To audit your organization's endpoint management and prevent a "Stryker-style" attack, you can use the following checklist derived from CISA's March 2026 alert and Microsoft's security best practices. [1, 2]

1. Administrative Access & Authentication

- **Phishing-Resistant MFA:** Are all admin accounts required to use FIDO2 hardware keys or certificate-based authentication?
- **Just-In-Time (JIT) Access:** Do you use a tool like Microsoft Entra Privileged Identity Management (PIM) to ensure admins only have elevated rights when performing specific tasks?
- **Account Separation:** Are administrative tasks performed using dedicated admin-only accounts that are separate from daily email and web browsing accounts? [1, 3]

2. Guarding High-Impact Actions

- **Multi-Admin Approval (MAA):** Is Multi-Admin Approval configured for destructive actions like **Wipe**, **Retire**, or **Delete**? (This prevents a single compromised account from triggering a mass wipe).
- **Bulk Action Thresholds:** Have you set up automated alerts for "Bulk Destructive Actions" (e.g., more than 5 wipes in 15 minutes)? [1, 3]

3. Policy & Device Management

- **Role-Based Access Control (RBAC):** Have you reviewed admin roles to ensure the principle of least privilege? Can only a few highly trusted individuals perform factory resets?
- **Conditional Access:** Does your configuration require a "Trusted Device" and a specific IP range (like a corporate VPN) for any access to the management console?
- **BYOD Evaluation:** Have you reviewed your BYOD enrollment policies? Consider if personal devices should be "Enrolled" (allowing a full wipe) or just "Managed" via App Protection Policies (only wiping work data). [1, 4, 5, 6]

4. Response & Resilience

- **Offline Backups:** Do you have regular, offline backups of critical configurations and data that cannot be deleted by a cloud-admin account?
- **Incident Response Drill:** Has your team rehearsed a scenario where 50%+ of your endpoint fleet is suddenly factory reset? [5]

[1] https://community.opentextcybersecurity.com
[2] https://www.reddit.com
[3] https://www.govinfosecurity.com
[4] https://www.reddit.com
[5] https://www.computerweekly.com
[6] https://www.bitget.com