A FREE GUIDE FROM VERI-TECH, INC.

The Stryker *Response* Pack.

10 Microsoft 365 controls that contain a 50 TB exfiltration plus mass-wipe blast radius. Mapped to MITRE ATT&CK, paraphrased from authoritative frameworks. Written for healthcare CISOs and IT directors.

Infrastructure became code. Compliance is next.

Why this exists

On March 11, 2026 a state-linked threat actor referred to in CISA reporting as "Handala" compromised Stryker Corporation, exfiltrated approximately 50 TB of data, and used the legitimate Microsoft Intune `wipe` command to wipe roughly 80,000 endpoints. CISA published a Microsoft Intune hardening directive seven days later, on March 18, 2026, naming the product by name and listing three explicit recommendations.

Most healthcare and DIB CISOs we have spoken to since are asking the same question: **could this happen to us?**

This pack is a tactical answer. It assumes you already operate Microsoft 365 and Intune. It walks through:

1. The shape of the incident, using only public-domain reporting.
2. A blast-radius map, framed against the MITRE ATT&CK kill chain.
3. The 10 Microsoft 365 controls that contain or would have contained the same pattern, with paraphrased control titles, framework references, and 60-second fixes.
4. A one-page tabletop checklist you can run with your team this week.

We built this from the same control registry that powers Veri-Guard, our M365 compliance scanner. If you want all 548 of our controls continuously evaluated against your tenant, see the back page.

What the public reporting actually says

Treat everything in this section as the limit of what a defender outside Stryker's incident-response loop can know. Internal post-mortem detail is not in scope here.

- **Date.** Initial intrusion attributed to early March 2026; mass-wipe event on or around March 11, 2026.
- **Actor.** State-linked actor identified in CISA reporting under the name "Handala."
- **Targeted environment.** Microsoft 365 tenant, Microsoft Intune as the device-management plane.
- **Impact, exfiltration.** Roughly 50 TB of data exfiltrated. Public reporting indicates a sustained collection-and-staging phase before exfil.
- **Impact, destruction.** Roughly 80,000 endpoints wiped using the legitimate Intune `wipe` action.
- **CISA response.** On March 18, 2026 CISA published a hardening directive naming Microsoft Intune by product. Three recommendations:
    1. Enforce least-privilege Intune RBAC roles.
    2. Require phishing-resistant MFA and tighten privileged-access hygiene.
    3. Require multi-admin approval for sensitive Intune actions, including wipe, app deploy, RBAC changes, and PowerShell scripts.

The mechanism that makes this incident matter to every M365 tenant on the planet. The attacker did not exploit a Microsoft vulnerability. The attacker abused legitimate, signed administrative tooling that every Intune tenant ships with by default. Containment is not a patch problem. It is a configuration problem.

Why healthcare orgs read this differently

A 24-hour mass-wipe event is bad for any business. For a covered entity it is also a HIPAA-reportable security incident under §164.308(a)(6) and a clock-starting impermissible-use determination under §164.402. The mass-wipe also takes EHR endpoints, scheduling clients, and clinician workstations offline simultaneously. Patient-care continuity becomes the second emergency, on top of the breach itself.

The controls in this pack map to:

- **HIPAA Security Rule** safeguards under §164.308 and §164.312.
- **HHS 405(d) Health Industry Cybersecurity Practices** sub-practices, particularly the medium-org access management and incident response groups.
- **CISA SCuBA M365** identity baseline.
- **CIS Microsoft 365 Foundations Benchmarks** across the identity and Intune device-management sections.
- **NIST 800-53 Rev. 5** access-control and audit families.
- **ISO/IEC 27001:2022** Annex A.5, A.7, and A.8.

Closing them moves your healthcare compliance posture across all of those frameworks at once, not one checkbox at a time.

The blast-radius map

This is the public-reporting attack pattern, mapped to the MITRE ATT&CK kill chain, with the M365 control category that breaks the chain at each link. The control numbers in the right column reference the 10 controls below.

