White Paper
YellowKey BitLocker Bypass: A Practical Guide for Defenders

Version 2026.1

May 26, 2026

FINAL

PREPARED BY

ASSURA®

Cybersecurity uncompromised.

ASSURA, INC. | 7330 STAPLES MILL ROAD | #292 | RICHMOND, VA | 23228

ASSURAINC.COM

Version Control

Version	Changes Made	Updated By
2026.1	First version.	Assura, Inc. - JAC

TABLE OF CONTENTS

TL;DR: YellowKey lets an attacker with brief physical access bypass BitLocker on Windows 11 and Windows Server versions 2022 and 2025 when TPM-only mode is in use. On May 20, 2026, Microsoft assigned CVE-2026-45585 (CVSS 6.8) and published mitigation guidance, but as of the date of this white paper, it has not yet shipped a full security update.

Organizations now have two defensible technical paths for mitigation: apply Microsoft's WinRE mitigation, or switch to TPM+PIN. Each carries trade-offs, and the right choice depends on the specific device class, operational profile, and regulatory environment.

1.0 EXECUTIVE SUMMARY

On May 12, 2026, a security researcher published a working proof of concept for an attack against BitLocker drive encryption that requires nothing more than a USB stick and a key press during boot. The exploit, named YellowKey, abuses how the Windows Recovery Environment (WinRE) processes transaction logs to spawn an unrestricted shell with the BitLocker-protected volume already mounted. Independent researchers reproduced it on current Windows 11 builds shortly after its release. On May 20, Microsoft assigned the issue CVE-2026-45585 (CVSS 6.8) and published manual mitigation guidance, but has not yet committed to a full security update timeline.

For any organization that relies on BitLocker as its data-at-rest control for lost or stolen Windows 11 endpoints, the practical implication is direct: a missing device in default TPM-only configuration should now be treated as a potential data exposure event, not a hardware loss. The same applies to physical access scenarios that previously seemed exotic but are not, including hotel-room theft, conference grab-and-run, malicious insiders, and unattended kiosks.

This paper is written for security leaders, IT directors, and compliance officers responsible for Windows endpoint security. It covers the four standard risk treatment options for YellowKey, a decision framework for choosing between the two available technical mitigations, the operational and change-management trade-offs of each, detection signals that indicate exploitation attempts, and the implications for organizations operating under compliance mandates such as PCI DSS, HIPAA, CJIS, and CMMC. The objective is to enable an informed, documented decision before the next missing-laptop incident, not after.

2.0 RISK TREATMENT OPTIONS

Risk decisions are centered on the four standard risk treatments or simply doing nothing (which is itself a risk decision). Each is defensible for the right environment. The wrong choice is an undocumented one.

Treatment	When It Fits	Recommended Approach
Accept	• Low data sensitivity on endpoints • Strong physical controls already in place (badge-access offices, no travel) • Short remaining device refresh horizon	• Document the decision, the rationale, and the compensating controls • Set a re-evaluation trigger: any change in workforce travel posture, a confirmed in-the-wild attack, or 90 days elapsed, whichever comes first • Update the lost-device playbook to treat a missing laptop as a data exposure event: revoke the user's sessions and tokens in Entra ID, disable the device object, and reset the user's password and any cached service credentials

Treatment	When It Fits	Recommended Approach
Mitigate	• Mixed fleet with both high and low sensitivity endpoints • Travel-heavy or distributed workforce • Regulated data on Windows 11 endpoints (e.g., PCI, NIST SP 800-53, SEC 530, CJIS, CUI, PHI, SSI, FTI)	*Recommended for most organizations* • Apply Microsoft's CVE-2026-45585 WinRE mitigation: remove the autofstx.exe value from BootExecute in the mounted WinRE image registry hive, then reestablish BitLocker trust for WinRE. This blocks the FsTx Auto Recovery Utility that the YellowKey exploit abuses • Or switch from TPM-only to TPM+PIN on high-value endpoints, then expand. Microsoft explicitly calls this out as a protection against YellowKey exploitation • Consider a combination of the two mitigations on highly sensitive devices. • Pair with UEFI password, USB boot disabled, and WinRE disabled, where a centralized recovery capability exists
Transfer	• Cyber insurance policy in place with coverage for lost-device data exposure • Contractual arrangements with managed service providers covering endpoint security	• Confirm the policy actually pays out when the loss vector is a known, unpatched vulnerability • Document insurance carrier notification requirements in advance, not after a loss *Transfer alone is rarely sufficient. Pair with at least one mitigation.*
Avoid	• Small population of ultra-sensitive endpoints • Executive, legal, or M&A workstations where exposure of a single device is unacceptable	• Move the sensitive workload to a VDI or cloud workspace; treat the local device as a thin client • Restrict the affected device class to on-premises use only until the Microsoft mitigation is verified or a full security update ships
No Risk Decision	• This is a defensible choice only when the organization formally accepts the risk in writing • It is not the same as Accept. Accept comes with documentation, triggers, and a refreshed playbook. Doing nothing is the absence of those. • Often chosen implicitly while waiting for a full Microsoft security update	• Microsoft has published manual mitigation steps for CVE-2026-45585, but has not committed to a full security update timeline. Choosing to do nothing means foregoing an officially supported mitigation that is available today • If choosing to wait, document the decision as a formal risk acceptance with a fixed expiration and a re-review date • Any reported loss during the wait should be handled as a data exposure event

