Macs: are they as locked down as your Windows PCs?

This quarter, enroll every company Mac through Apple Business with locked enrollment, enforce macOS updates with a 7-day deadline and give users standard accounts with FileVault keys escrowed. Then push your EDR's extensions and permissions so users can't remove them, and judge the rest by whether it would stop a pasted Terminal command.

Reviewed	Next review	Version	Written for	Latest version
5 Nov 2026	**5 Dec 2026**	**1.0**	**IT and security teams managing company Macs with Intune, Jamf or another MDM**	**sheets.einblick.dev/macos/**

If you only do five things

1. **Enroll every Mac through Apple Business, locked.** Buy from Apple or an authorized reseller so the serial number lands in Apple Business, free since April 2026[1]. Set **Locked enrollment**[2]; a registered Mac on macOS 14+ can put off enrollment only once, for 8 hours[3].
2. **Enforce updates with a deadline.** Use declarative update enforcement: in Intune, **Software Update Enforce Latest** with **Delay in Days** at 7[5]. When Apple says a flaw may have been exploited, enforce that version within 72 hours, as the browsers sheet does. Pilot major upgrades first.
3. **Give users standard accounts.** Let enrollment create a hidden admin and a standard user. Intune's macOS LAPS gives the admin a 15-character password, rotates it every 6 months and audits each view[11].
4. **Turn on FileVault in Setup Assistant.** Set **Force Enable in Setup Assistant** with **Defer** enabled (macOS 14+), so Intune escrows the key before encryption starts[15]. The BSI says the key must not be stored online with Apple[31].
5. **Run EDR with permissions users can't undo.** Preapprove Defender's system extensions and permissions with MDM profiles[17], and set tamper protection as the endpoints and email sheet says. Set `AllowUserOverrides` to false and list the EDR in `NonRemovableSystemExtensions` (macOS 15+)[18].

Set up a new Mac in this order

1. **Is the serial number in Apple Business?** If not, erase the Mac and add it with Apple Configurator for iPhone. The user can still release it within 30 days of enrollment[4].
2. **Does setup wait for your policies?** Turn on **Await final configuration**[2] and require a minimum macOS version, so Setup Assistant updates the Mac first[3].
3. **How do users sign in?** Use Platform SSO with the Secure Enclave method: Microsoft counts it as phishing-resistant, and every Intune plan includes it[12]. Since macOS 26, MDM can enforce it in Setup Assistant[8]. Okta offers it through Okta Device Access[14].
4. **Which permissions does each tool need?** Grant Full Disk Access (**System Policy All Files**) with privacy profiles (PPPC); MDM can only deny camera, microphone and screen recording[19]. macOS 27 lets users revoke Accessibility that MDM granted[7].
5. **Does access depend on compliance?** Require System Integrity Protection, encryption, Gatekeeper at **Mac App Store and identified developers** and a minimum OS build[16]. Then require a compliant device (passkeys and MFA sheet).

Versions and updates in November 2026

- **Three versions still get fixes.** On 26 October 2026, Apple patched macOS 27.2, Tahoe 26.7.2 and Sequoia 15.8.2; Sonoma's last OS fix came on 6 August[9]. Older versions don't get every fix[10], so set an end date for Sequoia.
- **Intel Macs can't move to macOS 27.** It runs only on Apple silicon[9]. Budget replacements now: the BSI says Macs without security updates shouldn't be used[31].
- **Keep security data updates on.** Force automatic security updates, which carry XProtect and Gatekeeper data. Background Security Improvements apply only to the latest minor version, so a deferral delays them too[6].
- **Warn users about the deadline.** When it passes, macOS quits open apps, even with unsaved documents, and restarts if needed[6]. Announce the date a week ahead.

How Macs get infected now

- **Atomic macOS Stealer leads.** Of the top five stealer families Microsoft Defender Experts saw, it had 50% of the activity, MacSync 7%. Mac-targeted activity has grown since late 2025[21].
- **Pasted commands skip Gatekeeper.** Fake troubleshooting guides have users paste a Terminal command that fetches a script with curl. Scripts started from Terminal don't get the checks Gatekeeper runs on apps opened in Finder[22].
- **Standard accounts don't stop them.** The stealer asks for the user's password, then takes Keychain entries, browser passwords, session cookies and wallets[22]. See the browsers sheet on cookie theft.
- **The paste warning is a speed bump.** It appears only when someone who rarely uses Terminal pastes a command from a website, chat or email, and they can choose Paste Anyway[23].
- **Gatekeeper overrides moved.** Since Sequoia, users allow unnotarized apps in Privacy & Security, not with Control-click[24]. On macOS 15+, Endpoint Security tools can log each bypass[25].

When a Mac is lost or compromised

- **Lost: lock it.** A remote lock restarts the Mac and asks for a six-digit PIN. Managed Lost Mode, with location, is only for iPhone and iPad[26].
- **Compromised: isolate it.** Isolate it in Defender[17] and follow the incident response sheet. Assume the Keychain, browser passwords and cookies are stolen[22], and reset them.

Mistakes that cost the most

- **Letting the first user be admin.** Without a managed admin account, the Setup Assistant account must be one[11].
- **Counting on that admin for FileVault.** Intune's LAPS admin gets no secure token[11]; keep the escrowed key.

- **Erase and re-enroll.** MDM erase uses Erase All Content and Settings; on Apple silicon it needs a bootstrap token[27]. Rotate a FileVault key or admin password after anyone views it[15,11].
- **Keep Activation Lock in your hands.** Leave it off unless MDM holds the bypass code, via **Activation Lock Allowed While Supervised**[29]. Apple Business can lift a user's lock on Macs added before it was on[30].
- **Requiring a password in a compliance policy.** It expires every password on the Mac, LAPS and Platform SSO accounts included[16].
- **Exempting developers.** Mac stealer campaigns aim at cloud and developer environments[21].
- **Wiping before copying the bypass code.** Intune deletes it at reset[29]. Add the step to the laptop return in the joiners and leavers sheet.

