Prepared for: Chief Technology Officer (CTO) / Chief Information Security Officer (CISO)
Source: Our 176-page FAQ for Preventing MDM Stryker Scenarios using Q-InfoSecur™ & Q-SecurKey™

Purpose of This Document

This Executive Summary summarizes the key findings from our 156-page internal FAQ document, **"Q-InfoSecur™ & Q-SecurKey™ for MDM Scenarios (Stryker)"** into actionable intelligence for senior technology and security leadership. Each finding is cross-referenced to the relevant FAQ page so that any section can be located quickly for deeper review.

It answers the three strategic questions directly material to an organisation's risk posture:

1. **What happened at Stryker Corporation, and why did it succeed?**
2. **Would Q-InfoSecur™ & Q-SecurKey™ have prevented it - and how specifically?**
3. **What is the implementation roadmap, and what is the financial return?**

Table of Contents

1. The Stryker Incident — What Happened and Why It Matters

1.1 Attack Summary

In March 2026, the pro-Iranian hacktivist group Handala carried out a catastrophic "living-off-the-land" cyberattack against Stryker Corporation, a Fortune 500 global medical-device manufacturer. The attackers did not use ransomware or custom malware. Instead, they compromised high-privilege administrative credentials for Microsoft Intune — Stryker's cloud-based Mobile Device Management (MDM) platform — and used Intune's own built-in remote-wipe feature to factory reset more than 200,000 managed devices simultaneously across 79 countries. [FAQ p.7]

Before triggering the wipe, the attackers exfiltrated approximately 50 terabytes of data, including sensitive corporate and operational information and potentially patient-linked information. The attack forced the organisation to revert to manual workflows across multiple international locations and necessitated the emergency removal of Intune management profiles from every enrolled device. [FAQ p.11]

Attack Dimension	Detail
Threat Actor	Handala (Iran-linked hacktivist group)
Attack Vector	Compromised Microsoft Intune admin credentials
Technique	"Living off the land" — weaponisation of legitimate MDM wipe function
Scale	200,000+ devices across 79 countries wiped in a single event
Data Exfiltrated	Approximately 50 TB before wipe execution
Estimated Impact	$10M–$25M in recovery, labour, forensics, and business interruption
Root Cause	No phishing-resistant MFA; no multi-admin approval; no anomaly detection on bulk wipe commands

1.2 Was This a Microsoft Intune Failure?

The FAQ document is unambiguous on this point: the attack was not the result of a vulnerability or gap in Microsoft Intune itself. Security analysts confirmed that Intune functioned exactly as designed. The root cause was a failure to properly secure the MDM administrative layer — treating it as a standard business application rather than a Tier-0 critical asset. [FAQ p.7]

Specifically, the following configuration failures created the conditions for the attack:

- Phishing-resistant MFA (FIDO2) was not enforced on administrator accounts, allowing credential bypass.
- No Multi-Admin Approval (MAA) policy was active, permitting a single compromised account to issue a global wipe command.

- BYOD devices enrolled under corporate MDM profiles were co-mingled with personally owned data, expanding the blast radius to personal devices.
- No anomaly-detection or automated alert was configured to flag an unusual volume of wipe commands, allowing the attack to proceed undetected until completion.

CRITICAL TAKEAWAY — FAQ p.7 & p.11

Every single failure vector in the Stryker incident is a solved problem in the Q-InfoSecur™ / Q-SecurKey™ / Transformativ IP architecture. This is not a capability gap - it is a deployment gap.

2. Technology Overview - Q-InfoSecur™, Q-SecurKey™ & Transformativ IP

2.1 What Each Component Does

The FAQ describes a three-layer "Triple-Lock" architecture built around three distinct but complementary technologies. Each layer directly addresses one of the failure modes observed in the Stryker attack. [FAQ p.8]

Layer & Technology	Function & Stryker Relevance
Q-InfoSecur™ (Biometric Identity Verification)	Provides live, 3D biometric face-scan verification (liveness check) as a "step-up" challenge before destructive commands are authorised. Prevents session hijacking: even if an attacker holds a valid session token, they cannot pass a live biometric scan. [FAQ p.8, 12, 17]
Q-SecurKey™ / HYPR (Phishing-Resistant FIDO2 Hardware Token)	Replaces shared secrets (passwords, SMS codes, push notifications) with a physical hardware-bound FIDO2 passkey. Eliminates credential theft: an attacker with a stolen password cannot log in without the physical device. [FAQ p.8, 13, 15, 16]
Transformativ IP (Architectural & Integration Strategy)	Provides the overarching secure-by-design framework: configuring Microsoft Intune MAA, Conditional Access policies, Post-Quantum Cryptography (PQC) integration, and Sentinel automation. Ensures the components work as a cohesive Zero Trust architecture rather than isolated tools. [FAQ p.9, 10, 13]

