POSTREMO IT

NOVEMBER 2026 EDITION

Choosing an MDM in 2026: a buyer's guide for UK organisations

A practical decision toolkit for comparing Jamf, Microsoft Intune, Iru, Omnissa Workspace ONE and JumpCloud: comparison tables, a requirements worksheet, questions for vendors, a licensing map and migration notes.

BEFORE YOU START

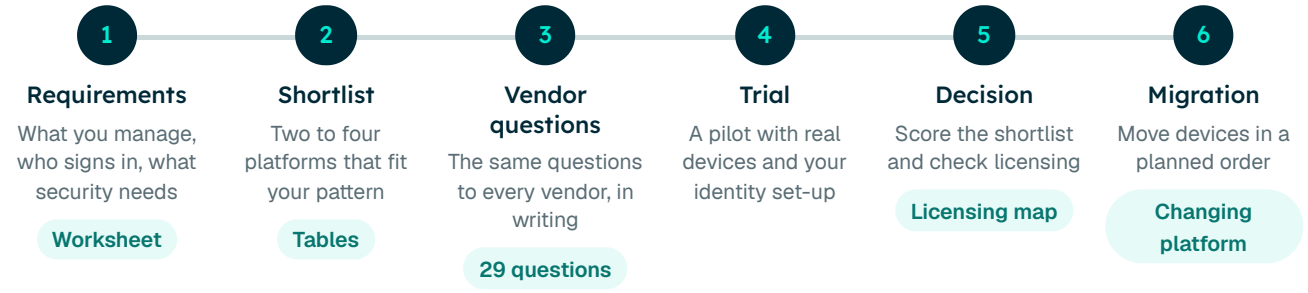
How to use this guide

A toolkit for making the decision: tables, a worksheet, vendor questions and a licensing map. Our web article at postremoit.com/insights/choosing-an-mdm/ explains each platform in more depth.

DIAGRAM 1

How a selection usually runs

Where each part of this guide fits.



Disclosure

We are a Jamf partner and we also deliver Microsoft Intune. This guide uses vendor documentation and third-party sources, checked in November 2026.

Vendor marketing claims are attributed (for example “Jamf says”) and announced features are labelled. No prices, vendor scores or analyst rankings.

All five products change often, so confirm current details with each vendor before you decide.

What is inside

01 Cover 1
02 How to use this guide 2
03 The five platforms in brief 3
04 Comparison tables 5
05 Requirements worksheet 10
06 Questions to ask each vendor 11
07 Licensing map 12
08 Changing platform 13
09 Sources 14
10 How we help 16

