# The Stryker Cyberattack: Lessons for Healthcare Security

*A Multi-Domain Failure—and How a Defense-in-Depth Approach*
*Including the Onclave TrustedPlatform® Could Have Changed the Outcome*
March 15, 2026

## What Happened

On March 11, 2026, Stryker Corporation, a Fortune 500 medical technology company with $25 billion in annual revenue, approximately 56,000 employees, and products reaching over 150 million patients annually, was struck by one of the most destructive cyberattacks in healthcare industry history. The Iran-linked hacktivist group Handala claimed responsibility, framing the attack as geopolitical retaliation tied to the ongoing U.S.-Israel-Iran conflict.

The attack was not ransomware. It was a coordinated **wiper operation** designed to permanently destroy data and cripple operations. Attackers compromised privileged administrative accounts within Stryker's Microsoft cloud environment, specifically Entra ID and the Microsoft Intune mobile device management (MDM) admin console and weaponized Stryker's own endpoint management infrastructure to issue mass remote wipe commands across its entire global device fleet. More than 200,000 devices, servers, and systems were wiped across 79 countries. Employees arrived to find laptops and phones disabled, login pages defaced with the Handala logo, and corporate systems completely inaccessible. Stryker's manufacturing, logistics, and communications infrastructure ground to a halt. The company instructed all employees to disconnect from networks and avoid powering on company-issued devices.

Handala claims to have exfiltrated approximately 50 terabytes of data prior to executing the wipe, potentially including device blueprints, manufacturing data, intellectual property, and partner or patient information. In a regulatory filing, Stryker stated that the breach will continue to disrupt operations and that a timeline for full restoration is not yet known. Shares dropped 4% immediately following the disclosure, and CISA has launched a formal investigation.

## Why This Matters Beyond Stryker

Stryker is not merely an enterprise IT operation. It is a critical node in the global healthcare supply chain. The company manufactures surgical instruments, orthopedic implants, hospital beds, and robotic surgery systems, including the Mako Robotic-Arm Assisted Surgery platform, that hospitals worldwide depend on for patient care. When Stryker's manufacturing and distribution hubs went dark, the ripple effects were immediate: surgical equipment shortages, delayed orthopedic and trauma procedures, and disrupted logistics across hospital networks that rely on just-in-time delivery of life-critical devices.

This attack underscores a structural vulnerability that the healthcare sector has failed to address. Over 80% of stolen health records are taken through third-party vendors, not hospital systems directly. The Stryker breach, like the Change Healthcare attack before it, demonstrates that a single vendor compromise can cascade across the entire healthcare ecosystem, disrupting patient care, halting revenue, exposing leadership to regulatory scrutiny, and threatening patient safety at scale.

## Anatomy of the Failure: What Went Wrong

The Stryker attack was not a single-vector exploit. It was a multi-phase operation that exploited failures across multiple security domains, from cloud identity governance to network architecture to compliance oversight. Understanding these distinct domains is essential, because no single tool addresses all of them.

**It is also critical to recognize what this attack functionally was: an insider attack.** Once the adversary obtained privileged administrative credentials to Stryker's Entra ID and Intune environments, they operated with the same authority as a trusted systems administrator. They issued legitimate MDM commands through legitimate administrative consoles using legitimate credentials. The systems responded exactly as designed, executing wipe commands that the platform was built to support. This is what makes the Stryker breach so instructive and so difficult to defend against: the attacker did not need to deploy malware or exploit a software vulnerability. They simply *became* a malicious insider. Insider attacks—whether from compromised credentials or actual malicious insiders, are widely recognized as the most difficult class of attacks to prevent, because the adversary operates within the boundaries of authorized access. Defending against them requires controls that limit the blast radius of any single credential, enforce least-privilege access at every boundary, and continuously validate that the posture of the environment matches its intended configuration.