2.2 The Triple-Lock Principle

When all three technologies are active, they create a sequential authentication chain that an attacker must defeat at three independent levels simultaneously. In the Stryker scenario, defeating any one layer would have stopped the attack entirely: [FAQ p.15]

1. **Lock 1 — Proof of Possession:** Q-SecurKey™ (FIDO2). The physical hardware token must be present. A remote attacker with stolen credentials cannot pass this challenge.
2. **Lock 2 — Proof of Identity:** Q-InfoSecur™ Biometrics. A live face scan confirms the person at the keyboard is the enrolled authorised administrator. Static photos and deepfake

images are rejected by the liveness check.

3. **Lock 3 — Governance Control:** Intune Multi-Admin Approval (MAA). No single administrator account, regardless of privilege level, can authorise a mass-wipe command without independent authorisation from a second verified administrator.

> **DIRECT PREVENTION — FAQ p.12 & p.13**
>
> "The specific combination of Q-InfoSecur™ and Q-SecurKey™ targets the exact blind spot identified in this breach." Had this architecture been active at Stryker, the attackers would have been stopped at the hardware layer (no Q-SecurKey™) before ever reaching the console.

3. Specific Architectural Changes That Would Have Prevented the Attack

3.1 Multi-Admin Approval (MAA) for Device Actions

The MAA policy enforces a "four-eyes" principle at the Intune level. Under this configuration, any device wipe or factory reset command targeting more than 10 devices is automatically intercepted and placed in a Pending queue. A second independent administrator — authenticated via Q-SecurKey™ — must approve the request before it executes. The approver must also pass a Q-InfoSecur™ biometric step-up challenge before the Approve button becomes active. Configuration path in Intune: Tenant Administration → Multi-Admin Approval → Access Policies → Create → Device Actions profile type. [FAQ p.13]

3.2 Conditional Access Policy: Phishing-Resistant MFA Enforcement

A Conditional Access policy targeting all Intune Administrator and Global Administrator accounts is configured to require phishing-resistant MFA. This configuration explicitly blocks SMS codes, voice calls, and standard Authenticator push notifications for these roles. Only a Q-SecurKey™ (FIDO2 token) or Windows Hello for Business biometric is accepted. This single policy change eliminates the MFA-fatigue and adversary-in-the-middle (AiTM) attacks used by Handala-affiliated groups. [FAQ p.13]

3.3 Mobile Application Management (MAM) Over Full MDM for BYOD

By shifting BYOD devices from full MDM enrolment to Mobile Application Management (MAM) with App Protection Policies, the blast radius of any future administrative compromise is radically reduced. Under MAM, an attacker who gains access to the Intune console can only trigger a selective wipe that removes corporate data from within managed applications — it cannot factory-reset the user's personal device or delete personal data. This directly addresses the BYOD impact that amplified the Stryker incident. [FAQ p.13]

3.4 Automated Threat Response via Microsoft Sentinel

The FAQ documents a complete Sentinel analytics rule (KQL query) that monitors Intune audit logs for spikes in wipe or factory-reset commands. If a single administrator account triggers more than five wipe commands within a 10-minute window — the exact pattern of the Stryker attack — Sentinel fires an alert and automatically invokes an Azure Automation Runbook that

revokes all active refresh tokens and session cookies for that administrator's account within 60 seconds. The attacker is ejected from the console before the attack can reach critical mass. [FAQ p.28]

4. Implementation Roadmap - From Vulnerable to Stryker-Proof in 4 Weeks

The FAQ documents a structured four-week Proof of Concept (PoC) timeline that transitions an organisation from its current state — where standard push-based MFA is the primary admin control — to full enforcement of the Triple-Lock architecture. [FAQ p.33]