Stage	MITRE ATT&CK	What the public reporting indicates	Where M365 controls cut the chain
Initial Access	T1566 Phishing	Targeted phishing of administrative staff.	Controls 4, 5 (phishing-resistant MFA + number matching)
Credential Access	T1556 Modify Authentication Process / T1111 Multi-Factor Authentication Interception	Session theft, MFA bypass via legacy or weaker factors.	Controls 4, 5, 9 (admin MFA + audit visibility)
Privilege Escalation	T1098.003 Account Manipulation: Additional Cloud Roles	Compromised account elevated to high-privilege Intune roles.	Controls 1, 2, 3, 6 (RBAC scoping + standing-privilege removal + approval)
Defense Evasion	T1078.004 Valid Accounts: Cloud Accounts	Use of legitimate, signed Intune tooling rather than malware.	Controls 1, 7, 8 (multi-admin approval + audit-log retention)
Collection / Exfiltration	T1119 Automated Collection / T1041 Exfiltration Over C2 Channel	Sustained 50 TB collection from accessible workloads.	Outside scope of this pack; covered by Defender, DLP, Purview
Impact	T1485 Data Destruction	Mass-wipe via legitimate Intune `wipe` against ~80K endpoints.	Controls 1, 2, 8, 10 (multi-admin approval + RBAC + audit + device scoping)

The two stages where M365 configuration is the load-bearing defense are **Privilege Escalation** and **Impact**. Phishing will continue to land. Endpoint exfil prevention is a separate product family. But the path from "an attacker got an admin session" to "an attacker wiped 80,000 devices" runs through tenant configuration that you control.

The 10 controls

Ordered by where they break the Stryker pattern, not alphabetically. Each one ships with a 60-second-or-less starting point. None of them require a license tier higher than what most healthcare orgs already pay for under M365 E3 + Entra P2 or M365 E5.

1. Require multi-admin approval for sensitive Intune actions

Paraphrased registry title: Intune multi-admin approval should be configured.

Why it matters: This is the single most direct mitigation against the Stryker pattern. With multi-admin approval (MAA) configured for the `delete`, `script`, and (in preview) `wipe` action policies, no single compromised admin session can issue a destructive Intune command on its own. A second authorized administrator must approve the action before it executes.

60-second starting point: Intune admin center, **Tenant administration > Multi Admin Approval > Access policies**. Create policies for "Apps" and "Scripts" first. Set approver group to your privileged-admin AU-scoped group. Document an out-of-band approval channel that is not Microsoft Teams in your IR playbook.

Maps to CISA-MS.AAD.7.6, MT-1096, NIST AC-3, NIST AC-6, ISO27001 A.5.15, HHS 405(d) 3.L.B.

---

2. Scope Intune RBAC role assignments to administrative units, not the tenant root

Paraphrased registry title: Intune RBAC groups protected by Restricted Management Administrative Units or role-assignable groups.

Why it matters: Default Intune role assignments target the tenant root. A compromised role-holder can act on every device in the tenant. Scoping the same role to a Restricted Management Administrative Unit (RMAU) or a role-assignable group limits the blast radius to a defined scope of devices and users. RMAUs in particular cannot be modified by a tenant-wide Global Administrator without first elevating into the AU itself, which is auditable.

60-second starting point: Entra admin center, **Identity > Roles & admins > Administrative units > New > Restricted management AU**. Add the user objects that should be in scope. In Intune, reassign each custom Intune RBAC role from "All devices, All users" to the RMAU.

Maps to MT-1103, NIST AC-2, NIST AC-6, ISO27001 A.5.18, HHS 405(d) 3.L.B.

---

3. Remove standing Global Administrators with PIM eligible-only assignments

Paraphrased registry title: Privileged Identity Management enabled for the Global Administrator role.

