The Stryker Wiper: When UEM Becomes a Weapon

Systemic Risk in Unified Endpoint Management and the Handala Attack on Stryker Corporation

Unofficial AI-assisted Research

Cloud Security Alliance AI Safety Initiative

2026-03-21

Key Takeaways

- On March 11, 2026, a threat actor linked to Iran's Ministry of Intelligence and Security (MOIS) used compromised Microsoft Entra ID Global Administrator credentials to issue a legitimate Remote Wipe command through Microsoft Intune, destroying an estimated 80,000 devices at Stryker Corporation across 79 countries in approximately three hours. No malware was deployed.

- The attack belongs to an emerging class termed "living off trusted services" (LoTS) — an extension of the established "living off the land" (LotL) concept applied to cloud-native administrative tooling — in which adversaries weaponize legitimate platform features rather than deploying malicious code. Because the destructive action was performed through valid platform features using valid credentials, traditional malware detection and endpoint detection and response (EDR) tools had no malware signatures to detect, and most SIEM deployments lacked configured alerting thresholds for bulk UEM administrative actions, leaving standard monitoring effectively blind to the event in progress.

- Unified Endpoint Management (UEM) platforms — including Microsoft Intune, Ivanti Endpoint Manager, VMware/Omnissa Workspace ONE, Jamf, and similar solutions — represent a structurally dangerous category of administrative infrastructure. A single compromised privileged credential in a UEM-integrated identity platform provides simultaneous, authenticated, trusted command over every enrolled device in an enterprise globally.

- The Stryker attack is not an isolated event. Concurrent CISA Known Exploited Vulnerability (KEV) additions in March 2026 include a critical authentication bypass in Ivanti Endpoint Manager (CVE-2026-1603) and a server-side request forgery flaw in Omnissa Workspace ONE UEM (CVE-2021-22054), while Palo Alto Unit 42 researchers have separately documented nation-state malware (Airstalk) that uses VMware AirWatch UEM API endpoints as a covert command-and-control channel.

- CISA, the FBI, and Microsoft have all issued formal guidance in response to the Stryker attack. The most critical control is Multi Admin Approval in Microsoft Intune, which requires a second administrative account's explicit approval before high-impact actions — including remote wipe,

script deployment, application installation, and role assignment — can execute. Organizations that have not enabled this control are operating with a single point of failure for their entire managed device fleet.

Background

Unified Endpoint Management platforms emerged as enterprises consolidated the fragmented tooling they had historically used to manage laptops, mobile phones, servers, and IoT devices. Rather than maintaining separate systems for Windows device management, Apple mobile device enrollment, and application deployment, UEM solutions offered a single administrative console through which IT and security teams could configure policies, push software, enforce compliance, and, when necessary, remotely lock or wipe devices across an entire organization. Microsoft Intune, which has become the most widely deployed cloud-native UEM platform as enterprises migrated to Microsoft 365, is deeply integrated with Microsoft Entra ID (formerly Azure AD), Microsoft Defender, and Azure Conditional Access. This integration creates powerful administrative leverage: from a single console, an authorized administrator can reach every enrolled device worldwide, regardless of geography or network connectivity.

That administrative leverage is precisely what makes UEM platforms a target of exceptional value to adversaries. The "keys to the kingdom" framing that security practitioners have traditionally applied to domain controllers and privileged access workstations must now extend to UEM management tenants. A domain controller compromise historically required an attacker to gain access to on-premises infrastructure, traverse the network, and perform technical exploitation. A UEM console compromise in a cloud-native enterprise can be accomplished with a set of stolen credentials and a web browser. The management plane is internet-accessible by design.

