Outlook

Intune Endpoint Morning Briefing — August 25, 2026

From John Marcum <jmarcum@systemcenteradmin.com>
Date Tue 8/25/2026 11:21 AM
To John Marcum <jmarcum@systemcenteradmin.com>

Good morning John — here is your Intune endpoint morning briefing.

Scope: Current live **bi_for_intune** Power BI semantic model, observed August 25, 2026. The model contains 6 managed devices, including 5 managed Windows devices. App Inventory currently covers 4 of 6 managed devices (66.7%).
Overall posture: Yellow — core protection looks healthy where telemetry exists, but patch visibility, encryption/key escrow, stale-device handling, and data coverage need attention.

Executive Summary

- **Patch risk is concentrated:** SCA-2MQ5080YL7 is on Windows 11 25H2 build 26200.9106 versus Microsoft's current 26200.9168 build, and the model marks its quality update as **Not Latest**.
- **CM is the highest-priority investigation candidate:** it has not checked in for 61 days, has no Windows Update scan, is not enrolled in Update Compliance, is **Not Evaluated** for compliance, is not encrypted, and has 18 configuration profiles in an **Unknown** state.
- **Encryption and escrow require validation:** 3 of 5 managed Windows devices are reported as not encrypted, and all 5 Windows devices report **OS Recovery Key Stored = false**.
- **Security telemetry is positive but incomplete:** the 4 Windows devices with Defender and firewall data are **Clean**, onboarded to MDE, and firewall-enabled; CM has no corresponding protection or firewall record.
- **Application drift is actionable:** CPC-NGRZP is at least one verified Microsoft 365 Apps Current Channel release behind, while Teams versions are fragmented across three older documented builds.

Priority Endpoint Concerns

Confirmed findings

- **Compliance:** No managed device was returned as *Non Compliant*; 5 are Compliant and CM is Not Evaluated.
- **Stale check-in:** CM last checked in June 25, 2026 — 61 days ago.
- **Windows Update visibility:** CM and CPC-NGRZP have no Last WU Scan value; both are also not enrolled in Update Compliance. That is 2 of 5 Windows devices (40%).
- **Patch currency:** 1 of 5 Windows devices (20%) is marked Not Latest for quality updates. No Windows device is confirmed by the model as missing the latest security update.
- **Configuration profiles:** CM has 18 Unknown states, including Windows Defender AV, Windows BitLocker, Onboard to Defender, Update Compliance v2, SCA Endpoint Protection, Exploit Protection, and Windows Autopatch - Data Collection. CPC-NGRZP has Unknown states for risk management browser signal detection and UAC Settings.
- **App deployments:** No Failed, Uninstall Failed, or other actionable app deployment failure rows were returned; nonblank deployment states were Installed or Not Applicable.
- **Encryption and BitLocker:** CM, CPC-NGRZP, and CPC-UUC1D are reported Not Encrypted. All 5 Windows devices report that the OS recovery key is not stored.
- **Defender/firewall:** CPC-NGRZP, CPC-UUC1D, SCA-2MQ5080YL7, and SCA-F1698G3 are Clean, MDE-onboarded, tamper-protected, real-time protected, and firewall-enabled. CM lacks this telemetry.
- **Disk and restart health:** CM reports 0 GB total and 0 GB free, which is more likely incomplete telemetry than a confirmed full disk and should be validated. SCA-F1698G3 has a 32-day restart age.
- **Battery health:** SCA-F1698G3 reports 59.3% battery health; SCA-2MQ5080YL7 reports 85.8%.
- **Storage type:** All 4 devices with physical-disk telemetry report SSD and Healthy status; CM and the MacBook lack comparable physical-disk data.
- **User/device relationships:** CM has no primary user. No managed device has a populated sign-in-user relationship. Julien's MacBook Pro has a last-logon record 142 days old despite a current Intune check-in.
- **Risky users/sign-ins:** No risky-user or risky-sign-in rows were returned.

- **App reliability:** No app-crash rows were returned, but coverage could not be established, so this should not be interpreted as proof of zero crashes.

Windows Patch Risk – Top 10 Devices to Investigate

Microsoft baseline: Microsoft's August 11, 2026 B release lists Windows 11 25H2 at **26200.9168 (KB5121003)**, 24H2 at **26100.9168 (KB5121003)**, 23H2 at **22631.7517 (KB5120240)**, and 26H1 at **28000.2704 (KB5121000)**. Microsoft notes that 26H1 is for new devices and is not an in-place update for existing 24H2/25H2 devices. Source: Windows 11 release information.