Week	Focus Area	Key Activity	Outcome
1	**Identity Enrolment**	Distribute Q-SecurKey™s to all IT admins; enrol admins in Q-InfoSecur™ biometric app via enterprise portal.	All privileged accounts have hardware token + biometric profile registered.
2	**Infrastructure Setup**	Configure Entra ID External Auth Methods (EAM) for Q-InfoSecur™; enable Intune Multi-Admin Approval (MAA) access policy.	Step-up challenge active in non-production environment.
3	**Policy Simulation**	Deploy Conditional Access in Report-Only mode; run live-fire tests of Q-InfoSecur™ step-up challenge on test tenant.	All policy gaps identified and remediated before enforcement.
4	**Full Enforcement**	Switch all CA policies to Enforce; deactivate legacy MFA (SMS/Push) for privileged accounts; activate Sentinel automation.	Organization is Stryker- proof. Zero single-point-of-failure for destructive commands.

4.1 Key Technical Milestones Proof of Concept (PoC) Success Checklist

The FAQ defines explicit pass/fail criteria for the PoC. The following are the highest-priority validation tests that confirm the architecture is functioning as designed: [FAQ p.33]

1. An admin attempts to log in with a known stolen password → Q-SecurKey™ FIDO2 requirement blocks access. No entry.
2. A simulated attacker triggers a "MFA fatigue" push-notification flood → Q-SecurKey™ FIDO2 protocol is immune; the attack has zero effect.
3. An admin initiates a device wipe for more than 10 devices → Intune MAA intercepts and places the command in the Pending queue; no wipe executes.
4. An approver attempts to use a static photograph for the Q-InfoSecur™ face scan → Liveness check detects a non-living face and blocks authorisation.
5. A scripted attack triggers 15 wipes in 60 seconds → Sentinel analytics rule fires; Azure Runbook revokes all admin sessions within 60 seconds.

5. Financial Case — Return on Investment and Insurance Implications

5.1 Cost of Inaction

The Stryker incident, involving more than 200,000 devices across 79 countries, is estimated to have incurred direct and indirect costs of $10M to $25M, encompassing hardware replacement, IT labour, forensic investigation, legal fees, and multi-week global productivity loss. This represents a single-event, "black swan" financial risk that exists in any organisation with a centralised MDM environment and inadequately secured administrative credentials. [FAQ p.30]

5.2 Cost of Implementation

The FAQ documents a detailed Financial Payback Analysis for a 100-administrator pilot. The total one-time capital expenditure is approximately $35,000, covering hardware tokens, professional services for Transformativ IP architectural setup, and internal integration labour. [FAQ p.37]

100-Administrator Pilot Costs

Q-SecurKey™	Estimate
Q-SecurKey™ FIDO2 Tokens (x100)	~$5,000
Backup Q-SecurKey™s (x100)	~$5,000
Transformativ IP Strategy & Setup (Prof. Services)	~$15,000
Integration & Internal Testing Labour	~$10,000
Total Cost for One-Time Implementation (CapEx)	**~$35,000**

Q-InfoSecur™	Estimate
Q-InfoSecur™ FIDO2 Tokens 100 users (x $110)	~$11,000
Q-InfoSecur™ FIDO2 Tokens Backup 100 users (x $110)	~$11,000
Q-InfoSecur™ Server	~$10,000
Transformativ IP Strategy & Setup (Prof. Services)	~$15,000
Integration & Internal Testing Labour	~$10,000
Total Cost for One-Time Implementation (CapEx)	**~$67,000**

5.3 Annual Insurance Savings

The FAQ cites 2026 cyber insurance underwriting trends directly. Organisations lacking phishing-resistant MFA controls face a 43% risk of policy denial or significantly reduced coverage limits. Implementing Q-SecurKey™ (FIDO2) and Q-InfoSecur™ (biometrics) qualifies as a "best-in-class" identity posture under current underwriter benchmarks and can unlock premium reductions of 15% to 50%. [FAQ p.36]

- For a mid-to-large enterprise paying an annual cyber insurance premium of $100,000 or more, a 30% to 50% reduction results in $30,000 to $50,000 in annual premium savings. The return on investment for implementing this measure is therefore under 14 months, not including the potential breach-avoidance benefits. [FAQ p.37]

Financial Metric	Value
Total Implementation Cost (CapEx)	~$35,000
Annual Premium Savings (30–50% reduction)	$30,000–$50,000 per year
Payback Period	0.7–1.1 years
Breach Avoidance Value (single Stryker-scale event)	$10M–$25M
Risk of Policy Denial (without FIDO2 MFA)	43% (per 2026 underwriter data)
Insurance Deductible Reduction (FIDO2 + Biometrics)	25–35% average reduction
Premium Discount Range (Best-in-Class Posture)	15–50%

INSURANCE UNDERWRITER POSITION — FAQ p.36

Cyber insurers now classify Standard Push MFA (mobile apps) as "Moderate Risk" and FIDO2/Biometric as "Best-in-Class." This classification directly determines both premium pricing and the availability of high-limit coverage. Insurers have denied claims of up to $18M where phishing-resistant MFA was absent from privileged environments.