The Stryker Corporation attack on March 11, 2026 is one of the most consequential public demonstrations of UEM weaponization to date, and the first publicly confirmed incident in which a cloud-native Remote Wipe command was used as a mass-destruction tool against a Fortune 500 enterprise. Stryker, a Fortune 500 medical technology manufacturer headquartered in Kalamazoo, Michigan, operates in 79 countries and employs approximately 56,000 people worldwide, producing surgical instruments, orthopedic implants, hospital beds, and connected medical devices [1][2]. The pro-Iranian hacktivist group Handala claimed responsibility for the attack, framing it as retaliation for Stryker's 2019 acquisition of Israeli company OrthoSpace and its U.S. military contracts [1][3]. U.S. authorities subsequently assessed Handala as operating under the direction or coordination of Iran's Ministry of

Intelligence and Security (MOIS), and on March 20, 2026, the U.S. Department of Justice formally accused MOIS of operating the group while the FBI seized Handala's data leak website and associated domains [4][5].

Security Analysis

Attack Chain: Credential Abuse at Administrative Scale

The Stryker attack was operationally simple and technically unsophisticated. The attack's simplicity is notable: it required no novel exploit, no malware, and no technical sophistication beyond credential possession — a characteristic that practitioners should find clarifying about the nature of the threat. Between approximately 05:00 and 08:00 UTC on March 11, 2026, attackers issued a Remote Wipe command through Microsoft Intune to all enrolled devices in Stryker's global Microsoft tenant [6][7]. An estimated 80,000 devices were wiped within that three-hour window, according to sources familiar with the investigation cited by BleepingComputer and The Register [7][8]. Handala's own claims of 200,000 wiped devices have not been independently verified; the higher figure is likely inflated. Stryker has publicly characterized the event as a destructive cyberattack and confirmed restoration efforts, while noting that there is "no indication of ransomware or malware" — a technically accurate statement given that no malicious software was deployed [2][9].

The entry point was a compromised Global Administrator account in Microsoft Entra ID. The precise method by which Handala obtained those credentials has not been officially confirmed, but security firm Push Security's analysis of the incident assessed the most probable vector as infostealer-sourced credentials obtained from historical breach data, with adversary-in-the-middle (AiTM) phishing and OAuth device code phishing as alternative hypotheses [10]. The critical observation is that once an attacker holds Global Administrator credentials in an Entra ID tenant, no additional exploitation is required. Global Administrator is the highest-privilege role in the Microsoft cloud identity hierarchy, and it confers direct administrative access to Microsoft Intune without any separate authentication challenge. In default Entra ID and Intune configurations, there is no independent access control boundary between the identity plane and the management plane — though Conditional Access policies, Privileged Access Workstations with device compliance requirements, and network-scoped restrictions can create meaningful boundaries when explicitly deployed. The attacker logged into the Intune console, selected enrolled devices, and issued the Remote Wipe command — the same workflow any legitimate IT administrator would follow for a routine device decommission.

The aftermath extended well beyond internal IT disruption. Workers at Stryker's Ireland hub were sent home as systems became unavailable [11]. Order processing, manufacturing operations, and global shipping were disrupted. Maryland hospitals proactively suspended connections to Stryker tools used to analyze patient vital signs and EKG data [12]. Bloomberg reported surgical delays for some patients [13]. Handala additionally claimed exfiltration of 50 terabytes of data — including design files, ERP and logistics data, supplier contracts, and hospital records — though Handala's subsequent claim of 12 petabytes of exfiltrated data has not been independently corroborated and is implausible given typical enterprise storage architecture at this scale [1][3].

The Structural Vulnerability: Administrative Blast Radius

What the Stryker attack illustrates most clearly is the extraordinary destructive leverage available to any adversary who gains privileged access to a UEM management tenant. In traditional enterprise environments, a compromised domain administrator account posed severe risk, but the scope of that risk was bounded by network segmentation, geographic distribution of infrastructure, and the time required to spread lateral movement across diverse systems. A UEM platform collapses those mitigating constraints. Remote Wipe is a cloud-queued command delivered through the MDM management channel. It reaches enrolled devices as soon as they connect to the Intune service, regardless of their network location or any local security software running on the device. Devices that are powered off or offline at the time the command is issued will receive and execute the wipe upon next check-in, providing a narrow window during which network isolation of offline devices may prevent execution. No malware signature exists to detect. No anomalous network traffic is generated by the wipe command itself — it arrives as a legitimate management instruction from the device's trusted management authority.