3.0 CHOOSING BETWEEN THE MITIGATIONS

Both mitigations block the public proof of concept. The right choice for any given organization is driven by device class, operational profile, and endpoint management maturity, not by which mitigation is technically "better." Many enterprises with mixed fleets will end up running both on different device populations.

Recommended mitigation by device class

Device Class	Recommended Mitigation	Why
Windows Server 2022/2025 systems (including Server Core)	Microsoft WinRE mitigation only	A PIN prompt on a server reboot is operationally untenable. Servers need an unattended boot for lights-out operations, scheduled maintenance, and remote management. WinRE mitigation preserves that. Servers should be in physically secure locations with protective, detective, and corrective security controls.
Laptops with low-value data where disclosure will not have a material operational, reputational, or regulatory impact	Microsoft WinRE mitigation only	This is a simpler change operationally than TPM+PIN, but a mitigation is still called for. The loss or theft of a laptop without sensitive material on it would not have a material downside, other than the expense of replacing the device.
Kiosk, shared, lab, and lights-out workstations	Microsoft WinRE mitigation only	No specific user owns the boot experience. A PIN prompt either blocks the device entirely or creates a shared secret, which defeats the purpose. WinRE mitigation is the only path that does not require workflow redesign.
Devices with unattended-boot dependencies (Wake-on-LAN, overnight patching)	Microsoft WinRE mitigation only	BitLocker+PIN breaks unattended boot by definition. WinRE mitigation preserves the operational profile while addressing the vulnerability.
Office desktops with regulated data *and* an existing PIN or smart-card culture	BitLocker+PIN only	Users are already authenticating with something at the keyboard at boot (PIV cards, Windows Hello for Business). Friction is low, the audit story is clean, and the control is easy to point to for regulators.
Office desktops *without* PIN or smart-card culture	Microsoft WinRE mitigation only	Physical loss is a lower-frequency event than for laptops, and introducing a new boot-time PIN is a substantial change-management lift. WinRE mitigation is invisible to users and gets the same protection against the public PoC.
Laptops and workstations with high-value data (e.g., executive, legal, M&A, classified data, regulated workstations under audit)	**Both**	Defense in depth is justified. If the researcher's claimed TPM+PIN bypass becomes public, the WinRE mitigation already removes the exploit primitive. The two layers fix the problem at different points in the boot chain.
Organizations under heavy regulatory frameworks (CJIS, CMMC L2+, PCI for CDE, financial sector)	**Both**	The audit narrative rewards "applied the vendor mitigation plus a compensating control." In these frameworks, "both" is the defensible answer for in-scope endpoints.

3.1 PROS AND CONS OF APPLYING MICROSOFT'S MITIGATION

Pros	Cons
• Officially supported mitigation from Microsoft for CVE-2026-45585 • Invisible to end users: no PIN prompt at boot, no change to the daily login experience, no help-desk surge for forgotten PINs • Preserves unattended boot workflows: Wake-on-LAN, overnight patching, scheduled reboots, and remote management continue to function • Compatible with kiosk, shared, and lab devices that cannot tolerate interactive boot • Targets the actual vulnerable component (autofstx.exe and the FsTx Auto Recovery Utility) rather than working around it • Lower change-management burden than BitLocker+PIN: no PIN policy, no user training, no help-desk runbook redesign	• Requires modifying the WinRE image on every affected endpoint; operationally heavier than a Group Policy push • Reestablishing BitLocker trust for WinRE has been a historical pain point; CVE-2022-41099 created similar challenges, and Microsoft eventually shipped a PowerShell helper script • No native Intune or Group Policy toggle; deployment requires scripted WinRE manipulation through Intune Win32 app, Configuration Manager, or remote PowerShell • Windows feature updates may replace the WinRE image and silently revert the mitigation, requiring re-application and ongoing verification • Does not protect against the researcher's claimed TPM+PIN bypass variant, should it become public • A failed WinRE modification can render device recovery unavailable; broken WinRE plus a TPM key release failure can lock a user out of their data