Limitation: The live model contains only 5 managed Windows devices, so all 5 are ranked below rather than inventing a top 10. Managed-device WUfB state/sub-state/error rows were not returned, so ring and feature-update data are used where available.

Rank	Device / user / Intune ID	Current Windows version	Latest expected Microsoft build	Patch gap or concern	WU scan / update state	Recommended next action
1	**CM** Primary user: unavailable f6f81c75-4925-0a4b-0efd-b1bd7a37760f	10.0.17763.7314 Release ID, edition, channel, build and revision fields missing	Not determinable from the Windows 11 baseline	61-day stale check-in; no patch telemetry; not evaluated; not encrypted; 18 Unknown configurations; multiple risk categories	No scan date; not enrolled in Update Compliance; no current ring or feature-update state	Confirm whether the VM is active. If active, restore Intune/WU telemetry, evaluate compliance, remediate security profiles, and encrypt it; otherwise retire stale records.
2	**SCA-2MQ5080YL7** John Marcum 4c8ee5e1-3f57-4d57-ae32-c2461df85533	Windows 11 25H2 26200.9106	26200.9168 KB5121003	Quality update Not Latest; 62 build-revision points behind. Security update is marked Latest.	Scanned Aug. 23 (2 days); ring Compliant but ring status is 32 days old; feature update Success / Update Installed; no error or rollback returned	Validate KB5121003 applicability, check ring/deadline assignment, trigger scan/install, and confirm the device reaches 26200.9168.
3	**CPC-NGRZP** Tracie Blackmon fe5e8293-84c8-4b5b-a199-d04699bc1380	Windows 11 25H2 26200.9168	26200.9168 KB5121003	Build is current, but quality/security status fields are blank; not encrypted; update and user telemetry gaps	No WU scan; not enrolled in Update Compliance; update ring status Unknown; no feature-update state	Repair Update Compliance enrollment and scan reporting, validate update-ring assignment, then confirm BitLocker and recovery-key escrow.
4	**SCA-F1698G3** John Marcum 6a64c5e7-ba74-46d7-8475-828fc3785e20	Windows Insider 26220.7872	No GA comparison; Microsoft GA 25H2 is 26200.9168	Model marks updates Latest, but Insider builds are not directly comparable to GA servicing; also 32-day restart age, 59.3% battery health, and no recovery-key escrow	Scanned Aug. 23 (2 days); ring Compliant on Aug. 25; feature update Success / Update Installed; no error or rollback returned	Confirm Insider enrollment is intentional and policy-approved; schedule a restart and assess battery replacement planning.
5	**CPC-UUC1D** Julien Moreau 8ca88aca-8220-4343-ba18-5b497ffb53c4	Windows 11 25H2 26200.9168	26200.9168 KB5121003	Patch-current; lower patch risk. Other concerns are missing encryption, recovery-key escrow, and sign-in-user data.	Scanned Aug. 23 (2 days); Update Compliance enrolled; ring Compliant on Aug. 20; no error, rollback, or on-hold state returned	Keep patch posture under normal monitoring; prioritize BitLocker/escrow and identity telemetry remediation.

Application Version Watchlist

Coverage note: The table uses current managed-device mappings for the 4 devices enrolled in App Inventory. Historical/orphan inventory rows were excluded where they could not be tied to a current managed device.

