THE STRYKER MDM ATTACK

How Q-InfoSecur & Q-SecurKey Would Have Prevented It

200K+	79	50 TB	$25M+
Devices Wiped Globally	Countries Affected	Data Exfiltrated	Estimated Recovery Cost

Threat Actor: Handala (Iran-linked hacktivist group) | March 2026

Transformativ IP

A proactive breakdown for CTO / CISO audiences | Source: Q-InfoSecur & Q-SecurKey for MDM Scenarios FAQ

WHAT HAPPENED

In March 2026, **Handala** — an Iran-linked hacktivist group — executed a devastating 'living-off-the-land' attack against Stryker Corporation. No ransomware. No custom malware. Just **Intune's own remote-wipe function, turned into a kill switch.**

1

Credential Compromise

Admin passwords + standard MFA bypassed via phishing / AiTM attack

2

Console Access

Attackers log into Microsoft Intune Admin Center with stolen credentials

3

Lateral Movement

50 TB of data quietly exfiltrated before triggering the wipe

4

Mass Wipe Command

Single admin account issues global factory-reset to 200,000+ devices

5

Global Disruption

79 countries offline. Manual workflows. Weeks of recovery.

Source: Q-InfoSecur & Q-SecurKey for MDM Scenarios FAQ — pp. 7, 11

5 CRITICAL SECURITY FAILURES THAT ENABLED THE ATTACK

01

[FAQ p.7]

No Phishing-Resistant MFA

Standard SMS/push MFA was in use for admin accounts — bypassed trivially via adversary-in-the-middle (AiTM) attacks. FIDO2 hardware tokens were not enforced.

02

[FAQ p.7, 13]

Single Admin Can Wipe Everything

No Multi-Admin Approval policy was active. A single compromised account had unchecked authority to issue a global factory-reset command to the entire 200,000-device fleet.

03

[FAQ p.8, 12]

No Identity Verification on Destructive Commands

Once logged in, the attacker's session was trusted unconditionally. No biometric step-up challenge was required before executing mass-destructive operations.

04

[FAQ p.7, 11]

BYOD Devices Co-Mingled in MDM Profile

Personal BYOD devices were enrolled under the same MDM profile as corporate hardware. Employees had personal phones, photos and data factory-reset with no warning.

05

[FAQ p.11, 28]

Zero Anomaly Detection on Wipe Commands

No alerting rule monitored for unusual volumes of wipe or factory-reset commands. The mass wipe executed completely before any detection or containment action.

THE SOLUTION: TRIPLE-LOCK ARCHITECTURE

Three independent layers — any one of which would have stopped the Stryker attack

LOCK 1

Q-SecurKey

Phishing-Resistant FIDO2 Hardware Token

Replaces passwords and push-based MFA with a physical hardware-bound passkey. An attacker with stolen credentials cannot log in without the physical device. Eliminates AiTM, MFA-fatigue, and credential-stuffing attacks.

STOPS: Credential-based admin access

LOCK 2

Q-InfoSecur

Live Biometric Identity Verification

Before any destructive command executes, a 3D liveness face scan confirms the authorised person is physically at the keyboard. Static photos and deep fake images are rejected. Session hijacking becomes impossible.

STOPS: Session hijacking & identity spoofing

LOCK 3

Multi-Admin Approval (MAA)

Governance Control via Intune + Transformativ IP

No single admin — regardless of privilege level — can authorise a mass-wipe command. A second independent administrator, authenticated via Q-SecurKey + Q-InfoSecur, must approve. Four-eyes principle enforced at the policy layer.

STOPS: Single-account global destruction

PROBLEM

Stolen Credentials Bypass Standard MFA

- Handala obtained Stryker admin passwords via phishing and/or a third-party IT provider compromise.
- Standard MFA (SMS codes, Authenticator push) was bypassed using Adversary-in-the-Middle (AiTM) techniques — a trivially available attack method.
- Once past MFA, the attacker had unrestricted access to the Intune Admin Center — the most powerful button in the entire infrastructure.
- There was no further identity check between login and executing the global wipe command.

FAQ Reference: pp. 7, 13, 15, 16

SOLUTION

Q-SecurKey: The Physical Trust Anchor

FIDO2 Hardware-Bound Authentication

Q-SecurKey uses cryptographic challenge-response that is physically bound to the hardware token. A remote attacker with a stolen password cannot log in without the physical device.