3.1.1 Change Management Considerations for Microsoft's Mitigation

Microsoft's mitigation modifies the WinRE image rather than the configuration. Treat it as a controlled change to recovery infrastructure, not a routine policy push.

Before rollout

- Inventory affected systems: Windows 11 versions 24H2, 25H2, and 26H1, plus Windows Server 2022/2025 and Windows Server 2022/2025 Server Core. Devices outside this scope do not need the mitigation.
- Confirm WinRE is present and healthy on each in-scope device. The command reagentc /info should return Enabled with a valid WinRE location. Devices with WinRE disabled are not exposed to YellowKey and do not require this mitigation.
- Confirm BitLocker recovery keys are escrowed and recoverable for 100% of in-scope endpoints before any WinRE modification. A broken WinRE combined with a TPM key release failure can lock a user out of their data without a recovery key.
- Develop and pilot the scripted mitigation on test devices that mirror the production WinRE image version and BitLocker configuration. The mitigation steps (mount WinRE, mount the registry hive, remove autofstx.exe from BootExecute, save and unload the hive, unmount and commit the image, reestablish BitLocker trust) must be encoded as a repeatable, unchanging script.
- Validate the BitLocker trust reestablishment step explicitly. This is the historically problematic part of WinRE servicing operations and the most likely failure point.
- Select a deployment vehicle appropriate to your endpoint management stack: Intune, Configuration Manager package, or remote PowerShell at scale. The script must run with SYSTEM privileges and report a clear success or specific failure code.
- Document a rollback procedure for cases where the WinRE image is corrupted during modification. A backup of the original WinRE image should be staged before the script runs.

During rollout

- Pilot to a small initial group of devices. Verify that each device boots cleanly, that BitLocker does not prompt for a recovery key on next boot, and that recovery still functions through reagentc.
- Phase by risk tier: executives, finance, legal, and regulated data users first; general workforce next; kiosks, shared devices, and edge cases last.
- Track per-device success in the endpoint management console. The deployment script should report explicit success or a specific failure code, not just an exit status.

- Watch for unexpected BitLocker recovery prompts on next boot. This is the leading indicator that BitLocker trust for WinRE was not reestablished cleanly.
- Pause the rollout if more than a small percentage of devices fail the mitigation or trigger unexpected recovery prompts. Diagnose before continuing.

After rollout

- Re-verify the mitigation after every Windows feature update. Feature updates can replace the WinRE image and silently revert the change. Add a compliance check that confirms autofstx.exe is absent from BootExecute in the current WinRE image.
- Add WinRE mitigation status to the endpoint compliance dashboard. Treat the absence of the mitigation on an in-scope device the same way you would treat a missing security patch.
- Update the asset register and system security plan to reflect the applied mitigation, including the date applied and the script version used.
- Plan for the eventual full Microsoft security update, which will supersede this manual mitigation. Remove the compliance check and the deployment script when the update ships and is verified deployed.
- Hold a brief lessons-learned, particularly on the BitLocker trust reestablishment step, to inform the next WinRE-touching project.

3.2 PROS AND CONS OF ENABLING BITLOCKER+PIN

Pros	Cons
• Blocks the public YellowKey proof of concept outright • Mitigates a broad class of cold-boot and offline attacks beyond YellowKey alone • No software purchase required; native to Windows • Microsoft explicitly recommends TPM+PIN as a protection against YellowKey exploitation, which strengthens a defensible posture for regulators and auditors • Aligns with Microsoft's officially published mitigation guidance for CVE-2026-45585 • Compatible with existing Intune, MDM, and Group Policy deployment workflows	• Adds a step to every cold boot, which users will feel and complain about • ***Likely to increase help-desk volume in the first several weeks due to forgotten PINs and lockouts*** • Breaks Wake-on-LAN, remote patching, and overnight reboot workflows that assume unattended boot • Recovery key escrow must be verified before rollout; the only way to get a device with a forgotten PIN without a recoverable key is to wipe and reload it • The researcher claims a TPM+PIN variant exists; the exploit is not public, but the claim is on the record • Kiosk, shared, and lab devices may not tolerate interactive boot without workflow redesign

3.2.1 Change Management Considerations for BitLocker+PIN

BitLocker+PIN touches every user on every boot. Treat it as a user-facing change, not a back-end security tweak. The Microsoft WinRE mitigation is lower-impact for users (no PIN prompt) but requires careful handling of recovery images on every device; the considerations below apply to a BitLocker+PIN rollout specifically.