Application	Publisher	Most common installed version	Other versions found	Newer verified version	Impact	Why it matters / recommended Intune action
Microsoft 365 Apps for enterprise	Microsoft Corporation	16.0.20326.20100 on 3 devices	16.0.20228.20124 on CPC-NGRZP	16.0.20326.20100, Current Channel, released Aug. 18, 2026	1 of 4 covered devices (25%) is at least one verified release behind	Productivity and security update currency. The model also marks CPC-NGRZP Outdated. **Action: Create detection/remediation script** after confirming the intended channel. Source: Microsoft 365 Apps update history.
Microsoft Edge	Microsoft Corporation	151.0.4129.101 on 3 devices	151.0.4129.107 on 1 device	Latest documented Stable build is 151.0.4129.101, released Aug. 20, 2026	0 confirmed behind; one device reports a numerically higher build not yet listed on the retrieved official page	Browser security is current on the documented baseline. Do not downgrade the higher build. **Action: No action needed**. Source: Microsoft Edge Stable release notes.
Microsoft OneDrive	Microsoft Corporation	26.150.0804.0011 on 3 devices	26.145.0728.0011 on CPC-NGRZP	Official page lists 26.145.0728.0011 as Production and 26.150.0804.0010 as rolling out	0 confirmed behind; three devices report a build one revision higher than the published rolling build	Both observed branches are consistent with current or rolling Production-ring servicing. **Action: No action needed**. Source: OneDrive Sync release notes.
Microsoft Teams	Microsoft	No single dominant version: 26183.1903.4892.4448, 26163.405.4842.717, and 26149.1205.4798.6437 on one current device each	Legacy MicrosoftTeams 23091.406.2009.3890 also appears on SCA-F1698G3	26213.1006.5014.9784, released Aug. 20, 2026	3 of 4 covered devices have Teams and all three new-client records are older than the newest documented build	Teams uses staged auto-update, and Microsoft says the version page is historical rather than a deployment-status report. Watch for persistent lag and validate legacy-client cleanup. **Action: Monitor only**. Source: Teams app version history.
Dell SupportAssist for PCs	Dell	4.6.2.0 on SCA-F1698G3	None found	Needs manual verification; Dell's official overview did not expose a current version number	1 of 4 covered devices (25%)	OEM support tools have broad device access and should have an owner and update path. **Action: Manual verification needed**. Source: Dell SupportAssist.
Claude	Publisher not populated	1.15200.0.0 on SCA-2MQ5080YL7	None found	Not compared	1 of 4 covered	The inventory record was not matched to a named managed

	devices (25%)	Application entry returned by the model. Validate business need, data handling, and ownership. **Action: Investigate unmanaged/shadow IT usage**.

No current managed-device App Inventory rows were returned for Google Chrome, Adobe Reader/Acrobat, Zoom, 7-Zip, WinRAR, Java, or VPN clients. Because App Inventory covers only 4 of 6 managed devices, this is not proof that those applications are absent.

Watchlist

- **CM:** repeat offender across stale check-in, missing WU scan, Update Compliance enrollment, compliance evaluation, encryption, security telemetry, disk telemetry, primary-user mapping, and 18 Unknown configuration profiles.
- **CPC-NGRZP:** current OS build but missing WU scan/status, not enrolled in Update Compliance, update ring Unknown, not encrypted, recovery key not stored, Microsoft 365 Apps outdated, and two Unknown configurations.
- **SCA-2MQ5080YL7:** the only confirmed Windows 11 quality-update laggard; recovery key also reports not stored.
- **SCA-F1698G3:** Windows Insider channel, 32-day restart age, 59.3% battery health, legacy Teams footprint, and no recorded recovery-key escrow.
- **Policy-state hygiene:** update-ring or feature-update records exist for unmanaged devices CPC-DCR1K, CPC-S31CH, and SCA-FK2WZT3, each with no Intune Device ID in the current Device inventory.
- **Telemetry coverage:** sign-in-user mapping is absent for all managed devices; app reliability returned no crash rows; App Inventory covers only 4 of 6 managed devices.

KPI Report Improvements

Suggested improvements

- Add a **Windows patch currency by OS release** visual that compares current build/revision with Microsoft's latest published B-release build and shows source date/KB.
- Add a **Top patch-lagging devices** score combining support status, security/quality currency, WU scan age, Update Compliance enrollment, update errors, compliance, encryption, and check-in age.
- Add a **telemetry coverage panel**: WU scan coverage, Update Compliance coverage, Defender/firewall coverage, App Inventory coverage, device-detail coverage, sign-in-user coverage, and app-reliability coverage.
- Separate **encryption status** from **BitLocker recovery-key escrow**; show exceptions by device and whether the source is Intune, Entra ID, or another system.
- Add **configuration profile success/failure/unknown rate** with last-status age and a drill-through to device and policy name.
- Add **update failure reasons, rollback, on-hold, error codes, and restart-required age** by current managed device.
- Add **restart age, low-disk, battery-health, and SSD/HDD exception counts** with threshold definitions visible in the report.
- Add **high-volume app version drift** with official-source version, source date, installed-version distribution, channel, and managed/unmanaged status.
- Add a **repeat offender heatmap** to identify devices appearing in multiple risk categories.
- Exclude or clearly label **unmanaged/orphaned policy-state rows** so old device records do not inflate active endpoint KPIs.