6. Regulatory Compliance & Standards Alignment

The architecture described in the FAQ satisfies the most demanding tier of current federal and international cybersecurity standards. This is significant because insurance underwriters, regulators, and litigants in post-breach proceedings increasingly use these standards as the benchmark for "reasonable" security practice. [FAQ p.37]

Standard / Framework	How Q-InfoSecur™ + Q-SecurKey™ Architecture Satisfies It
NIST SP 800-63B — AAL3 (Authenticator Assurance Level 3)	The Triple-Lock architecture (Q-SecurKey™ FIDO2 + Q-InfoSecur™ Biometric) meets AAL3 — the highest level of identity assurance, requiring hardware-bound multi-factor authentication with phishing resistance and biometric verification. [FAQ p.30, 37]
NIST SP 800-207 Zero Trust Architecture	Conditional Access policies, MAA governance, and continuous session re-validation implement the core Zero Trust principle: "never trust, always

	verify," applied specifically to the highest-risk MDM administrative layer. [FAQ p.37]
FDA "Secure by Design" (2023 Medical Device Guidance)	Q-SecurKey™ and Q-InfoSecur™ support Post-Quantum Cryptography (PQC) key management via NIST FIPS 203–205 algorithms, satisfying FDA requirements for long-lived connected medical devices against "harvest now, decrypt later" quantum threats. [FAQ p.9, 10]
Cyber Insurance Underwriting (2026 Benchmarks)	FIDO2 + Biometric posture qualifies as "Best-in-Class" under 2026 underwriter criteria, directly unlocking premium discounts and avoiding the 43% policy-denial risk associated with legacy MFA. [FAQ p.36]

7. Post-Quantum Cryptography — The Forward-Looking Layer

Beyond the immediate Stryker-prevention use case, the FAQ provides significant technical detail on the Post-Quantum Cryptography (PQC) capabilities of the Transformativ IP stack. For medical device manufacturers and healthcare-adjacent enterprises, this has direct regulatory relevance. [FAQ p.9]

The "harvest now, decrypt later" attack vector is an active threat: sophisticated state-sponsored actors (including Handala-affiliated groups) are known to exfiltrate encrypted data today, in anticipation of decrypting it with quantum computers within the next decade. For data that must remain confidential for 10 to 30 years — including patient records, clinical trial data, and proprietary device firmware — this represents a compounding risk that standard AES-256 encryption alone cannot address. [FAQ p.9]

Transformativ IP's PQC+ implementation approach, as documented in FAQs, involves:

- Replacing legacy RSA/ECC algorithms with NIST-standardised PQC algorithms (FIPS 203 ML-KEM, FIPS 204 ML-DSA, FIPS 205 SLH-DSA).
- Integrating Q-SecurKey™'s Hardware Security Module (HSM) capability as the hardware root of trust for PQC key generation and storage.
- Implementing crypto-agile architecture that allows algorithm "hot-swapping" as PQC standards evolve, eliminating future hardware redesign costs.
- Satisfying FDA 2023 premarket guidance requirements for Cryptographic Bills of Materials (CBOMs) in connected medical device submissions.

8. Deployment Risk Management

The FAQ documents a Project Risk Registry that identifies and mitigates the primary operational risks associated with deploying the Q-InfoSecur™/Q-SecurKey™ architecture in a live enterprise environment. The following risks are rated highest probability and are therefore the most relevant for executive decision-making: [FAQ p.39]

Risk	Probability	Impact	Mitigation (per FAQ)