Before rollout

- Confirm BitLocker recovery keys are escrowed and recoverable for 100% of in-scope endpoints. Run a sample restore test before any production change.
- Inventory the fleet by BitLocker protector type. Identify TPM-only devices, kiosks, shared workstations, and devices used for unattended overnight tasks.
- Identify devices that depend on unattended boot, including overnight patching, scheduled reboots after updates, and Wake-on-LAN workflows. Plan exceptions or redesign.
- Define a PIN policy: minimum length, complexity, lockout threshold, and reset process. Align with the existing password/PIN policy for mobile devices so users do not learn two different rule sets.

- Develop a help-desk runbook for forgotten PINs, including identity verification steps and recovery key delivery process. Identity verification can be easily facilitated using MFA solutions such as Duo (and potentially others) by sending a push notification to the end user's mobile device and having them verify it.
- Draft user communications: a "why this matters" note from leadership, a one-page how-to with screenshots, and a short FAQ.

During rollout

- Pilot with IT first, then a subset of users in a friendly business unit, before any broad rollout.
- Phase by risk tier: executives, finance, legal, and regulated data users first; general workforce next; kiosks and edge cases last.
- Push policy via Group Policy or Intune; do not rely on individual users running manage-bde commands.
- Monitor help-desk ticket volume daily during the first two weeks. Adjust the rollout pace if ticket volume spikes.
- Track completion in your endpoint management console, not in a spreadsheet. Stragglers will exist; they need a named owner.

After rollout

- Update the asset register and the system security plan for affected devices to reflect the new configuration.
- Update the incident response and lost-device playbooks to reflect the new control.
- Re-run the BitLocker status report 30 days post-rollout to catch devices that reverted or were re-imaged without the new control.
- Hold a brief lessons-learned with the help desk and document what changes for the next security-driven endpoint rollout.

4.0 DETECTION SIGNALS

Mitigation reduces exposure; detection catches what mitigation misses. The following signals are useful for security operations teams, whether or not a mitigation is applied.

- Unexpected boots into WinRE, especially on devices with no corresponding support ticket. WinRE boots are visible in Event ID 1 from Microsoft-Windows-Kernel-Boot and through boot configuration logs.
- USB mass-storage insertions on locked or recently restarted endpoints. Correlate with WinRE boot events on the same host within a short window.
- Creation of System Volume Information\FsTx\ directory trees on removable media seen by EDR file telemetry. The presence of an FsTx folder on a USB device is not normal user activity.
- Modifications to X:\Windows\System32\winpeshl.ini outside an authorized servicing window. This is the file the exploit deletes to spawn an unrestricted shell.
- Unexpected use of diskpart, manage-bde, or BitLocker tools from a recovery shell context.
- If the Microsoft mitigation has been applied: presence of the autofstx.exe value in BootExecute on the current WinRE image. This indicates the mitigation has reverted, typically after a feature update.
- Devices in scope for the vulnerability where reagentc /info shows WinRE present, but the mitigation status is unknown or stale.

5.0 COMPLIANCE IMPLICATIONS

YellowKey changes the data-at-rest control story for any organization that relies on BitLocker in its compliance posture. The following frameworks are the most directly affected.

PCI DSS

PCI DSS v4.0 Requirement 3.5.1 requires that primary account number (PAN) data is rendered unreadable wherever it is stored, including on portable digital media. Organizations that rely on BitLocker as the control for laptops and workstations in the cardholder data environment (CDE) should consider TPM-only BitLocker as no longer providing strong assurance against the requirement, particularly for travel-heavy users. Applying a mitigation is the most direct path to maintaining the control. A documented risk acceptance without mitigation is unlikely to survive QSA scrutiny for devices that store, process, or transmit PAN.

