STRYKER INCIDENT ADVISORY

Prepared by Ekco Cyber Resilience Team

SUMMARY

On 11 March 2026, Stryker Corporation experienced a destructive cyberattack that crippled employee devices across its global Microsoft Intune and Microsoft 365 environment, disrupting orders, manufacturing, and shipping operations. Connected medical devices and patient-facing systems remained unaffected.

The pro-Iranian threat group Handala claimed responsibility and posted messages alleging data exfiltration and widespread wiping of corporate systems.

Analysis suggests the attackers abused privileged access to Intune, Microsoft's cloud endpoint management platform, to issue mass device wipe commands across Windows, macOS, and mobile endpoints simultaneously.

By compromising Intune administrative privileges, the attackers effectively turned the organisation’s own management platform into a destructive command-and-control system, rendering thousands of devices inoperable.

This attack highlights a critical reality:

Endpoint management platforms like Intune are essentially "root control planes" for corporate devices. If attackers control them, they control the entire endpoint fleet which is why every organisation should move to immediately ensure threat actors cannot use legitimate corporate tools against them.

Microsoft Intune has become the de-facto tool for managing devices. In this incident no malware was deployed that could be detected, no software was mass deployed that could be detected.

A privileged user account was compromised and allowed for the complete destruction of all corporate and BYOD devices connected to the business. Using legitimate tools for illegitimate means with no option but to rebuild and restore.

WHY THIS MATTERS

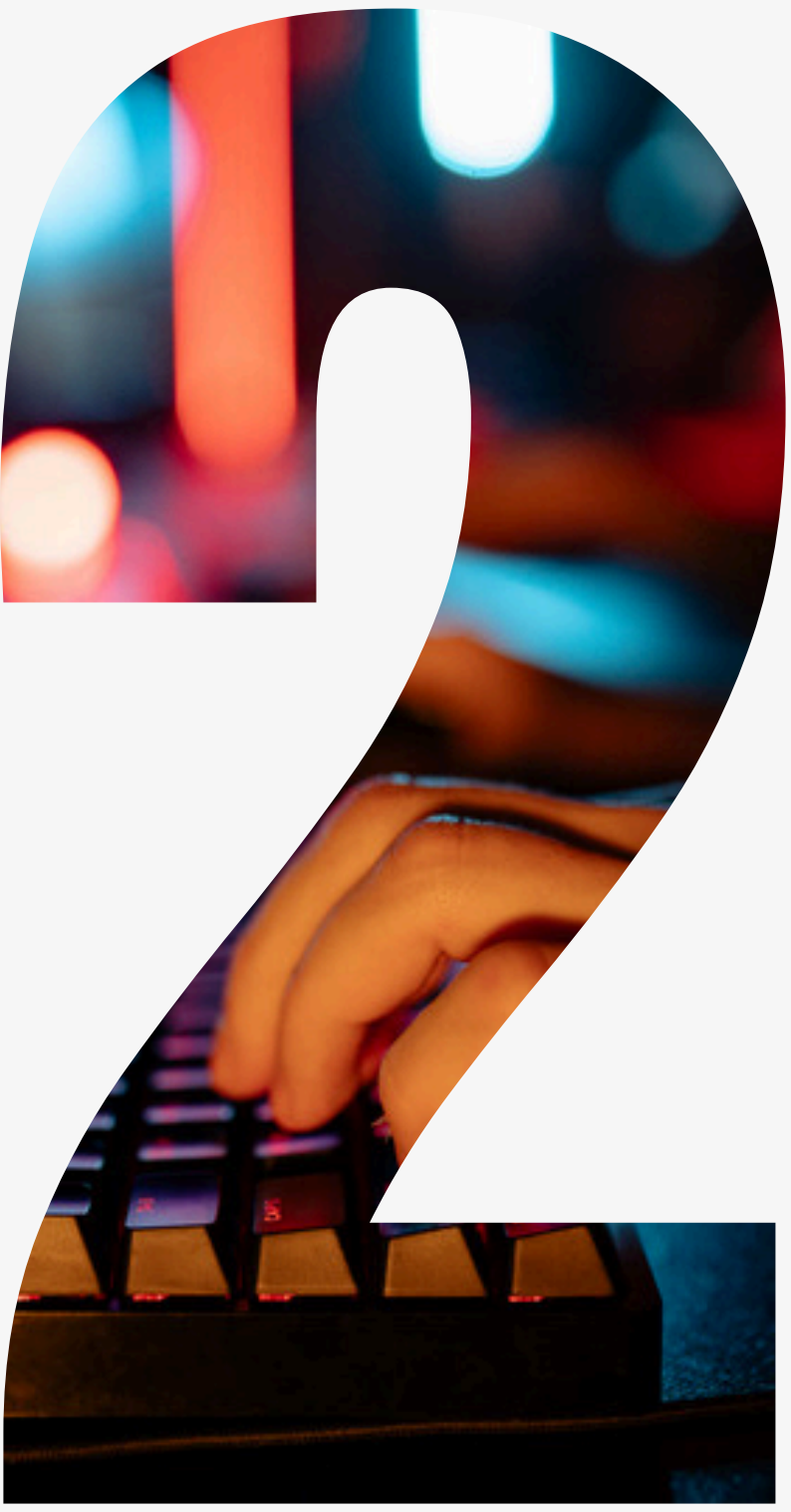
Endpoint management platforms are now high-value attack targets

