Stryker Was Not Ransomwared. It Was Remotely Wiped Using Trusted Infrastructure. And How Smallstep Closes This Gap.

At a glance

One compromised credential. A legitimate admin console. Tens of thousands of devices wiped across 79 countries. No malware required.

TL;DR

On March 11, 2026, an Iran-linked group reportedly used Stryker's own Microsoft Intune console to remotely wipe tens of thousands of devices across 79 countries. No malware. No exploit. A compromised admin credential, used through a legitimate management channel.Surgeries were delayed. Hospitals could not order equipment. Stryker filed an SEC 8-K.The attacker succeeded because Stryker's infrastructure could not distinguish between a legitimate admin workstation and an attacker holding a valid credential from somewhere else. That is the gap. **Smallstep closes it.**

ACME Device Attestation, co-developed with Google, binds identity to hardware keys in the TPM. The credential only works from a device the organization has cryptographically enrolled and still controls. A stolen credential from an unattested device is rejected before the session begins. The wipe command is never issued.This is not a replacement for MFA, PAM, or admin governance. It is the missing layer underneath them: proving the physical origin of a privileged session. Even with phishing-resistant MFA and strict admin controls in place, session origin remains difficult to prove without hardware-bound identity. **Deployable in weeks. Start with admin console access.**

HOW SMALLSTEP ELIMINATES THIS ATTACK PATH

ACME Device Attestation (ACME DA), co-developed with Google, binds device identity to hardware keys in the TPM or Secure Enclave. The private key never leaves the hardware. The certificate proves the request originates from a specific physical device, not just that someone holds valid credentials.

By issuing cryptographic device identity anchored in hardware and requiring that identity at the point of access, we eliminate the ambiguity between a legitimate admin workstation and an attacker replaying a valid session from somewhere else. **This is not another signal layered into policy. It is a gate.**

Enforcement is configured at access points where certificate validation is supported: Entra ID, VPN gateways, and administrative consoles. The specific integration depends on the customer's architecture and what their access layer supports. Where certificate validation can be made a prerequisite to authentication, the device must prove itself before the session begins.

Because device attestation is transparent to the user, it addresses the MFA deployment problem differently. There is no additional workflow. No token to fumble. No prompt to approve. The device proves itself at the hardware level, every time it connects. **This functions as a hardware-backed authentication factor without user interaction, which removes one of the main reasons MFA exceptions exist in the first place.**

WHERE OUR CUSTOMERS START:

1. Admin console access.
2. Privilege boundaries.
3. BYOD scope enforcement.

DEPLOYMENT SUMMARY

Replaces	Reliance on software-based device compliance as the primary trust signal at administrative and privilege boundaries.
Budget	IAM or zero trust program. Infrastructure control, not endpoint agent.
First project	ACME DA on admin workstations, enforced at Intune and Entra ID console access. Weeks, not months.
CMMC	NIST 800-171 Rev. 3 Control 3.5.2 requires authentication of users, processes, and devices before access. Hardware-bound device attestation is one of the stronger implementations for high-assurance boundaries. NIST 800-172 provides enhanced controls for protection against nation-state actors. Phase 2 mandatory C3PAO assessments begin November 2026.

WHAT THIS DOES NOT FIX

Insider threat from an attested device.

Compromise of the attested device itself.

Smallstep eliminates the credential-origin ambiguity attack path when enforced. That is one of the critical gaps that enabled the outcome at Stryker. It does not replace every other control. We think clarity about boundaries is more valuable than a slide deck that claims to solve everything.

WHAT HAPPENED

On March 11, 2026, an Iran-linked group attacked Stryker Corporation. Based on reporting from KrebsOnSecurity, BleepingComputer, and Reuters, the attackers appear to have used Stryker's Microsoft Intune console to issue a mass remote wipe, reportedly destroying tens of thousands of devices across 79 countries within hours. No malware was deployed. No software vulnerability was exploited. According to public reporting, the attackers compromised an administrator credential and issued the wipe through the same administrative channel Stryker's IT team uses every day.

