- **Fix:** Create custom RBAC roles without wipe permissions. Limit wipe capability to 2 break-glass accounts only. (See Controls 8, 9)

```
POST /deviceManagement/managedDevices/{id}/wipe   ← This is the
Intune wipe endpoint attackers would use in this type of attack
```

Misconfiguration 2: Admin Access Allowed from Unmanaged Devices

Administrators can often access the Intune portal from any device, anywhere. Attackers who steal credentials log in from their own infrastructure and execute destructive actions.

- **Fix:** Conditional Access policies requiring compliant devices + phishing-resistant MFA + named network locations for all admin portal access. (See Controls 5, 6)

Misconfiguration 3: Permanent Administrative Role Assignments

Privileged roles like Intune Administrator and Global Administrator are often permanently assigned. A compromised credential immediately grants destructive capabilities with no approval gate.

- **Fix:** Privileged Identity Management (PIM) with eligible-only assignments, MFA, approval workflows, and 1-hour activation windows. (See Control 2)

Misconfiguration 4: OAuth Application Consent Enabled for Users

When user consent is enabled, attackers can trick users into granting API access to malicious applications—including permissions that allow device management operations.

- **Fix:** Disable user consent tenant-wide. Require admin approval for all application permissions.(See Controls 12, 13, 14)

TOP 10 ACTIONS TO IMPLEMENT IMMEDIATELY

Start here. Effort estimates assume a mid-size organization with existing M365 E5 licensing.

If you only implement five controls from this guide, start with these:

1. **FIDO2 for admin accounts** (Control 1) — Stops AiTM phishing of admin credentials
2. **Remove wipe permissions from standard roles** (Control 8) — Directly prevents mass device destruction
3. **Restrict admin portal access to managed devices** (Control 6) — Blocks attackers from using stolen credentials remotely
4. **PIM for admin roles** (Control 2) — Eliminates permanent standing admin access
5. **Disable OAuth user consent** (Control 14) — Closes the malicious app registration vector

These five controls alone stop most tenant-destruction attack paths. The remaining controls add depth, detection, and resilience.

#	Action	Priority	Effort
1	Enforce phishing-resistant MFA (FIDO2) for all admin roles. Standard push MFA with number matching for regular users.	CRITICAL	4 hours
2	Remove bulk Wipe/Retire/Delete permissions from all standard Intune roles via custom RBAC	CRITICAL	2 hours
3	Enable PIM for Intune Administrator—no permanent assignments, require approval + justification	CRITICAL	4 hours
4	Restrict Intune/Graph admin portal access to compliant devices + named network locations via Conditional Access	CRITICAL	4 hours
5	Disable user OAuth consent and app registration tenant-wide; audit existing service principals	CRITICAL	2 hours
6	Deploy SIEM alert rules for bulk device wipe events (≥5 wipes in 10 min) with automated response	HIGH	4 hours
7	Review and restrict app registrations with DeviceManagementManagedDevices.PrivilegedOperations.All; require admin consent for all application permission grants	HIGH	2 hours
8	Implement Intune Scope Tags to segment device management by region/business unit	HIGH	1 day
9	Establish out-of-band emergency comms plan (not dependent on corporate MDM or M365)	HIGH	1 day
10	Back up Intune device configs, Conditional Access policies, and Entra ID config to offline storage	HIGH	1 day

DETAILED HARDENING CONTROLS

IDENTITY & ACCESS CONTROLS

1. Enforce MFA Appropriately by Role

Not all MFA is equal, and not all users need the same level. The key distinction: admin accounts need phishing-resistant MFA (FIDO2 hardware keys), while regular users can use standard push MFA with number matching.

- **For admin roles (Global Admin, Intune Admin, Cloud Device Admin, Security Admin, Privileged Role Admin):**

```
Entra ID → Security → Authentication Methods → FIDO2 Security Key
→ Enable
Conditional Access → New Policy:
  Name: Require phishing-resistant MFA for admins
  Users: Include → Directory roles → [all admin roles]
  Cloud apps: All cloud apps
  Grant: Require authentication strength → Phishing-resistant MFA
```

- **For regular users:**

```
Entra ID → Security → Authentication Methods → Microsoft
Authenticator
  Number matching: Enabled (required)
  Show additional context: Enabled (shows app name + location)
Conditional Access → New Policy:
  Name: Require MFA for all users
  Users: All users
  Cloud apps: All cloud apps
  Grant: Require multifactor authentication
```

> **Practical Note:** *Why FIDO2 for admins specifically? AiTM phishing kits like EvilGinx intercept both passwords and push MFA tokens in real-time by proxying the legitimate login page. FIDO2 keys are bound to the legitimate domain and cannot be phished this way. Regular users benefit from number matching, which makes push fatigue attacks significantly harder—but it's not immune to AiTM. For admin accounts, the risk justifies the hardware investment.*

Critical Addition — Block Legacy Authentication: Create a Conditional Access policy to block legacy authentication protocols (Exchange ActiveSync, IMAP, POP3, SMTP, and other legacy clients). Legacy protocols do not support MFA and are a common vector for credential-based attacks. This is one of the highest-impact controls you can deploy. Conditional Access → New Policy: Name: Block Legacy Authentication. Users: All users. Client Apps: Exchange ActiveSync clients, Other clients. Grant: Block access.

2. Enable Privileged Identity Management (PIM)

No admin should have permanent access to destructive capabilities. PIM forces just-in-time activation with approval.

- **Exact Path:** Entra ID → Privileged Identity Management → Roles → Intune Administrator

```
Assignment type: Eligible (not Active/Permanent)
Activation maximum duration: 1 hour
Require on activation: MFA + justification + approval
Approver: Security Operations team lead
Notification: security-ops@[company].com on every activation
```

- Apply identical settings to: Global Administrator, Cloud Device Administrator, Security Administrator

> **Practical Note:** *PIM requires Entra ID P2 licensing. If you're on P1, the minimum alternative is to reduce the number of permanent admin accounts to the absolute minimum (2 break-glass only) and monitor all admin sign-ins via SIEM.*

3. Enable Continuous Access Evaluation (CAE)

CAE ensures revoked tokens are immediately invalidated rather than remaining valid for 60–90 minutes (the default access token lifetime without CAE).

- **Exact Path:** Entra ID → Security → Conditional Access → Session → Customize continuous access evaluation

```
Continuous Access Evaluation: Enabled
Strictly enforce location policies: Enabled (optional—see note
below)
```

> **Practical Note:** *Without CAE, if you detect an attack and disable the compromised admin account, their existing session token keeps working for 60–90 minutes. That's enough time to wipe thousands of devices. With CAE, revocation propagates in near real-time, typically within minutes depending on the service. Note on strict location enforcement: Microsoft documents this as a separate, more restrictive CAE enforcement mode with specific networking requirements (e.g., compliant network checks, IP-based location accuracy). Evaluate this for mature environments with well-defined network boundaries. For initial deployment, enable standard CAE first and add strict enforcement after validating your named location configuration.*

4. Deploy Identity Threat Detection

Detect AiTM phishing and token theft before they lead to destructive actions.