Platforms such as Microsoft Intune, Microsoft Endpoint Configuration Manager, and similar EMM/MDM systems have direct authority over every enrolled device.

If compromised, an attacker can:

- Wipe or lock thousands of endpoints
- Deploy malicious configurations or scripts
- Remove security tools
- Push ransomware or destructive payloads
- Break authentication mechanisms

In modern cloud environments, control of Intune equals control of the endpoint estate.



WHY THIS MATTERS

This attack appears destructive rather than extortion-driven

Unlike typical ransomware incidents, the attack reportedly used mass device wiping.

That means:

- No ransom negotiation
- Recovery depends entirely on resilience and rebuild capability
- Operational downtime becomes the primary impact

WHY THIS MATTERS

Healthcare and supply-chain manufacturers are strategic targets

Organisations like Stryker Corporation operate in sectors where disruption cascades downstream.
Impacts can include:

- Delayed medical equipment shipments halted manufacturing lines
- Disrupted hospital supply chains
- Geopolitically motivated actors increasingly target private companies with systemic operational impact

WHY THIS MATTERS

Cloud identity compromise enables large-scale remote destruction

In traditional breaches, attackers needed lateral movement across networks.

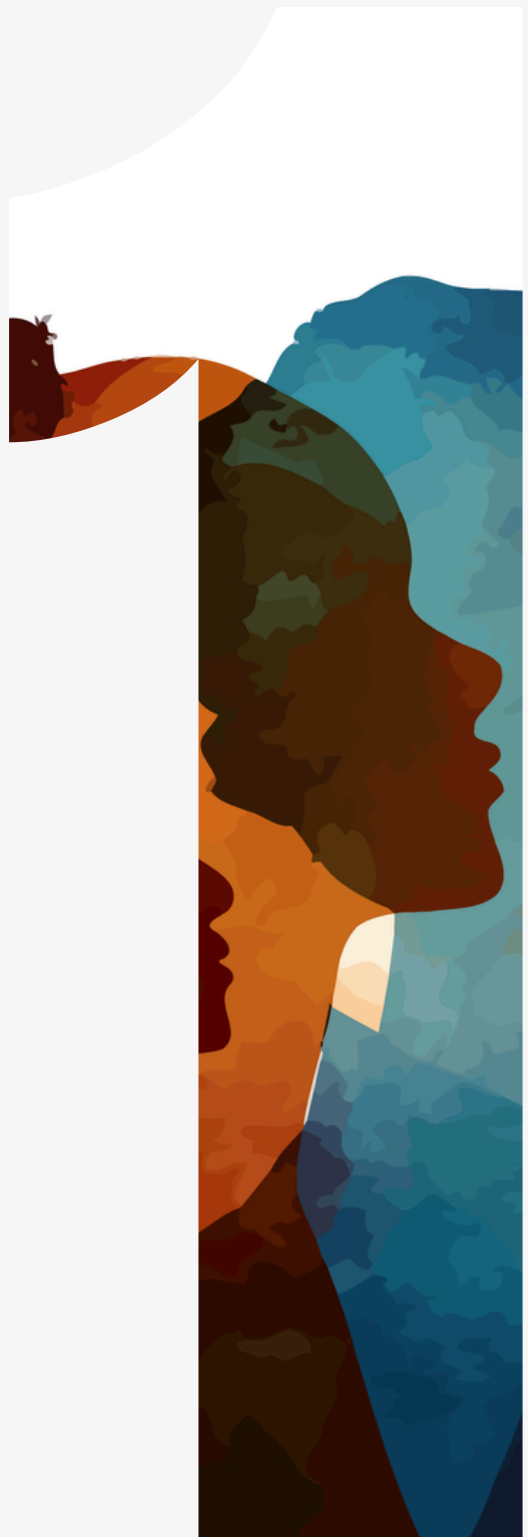
With platforms like Microsoft Intune, a single compromised cloud administrator account can trigger global destructive actions within minutes.