Immune to AiTM & MFA Fatigue

FIDO2 origin-binding makes man-in-the-middle interception mathematically impossible. Push notification spam has zero effect — the key must be physically touched.

Conditional Access Enforcement

A CA policy set to 'Require Phishing-Resistant MFA' blocks all login attempts using SMS, voice, or push — even if the password is correct. Only Q-SecurKey is accepted.

PROBLEM

One Account, One Click: 200,000 Devices Gone

- No Multi-Admin Approval policy was configured in Intune. Any single administrator with sufficient role privileges could issue a mass-wipe command with no second check.
- The architecture treated the 'wipe all devices' function identically to routine management tasks — no elevation, no justification required.
- This created a single point of catastrophic failure: compromise one account = destroy the entire global fleet.
- Recovery required manual re-enrolment of 200,000+ devices across 79 countries — weeks of lost productivity.

FAQ Reference: pp. 13, 15, 17

SOLUTION

Multi-Admin Approval + Q-InfoSecur Step-Up

1. Admin initiates wipe command in Intune
2. MAA policy intercepts — command placed in Pending queue
3. Second authorised admin receives alert
4. Approver must authenticate with Q-SecurKey (FIDO2)
5. Q-InfoSecur biometric face scan confirms live identity
6. Only then is the Approve button unlocked

PROBLEM

Session Hijacking: The Attacker is Already Inside

- Once authenticated, admin browser sessions are persistent. A compromised session token gives an attacker ongoing access even without the original password.
- Session hijacking means an attacker can act entirely within a valid, trusted identity context — the system has no way to distinguish the real admin from the attacker.
- No secondary identity verification was required before the wipe command was executed. The session was assumed to be legitimate throughout.

FAQ Reference: pp. 8, 12, 17, 18

SOLUTION

Q-InfoSecur: The Human Firewall

When an admin attempts a destructive command, Q-InfoSecur triggers a biometric 'Step-Up' challenge:

- QR code appears on the admin's desktop screen
- Admin scans with their registered corporate mobile device
- Q-InfoSecur performs a 3D liveness check (face scan)
- Biometric match confirmed — session is unlocked for that action only

A static photo, deepfake, or hijacked session cannot pass the 3D liveness check.

PROBLEMS 4 & 5: BYOD BLAST RADIUS + ZERO DETECTION

BYOD Devices: Unacceptable Blast Radius

THE PROBLEM: Personal devices enrolled in Intune MDM had the same wipe-scope as corporate hardware. Employees lost personal photos, messages and data with zero warning.

THE FIX — Mobile App Management (MAM):

- MAM manages corporate data within specific apps (Outlook, Teams) — not the entire device.
- If triggered, an attacker can only perform a Selective Wipe: removes corporate app data only. Personal photos, messages, and contacts are untouched.
- App Protection Policies require Q-InfoSecur biometric authentication to re-open managed apps after a wipe event.

[FAQ pp. 7, 13]

Zero Detection: The Attack Ran Unopposed

THE PROBLEM: No Sentinel rule monitored for anomalous wipe command volumes. The attack completed entirely before any alert fired or any containment action was taken.

THE FIX — Sentinel KQL + Azure Automation:

- KQL analytics rule monitors Intune logs for >5 wipe commands from one admin in 10 minutes — exact Stryker pattern.
- Alert fires automatically. Azure Logic App/Runbook revokes all active admin refresh tokens within 60 seconds.
- Attacker is ejected. Q-SecurKey + Q-InfoSecur re-authentication is required to regain access — which the attacker cannot pass.

[FAQ pp. 11, 28, 29]

PROBLEM → SOLUTION: THE COMPLETE MAPPING

Stryker Failure	Root Cause	Technology Fix	How It Prevents Recurrence	FAQ
Admin credentials stolen & MFA bypassed	Standard Push / SMS MFA	**Q-SecurKey (FIDO2)**	Physical hardware token required. No token = no login, even with correct password.	*p.7,13,16*
Single account triggers global wipe	No Multi-Admin Approval policy	**Intune MAA + Q-SecurKey**	Four-eyes principle: 2nd admin must authenticate via FIDO2 to approve any mass-wipe command.	*p.13,15*
Session hijacking — attacker acts as real admin	No step-up identity verification	**Q-InfoSecur Biometrics**	Live 3D face scan required before destructive command. Session tokens alone are insufficient.	*p.8,12,17*
Personal BYOD devices wiped alongside corporate	Full MDM applied to personal devices	**MAM + App Protection Policies**	Selective wipe removes only corporate app data. Personal content is never in scope.	*p.7,13*
Attack completed before any alert fired	No anomaly detection on wipe volume	**Sentinel KQL + Azure Runbook**	Automated session revocation within 60 seconds of anomalous wipe spike detection.	*p.28,29*