- **Entra ID Protection:** Entra ID → Security → Identity Protection

```
Sign-in risk policy: Require MFA for medium + high risk sign-ins
User risk policy: Require password change for high-risk users
```

- Enable Token Protection (preview — pilot in a test group before broad deployment, as this is not yet generally available) to bind tokens to the device they were issued on
- **SIEM Starter Detections (KQL — adapt to your SIEM platform; validate schema and enrich with watchlists before production deployment):**

```
# Detect token replay / AiTM:
# Detect risky sign-ins indicating possible token replay or AiTM:
SigninLogs | where ResultType == 0 | where RiskLevelDuringSignIn
in ("medium", "high") | where RiskEventTypes_V2 has_any
("anomalousToken", "tokenIssuerAnomaly", "unfamiliarFeatures") |
project TimeGenerated, UserPrincipalName, AppDisplayName,
IPAddress, RiskLevelDuringSignIn, RiskEventTypes_V2

# Detect risky admin sign-ins:
SigninLogs | where RiskState == "atRisk" and UserPrincipalName
contains "admin"

# Detect service principal abuse from unknown IPs:
AADServicePrincipalSignInLogs | where IsInteractive == false and
IPAddress !in (known_corp_ips)
```

5. Restrict Admin Login Locations

- **Exact Path:** Entra ID → Security → Conditional Access → Named Locations

```
Define: Corporate VPN ranges, SOC network ranges
Block: All locations not in named locations for admin roles
Block: TOR exit nodes, anonymous proxies, high-risk geographies
```

6. Require Admin Access from Managed Devices Only

```
Conditional Access → New Policy:
  Name: Block admin access from unmanaged devices
  Users: All admin roles
  Cloud apps: Microsoft Admin Portals, Intune, Graph, Azure Management
  Grant: Require compliant device OR Microsoft Entra hybrid joined
device
  Client apps: Browser, Mobile apps and desktop clients
  Session: Sign-in frequency = 1 hour
```

> **Practical Note:** *If you don't have Privileged Access Workstations (PAWs) yet, start with requiring compliant corporate devices on corporate IP ranges. That alone blocks attackers from using stolen credentials remotely. Plan PAW deployment as a 90-day initiative.*

7. Harden Break-Glass Accounts

Break-glass accounts are excluded from Conditional Access by design, making them high-value targets.

- Use passwords of 32+ characters, randomly generated, as a backup credential
- No mailbox, no phone number. Use phishing-resistant authentication (FIDO2 security keys or certificate-based authentication) rather than passwords alone. Store FIDO2 keys in a physical safe with dual-custody access, separate from the password
- Excluded from ALL Conditional Access policies
- Test quarterly. Log every use. Any unplanned login = immediate P1 incident.

```
# Alert on ANY break-glass sign-in:
SigninLogs | where UserPrincipalName in ("breakglass1@...",
"breakglass2@...")
```

> **Practical Note:** *Federated & Hybrid Identity Warning: If your M365 tenant federates authentication with an external identity provider—such as Okta, Ping Identity, on-premises ADFS, or Google Workspace—a compromised upstream IdP bypasses every Entra ID control above. The authentication decision happens before the token reaches Microsoft. See Appendix H for a dedicated section on securing federated identity providers, including SCIM provisioning abuse, Golden SAML prevention, and the critical requirement to enforce Entra-native FIDO2 for admin roles even when authentication is federated.*

IDENTITY & ACCESS CONTROLS

8. Remove Bulk Wipe Capability from Standard Roles

This is the single control that would most directly reduce the risk of a Stryker-style attack. No standard admin role should have bulk wipe permissions.

- **Exact Path:** Intune Admin Center → Tenant Administration → Roles → Create Custom Role

```
Role name: Intune Device Manager - No Wipe
Permissions: Enable all EXCEPT:
  ✘ Remote tasks → Wipe
  ✘ Remote tasks → Retire
  ✘ Remote tasks → Factory Reset
  ✘ Remote tasks → Autopilot Reset
  ✘ Remote tasks → Delete
```

- Assign this custom role to ALL Intune admins. Reserve wipe capability for break-glass accounts only (permanent active assignment—break-glass accounts must not be PIM-eligible).

9. Implement Approval Workflow for Device Wipes

No destructive action—Wipe, Retire, or Delete—should execute without a second administrator's approval. Intune provides a native Multi Admin Approval (MAA) feature that enforces this directly. For organizations that need custom logic or broader coverage, a Logic App/Power Automate workflow can supplement or replace MAA.

Option A (Recommended): Intune Multi Admin Approval

MAA is a native Intune feature that requires a second administrator to approve protected operations before they execute. MAA now covers destructive device actions (Wipe, Retire, Delete) as well as changes to apps, scripts, configuration profiles, compliance policies, and RBAC roles. Coverage continues to expand. This is the simplest and fastest way to add an approval gate.

Prerequisites: Intune Plan 1 license (or Intune role assignment) for each approver. At least two administrator accounts in the tenant.

Step 1 — Create Approver Security Group: Intune Admin Center → Groups → All Groups → New Group. Add at least two senior security administrators as members. This group must also be a member of at least one Intune role assignment (otherwise members are periodically removed).

Step 2 — Create Custom Intune Role for Approvers: Intune Admin Center → Tenant Administration → Roles → Create → Intune Role. Grant the "Approval for Multi Admin Approval" permission. Assign the approver security group to this role.

Step 3 — Create Access Policy: Intune Admin Center → Tenant Administration → Multi Admin Approval → Access Policies → Create. Set the Profile Type to the resource you want to protect (device actions including Wipe, Retire, Delete are supported). Select the approver security group. Create separate policies for Windows and Non-Windows platforms if needed.

Workflow: When an admin attempts a protected action, they must submit a business justification. A different admin from the approver group reviews and approves or rejects the request. If approved, the original requestor completes the action. Requests expire after 30 days if not acted upon.

Limitation: MAA does not send built-in notifications when a request is created or changes status. Consider pairing it with a Power Automate flow that monitors the Unified Audit Log for MAA events and sends Teams/email alerts to the approver group.

Option B (Advanced): Custom Logic App / Power Automate Workflow

For organizations that need custom approval logic, richer notifications, SOAR integration, or coverage beyond what MAA currently supports (e.g., Compliance Policies, Configuration Policies), build a custom workflow:

```
Architecture: Azure Logic App or Power Automate:
  Trigger: HTTP webhook from custom admin portal
  → Send Teams Adaptive Card to Security Ops channel
  → Require approval from 2 members of SG-DeviceWipe-Approvers
  → On approval: Execute Graph API wipe call with full audit logging
  → On rejection: Log and notify requestor
  → Timeout: 30 minutes → auto-reject
```

> **Practical Note — MAA vs. PIM:** Multi Admin Approval and Privileged Identity Management (Control 2) are complementary controls, not redundant. PIM gates role activation—an admin must request and justify activating the Intune Administrator role before they can access device management at all. MAA gates specific actions within an already-activated role—even after an admin has legitimately activated their role via PIM, a second administrator must still approve destructive operations like Wipe, Retire, or Delete. Together, they create two independent approval gates: one to get the role, and one to use its most dangerous capabilities. An attacker would need to compromise both workflows.

10. Restrict Device Enrollment and Protect BYOD

In the Stryker attack, personal phones enrolled in the company portal were also wiped—employees lost personal data, photos, and 2FA authenticator apps. This is one of the most operationally painful consequences of the attack and is entirely preventable.

The key distinction: MDM enrollment gives the organization full device control (including full wipe), while MAM-only enrollment protects corporate data at the app level without device-level control. Personal devices should never be under full MDM.

- **For corporate-owned devices:**

```
Intune Admin Center → Devices → Enrollment Restrictions
  Default platform restriction: Corporate-owned or Windows
Autopilot devices
  Device limit restriction: 5 devices per user (adjust per policy)
```

- **For BYOD / personal devices (MAM-only — no device wipe capability):**

```
Intune Admin Center → Apps → App Protection Policies → Create
Policy
  Platform: iOS/iPadOS or Android
  Apps: Select corporate apps (Outlook, Teams, OneDrive, etc.)
  Data protection: Prevent copy/paste to unmanaged apps
  Data protection: Encrypt corporate data within managed apps
  Access requirements: Require PIN or biometric for app access
  Conditional launch: Block access if device is jailbroken/rooted
```

With MAM-only, a compromised admin can issue a selective wipe (removing only corporate app data)—but cannot issue a full device wipe. Personal photos, authenticator apps, and personal data remain untouched.

- **Enrollment restriction to prevent personal devices from MDM:**

```
Intune Admin Center → Devices → Enrollment Restrictions → Device
Type Restrictions
  Create restriction: Block personally owned → Android, iOS
  Assign to: All Users
```

> **Practical Note:** *If your organization currently enrolls personal devices under full MDM, migrating to MAM-only is a high-priority project. Communicate the change to employees as a privacy improvement—their personal data will no longer be visible to or wipeable by IT. This also reduces your organization's legal liability in the event of an inadvertent wipe.*

11. Segment Device Management with Intune Scope Tags

Scope Tags are the blast radius containment control that would have changed the Stryker outcome from catastrophic to contained. Without Scope Tags, a compromised Intune admin

can reach every managed device in the tenant. With Scope Tags, they can only affect devices within their assigned scope.