The detection gap is particularly acute because UEM administrative actions are generally excluded from security alerting thresholds to avoid noise from routine IT operations. Large organizations routinely wipe hundreds of devices monthly during employee offboarding, hardware refreshes, and compliance enforcement cycles. A bulk wipe command issued outside business hours might generate alerts, but the speed of execution — 80,000 devices in approximately three hours — substantially limits the response window even when detection occurs promptly. By the time most security operations centers correlate the unusual volume, a substantial portion of the destruction is likely already complete.

The reach of the wipe command extends further than organizations often recognize. BYOD programs, in which employees enroll personal devices in corporate MDM for access to enterprise email and collaboration tools, mean that an attacker's remote wipe may destroy personal photographs, banking application data, two-factor authentication tokens, and subscriber identity data stored in eSIMs

alongside corporate assets [10]. Stryker employees reported personal data loss alongside corporate data destruction [10]. This exposure creates legal, regulatory, and employment relations consequences that compound the operational disruption.

Concurrent Threats: A Systemically Targeted Attack Surface

The Stryker attack did not occur in isolation. In the same week, CISA added to its Known Exploited Vulnerabilities (KEV) catalog two critical flaws affecting Ivanti Endpoint Manager (EPM), a widely deployed UEM platform. CVE-2026-1603, rated 8.6 on the CVSS scale, is an authentication bypass vulnerability affecting all Ivanti EPM versions prior to 2024 SU5 [14]. An unauthenticated remote attacker can send a crafted HTTP request to bypass authentication entirely and access the EPM Credential Vault, which stores domain administrator password hashes and service account credentials for the managed environment — based on the characterization in the CISA KEV entry and Security Affairs coverage, though Qualys' advisory for the same CVE describes the attacker as authenticated, reflecting an unresolved discrepancy between vendor analyses [14][15]. A companion SQL injection vulnerability in Ivanti EPM, CVE-2026-1602, can be chained with CVE-2026-1603 to achieve arbitrary database reads following the initial authentication bypass. Federal civilian agencies face a mandatory patch deadline of March 23, 2026 under the CISA Binding Operational Directive, and enterprise organizations should treat the same timeline as a priority [15]. CISA separately added CVE-2021-22054, an unauthenticated server-side request forgery (SSRF) vulnerability in Omnissa (formerly VMware) Workspace ONE UEM, to the KEV catalog in March 2026 [14].

A distinct but structurally similar threat was documented by Palo Alto Unit 42 researchers in the Airstalk campaign, attributed to a suspected Chinese nation-state actor tracked as CL-STA-1009 [16]. The Airstalk malware abuses VMware AirWatch and Workspace ONE UEM API endpoints — specifically `/api/mdm/devices/` for command-and-control communications and `/api/mam/blobs/uploadblob` for data exfiltration — as a covert channel. By routing communications through the organization's own trusted management infrastructure, the malware evades network-layer detection controls that would flag outbound traffic to unknown external endpoints. The pattern is the inverse of the Handala attack — rather than using UEM to destroy, the Airstalk operator uses UEM to persist invisibly — but both illustrate the same fundamental insight: the management plane that organizations depend upon for device security is itself a high-value, insufficiently protected attack surface.