SECTION 3

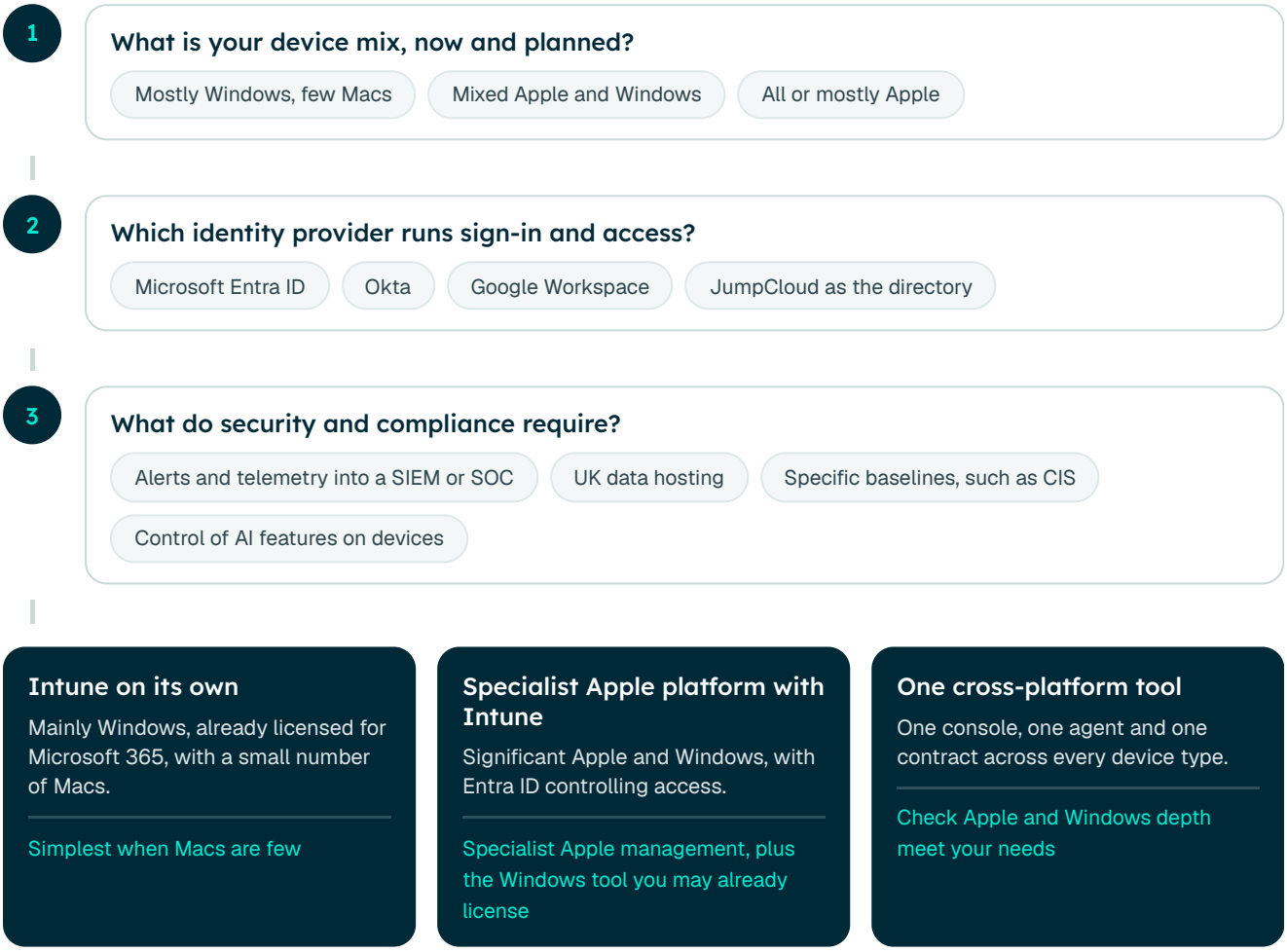
The five platforms in brief

They start from different places: some around Apple, some around Windows and Microsoft 365, and one around identity. Start with the pattern, then the platform.

DIAGRAM 2

Which pattern fits your estate?

A starting point, not a verdict. It points to a pattern; the rest of the guide helps you pick the platform within it.



The comparison tables show how each platform fits these patterns.

Jamf APPLE-FOCUSED

Jamf focuses on Apple; Francisco Partners completed its acquisition on 30 January 2026, taking it private. Jamf for Mac and Jamf for Mobile are both powered by Jamf Pro, Jamf Connect and Jamf Protect. Blueprints bring declarative device management, Compliance Benchmarks include CIS and NIST 800-53 templates with a compliance score, and Jamf Pro is an Intune compliance partner. Jamf Cloud has London and Frankfurt regions.

To weigh up: Jamf does not manage Windows, so mixed estates pair it with a Windows tool. If you host Jamf Pro yourself, check Jamf's current Blueprints requirements.

Microsoft Intune WINDOWS AND MICROSOFT 365

Microsoft's cloud endpoint management service for Windows, macOS, iOS, iPadOS, Android, Linux and ChromeOS. Intune Plan 1 is included in Microsoft 365 Business Premium, E3 and E5, licensed per user. Autopilot, Autopatch and co-management cover Windows, and other MDMs report compliance into Intune for Entra Conditional Access.

To weigh up: no blanket same-day promise for Apple; Microsoft reported day-zero support for OS 27 AI settings and adds other items in monthly releases. Intune supports the three most recent Apple versions and has no UK geography.

Iru (formerly Kandji) APPLE-FIRST, CROSS-PLATFORM

Kandji rebranded as Iru on 22 October 2025 and added Windows and Android; Iru says “Apple remains the foundation, with a dedicated Apple team”. It fits Apple-first organisations that also want Windows and Android in the same tool. Iru documents Managed OS, Auto Apps and Platform SSO with Entra ID, is an Intune compliance partner, and offers EDR and vulnerability management for Mac and Windows.

To weigh up: Windows and Android arrived in October 2025, so check the Windows features you need; Autopilot needs Entra ID and Microsoft licensing. Kandji tenants must upgrade by 1 December 2026. We found no UK region.