- **Exact Path:** Intune Admin Center → Tenant Administration → Roles → Scope (Tags)

```
Step 1 — Create Scope Tags by segment:
  Scope Tag: Region-NorthAmerica
  Scope Tag: Region-EMEA
  Scope Tag: Region-APAC
  Scope Tag: Dept-Engineering
  Scope Tag: Dept-Finance

Step 2 — Assign Scope Tags to devices:
  Intune → Devices → All Devices → Select device group →
Properties → Scope Tags
  Assign appropriate tag based on device location or department

Step 3 — Assign Scope Tags to admin roles:
  Intune → Tenant Administration → Roles → [Custom Role] →
Assignments
  Scope (Tags): Select only the tags for the admin's
region/department
```

- **Combine with Entra ID Administrative Units:** For identity-level segmentation, create Administrative Units in Entra ID that mirror your Scope Tag structure. Assign admin roles scoped to specific AUs so that even identity operations are limited.

```
Entra ID → Roles and Administrators → Administrative Units → Create
  Name: AU-NorthAmerica
  Members: Add user/device groups for the region
  Assign Helpdesk Admin role scoped to this AU only
```

> **Practical Note:** *In the Stryker attack, a single compromised admin reportedly wiped 200,000+ devices across 79 countries. With Scope Tags, that same compromised admin would have been limited to their assigned region—potentially 5,000–10,000 devices instead of 200,000. Scope Tags don't prevent the attack, but they contain the blast radius to a recoverable scale. Combined with the RBAC controls in Control 8, this is defense-in-depth for device management.*

API & APPLICATION CONTROLS

12. Restrict Microsoft Graph Device Management Operations

The attackers likely scripted mass wipes via Graph API. Lock down these permissions.

- **Exact Path:** Entra ID → Enterprise Applications → Consent and Permissions → Set "Users can consent to apps" to No

- **Review all app registrations and service principals for the following high-risk Graph API permissions, and remove or restrict access where not operationally required. Note: Microsoft does not provide a native tenant-wide control to block specific Graph permissions by name. The correct approach is to disable user consent, enable admin consent workflow, and then review and remediate existing grants. Only Global Administrators can approve application-level permission requests. High-risk permissions to audit:**
  - DeviceManagementManagedDevices.PrivilegedOperations.All
  - DeviceManagementConfiguration.ReadWrite.All
  - DeviceManagementApps.ReadWrite.All
  - DeviceManagementServiceConfig.ReadWrite.All

13. Restrict App Registrations

- **Exact Path:** Entra ID → User Settings → App Registrations → Set "Users can register applications" to No
- **Create** a security group (e.g., SG-AppRegistration-Admins) and grant only this group the Application Developer role
- Review existing app registrations monthly—look for orphaned apps, apps with high-privilege permissions, and apps with credentials that haven't been rotated

14. Prevent Rogue OAuth Applications

```
Entra ID → Enterprise Applications → Consent and Permissions
  User consent: Do not allow user consent
  Admin consent workflow: Enabled
  Reviewers: Security Operations group
```

- Monitor audit logs for: service principal creation, admin consent grants, app role assignment changes, new credentials added to existing apps

15. Audit Existing Service Principals and Managed Identities

Controls 12–14 lock down new application access. But your tenant likely already has legacy service principals and managed identities with overprivileged device management permissions that were granted years ago and forgotten. This is a Day 1 audit.

- **Enumerate all service principals with device management permissions:**

```
# List all service principals with DeviceManagement Graph
permissions:
Connect-MgGraph -Scopes "Application.Read.All"
$apps = Get-MgServicePrincipal -All
foreach ($app in $apps) {
  $grants = Get-MgServicePrincipalOAuth2PermissionGrant -
ServicePrincipalId $app.Id
  $roles = Get-MgServicePrincipalAppRoleAssignment -
ServicePrincipalId $app.Id   # NOTE: AppRoleId values are GUIDs.
Resolve to permission names by   # cross-referencing with Get-
MgServicePrincipal -ServicePrincipalId $graphSP.Id   # See
Microsoft Graph AppRole definitions for name mapping.
  $devicePerms = $roles | Where-Object { $_.AppRoleId -and
$_.ResourceDisplayName -eq 'Microsoft Graph' }
  if ($devicePerms) {
    Write-Output "App: $($app.DisplayName) | AppId: $($app.AppId)"
    # Resolve AppRoleId GUIDs to human-readable permission names:
$graphSP = Get-MgServicePrincipal -Filter "AppId eq '00000003-
0000-0000-c000-000000000000'"     $devicePerms | ForEach-Object {
$assignment = $_       $roleName = ($graphSP.AppRoles | Where-
Object { $_.Id -eq $assignment.AppRoleId }).Value       Write-
Output "  Permission: $roleName ($($assignment.AppRoleId))"     }
  }
}
```

- For each result, ask: Is this app still in use? Does it need DeviceManagement permissions? When was the credential last rotated?
- Remove or reduce permissions for any service principal that does not have an active, documented business justification
- Set a calendar reminder to repeat this audit quarterly

> **Practical Note:** *In many organizations, legacy app registrations from pilot projects, former vendors, or decommissioned integrations still hold powerful Graph API permissions. These are invisible to most security reviews because they don't appear in user-facing admin consoles. A single forgotten service principal with DeviceManagementManagedDevices.PrivilegedOperations.All is a backdoor waiting to be exploited.*

DETECTION & MONITORING

16. Monitor Mass Device Actions via SIEM with Automated Response

This is your last line of defense. If all preventive controls fail, this detection rule catches the attack in progress—and the automated playbook stops it.

- **SIEM Starter Detection (KQL syntax — adapt to your SIEM platform and validate field paths against your workspace schema before production deployment):**

```
IntuneAuditLogs
| where OperationName in ("wipeDevice", "retireDevice",
"deleteDevice")
| extend UPN = tostring(parse_json(Properties).UserPrincipalName
// Verify field path in your workspace) | summarize WipeCount =
count() by UPN, bin(TimeGenerated, 10m)
| where WipeCount >= 5
| project TimeGenerated, UPN, WipeCount
```

- Set alert severity: Critical. This should auto-trigger your automated response playbook.
- Also monitor: bulk compliance policy changes, new configuration profiles pushed to "All Devices", and Conditional Access policy modifications.

Automated Response Playbook

When the SIEM alert fires, the following sequence should execute automatically via your automation platform (LMNTRIX SOAR, Splunk, or equivalent). The goal is to contain the attack within minutes, not hours.

- **Step 1 — Disable the offending admin account:**

```
# Automatic — triggered by automation:
Update-MgUser -UserId $attackerUPN -AccountEnabled:$false
```

- **Step 2 — Revoke all active sessions:**

```
Revoke-MgUserSignInSession -UserId $attackerUPN
```

- **Step 3 — Block the source IP in Conditional Access:**

```
# Add source IP to Named Location blocklist via Graph API:
# PATCH /identity/conditionalAccess/namedLocations/{blocklist-id}
```

- **Step 4 — Send out-of-band alert to IR team:** Trigger Signal/PagerDuty/OpsGenie notification to the IR team with attack details (identity, wipe count, source IP, affected device scope).
- **Step 5 — Freeze further destructive actions:** Temporarily block all device wipe/retire/delete operations at the Conditional Access level by requiring a specific compliant device claim that no session currently satisfies.

> **Practical Note:** *This 5-step sequence turns your detection into an automated kill switch. Without automation, the typical response time from SIEM alert to admin account disabled is 30–60 minutes—during which thousands of devices could be wiped. With automation, containment happens in under 2 minutes. Test this playbook as part of Simulated Wipe Day (Appendix D).*

17. Monitor Graph API Device Management Endpoints

Monitor these endpoints in your SIEM:

```
POST /deviceManagement/managedDevices/{id}/wipe
POST /deviceManagement/managedDevices/{id}/retire
POST /deviceManagement/managedDevices/{id}/resetPasscode
POST /deviceManagement/managedDevices/{id}/remoteLock
PATCH /deviceManagement/deviceConfigurations/{id}
```

- Alert on: calls from unusual IPs, new or unknown service principals, outside business hours, or any identity targeting >10 devices in a short window

18. Monitor App Registration and OAuth Activity

- **Alert on these Entra ID audit events:**
- Add service principal
- Add app role assignment
- Consent to application (admin consent granted)
- Add application credentials (new secrets or certificates on existing apps)
- Update application permissions

19. Configure Audit Log Retention for Forensic Readiness

Detection is critical, but what happens after detection matters too. Standard Microsoft 365 audit logs are retained for only 180 days (1 year with E5 Compliance). If the attacker had dwell time of months before triggering the wipe—common in APT operations—you could lose critical forensic evidence before the investigation completes.