Why Recovery Is Categorically More Difficult Than Ransomware

Enterprise incident response has developed substantial muscle memory for ransomware, including backup restoration procedures, decryption key negotiation, and staged recovery prioritization. Wiper attacks present a categorically different recovery challenge. There are no encrypted files that can be restored with the right key. There is no adversary to negotiate with for a decryption tool. Each wiped device must be re-provisioned: operating system reinstalled, applications redeployed, user data restored from backup. For organizations without pre-configured zero-touch provisioning — such as Windows Autopilot or Apple Automated Device Enrollment — this may require physical access to each device. Organizations with mature cloud-native provisioning pipelines can initiate remote recovery at scale, but this requires prior investment in Autopilot profiles, cloud-only identity binding, and synchronized user data — investments that the Stryker incident should prompt organizations to make if they have not already done so. For an 80,000-device fleet spanning 79 countries, even a remote-provisioning recovery is measured in weeks, not days. Stryker publicly indicated it was still restoring systems as of March 17, 2026 — six days after the attack — and the full operational recovery timeline has not been publicly disclosed [9].

Recommendations

Immediate Actions

Organizations running Microsoft Intune should enable **Multi Admin Approval** immediately. This feature, which CISA explicitly highlighted in its March 18, 2026 hardening alert, requires a second administrative account's explicit approval before any of the following actions can execute: remote device wipe, application deployment, script execution, RBAC role modification, and configuration profile changes [17]. Had Multi Admin Approval been enabled at Stryker, the attacker would have needed to compromise a second independent administrative account to authorize the bulk wipe — a significantly higher bar than the single credential used in the attack. CISA has specifically identified this control as one that would have materially impeded the attack's execution [17].

All UEM administrative accounts — without exception — must be protected by phishing-resistant multi-factor authentication. FIDO2 hardware security keys, device-bound passkeys, and certificate-based authentication (CBA) using PKI-issued smart cards or device certificates represent the authenticator categories recognized by CISA and NIST as cryptographically resistant to adversary-in-the-middle phishing and session relay attacks. Organizations that have deployed Microsoft Authenticator push notifications or SMS one-time passwords as their administrative MFA should treat migration to one of

these phishing-resistant methods as an urgent remediation, not a roadmap item. Documented campaigns involving the Starkiller phishing-as-a-service platform and related AiTM toolkits have demonstrated in practice that push-notification and TOTP-based MFA can be defeated in real time at scale [18].

Organizations running Ivanti EPM should apply the 2024 SU5 patch immediately to address CVE-2026-1603 and CVE-2026-1602. Network-level controls should block external access to EPM administrative interfaces where that is operationally feasible while patching is completed. Organizations running Omnissa Workspace ONE UEM should verify patch status for CVE-2021-22054 and audit for evidence of unauthorized SSRF usage in web server logs.

Short-Term Mitigations

Privileged Identity Management (PIM), available in Microsoft Entra ID P2 licensing, provides just-in-time privileged access for administrative roles including Intune Service Administrator. Rather than granting permanent Global Administrator or Intune administrative role assignment, PIM requires administrators to activate their elevated permissions on-demand with business justification and time limits, and records every activation with full audit logging. This reduces the standing exposure window for any compromised privileged credential, limiting attacker access to the activation duration — typically one to eight hours — rather than a permanently active role. CISA's March 2026 advisory explicitly references PIM deployment as a recommended control [17].

Conditional Access policies should require compliant devices and specific named locations for any access to Intune management interfaces. UEM consoles should not be accessible from unmanaged personal devices or from geographies inconsistent with the organization's administrative workforce. Microsoft Entra ID risk-based Conditional Access can automatically block sign-in attempts from identities flagged as high-risk by Microsoft's threat intelligence signals, providing real-time response to in-progress credential abuse attempts.

Audit log monitoring for UEM environments must be explicitly configured and reviewed. Organizations should establish alerting thresholds for bulk device actions — specifically, any remote wipe, remote lock, or bulk policy change affecting more than a defined number of devices within a configurable time window. Audit logs from Microsoft Intune, Entra ID, and related services should be integrated into the central SIEM and treated as high-priority security telemetry rather than operational logs.