Suggested Follow-Up Actions

- **Tier 2:** Take ownership of CM. Confirm active/decommissioned status, restore check-in and Windows Update telemetry if active, and investigate its 18 Unknown policy states.
- **Tier 2:** Validate and remediate SCA-2MQ5080YL7 to Windows 11 25H2 build 26200.9168 / KB5121003.
- **Service Desk:** Confirm whether SCA-F1698G3 should remain in Windows Insider, schedule a restart, and assess the 59.3% battery-health reading.
- **Endpoint engineering:** Repair Update Compliance enrollment and WU scan reporting on CPC-NGRZP; validate its update-ring assignment and Microsoft 365 update channel.
- **Security:** Validate BitLocker state and recovery-key escrow for all 5 Windows devices, starting with CM, CPC-NGRZP, and CPC-UUC1D.

- **Application management:** Monitor Teams auto-update drift, remediate CPC-NGRZP's Microsoft 365 Apps lag, verify Dell SupportAssist ownership/version, and review the unmanaged Claude installation.
- **PowerStacks:** Review missing managed-device WUfB detail, sign-in-user coverage, app-reliability coverage, the Microsoft 365 latest-version mismatch, and orphaned update-policy records.

Leadership-Friendly Summary

The environment is generally stable where endpoint telemetry is complete: most Windows 11 devices are on the current Microsoft build, and reported Defender and firewall posture is healthy. The main risks are concentrated in a stale device with broad visibility gaps, one confirmed Windows quality-update laggard, incomplete BitLocker/recovery-key reporting, and uneven application/update telemetry. Today's priority should be to resolve those named exceptions and improve reporting coverage so the team can move from reactive investigation to consistently proactive endpoint management.

Questions I Should Ask

1. Is CM still an active production device, or should it and its associated policy-state records be retired?
2. Why are CM and CPC-NGRZP missing Windows Update scan data and Update Compliance enrollment — policy assignment, inactivity, agent health, or data-model ingestion?
3. Is Windows Insider enrollment on SCA-F1698G3 intentional and approved for this user/device role?
4. Should every managed Windows device have BitLocker enabled and a recovery key escrowed, and is the PowerStacks recovery-key field mapped to the authoritative source?
5. Which applications should be formally managed or allowlisted through Intune, and should App Inventory and app-reliability coverage be expanded to all managed devices?

Potential KPI Gaps

Missing metric	Why it would be useful	Suggested source or next step
Managed-device WUfB state, sub-state, error, rollback, on-hold, and restart-required detail	Separates policy delay, device inactivity, user deferral, and technical failure	Validate Update Compliance State relationships and ingestion with PowerStacks
App reliability enrollment/coverage and crash trend	Avoids interpreting an empty crash table as zero crashes	Expose Endpoint Analytics/App Reliability coverage and last refresh
Sign-in-user and risky-sign-in coverage by managed device	Supports user/device mismatch, stale ownership, and identity-risk investigation	Review Entra sign-in and User Devices joins; publish coverage percentage
Authoritative BitLocker key-escrow status and exception reason	Distinguishes true escrow failures from source/mapping gaps	Cross-check Intune encryption report and Entra recovery-key inventory
App Inventory coverage for all managed devices and authoritative latest-version feed	Makes version-drift and shadow-IT percentages reliable	Add enrollment/last-refresh KPIs and curated Microsoft/vendor version sources
Complete OS release ID, edition, servicing channel, build, and lifecycle mapping for CM	Enables exact support and patch comparison instead of a visibility-only risk flag	Repair device inventory ingestion or retire the stale device record

Source note: Confirmed endpoint findings come from the live **bi_for_intune** Power BI semantic model and related **bi_for_intune** Power BI report. Public version comparisons use Microsoft Learn and Dell's official support site linked above. Suggested improvements are recommendations, not confirmed current-state metrics.

Recommended Focus for Today

1. **Resolve CM's status:** active remediation or formal retirement.
2. **Patch SCA-2MQ5080YL7** to Windows 11 25H2 build 26200.9168 / KB5121003 and refresh its ring status.
3. **Validate BitLocker and recovery-key escrow** across all Windows devices, prioritizing the three reported Not Encrypted.
4. **Restore CPC-NGRZP visibility and currency:** WU scan, Update Compliance, update-ring status, encryption, and Microsoft 365 Apps.
5. **Raise PowerStacks data gaps** for WUfB detail, sign-in-user coverage, app reliability, App Inventory coverage, and orphaned policy-state rows.

Sent by Copilot Cowork