- **Enable Audit (Premium) retention policies:**

```
Microsoft Purview Compliance Portal → Audit → Audit Retention
Policies
```

```
  Create policy:
  Record type: Select the applicable record types for your
environment (verify exact names in your tenant's Purview Compliance
Portal, as available record types may vary)
  Duration: 1 year (E5 default; 10-year retention requires the 10-
Year Audit Log Retention add-on license)
  Priority: 1 (highest)
```

If you do not have E5 Compliance licensing for Audit (Premium), export logs to external storage:

- **Export to SIEM or cold storage:**

```
# Export Unified Audit Log to external storage on a scheduled basis:
Search-UnifiedAuditLog -StartDate (Get-Date).AddDays(-1) -EndDate
(Get-Date) \
  -RecordType AzureActiveDirectory -ResultSize 5000 \ # NOTE: -
RecordType accepts only a single value. Run separate queries # for
each RecordType (e.g., IntuneOperations) and combine results. # For
production automation, consider the Management Activity API instead.
  | Export-Csv -Path "audit-export-$(Get-Date -Format yyyyMMdd).csv"

# Upload to immutable blob storage (Azure) or S3 with Object Lock
(AWS):
# Ensure storage is air-gapped from the M365 tenant—attacker should
not be
# able to delete audit logs using the same compromised credentials
```

> **Practical Note:** *The key principle: audit logs must survive the attack. If the attacker compromises your M365 tenant and your audit logs live exclusively in M365, they can potentially tamper with or delete them. Export to a separate, immutable storage location that requires different credentials. LMNTRIX SIEM customers have log retention built in—verify your retention period covers at least 12 months.*

Advanced Note — Rate Limiting Destructive Graph API Calls: Microsoft does not natively rate-limit wipe commands issued via Graph API. For organizations with mature engineering teams, it is possible to build a custom throttle using Azure API Management or a reverse proxy that sits between admin tooling and Graph API. If more than N wipe commands are issued within a defined time window, the proxy blocks further calls and alerts the SOC. This is a defense-in-depth control that works even if RBAC and PIM are somehow bypassed. Note: this requires significant engineering effort to implement and maintain, and is not trivial—it should be considered an advanced control for organizations with dedicated cloud security engineering resources.

DATA EXFILTRATION DETECTION (IF YOU DON'T HAVE MICROSOFT PURVIEW)

Handala claimed to have exfiltrated 50TB of data before executing the wipe; this figure has not been independently verified. Detecting and preventing data exfiltration is critical—but not every organization has Microsoft Purview or E5 Compliance licensing, which is where Microsoft's native DLP lives.

The good news: every preventive control in this guide (RBAC, PIM, Conditional Access, FIDO2, OAuth lockdown) works on standard E3 or E5 licensing. Purview is not required for any of them. Where the gap appears is specifically on detecting and blocking large-scale data theft.

What You Can Do Without Purview

20. Network-Level Exfiltration Detection

If the threat actor gains access to the cloud tenant, data exfiltration will likely occur through Microsoft Graph API calls, SharePoint/OneDrive bulk downloads, or Exchange Online mailbox exports. But if they pivot to the internal network, exfiltration shifts to endpoints and network egress points.

- **For cloud-layer exfiltration:**
- Enable Unified Audit Log in Microsoft 365 (enabled by default on E3/E5)—this captures SharePoint file access, OneDrive downloads, and Exchange mailbox exports
- Monitor for bulk file download events: Search the Unified Audit Log for "FileDownloaded" and "FileSyncDownloadedFull" operations with abnormally high counts per user per day
- If you have Microsoft Defender for Cloud Apps (MCAS)—included in E5 Security—configure anomaly detection policies for "Mass download" and "Unusual file share activity"

```
# Unified Audit Log query for bulk downloads (PowerShell):
Search-UnifiedAuditLog -StartDate (Get-Date).AddDays(-7) -EndDate
(Get-Date) \
  -Operations FileDownloaded,FileSyncDownloadedFull \
  -ResultSize 5000 | Group-Object UserIds | Sort-Object Count -
Descending | Select -First 20
```

- **For internal network exfiltration:** If the threat actor pivots from the cloud tenant to the internal network—which is common in APT operations—data exfiltration will occur through internal network egress points. This is where endpoint and network detection become essential.

- Organizations running an EDR/NDR combination (such as LMNTRIX's managed EDR and NDR) already have coverage here—NDR monitors for anomalous data flows, large outbound transfers, beaconing to C2 infrastructure, and lateral movement patterns that precede exfiltration
- EDR on managed endpoints detects staging behavior: archive creation (zip/rar of sensitive directories), use of exfiltration tools (rclone, MEGAcmd, WinSCP), and uploads to cloud storage services from endpoints
- If you don't have NDR, monitor firewall and proxy logs for: single endpoints transferring >1GB outbound in a short window, connections to known file-sharing services (mega.nz, transfer.sh, anonfiles), and DNS queries to newly registered domains

> **Practical Note:** *The Stryker attack was primarily a destructive wipe, not a targeted data theft operation. But the exfiltration claim shows that attackers will take whatever data they can access before pulling the trigger on destruction. Preventing the wipe (Controls 1–19) is the higher priority, but exfiltration detection closes the loop. If you already have EDR/NDR deployed, your internal network exfiltration coverage is in place—focus your gap-closing effort on cloud-layer audit log monitoring.*

21. Alternatives to Purview DLP by License Tier

License	What You Have	Gap to Close
Business Premium	Defender for Business (endpoint), Basic audit logs, Conditional Access	No DLP, no CASB, no advanced audit. Use firewall/proxy logs and EDR/NDR for exfiltration detection.
E3	Unified Audit Log, Conditional Access, Intune, Defender for Endpoint Plan 1	No DLP, no CASB, no anomaly detection. Enable audit log monitoring. EDR/NDR covers network layer.
E5 Security	Defender for Endpoint P2, MCAS (Defender for Cloud Apps), Identity Protection	MCAS provides basic DLP and anomaly detection for cloud apps. Good coverage with EDR/NDR for network.
E5 / E5 Compliance	Full Purview DLP, Information Protection, Insider Risk Management, Advanced Audit	Full native coverage. Supplement with EDR/NDR for internal network visibility.

> **Practical Note:** *You do not need E5 Compliance to implement the controls in this guide. Every preventive and detective control works on E3 or above. Purview DLP adds depth on the data protection side, but it is not a prerequisite for stopping a Stryker-style wipe attack.*

RESILIENCE & RECOVERY

22. Establish Out-of-Band Emergency Communications

When all corporate devices are wiped, your Teams, email, Slack, and phone system are gone. You need a communication plan that survives this.

- Maintain an emergency contact list on paper and in a non-corporate messaging app (Signal group for the IR team)
- Pre-configure an emergency email distribution list on a separate domain/provider not tied to Microsoft 365
- Store Intune/Entra backup configs and break-glass credentials in a physically secured location
- Pre-provision emergency communication channels now—do not wait for an incident. Set up and test a dedicated Signal group, an emergency Slack workspace on a separate tenant, or a satellite/mesh communications plan before you need them
- Maintain a printed, offline incident response playbook stored alongside break-glass credentials. This playbook should include step-by-step recovery procedures, vendor contact numbers, and escalation paths that do not depend on any digital corporate system
- Conduct a tabletop exercise for this specific scenario: "All corporate devices wiped, zero M365 access"

> **Practical Note:** *Stryker employees could not communicate or access any corporate systems after the wipe—including personal phones enrolled in the company portal. Your IR plan must assume zero corporate infrastructure availability. If you haven't tested this, you don't have a plan.*

23. Backup and Recovery for Cloud Configurations

Treat Intune configurations and Conditional Access policies as critical infrastructure. Back them up.