Why it matters: Permanent Global Admin accounts are the highest-value target in any tenant. PIM cuts the attack window from "always" to "the time the admin needed it." Activations are time-bound, justification-logged, and revocable. If the Stryker attacker had landed on an account with eligible-only Global Admin instead of standing Global Admin, they would have left a PIM activation event in the audit log before they could touch Intune RBAC.

60-second starting point: Entra, **Identity Governance > Privileged Identity Management > Microsoft Entra roles > Global Administrator**. For each member, change Assignment type from Active to Eligible. Configure activation: max 4 hours, require justification, require approval for at least one role.

Requires Entra ID P2. Maps to CIS-1.1.5, NIST AC-6(7), ISO27001 A.8.2, SOC2 CC6.3, HHS 405(d) 3.L.B.

---

4. Require phishing-resistant MFA for administrators

Paraphrased registry title: Require phishing-resistant MFA for admins.

Why it matters: SMS, voice, and push-only MFA are all phishable through real-time relay attacks. FIDO2 security keys, certificate-based authentication, and Windows Hello for Business are not. Phishing-resistant MFA

on administrative roles closes the most common path from a phished credential to a session token. CISA's hardening directive lists this as recommendation #2 for a reason.

60-second starting point: Entra, **Protection > Authentication methods > Policies**. Enable FIDO2 security key for "Privileged users" group. Then create a Conditional Access policy requiring authentication strength = Phishing-resistant MFA, scoped to the Microsoft Entra Roles assignment that contains your privileged role list (Global Admin, Intune Admin, Privileged Auth Admin, Authentication Admin, Conditional Access Admin, Security Admin, Application Admin, Cloud Application Admin, Helpdesk Admin, User Admin).

Maps to CISA-MS.AAD.3.7, NIST IA-2(1), ISO27001 A.5.16, HHS 405(d) 3.M.D.

---

5. Require number matching for Microsoft Authenticator MFA

Paraphrased registry title: Authenticator requires number matching for MFA.

Why it matters: Number matching defeats MFA-fatigue attacks, where an attacker spams a user with push prompts hoping for an accidental approval. Microsoft made this the default in 2023; your tenant may still have legacy push policies overriding it. Costs nothing to enable. Closes a documented attack path that has been used in multiple high-profile breaches.

60-second starting point: Entra, **Protection > Authentication methods > Microsoft Authenticator > Configure**. Set "Require number matching for push notifications" = Enabled, scope = All users.

Maps to EIDSCA-AP14, CIS 6.1.2, NIST IA-2(6), ISO27001 A.5.16, HHS 405(d) 3.M.D.

---

6. Require approval to activate the Global Administrator role

Paraphrased registry title: Activation of the Global Administrator role requires approval.

Why it matters: PIM eligibility (control #3) removes standing privilege. Approval-gated activation adds a second human in the loop before privilege is actually granted. Even if an attacker compromises an eligible Global Admin's credentials, they need an approver to act before the role is active. This is a force-multiplier on PIM, not a duplicate of it.

60-second starting point: Entra, **Identity Governance > Privileged Identity Management > Microsoft Entra roles > Roles > Global Administrator > Settings**. Edit "Activation". Enable "Require approval to activate". Set approvers to a separate group that does not overlap with the eligible Global Admin group.

Requires Entra ID P2. Maps to CISA-MS.AAD.7.6, NIST AC-3, NIST AC-6, ISO27001 A.5.15, HHS 405(d) 3.L.B.

---

7. Alert on every Global Administrator activation

Paraphrased registry title: User activation of the Global Administrator role triggers an alert.

Why it matters: Any activation of Global Admin is a high-signal event. In a healthy tenant it happens rarely. An anomalous activation (off-hours, from an unusual IP, or by an account that has never activated before) is a

leading indicator of compromise. Wire the alert to whichever channel actually gets read at 2am, not just to email.

60-second starting point: Entra, **Privileged Identity Management > Microsoft Entra roles > Roles > Global Administrator > Settings > Notifications**. Enable "Notification on activation" with a custom recipient list pointing at your IR distribution group + a Sentinel or webhook integration if you run one.