This shifts the defensive focus to identity protection and privileged access governance.

PRACTICAL DEFENSIVE ACTIONS FOR ORGANISATIONS

Treat Identity as Critical Infrastructure

Protect cloud identity platforms with the same rigor as production systems.



Implement:

- Phishing-resistant MFA (FIDO2/passkeys)
- Strict conditional access policies
- Continuous sign-in monitoring
- Impossible-travel detection
- Token abuse detection
- Privileged role alerts

Identity compromise is often the first step in control plane takeover.

DEFENSIVE ACTIONS

Harden and Protect Intune as a Critical Control Plane

Organisations should treat Microsoft Intune as Tier-0 infrastructure, equivalent to domain controllers.

Key protections include:

- Restrict administrative access
- Limit Intune administrative roles to dedicated security personnel
- Use separate admin identities (never daily-use accounts)
- Enforce phishing-resistant MFA
- Use hardened administrative workstations

Require administrators to manage Intune only from:

- Privileged Access Workstations (PAWs)
- Hardened, monitored devices
- Isolated admin environments

This prevents attackers from hijacking admin sessions from compromised endpoints.

Monitor for high-risk Intune actions
Alert on:

- Mass device wipe commands
- Bulk policy deployments
- Unusual device retirements
- New administrator role assignments
- Sudden configuration changes

These actions are early indicators of destructive abuse.

DEFENSIVE ACTIONS

Implement Just-In-Time (JIT) Privileged Access

Standing administrative privileges create a permanent attack opportunity.

Instead, organiSations should implement Just-In-Time (JIT) elevation, using tools such as Microsoft Entra ID and Microsoft Entra Privileged Identity Management.

JIT reduces risk by ensuring:

- Administrators do not permanently hold Intune privileges
- Access must be explicitly requested and approved
- Privileges are time-limited (e.g., 15–60 minutes)
- All elevation events are logged and monitored

If attackers compromise an admin account without active elevation, they cannot immediately control Intune.

This dramatically reduces the blast radius of identity compromise.

DEFENSIVE ACTIONS

Assume Destructive Actors - Harden Recovery

Organisations must prepare for device fleet destruction scenarios.

Key measures:

- Immutable backups
- Air-gapped backup infrastructure
- Separate authentication domains for backups
- Gold device images
- Automated device rebuild pipelines

The goal is rapid fleet reconstruction, not negotiation.

Operationalise Incident Response

Many organisations have incident response plans that are never exercised.

To ensure readiness:

- Conduct regular tabletop exercises
- Include IT, security, legal, communications, and executives
- Pre-contract digital forensics and incident response firms
- Pre-stage crisis communication procedures

Speed matters in destructive incidents.

DEFENSIVE ACTIONS

EKCO

DEFENSIVE ACTIONS

Practice Business Continuity Without Core IT

Prepare for 24–72 hours of degraded IT availability.
Develop manual procedures for:

- Order processing
- Manufacturing coordination
- Shipping and logistics
- Supplier communications

Organisations should maintain offline procedures and alternate communication channels.

DEFENSIVE ACTIONS

Segment Critical Management Planes (Zero Trust)

Apply Zero Trust segmentation across:

- Identity infrastructure
- Endpoint management platforms
- Backup systems
- Operational technology networks
- Administrative environments

This reduces the likelihood that compromise in one area results in total environment control.

QUICK DETECTION & HUNTING CUES

1. Sudden mass logout/disabled devices, defaced login screens, or unexpected mass policy changes on your MDM/Intune console

2. Alerts indicating large data downloads from file shares or archive systems shortly before device failure

3. Unusual administrative token issuance or service account activity originating from home/foreign IP ranges.

Is your organisation protected against Intune-level compromise? Let’s assess it together

info@ek.co

Get in touch

ek.co