What changed in 2026

- **Apple Business replaced Apple Business Manager.** Since 14 April 2026, it is free and includes a built-in MDM[1].
- **macOS 27 dropped Intel and legacy update management.** Since 14 September 2026, it runs only on Apple silicon[9] and ignores MDM update commands[7].
- **macOS 27 can block binaries.** Supervised Macs can enforce allow or deny lists through a built-in Endpoint Security client[20].
- **Intune ended legacy Setup Assistant authentication.** Since October 2026, profiles use modern authentication[2]; test it now.

What you can skip

- **A second antivirus beside the EDR.** Defender for Endpoint on Mac includes antivirus[17], on top of XProtect's signatures[25].
- **Binding Macs to Active Directory.** Platform SSO can map on-premises Kerberos tickets from Entra ID[13].
- **Blocking Terminal for everyone.** Developers and IT need it. EDR and binary control cover the risk better.
- **BSI steps older than Apple silicon.** SYS.2.4 asks for NVRAM and SMC resets and a firmware password[31]. On Apple silicon, erasing makes data cryptographically inaccessible[27] and FileVault replaces the password[28].

What this looks like at your size

Small team, no security staff

- Without Intune or Jamf, start with Apple Business's free built-in MDM[1].
- Run Defender for Business on every Mac, as the endpoints and email sheet says.
- Ask your reseller to register every Mac in Apple Business.

Growing, with IT or security staff

- Grant admin rights for minutes, with a reason: Jamf Connect's Self Service+ defaults to 5[33]; SAP's Privileges is open source[34].
- Report weekly per Mac: macOS version, escrowed key, EDR health.
- Switch MDM without a wipe: Apple Business migrates macOS 26 Macs[8].

Enterprise or regulated

- Generate a CIS Level 1 baseline and MDM profiles with NIST's mSCP, updated for each macOS release[32].
- Pilot binary allow lists for admins and finance.
- Map your profiles to BSI SYS.2.4 for audits[31].

Version history

5 Nov 2026, version 1.0 Published after a copy edit and a source-by-source fact check, which aligned the update deadline for exploited flaws with the browsers sheet, scoped Microsoft's stealer figures and the paste warning to what the sources say and narrowed the Intune enrollment change to authentication.

Sources

1. Introducing Apple Business. Apple Newsroom, 24 Mar 2026. apple.com
2. Set up ADE for macOS. Microsoft Learn, 28 Oct 2026. learn.microsoft.com
3. Automated enrollment. Apple Support, 17 Sep 2026. support.apple.com
4. Apple Configurator. Apple Support, 14 Apr 2026. support.apple.com
5. Apple update policies. Microsoft Learn, 24 Feb 2026. learn.microsoft.com
6. Enforce software updates. Apple Support, 24 Sep 2025. support.apple.com
7. macOS 27 for enterprise. Apple Support, 26 Oct 2026. support.apple.com
8. macOS 26 for enterprise. Apple Support, 27 Jul 2026. support.apple.com
9. Apple security releases. Apple Support, 30 Oct 2026. support.apple.com
10. About software updates. Apple Support, 3 Nov 2026. support.apple.com
11. macOS LAPS in Intune. Microsoft Learn, 1 Apr 2026. learn.microsoft.com
12. Platform SSO setup. Microsoft Learn, 22 Jun 2026. learn.microsoft.com
13. Platform SSO scenarios. Microsoft Learn, 11 May 2026. learn.microsoft.com
14. Platform SSO for macOS. Okta Help, checked 5 Nov 2026. help.okta.com
15. FileVault with Intune. Microsoft Learn, 3 Dec 2025. learn.microsoft.com
16. macOS compliance. Microsoft Learn, 5 Sep 2025. learn.microsoft.com
17. Defender on macOS. Microsoft Learn, 18 Sep 2026. learn.microsoft.com
18. SystemExtensions. Apple Developer, checked 5 Nov 2026. developer.apple.com
19. PPPC payload settings. Apple Support, 29 Jul 2024. support.apple.com
20. Allow and deny binaries. Apple Support, 17 Sep 2026. support.apple.com
21. Microsoft Digital Defense Report 2026. Microsoft Threat Intelligence, Oct 2026. cdn-dynmedia-1.microsoft.com
22. ClickFix campaign uses fake macOS utilities lures. Microsoft Defender Security Research Team, 6 May 2026. microsoft.com
23. Terminal paste blocked. Apple Support, 15 Jun 2026. support.apple.com
24. Runtime protection in macOS Sequoia. Apple Developer, 6 Aug 2024. developer.apple.com
25. macOS malware protection. Apple Support, 19 Dec 2024. support.apple.com
26. Lock and locate devices. Apple Support, 27 Oct 2021. support.apple.com
27. Erase Apple devices. Apple Support, 25 Oct 2023. support.apple.com
28. Set a firmware password on your Mac. Apple Support, 22 Jun 2026. support.apple.com
29. Disable Activation Lock. Microsoft Learn, 27 Oct 2025. learn.microsoft.com
30. Turn off Activation Lock. Apple Support, 14 Apr 2026. support.apple.com
31. SYS.2.4 Clients unter macOS. BSI, Edition 2023. bsi.bund.de
32. mSCP introduction. NIST, checked 5 Nov 2026. pages.nist.gov
33. Privilege Elevation Settings. Jamf, checked 5 Nov 2026. learn.jamf.com
34. Privileges. SAP (GitHub), checked 5 Nov 2026. github.com