Maps to CISA-MS.AAD.7.8, NIST AU-6, NIST IR-4, ISO27001 A.5.25, HHS 405(d) 3.L.B.

---

8. Retain Intune audit logs and stream them off-tenant

Paraphrased registry title: Intune audit logs should be retained.

Why it matters: Default Intune audit-log retention is 365 days inside the tenant. If an attacker is willing to wipe 80,000 endpoints, they are willing to disable or delete an audit trail you have not exported. Retention plus off-tenant streaming gives your incident-response team something to investigate after the wipe, even if in-tenant evidence is destroyed. This is also where most healthcare audit findings land, because OCR investigators want six years of audit retention under §164.316(b)(2).

60-second starting point: Intune admin center, **Tenant administration > Diagnostic settings > Add diagnostic setting**. Send `AuditLogs` and `OperationalLogs` to a Log Analytics workspace in a separate subscription, or to an event hub forwarding to your SIEM. Confirm the workspace retention is set to 6 years for healthcare workloads.

Maps to MT-1100, NIST AU-11, ISO27001 A.8.15, HIPAA §164.316(b)(2), HHS 405(d) 8.M.A.

---

9. Enable the Microsoft 365 Unified Audit Log

Paraphrased registry title: Unified audit logging enabled.

Why it matters: The Intune audit log (control #8) covers Intune actions. The Unified Audit Log covers everything else: Exchange admin actions, SharePoint sharing changes, Entra role changes, mailbox access, Conditional Access policy edits. A 50 TB exfil pattern leaves traces in Exchange and SharePoint that are only recoverable if UAL was on at the time. Microsoft turns this on by default for tenants created after 2023, but older tenants and several sovereign clouds still ship with it disabled.

60-second starting point: PowerShell:

```
Connect-ExchangeOnline
Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled $true
```

Maps to CISA-MS.EXO.8.1, CIS 6.5.3, NIST AU-2, ISO27001 A.8.15, HIPAA §164.312(b), HHS 405(d) 8.M.A.

---

10. Require Conditional Access compliant device for all administrators

Paraphrased registry title: Require compliant device for admins.

Why it matters: Even if an attacker has phished a credential and bypassed MFA somehow, requiring an Intune-compliant device for the sign-in shifts the attack from "any laptop on the internet" to "a device the attacker has independently compromised AND enrolled to your tenant." For a small admin population this is operationally feasible. It is also the same control that limits an attacker who has compromised a personal BYOD device from pivoting into administrative work.

60-second starting point: Entra, **Protection > Conditional Access > New policy**. Assignments: Users = directory roles (Global Admin, Intune Admin, Privileged Auth Admin, Application Admin, Cloud Application Admin, Authentication Admin, Conditional Access Admin, Security Admin, Helpdesk Admin, User Admin). Cloud apps = All. Grant: Require device to be marked as compliant, AND require MFA. Enable in report-only mode for one week before enforcing.

Maps to CIS-1.3.2, NIST AC-19, ISO27001 A.7.9, SOC2 CC6.1, HHS 405(d) 2.M.B.

One-page tabletop checklist

Run this with your IR team. The goal is not to prove you are perfect. The goal is to surface the gaps before you have to find them in production.

Setup, 5 minutes. Convene the table. Roles needed: incident commander, Intune admin, Entra admin, communications lead, legal/privacy lead. The scenario starts at minute zero of detection.

Scenario. Helpdesk receives 14 calls in 6 minutes that company-managed laptops have spontaneously started displaying "Hi, set up your iPhone" or the Windows OOBE. Splunk shows a spike in Intune `wipe` actions originating from a single admin account over the last 12 minutes.

Round 1, contain (20 minutes).