**Cloud Identity and Access Governance Failures.** The destructive wipe command was executed through the Microsoft Intune admin console, a SaaS application served publicly over the internet. Intune does not flow through private networks and does not support Azure Private Endpoints. This means the primary control surface for protecting the admin console is **Microsoft's Conditional Access Policies**, which can restrict access based on source IP ranges, geographic location, device compliance state, and multi-factor authentication requirements. For an attacker to have gained unrestricted administrative access to the Intune console and executed a global wipe, Stryker's conditional access policies were either absent, misconfigured, or insufficiently enforced. Properly configured, these policies would have prevented access to the admin console from unauthorized locations, unapproved devices, or sessions lacking step-up authentication. Additionally, Microsoft's Privileged Identity Management (PIM) tool, which provides time-limited, approval-gated elevation to administrative roles, appears not to have been in place, or was improperly configured. For a company of Stryker's scale, this represents a likely violation of SOC 2 controls and, given the healthcare data involved, a probable HIPAA Security Rule failure.

**Network Architecture Failures.** While the wipe command was delivered through the cloud, the *preceding phases of the attack,* reconnaissance, credential harvesting, lateral movement, and the exfiltration of 50 terabytes of data ,occurred within Stryker's enterprise network. Attackers infiltrated the environment during an extended pre-positioning phase believed to have begun before February 28, moving laterally across network segments, escalating privileges, and staging data for exfiltration. This was possible because Stryker's internal network lacked meaningful cryptographic segmentation, allowed IP-visible and discoverable assets to be scanned and targeted, and did not enforce isolation between its manufacturing, logistics, corporate IT, and communications environments. These are the classic symptoms of a flat or poorly segmented enterprise network, the exact conditions that enable a state-sponsored adversary to turn a single initial foothold into a global catastrophe.

**Compliance and Governance Failures.** Conditional Access Policies require a minimum Microsoft license level (M365 Business Premium, M365 E3, M365 F1/F3, or Enterprise Mobility + Security E3), all standard for enterprise organizations. PIM, MFA enforcement, and password leak detection through enterprise password management are baseline SOC 2 requirements and are indirectly mandated under HIPAA for organizations handling protected health information. That these controls appear to have been absent or misconfigured at a $25 billion healthcare company suggests fundamental governance failures, not merely a technical oversight.

## Where the Onclave TrustedPlatform® Fits—and Where It Doesn't

***A note on precision:*** *The Intune admin console is a cloud-hosted SaaS surface. TrustedPlatform does not directly govern access to public SaaS administrative consoles. The proper controls for that specific attack vector are Microsoft's Conditional Access Policies, PIM, and MFA enforcement. We believe transparency builds trust, which is why we draw this distinction clearly for our clients.*

That said, the Stryker attack was not a single-domain event. It was a multi-phase campaign, and TrustedPlatform plays a material role across multiple stages:

**Enforcing Cloud Access Controls as a Network Utility.** Microsoft's Conditional Access Policies can restrict Intune admin console access to a defined set of authorized public IP addresses. TrustedPlatform serves as the enforcement mechanism for this control by tunneling all administrative traffic through authorized network egress points within secured enclaves. Administrators connecting through a TrustedPlatform enclave exit through a known, authorized IP, ensuring that Conditional Access location-based policies are consistently enforced regardless of where the administrator is physically located. Without a network architecture that controls egress, location-based conditional access policies are only as strong as the discipline of each individual user's connection practices.

**Preventing the Reconnaissance, Lateral Movement, and Exfiltration That Enabled the Attack.** The wipe command was the final act of a campaign that required weeks of undetected access to Stryker's internal network. TrustedPlatform directly addresses this entire pre-positioning phase. By moving data communications from OSI Layer 3 (network layer) to an encrypted Layer 2 (data link layer) overlay, the platform creates cryptographically isolated enclaves using AES-256 GCM encryption. Devices protected behind TrustedEdges become non-discoverable, they cannot be scanned, probed, or targeted because they do not exist on the addressable IP network. Cross-enclave trust is architecturally impossible, not merely policy-restricted: the TrustedBlockchain CA generates a new, enclave-specific certificate set for every assigned TrustedEdge and TrustedBroker at the moment of assignment. In a TrustedPlatform-protected environment, the reconnaissance that mapped Stryker's infrastructure would have found nothing. The lateral movement across manufacturing, logistics, and corporate IT segments would have been blocked at the cryptographic boundary of each enclave. And the exfiltration of 50 terabytes of data—which required sustained, high-volume outbound transfer—would have been contained within the segment where the initial foothold occurred, drastically limiting the blast radius of the compromise.