Strategic Considerations

Enterprises should conduct a formal review of the separation between their identity management plane and their device management plane. The tight integration between Microsoft Entra ID and Intune — while operationally convenient — means that a single compromised cloud identity account can yield both authentication infrastructure control and mass endpoint destruction capability. Where operationally feasible, organizations should explore whether UEM administrative roles can be scoped to dedicated identities separate from general M365 administration, reducing the blast radius of a general administrative account compromise.

Backup and recovery planning must explicitly account for mass device wipe scenarios. This requires validating that critical data is being continuously synchronized to cloud-based or network-accessible storage that survives a device wipe, establishing pre-provisioned device staging capability for rapid re-deployment, and defining recovery prioritization tiers for which systems are restored first based on operational criticality. BYOD programs warrant particular scrutiny: employees should be informed that corporate MDM enrollment creates a remote wipe exposure for personal data, and organizations should evaluate whether personal device enrollment is a justified risk given the employee data loss implications demonstrated in the Stryker incident.

Third-party UEM platforms — Ivanti, Omnissa, Jamf, Hexnode, and others — should be evaluated against the same privileged access controls applied to Microsoft Intune. The active exploitation of Ivanti EPM and the documented abuse of Workspace ONE APIs demonstrate that this risk class is not Microsoft-specific. Any platform with the technical capability to remotely wipe, reconfigure, or exfiltrate data from enrolled devices should be treated as critical infrastructure requiring the highest tier of privileged access protection.

CSA Resource Alignment

The Stryker attack and the broader UEM threat landscape intersect with multiple CSA frameworks and publications. The AI Cloud Matrix (AICM), as a superset of the Cloud Controls Matrix (CCM), provides the relevant control families through which organizations should evaluate their UEM security posture. CCM control domain IAM (Identity and Access Management) maps directly to the recommendations above regarding phishing-resistant MFA, just-in-time privileged access, and administrative account separation. CCM control domain SEF (Security Incident Management, E-Discovery, and Cloud Forensics) governs the logging and alerting requirements for detecting bulk device actions and preserving audit evidence for post-incident analysis.

CSA's Zero Trust guidance is particularly applicable to UEM management plane protection. The Zero Trust principle of "never trust, always verify" is violated by any architecture in which a single valid credential provides uncontested access to mass device management capabilities. Continuous verification — including risk-based authentication, device posture evaluation, and session anomaly detection — applied consistently to UEM administrative access aligns with Zero Trust's core model of eliminating implicit trust zones from administrative infrastructure.

The MAESTRO framework for agentic AI threat modeling is relevant to an emerging dimension of this threat surface: AI-assisted or autonomous device management. As organizations adopt AI-driven IT operations tools that interface with UEM APIs to automate device remediation, patch deployment, and compliance enforcement, those AI agents will require UEM-scoped credentials. The MAESTRO framework's guidance on privilege minimization, human-in-the-loop controls for consequential actions, and audit trail requirements for agent-initiated changes should be applied to AI-driven UEM integrations before they are production-deployed. An AI orchestration agent with delegated Intune administrative permissions represents an additional credential surface that adversaries could target to obtain UEM administrative access.

CSA's prior guidance on mobile device management, documented in the 2012 Security Guidance for Critical Areas of Mobile Computing — foundational work that established the core risk categories for remote wipe capabilities and BYOD enrollment at a time when on-premises MDM was the dominant model — anticipated the risks now playing out in cloud-native UEM deployments. The Stryker attack validates those foundational concerns at enterprise scale and urgently extends them to the cloud-native context. CSA encourages organizations to revisit and update their BYOD program risk assessments in light of the demonstrated consequences of mass remote wipe affecting enrolled personal devices.