Omnissa Workspace ONE BROAD DEVICE COVERAGE

The former VMware End-User Computing business, independent since KKR completed its purchase from Broadcom on 1 July 2024. Workspace ONE UEM covers Windows and Windows Server, macOS, iOS, Android, Linux, ChromeOS and rugged devices. Omnissa claims day-zero support for new Apple releases. The SaaS service has a UK region, and it is an Intune compliance partner.

To weigh up: features sit across editions, with vulnerability management and remote support in Platinum. Autopilot needs Entra ID and Microsoft licensing (Entra ID P1).

JumpCloud IDENTITY-LED

A privately held company in Louisville, Colorado, that describes itself as a unified IT management platform: directory, SSO, MFA and device management together. Its agent covers macOS, Windows and Linux, with iOS, iPadOS and Android through native MDM, and it offers DDM-based macOS update policies. New EU customers can choose hosting in Frankfurt.

To weigh up: JumpCloud is not a listed Intune compliance partner and says its conditional access uses its own policies. There is no UK region.

SECTION 4

Comparison tables

DIAGRAM 3

Specialist or broad?

Two ways to approach device management. Neither is better in itself; the right one depends on your estate.

Apple specialist

Built specifically for Mac, iPhone and iPad

Jamf

- Apple management, identity and security in one plan
- Pairs with Intune for Windows, sharing compliance through Entra
- Suits all-Apple estates and Apple-heavy mixed estates

Cross-platform

One tool across several device types

Microsoft Intune

Omnissa Workspace ONE

JumpCloud

Iru
Apple-first, Windows since 2025

- One console across Apple, Windows and more
- Depth varies by platform: check what you need
- Suits estates that want a single tool

Identity providers

Capability	Jamf	Intune	Iru	Workspace ONE	JumpCloud
Platform SSO identity providers documented	Entra ID, Okta	Entra ID; Okta publishes an Intune guide	Entra ID, Okta (Okta item labelled Early Access by Iru)	Omnissa Access, Entra ID, Okta	Deploys another provider's extension
Platform SSO in Setup Assistant (macOS 26)	Yes, Simplified Setup	Yes, Entra ID only	Documented for Okta	Yes, with Access, Entra ID or Okta	Not found in the documents we checked
Mac sign-in tool	Jamf Connect: Entra ID, Okta, Google and others	Platform SSO	Passport: Google, Entra ID, Okta, OneLogin and other OIDC providers	Platform SSO, including with Omnissa Access	JumpCloud agent with JumpCloud credentials
Sign-in during enrolment	SAML providers, with guides for Okta and Google	Entra ID	Custom SAML, Google, Entra ID	Access, Entra ID or Okta, with Platform SSO	JumpCloud
Entra Conditional Access	Compliance partner	Native	Compliance partner	Compliance partner	Not listed; own access policies
Okta device trust	Regularly tested by Okta	Regularly tested by Okta	Iru documents an Okta integration	Regularly tested by Okta	Desktop device trust factor for Okta
Google context-aware access partner	Yes	Desktop devices only	Not listed by Google	Yes	Not listed by Google

On a Mac, the MDM delivers the Platform SSO configuration and the identity provider supplies the extension, which must support each feature you use. Managed Apple Accounts are federated in Apple Business, not the MDM.