**Constraining the Blast Radius of Insider-Style Attacks.** Because the Stryker attack functionally operated as an insider attack, the most relevant defensive question is not just *how do we keep adversaries out* but *how do we limit what a compromised credential can reach*. TrustedPlatform's enclave architecture directly answers this. Each enclave enforces its own independent trust boundary with enclave-scoped certificates, session-unique ephemeral keys, and bilateral trust

negotiation between TrustedEdges and TrustedBrokers. A credential compromise in one enclave provides zero access to any other enclave. There is no trust inheritance, no lateral bleed-over, and no global administrative command surface that spans the entire environment. This architectural constraint, limiting the reach of any single identity to the boundaries of its assigned enclave, is the most effective structural defense against insider-style attacks.

**Rapid Quarantine Through Dynamic Network Refactoring™.** Had anomalous activity been detected during the pre-positioning phase, TrustedPlatform's Dynamic Network Refactoring (DNR) would have enabled operators to instantly move compromised or suspect devices into quarantine enclaves, isolating them for investigation and remediation without disrupting mission-critical operations. DNR allows the secure communications fabric to be dynamically re-instantiated around an active enclave context, enabling devices to be patched and restored without ever exposing operations enclaves to hostile activity.

**Separation of Data and Management Planes.** TrustedPlatform enforces bimodal communication with fully separated data and management channels, aligned with NIST 800-207 Zero Trust Architecture requirements. An attacker who gained access to one communication plane could not pivot to the other, adding a structural barrier that does not exist in flat enterprise networks where a single credential escalation path can traverse from identity systems to operational control.

## The Complete Picture: Defense in Depth

The Stryker attack reinforces a principle that serious security practitioners understand: no single technology prevents every attack, especially an insider-style attack executed with legitimate credentials. Effective defense requires controls across every security domain, each addressing a specific attack surface. The proper response to the Stryker breach includes:

**Cloud Identity Governance:** Properly configured Conditional Access Policies restricting Intune admin console access by IP, location, device compliance, and MFA requirements. Privileged Identity Management (PIM) enforcing time-limited, approval-gated admin role elevation. Enterprise password management with leak detection. These are foundational controls that should be in place at every organization managing endpoints through cloud-hosted SaaS platforms.

**Zero Trust Network Architecture:** The Onclave TrustedPlatform® providing cryptographic micro-segmentation, non-discoverable assets, enclave-scoped identity management, separated control planes, and Dynamic Network Refactoring, eliminating the network-level attack surface that enabled the reconnaissance, lateral movement, and massive data exfiltration that preceded the destructive payload, while constraining the blast radius of any insider-style credential compromise.

**Compliance Governance:** Active SOC 2 and HIPAA Security Rule compliance programs that audit and verify the configuration of these controls continuously, not annually. The proposed HIPAA Security Rule overhaul will make all controls mandatory, including network segmentation, encryption of all ePHI at rest and in transit, and annual penetration testing, with an estimated $34 billion in industry-wide compliance costs over five years.

## Looking Ahead: AI-Driven Compliance Verification

The Stryker breach exposes a fundamental limitation in how organizations currently approach security compliance. The controls that would have prevented this attack, Conditional Access Policies, PIM configuration, MFA enforcement, network segmentation, least-privilege access, are

not exotic or cutting-edge technologies. They are baseline requirements that appear in every major compliance framework (SOC 2, HIPAA, NIST CSF 2.0, HHS 405(d)). The failure was not a lack of available technology. It was a failure to verify that the controls were actually configured, enforced, and functioning as intended across a complex, global environment.