Admin Resistance / Friction (Triple-Lock seen as workflow burden)	High	Medium	Apply Q-InfoSecur™ biometric step-up only to destructive commands (wipes/deletions), not routine logins. Frame as career protection, not surveillance. [FAQ p.39, 40]
Legacy App Incompatibility (CLI scripts, older tools lack FIDO2 support)	High	Medium	Scope Q-SecurKey™ requirement specifically to Azure/Intune portals initially. Use Managed Identities and Conditional Access Workload Identities for automated scripts. [FAQ p.39]
Biometric False Rejects (Low light, glasses, environmental factors)	Medium	Low	Establish a Break-Glass video-verification protocol and Temporary Access Pass (TAP) process. Average false rejection rate seen in deployment: <1%. [FAQ p.39, 42]
Hardware Supply Chain Delays (FIDO2 token procurement lead times)	Medium	Medium	Ensure Transformativ IP strategy includes at least two FIDO2-certified hardware vendors (e.g., HYPR and YubiKey) as contingency alternatives. [FAQ p.39]

8.1 Break-Glass Procedure

The FAQ documents a formal Break-Glass procedure for scenarios where an administrator loses their Q-SecurKey™ during a live incident. The procedure uses a Q-InfoSecur™ biometric verification conducted over a recorded video call with the SOC, followed by issuance of a one-hour, single-use Microsoft Entra Temporary Access Pass (TAP) delivered via an encrypted out-of-band channel. The TAP automatically expires and the break-glass exclusion group membership is automatically revoked via Privileged Identity Management (PIM), re-enforcing Q-SecurKey™ requirements within two hours. [FAQ p.42]

9. Executive FAQ Navigator — Key Sections by Role

The following table maps the most strategically significant sections of our 176-page FAQ document which is organized into 13 sections for ease of reading. Use this as a rapid-access FAQ guide to the underlying technology.

FAQ Page	Topic	Relevant To	Why It Matters
p.5	**MDM Market Share & Vendor Landscape**	CTO, CIO	Confirms Microsoft Intune's dominance (20–25% market share); frames the scope of the risk class.
p.7	**Root Cause: Stryker / Intune Misconfiguration**	CISO, Legal	Definitively establishes the attack was a configuration failure, not a product vulnerability — relevant to liability analysis.

p.8	**Q-InfoSecur™ & Q-SecurKey™ Prevention Case**	CISO, Board	Direct answer: yes, these technologies address the exact vulnerabilities exploited.
p.9–10	**PQC & FDA Secure-by-Design Implementation**	CTO, &D, Regulatory	Step-by-step PQC activation for medical device firmware and data protection.
p.13	**Intune Architecture: MAA, CA & MAM Changes**	CTO, CISO, IT Lead	The specific Intune configuration changes required — the technical blueprint for prevention.
p.15	**Multi-Admin Approval Configuration Guide**	IT Lead, SOC	Step-by-step MAA configuration walkthrough.
p.16	**PowerShell: Audit Vulnerable Admin Accounts**	IT Lead, SOC	Immediate actionable script to identify all Global Admins currently lacking phishing-resistant MFA.
p.17	**Biometric Step-Up Automation: Q-InfoSecur™ Workflow**	Security Architect	Technical workflow for integrating Q-InfoSecur™ as an Entra ID External Authentication Method.
p.28	**KQL: Sentinel Mass-Wipe Detection Rule**	SOC, SIEM Team	Production-ready KQL query — deploy immediately to gain detection capability for Stryker-pattern attacks.
p.30	**Board-Level Risk Mitigation Summary**	CISO, Board, CFO	One-page executive table mapping each Stryker threat vector to its specific countermeasure and business impact.
p.32	**Technical Requirements Document (TRD)**	CISO, Procurement	Ready-to-use TRD for the Q-InfoSecur™ / Q-SecurKey™ pilot — submit to procurement directly.
p.33	**4-Week PoC Timeline & Checklist**	CTO, Project Lead	Structured implementation plan with explicit pass/fail success criteria.
p.36	**C-Suite ROI Communication: Insurance Savings**	CFO, CISO	The 43% policy-denial risk and premium-reduction data — the financial justification for the investment.
p.37	**Project Executive Charter & Financial Payback**	CFO, CISO, Sponsor	$35K investment vs. $30K–$50K annual savings; payback period <14 months. Includes NIST AAL3 compliance framing.
p.39	**Project Risk Registry**	CTO, Project Lead	Deployment risks with mitigation strategies — required reading before procurement approval.