- Use Microsoft 365 DSC or a third-party tool to export Intune device configs, compliance policies, and app configurations weekly
- Export Conditional Access policies via Graph API to a version-controlled, air-gapped repository
- Document all custom RBAC roles, PIM settings, and named locations so you can rebuild quickly
- **PowerShell — run these on a schedule:**

```
# Export Conditional Access policies:
Connect-MgGraph -Scopes "Policy.Read.All"
Get-MgIdentityConditionalAccessPolicy | ConvertTo-Json -Depth 10 >
CA-backup.json

# Export Intune device configurations:
Connect-MgGraph -Scopes "DeviceManagementConfiguration.Read.All"
# NOTE: This exports deviceConfigurations only. For comprehensive
backup # covering Settings Catalog, security baselines, compliance
policies, # scripts, and apps, use Microsoft365DSC or multi-
endpoint Graph queries. Get-MgDeviceManagementDeviceConfiguration
| ConvertTo-Json -Depth 10 > Intune-configs.json
```

> **Practical Note:** *Recovery from a Stryker-scale attack means rebuilding the entire Intune environment from scratch. Without config backups, that's weeks of work. With backups, you're looking at days.*

24. Conditional Access Kill Switch (Emergency Brake)

> **This is not a routine hardening control—this is an emergency action.** Pre-stage a Conditional Access policy that blocks all admin access to all cloud apps with a single click. Keep it disabled. Enable it only during an active incident when you need to freeze the entire management plane immediately.

Why this matters: Even with the best automation (Control 16), there can be a delay in identifying all compromised accounts or source IPs during a multi-identity attack. A pre-staged kill switch lets a security leader stop the bleeding across the entire tenant with a single action while the IR team transitions to out-of-band communications and begins containment. In the chaos of a mass device wipe, the IR team needs a clear emergency brake.

Implementation:

```
Entra ID → Security → Conditional Access → New Policy
  Name: EMERGENCY_BRAKE_BLOCK_ALL_ADMINS
  Users: Include → Directory roles → [All Administrator roles]
  Exclude (MANDATORY): Your two Break-Glass accounts
  Target Resources: All Cloud Apps
  Conditions: None (apply globally)
  Grant: Block Access
  Enable Policy: OFF (disabled until needed)
```

Critical Implementation Rules:

- **Break-Glass Exclusion is MANDATORY.** This policy must explicitly exclude your two break-glass accounts (Control 7). If you block all admins without an excluded account, you will be permanently locked out of your tenant, requiring a multi-day identity verification process with Microsoft Support to regain access. Verify this exclusion before saving the policy.
- **CAE must be enabled for instant effect.** Without Continuous Access Evaluation (Control 3), an attacker's existing session token could remain valid for up to 90 minutes even after you enable this policy. With CAE, the block propagates within minutes. Verify CAE is active before relying on this control.
- **Test in Report-Only mode first.** Before staging this policy as disabled, run it in Report-Only mode for one week. Verify the break-glass exclusion works correctly and confirm you haven't missed any service accounts that would break critical automation (backup scripts, SIEM ingestion, playbooks). The last thing you want during an incident is to discover your kill switch also killed your security tooling.

> **Practical Note:** *Include this policy in your IR runbook with clear escalation criteria for when to enable it. Define in advance who has authority to pull this lever—typically the CISO or Security Operations lead—and under what conditions (e.g., confirmed multi-identity compromise, mass wipe in progress, automation unable to contain). Test it quarterly alongside your Simulated Wipe Day exercise (Appendix D). When you pull this lever, your only remaining access is through the break-glass accounts—make sure they work.*

5 QUESTIONS TO ASK YOUR MICROSOFT SECURITY TEAM RIGHT NOW

Use these questions to quickly assess your exposure. If your team cannot confidently answer each one, you have work to do.

1. How many accounts in our tenant can wipe devices—and do we know exactly who they are?

Why it matters: *In the Stryker attack, a single compromised admin account reportedly wiped 200,000+ devices. Most organizations have far more accounts with wipe permissions than they realize. If you cannot answer this with an exact number today, start with Control 8.*

2. **Can an Intune administrator access the management portal right now from a personal laptop on public Wi-Fi?**

   Why it matters: *If yes, an attacker who steals admin credentials via phishing can log in from anywhere and execute destructive actions. Conditional Access restricting admin portal access to compliant devices on named networks would materially reduce the risk of an attacker executing destructive actions remotely.*

3. **Are all privileged roles protected with PIM, requiring approval and justification for every activation?**

   Why it matters: *Permanently assigned admin roles mean an attacker gains destructive capabilities the instant they compromise a credential. PIM adds a human-in-the-loop gate—the attacker would need to request activation through an approval workflow, which generates alerts and requires justification.*

4. **Is user OAuth application consent disabled across our entire tenant?**

   Why it matters: *Enabled user consent allows attackers to trick employees into granting malicious applications access to device management APIs. A single consent click can give an attacker the Graph API permissions needed to wipe every device in your environment.*

5. **Do we have SIEM alerts that would fire within minutes if someone attempted to wipe more than 5 devices in a 10-minute window?**

   Why it matters: *The Stryker wipe reportedly affected 200,000+ devices and took hours to complete. An organization with proper monitoring could detect and respond to this type of attack within the first few minutes, limiting damage to a small fraction of what Stryker experienced. The starter KQL query in Control 16 takes 10 minutes to deploy and should be tuned to your environment.*

APPENDIX A: ADMINISTRATIVE BLAST RADIUS

Before locking down permissions, your team needs to understand how much damage each admin role can inflict if compromised. This table defines the "blast radius"—the scope of destruction a single compromised account can cause based on its assigned role.

Role Type	Device Scope	Potential Impact	Recommended Mitigation
Global Admin	Entire Tenant	Total destruction: identity, data, and device loss across all services	Limit to 2 break-glass accounts with permanent Global Administrator assignment. These must NOT be PIM-eligible—emergency access must always work, including during PIM or Entra ID outages.
Intune Admin	All Managed Devices	100% device wipe capability (200K+ endpoints in Stryker's case)	Custom RBAC role without wipe permissions. PIM with 1-hour window. SIEM alerts on activation.
Cloud Device Admin	All Cloud Devices	Can disable, delete, and manage BitLocker keys for all Entra-joined devices	PIM activation only. Restrict to compliant devices on corporate network.
Helpdesk / Dept Admin	Scope Tag Limited	Limited to devices within assigned Scope Tag (department, region, office)	Use Intune Scope Tags to restrict admin reach. Lowest-privilege assignment.
Application Admin	App Registrations	Can create rogue OAuth apps with device management API permissions	Disable user app registration. Require admin consent workflow for all permission grants.

> **Practical Note:** *Run this PowerShell command to audit who currently has wipe permissions in your tenant. The output will likely surprise you:*

```
# List all users with Intune Administrator or Global Administrator
role:
# NOTE: Get-MgDirectoryRole only returns roles that have been
activated (instantiated) # in your tenant. If a role has never been
assigned, it won't appear. Use # Get-MgDirectoryRoleTemplate to list
all available roles, or activate the role first. Get-
MgDirectoryRoleMember -DirectoryRoleId (Get-MgDirectoryRole -Filter
"displayName eq 'Intune Administrator'").Id
Get-MgDirectoryRoleMember -DirectoryRoleId (Get-MgDirectoryRole -
Filter "displayName eq 'Global Administrator'").Id
```

Use Intune Scope Tags (Control 11) to reduce the blast radius for regional or departmental admins. A helpdesk admin in the London office should not be able to wipe devices in Tokyo.

APPENDIX B: INCIDENT RESPONSE PHYSICAL SURVIVAL KIT

Control 22 establishes out-of-band communications. This appendix specifies exactly what should be in the physical "IR Go-Bag" stored in a secure, dual-custody safe. When every digital system is destroyed, this is what your incident response team reaches for.