According to public reporting, the credential was available for purchase on the dark web. The password was reportedly weak, containing common English words. Reports indicate it had not been rotated, that multi-factor authentication was not consistently enforced on the admin account, and that multi-admin approval was not enabled in Intune. If reporting is accurate, the attack may have required little more than acquiring valid credentials and using them through legitimate administrative channels.

Stryker filed an SEC 8-K confirming a cyberattack, global disruption to its Microsoft environment, and that no ransomware or malware was detected. Based on reporting, the wipe was executed through Intune's native remote management capabilities and affected laptops, servers, and personal phones enrolled through BYOD. The system did exactly what it was asked to do.

THE OPERATIONAL IMPACT

Stryker manufactures surgical equipment, medical devices, and implants used in hospitals across 79 countries. When tens of thousands of devices went offline, the impact reached operating rooms.

Hospitals reported delayed surgeries. Medical facilities could not order equipment or replacement parts through Stryker's systems. The company's electronic ordering system went offline. Stryker was forced to confirm product-by-product that its critical medical devices, including Mako surgical systems, LIFEPAK defibrillators, Vocera communication badges, and LIFENET transmission systems, remained safe to use.

The attacker's goal was not financial. Handala, the group that claimed responsibility, is reportedly linked to Iranian state interests. Reuters and multiple security researchers describe the attack as retaliation against the US. The point was destruction. The visible cost of the initial access, reportedly purchasing stolen credentials, appears disproportionately low relative to the operational crisis it created across a $20B+ medical technology company's global operations.

Stryker is also a supplier to the US Department of Defense. That makes this incident directly relevant to CMMC compliance and the protections NIST has already codified for the defense industrial base. Controls designed to reduce the likelihood and impact of this class of attack already exist. Based on reporting, several were not in place.

The operational cost of this attack appears to have been low relative to the damage achieved.

THE ARCHITECTURAL FLAW

This was not a failure of detection. It was a failure of control.
The attacker did not need to bypass MFA, because MFA was not enforced. They did not need to jailbreak a device. They did not need to defeat endpoint protection. They only needed one thing: **a valid session that the system could not distinguish from a legitimate one.**

Modern identity systems are very good at verifying who a user is. They are much weaker at verifying where that identity is being exercised from. Conditional Access, MDM compliance, and device posture checks all operate on signals that can be replayed, proxied, or inherited. In many implementations, they do not reliably answer the question that matters most in this scenario:
"**Is this request coming from a device we issued and still control?**"

In the Stryker case, the answer was effectively: we assume so. **That assumption is what failed.**

WHY MFA AND CONDITIONAL ACCESS DID NOT STOP THIS

Stryker's Intune admin account reportedly did not have MFA consistently enforced. CISA's advisory in response to the incident specifically called out MFA as a gap. That alone is worth sitting with: one of the most basic and widely recommended controls was not in place on an account with fleet-wide destructive authority.

But even in environments where MFA is properly deployed, this class of attack is not fully prevented. Adversary-in-the-middle phishing captures the session token after the victim completes a real MFA challenge on the real Microsoft login page. The attacker does not bypass MFA. They inherit its output.

Conditional Access evaluates device compliance based on self-reported signals: OS version, encryption status, MDM enrollment. An attacker replaying a session token from a compliant device passes the check. Tightening the policy raises the bar. It does not close the gap.

Conditional Access answers: **"Does this device meet policy?"** based on what the device reports. Device attestation answers: **"Is this the specific physical machine we enrolled?"** based on a cryptographic challenge to the TPM. One accepts claims. The other requires proof.

WHERE THIS EXISTS IN YOUR ENVIRONMENT TODAY

If your environment has the following, it shares the architectural weakness exploited at Stryker:

- **Entra ID administrative access** reachable from any device that passes a compliance check.
- **Intune controlling fleet-wide actions** including factory reset, from a single administrative console without multi-admin approval.
- **AD Connect synchronizing credentials** between on-premises Active Directory and cloud identity, so one compromised credential works in both environments.
- **BYOD devices enrolled in the same MDM scope** as corporate endpoints, subject to the same management actions including remote wipe.
- **Administrative credentials that are not hardware-bound**, meaning they can be used from any device, anywhere, by anyone who possesses them.