HOW THE TRIPLE-LOCK STOPS THE ATTACK IN REAL TIME

The attack flow that succeeded at Stryker — and exactly where each layer stops it

Attacker obtains stolen admin password	✗ **Attack proceeds in Stryker environment**
Attacker attempts Intune Admin login	✓ **Q-SecurKey BLOCKS** FIDO2 token required — attacker has no physical key
Admin initiates mass wipe (>10 devices)	✓ **Intune MAA INTERCEPTS** Command placed in Pending queue — second admin approval required
Approver receives Q-InfoSecur challenge	✓ **Q-InfoSecur VERIFIES** 3D liveness face scan confirms physical identity of approver
Sentinel detects wipe volume spike	✓ **SENTINEL AUTO-REVOKES** All admin sessions revoked within 60 seconds

FINANCIAL IMPACT & ROI: THE BUSINESS CASE

$25M+
Stryker-Scale Breach Recovery Cost

$35K
Total Pilot Implementation Cost

<14 mo
Payback Period on Investment

43%
Risk of Policy Denial Without FIDO2 MFA

Cyber Insurance Premium Savings

Scenario	Risk Classification	Financial Outcome
Current Posture (Push MFA)	Moderate Risk	Full Premium / Risk of Denial
After Q-SecurKey + Q-InfoSecur	Best-in-Class	15–50% Premium Reduction
Annual Premium (Mid-Large Ent.)	$100,000+	$30,000–$50,000 annual savings
Deductible Reduction	Average 25–35%	Fewer claims = lower deductibles

Breach Avoidance Value

Direct Recovery & Hardware	$5M–$10M
IT Labour & Re-enrolment	$3M–$8M
Legal & Forensic Costs	$2M–$5M
Productivity Loss (Global)	$2M–$5M
TOTAL AVOIDED COST	**$10M–$25M**

FAQ Reference: pp. 30, 36, 37

FROM VULNERABLE TO STRYKER-PROOF: 4-WEEK ROADMAP

Week 1

Identity Enrolment

- Distribute Q-SecurKey tokens to all IT admins
- Enrol all admin accounts in Q-InfoSecur biometric app
- Register backup keys for every admin (2 per person)
- Verify FIDO2 compatibility across all browsers used

Week 2

Infrastructure Setup

- Configure Entra ID External Auth Methods for Q-InfoSecur
- Enable Intune Multi-Admin Approval (MAA) access policy
- Register Q-InfoSecur as External Authentication Method
- Configure Conditional Access (Report-Only mode first)

Week 3

Policy Simulation

- Run live-fire Q-InfoSecur step-up tests (non-production)
- Simulate mass-wipe attempt — verify MAA intercepts
- Test Sentinel KQL alert on wipe volume spike
- Identify and remediate any legacy app FIDO2 blockers

Week 4

Full Enforcement

- Switch all CA policies from Report-Only to Enforce
- Deactivate SMS/push MFA for all privileged accounts
- Activate Azure Automation runbook for auto-revocation
- Stryker-proof posture achieved ✓

FAQ Reference: pp. 32–34 | PoC Success Checklist: p.33

THE VERDICT

The Stryker attack was **100% preventable.**

Every failure vector is a solved problem in the Q-InfoSecur / Q-SecurKey / Transformativ IP architecture.

5 IMMEDIATE ACTIONS FOR YOUR TEAM

1. Run PowerShell audit — identify every admin lacking phishing-resistant FIDO2 MFA [FAQ p.16]
2. Enable Intune Multi-Admin Approval (MAA) for Device Actions — zero cost, immediate [FAQ p.13]
3. Deploy Sentinel KQL mass-wipe detection rule + Azure auto-revocation runbook [FAQ p.28]
4. Issue TRD & RFQ to procurement for Q-SecurKey + Q-InfoSecur pilot enrolment [FAQ p.32, 49]
5. Present insurance ROI to CFO — 43% policy-denial risk, 30–50% premium savings [FAQ p.36]

Source: Q-InfoSecur & Q-SecurKey for MDM Scenarios (Stryker) — 156-page FAQ, March 2026 | Transformativ IP Security Briefing