Item	Details
Laminated Break-Glass Credentials	FIDO2 security keys for both break-glass accounts, plus printed 32+ character backup passwords. Store keys and passwords separately under dual-custody access. Laminate printed credentials to prevent water damage. Update immediately after any use.
Pre-Provisioned FIDO2 Keys	2–4 spare FIDO2 hardware keys, already registered as backup authentication methods for break-glass accounts and key security personnel. Test quarterly.
Encrypted Offline Drive (USB)	Contains: CA-backup.json (Conditional Access policies), Intune-configs.json (device configurations), RBAC role definitions, named location definitions, PIM settings. Refresh weekly via scheduled PowerShell export (see Control 23).
Hard Copy Phone Tree	Personal mobile numbers for: CISO, CIO, IT Director, Security Ops lead, Legal counsel, Communications lead, and key vendor contacts. Include Signal group invite QR codes for the emergency channel.
Network Diagram (Printed)	Physical copy of network topology, DNS configuration, VPN endpoints, and ISP contact information. If all systems are wiped, you need this to rebuild network access.
Vendor Emergency Contacts	Microsoft Premier Support case number and PIN, LMNTRIX SOC hotline, ISP emergency contact, cyber insurance carrier claims number and policy ID.

> **Practical Note:** *If your organization does not have a physical IR safe today, this is a half-day project. Buy a fireproof safe with dual-combination lock, populate the items above, and assign*

> *two keyholders (CISO + IT Director). Test the contents quarterly alongside your break-glass account test.*

APPENDIX C: THE MANAGEMENT PLANE VS. DATA PLANE DETECTION GAP

The Stryker attack exposed a fundamental blind spot in most security architectures. To understand why traditional security tools failed, you need to understand the difference between where your tools watch and where the attack happened.

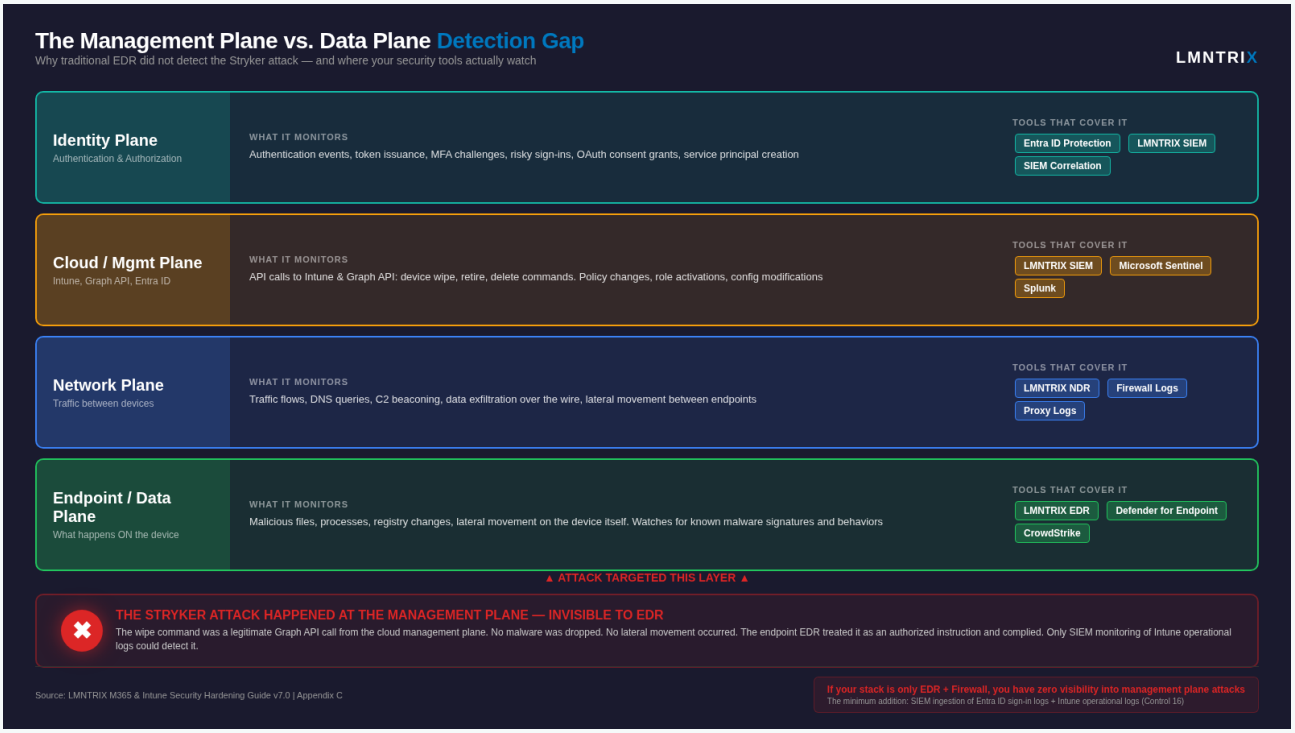

Figure: *The four security monitoring layers. The Stryker attack targeted the Cloud / Management Plane—a layer invisible to EDR.*

Where Your Security Tools Watch

Layer	What It Monitors	Tools That Cover It
Data Plane (Endpoint/Mobile)	Malicious files, processes, registry changes, lateral movement on the device itself	EDR (e.g., LMNTRIX EDR, LMNTRIX Mobile Agent, Defender for Endpoint, CrowdStrike). Watches what happens ON the device
Network Plane	Traffic flows, DNS queries, C2 beaconing, data exfiltration over the wire	NDR (e.g., LMNTRIX NDR, LMNTRIX Packets), firewall logs, proxy logs. Watches what moves BETWEEN devices (North/South and East/West)
Management Plane (Cloud)	API calls to Intune, Entra ID, Graph API. Administrative actions like wipe, policy changes, role activations.	LMNTRIX SIEM ingesting Entra ID sign-in logs, Intune operational logs, and Graph API audit logs, LMNTRIX CNAPP
Identity Plane	Authentication events, token issuance, MFA challenges, risky sign-ins, consent grants	Entra ID Protection, SIEM correlation rules, LMNTRIX SIEM, LMNTRIX Identity Module, monitoring.

The Gap That Stryker Exposed

When a “wipe” command comes from the Intune management plane via a legitimate Graph API call, the EDR on the endpoint treats it as an authorized instruction from the device owner—not as an attack. The device complies and erases itself. There is no malicious file to detect, no suspicious process to kill, no lateral movement to flag.

This is why Control 16 (SIEM monitoring for bulk wipe events) is the only way to “see” this attack in progress. The detection must happen at the management plane and identity plane—not at the endpoint.

> **Practical Note:** *If your security stack today consists only of EDR + firewall, you have zero visibility into management plane attacks. The minimum addition is SIEM ingestion of Entra ID sign-in logs and Intune operational logs, with the KQL alert rules from Control 16. If you're running LMNTRIX SIEM, these log sources can be onboarded and starter detection rules deployed within hours.*

APPENDIX D: SIMULATED WIPE DAY — TESTING YOUR DEFENSES

Most security teams have never tested their detection and recovery for a mass-wipe scenario. You back up your Intune configs, but have you ever actually restored from them? You deployed SIEM alerts, but have you verified they fire? This appendix outlines a controlled test.