At a glance

Area	Jamf	Intune	Iru	Workspace ONE	JumpCloud
Platforms managed	macOS, iOS, iPadOS, tvOS, watchOS, visionOS and Android. No Windows.	Windows, macOS, iOS, iPadOS, Android, Linux and ChromeOS	Apple, Windows and Android	Windows and Windows Server, macOS, iOS, iPadOS, Android, Linux, ChromeOS, rugged devices; tvOS and visionOS for specialised use (Omnissa says)	macOS, Windows and Linux by agent; iOS, iPadOS and Android by MDM
New Apple releases	Jamf says same-day; ask what it covers	No blanket same-day promise; Microsoft reported day-zero support for OS 27 AI settings, other items in monthly releases	Iru added iOS, iPadOS and tvOS 27 Managed OS support on release day; ask what it covers	Omnissa says day-zero; no OS 27 post found; ask what it covers	JumpCloud says Day 0; ask what it covers
Declarative device management	Yes, through Blueprints	Yes, DDM update policies	Yes, Managed OS	Omnissa says DDM is core	Yes, DDM patch policies
Platform SSO with Entra ID	Documented	Documented, in all plans	Documented	Documented	Not found in the documents we checked
Windows	Not offered	Autopilot, Autopatch, co-management	Microsoft MDM framework plus Iru Agent; Autopilot (needs Entra ID and Microsoft licensing)	Autopilot (needs Entra ID and Microsoft licensing), Windows Update for Business	Agent on Windows 10, 11 and Server
Entra compliance partner	Yes	Native	Yes	Yes	Not listed; own access policies
Security add-ons	Jamf Protect and Jamf Connect, in the Jamf plans	Intune Suite tools, such as Endpoint Privilege Management	EDR and vulnerability management (Mac and Windows)	Vulnerability management and remote support (Platinum)	Identity (directory, SSO, MFA); partner EDR
Hosting and data region	Jamf Cloud, with London and Frankfurt regions	Cloud; Europe geography, no UK geography	Cloud; EU tenant region, location not stated	SaaS with a UK region	US by default; EU (Frankfurt) for new customers
Licensing	Per device, annual, 25-device minimum	Per user, included in Microsoft 365 Business Premium, E3 and E5	Quote-based, on users and devices	Per device or per user, annual, in editions	Per user, in packages

“Same-day” and “day-zero” mean different things to each vendor, so ask what each covers. Partner compliance reaches Entra ID for Android, iOS, iPadOS and macOS, not Windows.

AI governance and admin AI

Every MDM here documents Apple Intelligence controls. Jamf added Apple Intelligence settings to Blueprints in April 2026 and offers Jamf AI Governance for Mac; Intune and Iru document the OS 27 additions. Apple uses a separate switch for each feature, needing OS 26.4 or later and supervision, so personal devices in User Enrolment cannot receive them. On Windows, Recall is disabled and removed by default on commercially managed devices, Microsoft recommends AppLocker for the Copilot app, and several controls need Enterprise or Education rather than Pro. The table compares each vendor's admin AI assistant.

Area	Jamf	Intune	Iru	Workspace ONE	JumpCloud
Default state	Off by default	Available once Security Copilot is provisioned, automatically for eligible E5 and E7 tenants; not included in E3 or Business Premium	On by default; Account Owners can turn it off, though some compliance features can still use it	Default state not stated in the documents we checked	Off by default; opt-in
Can it make changes?	No, read-only, under the admin's own permissions	Follows Intune roles and scope tags; agents need admin approval	An Actions agent runs actions the admin authorises, logged in Activity	Not stated; tools include Knowledge Search and Data Analysis; its MCP server is limited by admin role	Yes, after asking for approval; mirrors the admin role (FAQ says public preview)
Model provider	Anthropic Claude through AWS Bedrock	Azure OpenAI	Not named in Iru's documentation	Azure OpenAI	Google Gemini, per JumpCloud's AI docs (its sub-processor list also names OpenAI)
Processing location	Jamf says US, Frankfurt or Tokyo, by customer region; London-hosted instances: not stated	Outside the EU Data Boundary; UK tenants' prompts processed globally (US, UK, EU, ANZ) by default	Not stated	Knowledge Search for UK customers hosted in Ireland	Not stated
Training and retention	Jamf says data is not used to train Anthropic's models; conversations deleted after 30 days	Microsoft says customer data is not used to train Azure OpenAI foundation models	Iru says conversations are not used to train models	LLM vendors barred from training on customer content; Omnissa uses feedback and usage data to improve Omni; kept 90 days	JumpCloud says customer data is not used to train LLMs

None of the five documents UK-only processing for its admin AI; for public sector, defence-related or DIFC-regulated work, get locations in writing. Jamf has announced Mac DLP and browser AI governance for the fourth quarter of 2026 (roadmap, not yet available); Omnissa says Elara, in beta, will govern AI tools.