These conditions are standard in modern Microsoft-centric environments, and multiple were present in the Stryker incident. In environments without hardware-bound device verification at administrative boundaries, a compromised admin credential is sufficient to reach the same outcome.

THE NATION-STATE REALITY

Based on public reporting, the Stryker attack did not require a sophisticated exploit. The initial access appears to have been a compromised credential. But the motivation behind it is what matters: this was not crime, it was warfare.

This was not a criminal enterprise looking for a ransom payment. Based on public reporting, this was a group reportedly linked to Iranian state interests conducting destructive cyber operations against a US company. Any large organization is a potential target, not just defense contractors or weapons manufacturers.

The asymmetry is notable. The visible cost of this attack appears to have been low relative to the operational damage it caused. The attack surface is not limited to classified systems or military infrastructure. It is every enterprise with centralized management tools and credential-only trust boundaries.

What should companies be doing to mitigate this broader threat?

The guidance already exists. NIST, CISA, DIBCAC, and DOD have spent the last decade developing and vetting protections against advanced persistent threats for the defense industrial base. That guidance is codified in CMMC Level 2 and Level 3, and in NIST 800-171 and 800-172. Most companies outside the defense industrial base are not regulated against these standards. But if you are wondering what best practices look like for protecting against nation-state attackers, the research has been done, the controls have been documented, and the frameworks are publicly available.

NIST 800-171 Rev. 3 Control 3.5.2 requires organizations to authenticate the identities of users, processes, and devices before granting access. Hardware-bound device attestation is one of the stronger ways to meet that requirement at high-assurance boundaries. Smallstep provides one path to that implementation.

WHY CUSTOMERS CHOOSE SMALLSTEP FOR THIS EXACT PROBLEM

The Stryker incident exposed multiple failures: credential compromise, missing MFA, excessive admin scope, lack of dual control, and a centralized management plane with fleet-wide destructive authority. Most security teams already know how to address these. They are deploying PAM, enforcing least privilege, rolling out phishing-resistant MFA, enabling multi-admin approval, and hardening Intune governance. That work matters and should be done.

Even with phishing-resistant MFA and strict admin controls in place, session origin remains difficult to prove without hardware-bound identity.

The gap that remains after all of that work is done: **can your infrastructure prove that privileged access is being exercised from a device you have cryptographically bound and still control?**

That is the specific residual problem customers come to Smallstep to close. Not a replacement for PAM, MFA, or admin governance. The missing layer underneath them: verifying the physical origin of a privileged session.

Since the Stryker incident, companies in our sales pipeline have reached out unprompted. Security teams saw the news, recognized their own architecture, and asked what we could do. For organizations where security teams already understood the gap but could not get executive buy-in to fund the fix, Stryker is the event that unlocks the budget conversation.

Smallstep is typically adopted when teams move from "We believe this is a managed device" to "**We can cryptographically require that it is.**"

Stryker appears to have suffered a control-plane attack enabled by compromised privileged access. Even where organizations harden passwords, enforce MFA, and tighten admin workflows, one gap often remains: proving that privileged access is being exercised from a device the organization has cryptographically bound and still controls.If your infrastructure cannot verify the physical device presenting a credential, then every credential you trust can be reused by someone you don't. **Smallstep exists to close that specific gap.**

Smallstep is the world's first Device Identity Platform™, enabling Zero Trust, certificate-based access to infrastructure, applications, and networks. Built in partnership with Apple and Google, Smallstep uses cryptographic attestation and short-lived, hardware-backed credentials to replace passwords, SSH keys, and VPN clients. By integrating with tools like Jamf, Intune, and Okta, Smallstep ensures that only trusted users on compliant devices can access sensitive systems—delivering true Zero Trust security without user friction.