The Exercise

- **Prerequisites:**
- 1 lab/test device enrolled in Intune (NOT a production device)
- SIEM alert rules from Control 16 deployed
- CA-backup.json and Intune-configs.json exports from Control 23 available
- IR team aware this is an exercise (you don't want a real P1 response)
- Automated playbook from Control 16 in test mode (validate it fires but do not disable production accounts)
- **Step 1 — Trigger the wipe via Graph API:**

```
# Connect to Graph API with appropriate permissions:
Connect-MgGraph -Scopes
"DeviceManagementManagedDevices.PrivilegedOperations.All"
```

```
# Get the test device ID:
$device = Get-MgDeviceManagementManagedDevice -Filter "deviceName
eq 'LAB-TEST-01'"
```

```
# Execute the wipe:
Invoke-MgGraphRequest -Method POST \
-Uri
"https://graph.microsoft.com/v1.0/deviceManagement/managedDevices/
$($device.Id)/wipe" \
-Body '{}'
```

- **Step 2 — Measure detection and automated response time:**

- Start a timer the moment the wipe command is executed
- Record how long it takes for the SIEM alert to fire (target: <5 minutes)
- Record how long it takes for the automation playbook to execute containment (target: <2 minutes after alert)
- Record how long it takes for the Security Ops team to be notified via out-of-band channel
- If the alert does NOT fire, you have a configuration problem—fix it before a real attack finds it
- **Step 3 — Test recovery from backup:**
- Re-enroll the test device in Intune via Windows Autopilot or manual enrollment
- Attempt to restore the device configuration from your Intune-configs.json backup
- Record how long the full cycle takes: wipe → re-enroll → compliant device (target: <4 hours)
- **Step 4 — Test out-of-band comms:**
- Simulate loss of Teams and corporate email—verify the Signal group is active and all IR team members can be reached
- Verify break-glass credentials from the physical safe still work
- Verify FIDO2 backup keys authenticate successfully

> **Practical Note:** *Run this exercise quarterly. Document results. The first time you run it, things will break—that's the point. Better to find the gaps in a controlled test than during a real 3 AM incident. Track improvement over time: detection speed, response time, recovery time, and comms reliability.*

APPENDIX E: BULK DEVICE RE-ENROLLMENT STRATEGY AFTER MASS WIPE

The controls in this guide focus on prevention. But if the worst happens and a mass wipe is executed, the question becomes: how do you get hundreds of thousands of devices back into Intune and productive?

This is a logistics problem as much as a technical one. The Stryker attack reportedly wiped devices across dozens of countries. Re-enrollment at that scale requires planning you should do now, not during the crisis.

Phase 1: Triage (Hours 0–24)

- Activate out-of-band comms (Control 22). Confirm IR team can communicate.
- Use break-glass accounts to regain tenant access and verify the attacker is locked out (disable compromised accounts, revoke all active sessions, rotate credentials).
- Assess scope: how many devices were wiped? Which regions? Use Intune audit logs (if accessible) or Entra ID sign-in logs to determine blast radius.
- Restore Conditional Access policies and Intune configurations from backup (Control 23) before re-enrolling any devices.

Phase 2: Prioritized Re-Enrollment (Days 1–7)

Not all devices are equal. Re-enroll in priority order:

- Priority 1 — Security and IT operations: SOC workstations, IT admin machines, PAWs. These are needed to manage the recovery itself.
- Priority 2 — Executive leadership and legal: Needed for crisis communications, regulatory reporting, and decision-making.
- Priority 3 — Revenue-critical roles: Sales, customer support, operations staff who directly impact business continuity.
- Priority 4 — General workforce: Remaining employees, starting with largest regional offices for efficiency.

Phase 3: Enrollment Methods at Scale

- **Windows Autopilot (preferred if pre-registered):** Devices with Autopilot hardware hashes already registered in the tenant can be re-enrolled by simply re-imaging and connecting to the internet. The device auto-enrolls, pulls its Intune profile, and becomes compliant.

```
# Verify Autopilot registrations survived the wipe (they live in
the cloud, not on device):
Get-MgDeviceManagementWindowsAutopilotDeviceIdentity | Measure-
Object
```

- **USB Provisioning Packages:** For devices not registered in Autopilot, create Windows Configuration Designer provisioning packages on a USB drive. These can bulk-enroll devices into Entra ID and Intune without manual setup per device.

```
# Create provisioning package via Windows Configuration Designer:
# Include: Entra ID join, Intune MDM enrollment URL, Wi-Fi profile
```

- **Manual Enrollment Stations:** For remote workers and BYOD, set up a self-service enrollment portal. Provide step-by-step instructions via the out-of-band comms channel (Signal/emergency email). Consider deploying temporary IT support at major office locations.

Phase 4: Validation and Compliance

- As devices re-enroll, verify they receive the correct configuration profiles, compliance policies, and application deployments from the restored Intune backup.
- Run compliance checks: ensure BitLocker is re-enabled, endpoint protection is active, and Conditional Access policies are enforcing correctly on re-enrolled devices.
- Audit for any devices that should NOT be re-enrolling—the attacker may attempt to enroll rogue devices during the chaos.
- Track progress via a re-enrollment dashboard: devices enrolled vs. total, by region, by priority tier.

> **Practical Note:** *The single most important preparation you can do right now: verify that your Windows Autopilot hardware hashes are registered in the cloud for all corporate devices.*

> *Autopilot registrations survive a device wipe because they're stored in the Intune service, not on the device. If your devices are Autopilot-registered, mass re-enrollment becomes dramatically faster. Run Get-MgDeviceManagementWindowsAutopilotDeviceIdentity today and compare the count against your total device fleet.*

APPENDIX F: STRYKER ATTACK KILL CHAIN & THREAT INTELLIGENCE

Reconstructed from public reporting and threat intelligence assessments. Each phase maps to the control that would mitigate it.

Phase	Technique	Mitigating Control
Initial Access	AiTM phishing or credential theft targeting M365 Global Admin	FIDO2 MFA (1), Identity Protection (4)
Persistence	Rogue OAuth app or service principal creation	Disable user consent (14), Monitor app registrations (13, 18)
Privilege Escalation	Activate Intune Admin role via Graph API	PIM with approval (2), CAE (3)
Discovery	Enumerate all managed devices via Graph API	Graph API monitoring (17), SIEM alerts (16)
Impact	Mass remote wipe via Intune (reportedly 200K+ devices)	Remove wipe permissions (8), Approval workflow (9), Scope Tags (11)
Impact	Exfiltrate data via cloud APIs and internal network (Handala claimed 50TB)	Audit log monitoring (20), EDR/NDR coverage (20)
Disruption	Corporate comms destroyed (Teams, email, phones wiped)	Out-of-band comms plan (22)
Recovery	Rebuild entire Intune environment from scratch	Cloud config backups (23), Re-enrollment strategy (Appendix E)

Known Handala / Void Manticore TTPs

Handala is assessed as a front for Void Manticore (Storm-0842), an MOIS-affiliated threat group tracked by Microsoft, Check Point Research, and multiple threat intelligence vendors. While formal IOCs specific to the Stryker attack are pending release from incident responders, the following TTPs are associated with Handala/Void Manticore operations based on historical reporting:

- Telegram-based command and control (C2) channels for operational coordination and public-facing claims of responsibility
- Device login page defacement with the Handala logo (a cartoon character symbolic of Palestinian resistance) as a psychological impact tactic
- Use of CaddyWiper and ZeroCleare-style destructive techniques—including IOCTL-based disk operations, custom wipers (BiBi Wiper, CI Wiper), and partition table destruction to render systems unrecoverable
- Living-off-the-land techniques using legitimate cloud management APIs (Graph API, Intune) rather than deploying custom malware to endpoints
- Targeting of on-premises Active Directory via compromised cloud credentials for hybrid environments

> **Practical Note:** *For historical Void Manticore indicators of compromise, refer to Check Point Research's public reporting on Void Manticore campaigns. LMNTRIX threat intelligence continuously ingests and operationalizes IOCs from multiple sources including government advisories, threat intelligence sharing communities, and commercial feeds—these indicators are automatically integrated into LMNTRIX SIEM and EDR detection rules for customers. If your organization identifies any of the above TTPs in your environment, treat it as a confirmed intrusion and activate your incident response plan immediately.*

APPENDIX G: 24-CONTROL QUICK-REFERENCE CHEAT SHEET

Print this page. Tape it to the SOC wall. Use it to brief your CISO in 5 minutes.