Security, SIEM and telemetry

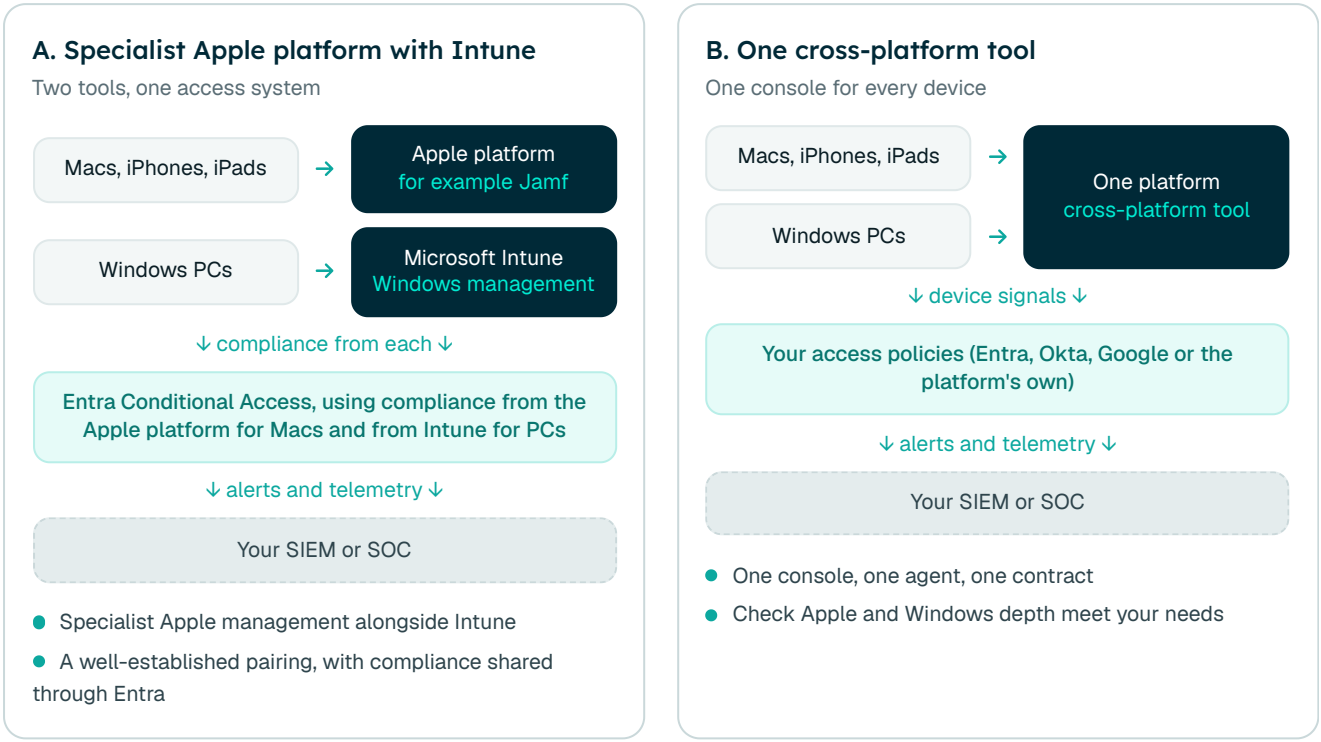
Area	Jamf	Intune	Iru	Workspace ONE	JumpCloud
Endpoint protection	Jamf Protect: Mac and mobile; built on Apple's Endpoint Security API	Defender for Endpoint: Windows, macOS, Linux, Android, iOS; Defender for Business in Business Premium	Iru EDR: Mac and Windows (Windows detection only)	Partner EDR such as Carbon Black through Omnissa Trust Network; Mobile Threat Defense (Lookout) for mobile	Partner EDR such as CrowdStrike and SentinelOne
Vulnerability management	Jamf says Protect reports CVEs for out-of-date OS versions	Defender Vulnerability Management, all major platforms (core in Defender for Endpoint Plan 2)	Mac and Windows, with automatic remediation through Auto Apps	Omnissa Intelligence dashboards for Windows and macOS (Platinum)	Patch management for OS updates and Chrome
macOS compliance baselines	Compliance Benchmarks built in: CIS Level 1 and 2, NIST 800-53 Rev 5 Low, Moderate and High (mSCP), with a compliance score	Security baselines are for Windows, including STIG audit baselines	CIS Level 1 and 2 templates	mSCP tutorial (NIST, STIG, CIS)	Not found in the documents we checked
Microsoft Sentinel	Jamf-supported connector: alerts, telemetry, unified logs	Native	Not in Microsoft's connector list	Microsoft-supported connector: inventory and apps	Not in Microsoft's connector list
Other SIEMs	Jamf add-on for Splunk; Elastic; Google SecOps; direct from the Mac by HTTP, syslog or Kafka	Event Hubs to Splunk, QRadar or Elastic	Hourly Amazon S3 export; Elastic (preview, audit and inventory); Datadog and Panther (their integrations)	Syslog in real time; Google SecOps; Lookout connector for mobile threats	Events API (Premium); Elastic
Admin audit log export	Log Stream to Splunk, S3, Datadog or HTTPS (Jamf Cloud Premium)	Event Hubs, Storage or Log Analytics; two years through Graph	Hourly to Amazon S3	Syslog, in real time	90 days as standard; 13 months through the Events API (Premium)
APIs and events	Jamf Pro API; webhooks for 22 event types	Microsoft Graph	Scoped API tokens; MCP server	REST APIs; event notifications	Directory Insights and System Insights APIs