p.42	**Break-Glass Emergency Procedure**	CISO, SOC, IT Lead	Critical operational procedure: what to do when an admin loses their Q-SecurKey™ during a live incident.
p.46	**Vendor Evaluation Matrix (vs. YubiKey / Duo)**	CFO, Procurement	Objective TCO comparison: Q-InfoSecur™/Q-SecurKey™ vs. YubiKey +Duo. Risk mitigation score: 95% vs. 40%.
p.47–49	**SOW and RFQ Templates**	Procurement, Legal	Ready-to-use Statement of Work and Request for Quote templates for vendor engagement.
p.59–67	**KQL Threat Hunting & Sentinel Workbooks**	SOC, Threat Intel	Advanced detection: biometric log correlation, unverified admin heat maps, automated alert thresholds.
p.164	**BEC / Deepfake Invoice Fraud Prevention**	CFO, Finance	Q-InfoSecur™ application to Business Email Compromise — out-of-band vendor payment verification workflow.
p.166–172	**Vendor Authentication Portal & Supply Chain Security**	Procurement, CISO	Extending biometric verification to all new vendors before system enrolment — supply chain hardening.

10. Recommended Immediate Actions

Based on the evidence in the FAQ document and the Stryker incident analysis, the following actions are recommended in order of priority. Each is executable within the existing Microsoft 365 / Azure environment without new infrastructure procurement for the first three items:

Priority & Action	Owner / Timeframe
1. Run the PowerShell Admin Audit Script [FAQ p.16] Identify every Global Administrator and Intune Administrator account that currently lacks phishing-resistant FIDO2 MFA. This is a zero-cost, immediate action that quantifies the current exposure.	IT Security Lead Immediate (Day 1)
2. Enable Intune Multi-Admin Approval (MAA) [FAQ p.13] Activate the MAA policy for Device Actions in the Intune Admin Center. No additional software or procurement is required — this is a native Microsoft feature that is off by default. Activation alone removes the single-point-of-failure for mass wipes.	IT Lead / Intune Admin 1–3 Business Days

3. Deploy Sentinel KQL Mass-Wipe Detection Rule [FAQ p.28] Deploy the Sentinel analytics rule to detect anomalous wipe-command spikes. Pair with an Azure Logic App or Automation Runbook to auto-revoke admin sessions. Provides detection capability while hardware procurement proceeds.	SOC / Sentinel Team 3–5 Business Days
4. Procure Q-SecurKey™ Tokens & Initiate Q-InfoSecur™ Enterprise Enrolment [FAQ p.32–33] Issue the Technical Requirements Document (TRD) [FAQ p.32] to procurement and submit the RFQ [FAQ p.49] to vendors. Begin Phase 1 pilot enrolment with the IT Security core team.	Procurement + CISO Week 1–2
5. Present Financial Case to CFO [FAQ p.36–37] Share the insurance-premium reduction analysis and the $35K vs. $10M+ breach-avoidance ROI with Finance. Initiate conversation with cyber insurance broker regarding underwriting credit for FIDO2/biometric implementation.	CISO + CFO Week 1–2

Summary

The Stryker/Handala cyberattack of March 2026 is the defining reference case for the class of threat now facing every enterprise operating a centralised Mobile Device Management platform. It demonstrated, at scale, that a single compromised administrator account with standard MFA is sufficient to destroy an entire global device fleet in a matter of minutes. [FAQ p.7]

Our 176-page FAQ document reviewed here is a technically rigorous, deployment-ready guide that answers every material question a CTO or CISO must ask before embarking on hard core due diligence or authorising such a security upgrade necessitating an architectural change. The answer to the central question — "Would Q-InfoSecur™ and Q-SecurKey™ have prevented the Stryker attack?" — is documented directly and without equivocation: yes, at multiple independent layers, any one of which would have been sufficient to stop the attack. [FAQ p.8]

At a total pilot cost of approximately $35,000, a projected insurance premium reduction of $30,000 to $50,000 annually, and a payback period of less than 14 months, the financial case is unambiguous. The operational risk of inaction — a Stryker-scale event costing $10M to $25M — is not a theoretical concern. It is a documented, repeatable attack class that is actively being deployed by nation-state-affiliated threat actors against enterprise MDM environments today. [FAQ p.30]

Our architecture is the immediate remediation for an active, documented, and financially quantifiable potentially devastating security vulnerability present in your environment today.

Additional Educational Resources available at: insert link here

- Videos
- Slide decks (some narrated)
- Tech Audios
- White papers
- FAQs