#	Control	What to Do	Where	Effort
1	**Role-Based MFA**	FIDO2 for admins, push MFA for users	Entra ID → Auth Methods + CA	4 hrs
2	**PIM**	Eligible-only admin roles, approval required	Entra ID → PIM → Roles	4 hrs
3	**CAE**	Enable Continuous Access Evaluation	CA → Session Controls	1 hr
4	**Identity Detection**	Risk-based CA + token protection	Entra ID → Identity Protection	4 hrs
5	**Admin Locations**	Restrict admin login to named networks	CA → Named Locations	2 hrs
6	**Managed Devices**	Require compliant device for admin access	CA → Grant Controls	2 hrs
7	**Break-Glass**	32+ char passwords, physical safe, monitor	Entra ID + Physical Security	2 hrs
8	**Remove Wipe**	Custom RBAC role without wipe/retire/delete	Intune → Roles → Custom	2 hrs
9	**Wipe Approval**	Enable native MAA for Wipe/Retire/Delete; optionally add Logic App for custom logic	Intune → Multi Admin Approval	1 day
10	**BYOD Protection**	MAM-only for personal devices, block MDM	Intune → App Protection	1 day
11	**Scope Tags**	Segment device mgmt by region/dept	Intune → Scope Tags + Entra AU	1 day

12	**Graph API Lock**	Restrict DeviceMgmt permissions; require admin consent	Entra ID → Enterprise Apps	2 hrs
13	**App Registration**	Disable user app reg, restrict to security group	Entra ID → User Settings	1 hr
14	**OAuth Consent**	Disable user consent, enable admin workflow	Entra ID → Consent Settings	1 hr
15	**SP/MI Audit**	Enumerate & review all service principal permissions	PowerShell + Graph API	4 hrs
16	**SIEM + Automation**	Bulk wipe alert + automated disable/revoke/block	SIEM + Automation platform	1 day
17	**Graph Monitoring**	Monitor wipe/retire/delete API endpoints	SIEM log ingestion	4 hrs
18	**OAuth Monitoring**	Alert on SP creation, consent grants, cred adds	SIEM + Entra audit logs	2 hrs
19	**Log Retention**	1yr retention (E5); 10yr requires add-on. Export to immutable storage	Purview Audit / External SIEM	4 hrs
20	**Exfil Detection**	Audit log monitoring + EDR/NDR for network layer	M365 Audit + EDR/NDR	1 day
21	**License Mapping**	Map your tier to available controls	Review license features	1 hr
22	**OOB Comms**	Signal group, printed phone tree, IR safe	Physical + Signal app	1 day
23	**Config Backup**	Weekly export of CA, Intune, RBAC configs	PowerShell scheduled task	4 hrs
24	**CA Kill Switch**	Pre-stage disabled "Block All Admins" CA policy (emergency only)	CA → Policies (disabled)	1 hr

APPENDIX H: SECURING FEDERATED AND THIRD-PARTY IDENTITY PROVIDERS

The controls in this guide assume Entra ID is the identity control plane. But many enterprises federate authentication to an external identity provider—Okta, Ping Identity, ADFS, or others. In those environments, the real control plane is upstream of Microsoft. If an attacker compromises your external IdP, every Entra ID Conditional Access policy, PIM configuration, and RBAC role becomes irrelevant—the attacker authenticates through the legitimate federation trust and arrives in your tenant as a fully authorized admin.

This appendix addresses that gap.

H.1 — Inventory All Federation Trusts

Most organizations do not have a current inventory of their federation trusts. Start here:

```
# Discover all federated domains in your tenant:
Get-MgDomain | Where-Object { $_.AuthenticationType -eq "Federated"
}
# Then pull federation config for each domain:
Get-MgDomainFederationConfiguration -DomainId [domain]
```

Verify each trust is still needed, that it points to the correct IdP endpoint, and that no unauthorized trusts have been added. Any unexpected federation trust is a critical finding.

H.2 — Monitor Federation Trust Changes in SIEM

Any modification to federation configuration should be treated as a critical alert. This is how Golden SAML attacks are established—the attacker modifies the federation trust to accept tokens they forge.

```
# Alert on federation configuration changes:
AuditLogs
| where OperationName in ("Set domain authentication",
    "Set federation settings on domain",
    "Set company information", "Update domain")
```

H.3 — Require Entra-Native MFA for Admin Roles, Not Federated MFA

This is the single most important control in this appendix. Even if you federate authentication to Okta or Ping, configure Conditional Access authentication strength policies to require Entra-side FIDO2 for all admin roles. This means even a Golden SAML attack cannot satisfy the MFA requirement—the FIDO2 challenge happens at Entra, not at the IdP.

The specific setting is: Conditional Access → Grant → Require authentication strength → Phishing-resistant MFA. This is the same policy from Control 1, but the critical distinction here

is that standard "Require MFA" policies may accept the federated MFA claim from your IdP. Authentication strength policies should cause the FIDO2 challenge to be evaluated at the Entra layer, which in most configurations means the federated IdP's MFA assertion alone is not sufficient. However, exact behavior depends on your specific federation design and token flow—verify this in your environment before treating it as a universal countermeasure—edge cases may exist depending on your IdP configuration and token flow.

H.4 — Audit and Restrict SCIM Provisioning from External IdPs

Okta and Ping often manage Entra ID users via SCIM provisioning. The service principal that performs this provisioning typically has broad write access to directory objects. If an attacker compromises the external IdP admin, they can modify SCIM provisioning rules to create new admin users, add themselves to privileged groups, or elevate existing accounts.

Mitigations:

- **Do NOT sync privileged role assignments via SCIM.** Manage all privileged roles exclusively in Entra ID via PIM (Control 2). The SCIM connector should never be able to assign admin roles.
- **Review the provisioning service principal's permissions quarterly** (same process as Control 15). It should not have DeviceManagementManagedDevices.PrivilegedOperations.All or any destructive Intune permissions.
- **Monitor SCIM write operations.** Alert on any provisioning-initiated role changes or group membership modifications to privileged groups.

H.5 — HSM-Protect IdP Signing Keys (On-Premises) / Verify Cloud IdP Key Management

The Midnight Blizzard (Nobelium) Golden SAML attack against SolarWinds demonstrated the catastrophic impact of stolen token-signing keys. If an attacker obtains your IdP's signing certificate, they can forge SAML assertions for any user—including Global Administrators—without ever authenticating.

- **On-premises ADFS or PingFederate:** Store token-signing certificates in a Hardware Security Module (HSM), not in the Windows certificate store. This is Microsoft's primary recommendation to prevent Golden SAML.
- **Cloud-hosted IdPs (Okta SaaS, Ping Cloud):** You don't control the HSM directly. Verify your vendor's key management practices, enable key rotation monitoring, and ensure you receive alerts on any signing key changes.

H.6 — Evaluate Your Federation Architecture

If running ADFS specifically: Microsoft's strategic direction is Entra-native authentication. Migrating from ADFS eliminates the federation server entirely—no signing key to steal

means no Golden SAML attack vector. Entra ID now supports Certificate-Based Authentication (CBA) natively for organizations that require smartcard/certificate auth.

If using cloud IdPs (Okta, Ping): For many enterprises, federation is not optional—regulatory, contractual, or multi-cloud requirements mandate an external IdP. The focus should be on hardening the federation trust (H.1–H.5 above) rather than eliminating it. Ensure the external IdP's admin portals are restricted to the same named network locations and managed device requirements as your Microsoft admin portals (Controls 5 and 6).

H.7 — Restrict Cross-Tenant MFA Trust

If your organization uses B2B collaboration, review your cross-tenant access settings. By default, Entra ID does not trust MFA claims from partner tenants. However, if your organization has enabled MFA trust in cross-tenant access settings—as many do for B2B collaboration convenience—a compromised partner tenant's MFA assertions would be accepted at face value.

```
Entra ID → External Identities → Cross-tenant access settings →
Trust settings
```

Configure MFA trust only for specific verified partner tenants, not blanket trust for all. For sensitive resource access, require authentication strength (FIDO2) regardless of partner MFA claims.

> **Practical Note:** *The minimum action every organization with a federated IdP should take today: (1) run the PowerShell commands in H.1 to inventory your federation trusts, (2) deploy the KQL alert from H.2 in your SIEM, and (3) configure Conditional Access authentication strength to require Entra-native FIDO2 for admin roles per H.3. These three actions can be completed in under 4 hours and close the most critical gaps.*

Need Help Implementing These Controls?

This guide is designed to be self-service, but implementing 24 controls across a production tenant requires careful planning, testing, and validation. Every organization's environment is different—license tiers, hybrid configurations, legacy app registrations, and operational constraints all affect the implementation path.

If your team needs assistance with any aspect—from initial assessment to full implementation, SIEM deployment, automation playbook configuration, or ongoing monitoring—the LMNTRIX SOC operates 24/7 and can have detection rules deployed within hours of engagement.

Contact your LMNTRIX account team or visit **lmntrix.com**