- [ ] Who has authority to disable an Entra account right now? Whose account is doing this? Confirm the answer is not "we have to wake somebody up."
- [ ] Can you revoke that user's session tokens AND require re-MFA on every session in the tenant from a single console action? *(Entra > Identity > Users > [user] > Revoke sessions. Then PIM > Settings > Activate Emergency lockout.)*
- [ ] What is your Intune Multi-Admin Approval state for `wipe` and `delete app`? If "not configured," control 1 is your single highest-priority follow-up after this exercise.
- [ ] Can you turn off the Intune service principal for the suspect account without disabling the account? Walk through the steps.

Round 2, scope (20 minutes).

- [ ] Pull the last 24 hours of Intune audit log. Confirm you can do this without the suspect admin's involvement.
- [ ] How many devices were already wiped before you noticed? How are you communicating "do not factory-reset, file an IT ticket" to the affected users when most of their phones and laptops are bricked?

- [ ] Identify every administrative role the suspect account held in the last 30 days. Use PIM history, not current state.
- [ ] If the attacker exfiltrated data alongside the wipe (which is the Stryker pattern), where would it have come from? Run through the user's likely SharePoint, OneDrive, and Exchange access in the last 30 days.

Round 3, communicate (15 minutes).

- [ ] Does this trigger your HIPAA breach-notification clock? Who decides? Document the criteria you used.
- [ ] What is your communications path to staff whose primary work device just got wiped? *(Hint: the answer is not "Teams," because their Teams client is gone.)*
- [ ] What is the public-disclosure decision process? Who has authority to talk to media? If your CEO is unreachable, who is the backup?
- [ ] Where is your Microsoft Premier or Unified Support contract number stored? Can you find it without your laptop?

Round 4, recover (15 minutes).

- [ ] What is the Intune device re-enrollment plan for 80,000 endpoints? For 800? For 80? Be honest about the timeline.
- [ ] Walk through the BitLocker recovery key dependency. Are recovery keys escrowed in Entra ID, or only in Configuration Manager? If only in CM, how do you reach CM after the wipe?
- [ ] If the attacker also disabled or deleted Conditional Access policies, what is your "rebuild CA from version control" runbook? Do you have one?

After-action. The output of this exercise is a punch list of 5-15 items. Half will be configuration changes (the 10 controls above are a good starting point). Half will be runbook gaps. Both are fixable inside 30 days.

What to do next

You just walked through a tabletop exercise. Here is the honest tradeoff: tabletops surface gaps once. They do not tell you when a Conditional Access policy gets disabled at 11pm by an admin who thought it was breaking sign-ins, or when somebody adds a new Global Administrator to bypass an approval queue.

That is the gap Veri-Tech closes.

Veri-Guard continuously scans your M365 tenant against 548 controls across 12 frameworks (CISA SCuBA, CIS Microsoft 365, NIST 800-53, NIST CSF 2.0, ISO 27001, HIPAA, HHS 405(d), GDPR, SOC 2, FFIEC, PCI DSS, MITRE ATT&CK). Every one of the 10 controls in this pack is in there. When any of them drift, you find out the same day.

Veri-Tune baselines your Intune environment against community-vetted standards and ours. When a policy gets edited or a new RBAC scope appears, you get a diff and a runbook before the next audit.

Veri-Vault keeps versioned snapshots of your Intune configuration plus tested restore runbooks. If you do have to rebuild after an incident, you are restoring known-good policy bundles, not reconstructing them from

screenshots.

Three ways to take the next step:

- **Compare us against alternatives:** veri-tech.net/compare. See how Veri-Guard, Veri-Tune, and Veri-Vault stack up against the broader compliance-platform market.
- **Try the interactive demo:** veri-tech.net/demo. Walk through the products against a simulated tenant. No credit card.
- **Talk to William directly:** veri-tech.net/book. 30-minute intro call with the founder, no sales team in the loop.

Veri-Tech is a Microsoft Partner Network member, Indiana-based, and veteran-founded. Healthcare BAA support is part of our healthcare package.

Infrastructure became code. Compliance is next.

Veri-Tech, Inc. Veteran-owned. Indiana-based. Founded 2026. veri-tech.net · security@veri-tech.net