This is the gap Onclave is building toward with our AI-driven compliance verification roadmap. Onclave's product roadmap includes the integration of artificial intelligence as a **continuous compliance check** within the TrustedPlatform ecosystem, an AI layer capable of evaluating whether the security controls an organization claims to have in place are actually configured, active, and consistent with policy. In the context of the Stryker attack, an AI compliance engine could have identified that Conditional Access Policies were not restricting Intune admin console access to authorized IPs, that PIM was not enforcing time-limited role elevation for global administrator accounts, that MFA was absent or insufficiently enforced for privileged access, and that network segmentation controls were not isolating critical manufacturing and logistics environments from corporate IT. These are not subjective assessments—they are verifiable configuration states that an AI system can audit continuously, flagging drift and misconfigurations before adversaries can exploit them.

The vision is to move healthcare organizations from point-in-time compliance audits, which capture a snapshot that may be outdated within days, to **continuous, AI-verified compliance posture** that validates the entire security stack in real time. When combined with TrustedPlatform's architectural controls, this creates a defense model where the network prevents lateral movement and limits blast radius by design, while AI continuously verifies that the surrounding controls, cloud identity governance, access policies, encryption configurations, and compliance attestations, remain in their intended state. For an industry where the cost of a breach averages $10.93 million and regulatory enforcement is tightening to include personal executive liability, this shift from periodic auditing to continuous verification is not optional, it is the standard that the threat landscape now demands.

## How TrustedPlatform Can Accelerate Recovery

For organizations facing catastrophic system-wide destruction, TrustedPlatform offers a structured path to recovery that simultaneously restores operations and hardens the environment against future attacks:

**Secure Rebuild Within Protected Enclaves.** As systems are rebuilt and brought back online, TrustedPlatform can be deployed as a network overlay, without requiring IP changes, network redesign, or disruption to the restoration process. Rebuilt systems are immediately placed within cryptographically isolated enclaves, ensuring that the recovery environment itself is protected from residual threats or secondary attacks targeting the restoration window.

**Phased Restoration with Zero Trust Controls from Day One.** Rather than restoring the entire network simultaneously and hoping that no attacker persistence remains, TrustedPlatform enables phased restoration where each segment is brought online within its own enclave with full Zero Trust controls, identity validation, cryptographic isolation, session ephemerality, and continuous verification, enforced from the first device reconnected.

**Protection of the Supply Chain During Recovery.** For Stryker's hospital customers, the critical question is when surgical equipment, implants, and medical device support will be restored. TrustedPlatform can secure the manufacturing-to-hospital supply chain with dedicated enclaves for

logistics, distribution, and clinical device connectivity, ensuring that restored systems are not only functional but defended.

**Brownfield Deployment Across Legacy and Modern Infrastructure.** TrustedPlatform is transport-agnostic and deploys into existing brownfield environments. It overlays the current network, integrates with existing services like Active Directory and PKI/KMS, and requires no changes to server IP addressing. For an organization facing an urgent, global recovery effort across heterogeneous infrastructure in 79 countries, this deployment model is critical, security can be applied without adding complexity to an already demanding restoration timeline.

## The Imperative

The Onclave TrustedPlatform® is the only purpose-built Zero Trust Architecture to hold an Authority to Operate (ATO eMASS 3551) on the Defense Health Agency and White House Communications Agency networks. It carries FIPS 140-3 certification, integrates NIST post-quantum cryptography validated by the U.S. Air Force, is referenced in NIST Special Publication 1800-30C for securing Telehealth Remote Patient Monitoring ecosystems, and is incorporated into the NATO ZAFE framework for deployable military medical environments. Onclave helped draft FDA standards for manufacturing medical devices and has established a strategic partnership with Vizient to accelerate adoption across the healthcare sector.

*The Stryker breach was preventable—but prevention required controls across every security domain, not a single tool. Cloud identity governance should have stopped the wipe command. Zero Trust network architecture should have stopped the reconnaissance, lateral movement, and 50-terabyte exfiltration that preceded it—and constrained the blast radius of what was functionally an insider attack. Compliance governance should have ensured both were in place. AI-driven continuous compliance verification should have caught the configuration gaps before adversaries did. The TrustedPlatform addresses the network architecture domain with government-validated, purpose-built Zero Trust controls that no other solution provides, serves as a critical enforcement utility for cloud identity controls, and is building toward AI-powered compliance verification that closes the governance gap. Together, these capabilities form the defense-in-depth posture that the healthcare industry can no longer afford to defer.*