HIPAA Security Rule

HIPAA treats encryption of electronic protected health information (ePHI) at rest as an addressable implementation specification under 45 CFR 164.312(a)(2)(iv). The HHS Breach Notification Rule provides a safe harbor when lost or stolen ePHI is rendered unusable, unreadable, or indecipherable through encryption that meets NIST guidance. YellowKey raises a substantive question about whether a stolen Windows 11 laptop in default TPM-only BitLocker configuration still meets that bar. Organizations should document either a mitigation or a risk decision and align with counsel on breach notification posture for devices lost during the unpatched window.

CJIS Security Policy

The CJIS Security Policy requires FIPS 140-2 or FIPS 140-3 validated encryption for criminal justice information (CJI) at rest on mobile devices and portable media (Policy Area 10, Section 5.10.1.2). BitLocker can be configured to meet FIPS validation, but the YellowKey exploit bypasses the access control regardless of the cryptographic module's validation status. Agencies with mobile devices that store or process CJI should apply a mitigation. Documentation of the applied mitigation should be available for the next CJIS audit.

CMMC and NIST SP 800-171

NIST SP 800-171 Rev. 3 requires that controlled unclassified information (CUI) on mobile devices be protected through encryption (controls 3.1.18 and 3.13.08). CMMC Level 2 and above inherit these requirements. Organizations in the Defense Industrial Base with CUI on Windows 11 endpoints should treat YellowKey as a control deficiency until a mitigation is applied. Defense contractors operating under DFARS 252.204-7012 should evaluate whether a lost device during the unpatched window constitutes a reportable cyber incident under the 72-hour reporting clause.

State data breach notification laws

Most U.S. state breach notification statutes include an encryption safe harbor that exempts the loss of encrypted personal information from notification requirements. The legal sufficiency of that safe harbor for YellowKey-vulnerable devices is a question for counsel, not a technical determination. The conservative posture during the unpatched window is to treat a lost or stolen Windows 11 laptop in default TPM-only BitLocker configuration as outside the safe harbor and to invoke the organization’s standard breach response workflow.

6.0 CONCLUSION

YellowKey is unusual in three respects. The exploit is trivial to execute: copy a folder, hold a key, get a shell. The protective control it defeats is the one most organizations rely on for lost-device response. And the path to a complete fix runs through the Windows Recovery Environment, which has historically been a difficult servicing surface and which Microsoft has not yet committed to fully patching on a public timeline.

For most organizations, the right response is not a single sweeping change. It is a deliberate, device-class-aware program that applies Microsoft’s WinRE mitigation where unattended boot is required, applies BitLocker+PIN where physical loss is the dominant exposure, and applies both on high-value or audit-driven endpoints where defense in depth is justified. The decision belongs to the organization, but the decision must be made. A missing Windows 11 laptop in default configuration is a data exposure event today, and the lost-device playbook should reflect that until a full Microsoft security update ships and is deployed.

The cost of the wrong choice is real. The cost of an undocumented choice is greater.

7.0 REFERENCES AND FURTHER READING

- Microsoft Security Response Center, CVE-2026-45585: Windows BitLocker Security Feature Bypass Vulnerability. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45585
- Microsoft Learn, BitLocker Group Policy settings reference, including Require additional authentication at startup. https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/
- CVE-2022-41099, the previous WinRE-based BitLocker bypass and the precedent for WinRE servicing complexity. KB5025175.
- PCI Security Standards Council, PCI DSS v4.0, Requirement 3.5.1.

- U.S. Department of Health and Human Services, HIPAA Security Rule, 45 CFR 164.312, and the HHS Breach Notification Rule encryption safe harbor guidance.
- FBI Criminal Justice Information Services, CJIS Security Policy, Policy Area 10, Section 5.10.1.2 on encryption of CJI at rest.
- NIST SP 800-171 Rev. 3, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, controls 3.1.18 and 3.13.08.
- DoD CIO, Cybersecurity Maturity Model Certification (CMMC) Level 2 Assessment Guide.
- BleepingComputer, Windows BitLocker zero-day gives access to protected drives, PoC released. May 12, 2026.
- Reproduction notes from Will Dormann (Mastodon) and Kevin Beaumont (X), May 12-13, 2026.

8.0 ABOUT ASSURA

Assura, Inc. is a cybersecurity and compliance services firm serving regulated industries, including aviation, public sector, healthcare, and financial services. Our offerings include GRC-as-a-Service, managed security services, and offensive security. We help organizations make defensible security decisions and document them in ways that survive audit, incident, and litigation.

For more information, visit assurainc.com.