References

[1] KrebsOnSecurity, "Iran-Backed Hackers Claim Wiper Attack on Medtech Firm Stryker," March 2026. https://krebsonsecurity.com/2026/03/iran-backed-hackers-claim-wiper-attack-on-medtech-firm-stryker/

[2] Stryker Corporation, Investor and Media Statement on Cybersecurity Incident, March 2026. https://www.stryker.com

[3] SecurityWeek, "MedTech Giant Stryker Crippled by Iran-Linked Hacker Attack," March 2026. https://www.securityweek.com/medtech-giant-stryker-crippled-by-iran-linked-hacker-attack/

[4] TechCrunch, "US accuses Iran's government of operating hacktivist group that hacked Stryker," March 20, 2026. https://techcrunch.com/2026/03/20/u-s-accuses-irans-government-of-operating-hacktivist-group-that-hacked-stryker/

[5] BleepingComputer, "FBI seizes Handala data leak site after Stryker cyberattack," March 2026. https://www.bleepingcomputer.com/news/security/fbi-seizes-handala-data-leak-site-after-stryker-cyberattack/

[6] Cybersecurity Dive, "Stryker attack raises concerns about role of device management tool," March 2026. https://www.cybersecuritydive.com/news/stryker-attack-device-management-microsoft-iran/814816/

[7] The Register, "Lock down Microsoft Intune, feds warn after Stryker attack," March 19, 2026. https://www.theregister.com/2026/03/19/microsoft_intune_lockdown_stryker/

[8] BleepingComputer, "CISA warns businesses to secure Microsoft Intune systems after Stryker breach," March 2026. https://www.bleepingcomputer.com/news/security/cisa-warns-businesses-to-secure-microsoft-intune-systems-after-stryker-breach/

[9] TechCrunch, "Stryker says it's restoring systems after pro-Iran hackers wiped thousands of employee devices," March 17, 2026. https://techcrunch.com/2026/03/17/stryker-says-its-restoring-systems-after-pro-iran-hackers-wiped-thousands-of-employee-devices/

[10] Push Security, "Analyzing Handala TTP Evolution," March 2026. https://pushsecurity.com/blog/stryker-handala-report

[11] The Record, "FBI, CISA warn on Microsoft Intune risks after Iran-linked cyberattack on Stryker," March 2026. https://therecord.media/fbi-cisa-warn-of-microsoft-intune-risks-stryker

[12] Modern Healthcare, "Stryker cyberattack highlights hospital cybersecurity needs," March 2026. https://www.modernhealthcare.com/medical-devices/mh-stryker-cyberattack-hospital-cybersecurity-intuitive-surgical/

[13] Bloomberg, "Stryker Cyberattack Delays Surgeries for Some Patients," March 18, 2026. https://www.bloomberg.com/news/articles/2026-03-18/stryker-cyberattack-delays-surgeries-for-some-patients

[14] Security Affairs, "U.S. CISA adds Ivanti EPM, SolarWinds, and Omnissa Workspace ONE flaws to KEV," March 2026. https://securityaffairs.com/189172/security/u-s-cisa-adds-ivanti-epm-solarwinds-and-omnissa-workspace-one-flaws-to-its-known-exploited-vulnerabilities-catalog.html

[15] Qualys ThreatPROTECT, "CISA Warns of Ivanti EPM Authentication Bypass CVE-2026-1603," March 11, 2026. https://threatprotect.qualys.com/2026/03/11/cisa-warns-about-ivanti-epm-vulnerability-exploited-in-attacks-cve-2026-1603/

[16] Palo Alto Unit 42, "Suspected Nation-State Threat Actor Uses New Airstalk Malware," October 2025. https://unit42.paloaltonetworks.com/new-windows-based-malware-family-airstalk/

[17] CISA, "CISA Urges Endpoint Management System Hardening After Cyberattack Against US Organization," March 18, 2026. https://www.cisa.gov/news-events/alerts/2026/03/18/cisa-urges-endpoint-management-system-hardening-after-cyberattack-against-us-organization

[18] KrebsOnSecurity, "'Starkiller' Phishing Service Proxies Real Login Pages, MFA," February 2026. https://krebsonsecurity.com/2026/02/starkiller-phishing-service-proxies-real-login-pages-mfa/