Workspace ONE and JumpCloud work with partner EDR, and Microsoft's Sentinel connector for Workspace ONE carries inventory, not audit events. Check editions: Jamf states Log Stream is on Jamf Cloud Premium, JumpCloud's 13-month Events API needs Directory Insights Premium, and Omnissa's vulnerability management is in Platinum.

DIAGRAM 4

Two common patterns for mixed estates

Both are well supported. The difference is where Apple management lives and how many tools you run.



Estate fit

How each platform tends to fit, based on the documented capabilities above.

Platform	Apple-only estate	Windows-only estate	Mixed estate
Jamf	Built around Apple: Blueprints, Compliance Benchmarks, Jamf Connect and Jamf Protect	Not applicable; Jamf does not manage Windows	The Apple side of a paired set-up, reporting compliance to Intune for Entra Conditional Access
Microsoft Intune	Suits Apple estates already licensed for Microsoft 365 and using Entra ID	Autopilot, Autopatch and co-management, often already licensed through Microsoft 365	One console for everything, or the Windows side alongside a specialist Apple platform
Iru	Apple-first, now also cross-platform, with Managed OS and Auto Apps	Windows management since October 2025, using Microsoft's MDM framework plus the Iru Agent, with Autopilot (needs Entra ID and Microsoft licensing)	One platform for Apple, Windows and Android, or the Apple side alongside Intune
Workspace ONE	DDM (Omnissa says), Platform SSO with Omnissa Access, Entra ID or Okta, UK SaaS region	Windows and Windows Server, with Autopilot (needs Entra ID and Microsoft licensing)	Apple, Windows, Android, Linux, ChromeOS and rugged devices in one console
JumpCloud	Agent plus MDM, with JumpCloud as the directory and sign-in for identity-led teams	Agent on Windows 10, 11 and Server; JumpCloud recommends Windows Pro	One identity and device platform across macOS, Windows, Linux and mobile, with its own access policies

The paired pattern uses a specialist Apple platform such as Jamf with Intune for Windows; Jamf Pro reports compliance to Intune, so Entra Conditional Access can use it for Macs and Intune's own for PCs. Iru and Workspace ONE are also Intune compliance partners, so the same pattern can work with them. A single cross-platform tool gives one console, one set of policies and one contract.

SECTION 5

Requirements worksheet

How to use it. Write your shortlist in the column headings. Tick “Must have” where failing the criterion rules a platform out. Weight each criterion from 1 (minor) to 5 (critical), score each platform from 1 to 5 using the tables and vendors' written answers, then multiply and add up. A platform that fails a must-have is out, whatever its total.

This worksheet is for your own assessment. Postremo IT does not score or rank the vendors.

Criterion	Must have	Weight 1 to 5	Platform A	Platform B	Platform C	Platform D
1. Platforms covered Apple, Windows, Android, Linux: now and planned						
2. Apple depth New releases, DDM, Platform SSO, Mac app updates						
3. Windows depth Autopilot, updates, co-management, editions						
4. Entra compliance Device compliance in Entra Conditional Access						
5. Other identity providers Okta, Google or JumpCloud: sign-in and device trust						
6. AI controls on devices Apple Intelligence, OS 27 keys, Copilot and Recall						
7. Admin AI data handling Default state, actions, model, processing location						
8. EDR and SIEM export Endpoint protection, SIEM connector, audit log export						
9. UK or EU hosting Main service, add-on products and admin AI						
10. Licensing fit What you already own; edition or package needed						
11. Team skills Who runs it daily; tools your team already knows						
12. Migration effort Enrolment method, rebuilds, timeline						
Weighted total Sum of weight × score, per platform						

SECTION 6

Questions to ask each vendor

Ask every shortlisted vendor the same questions and ask for written answers with links to current documentation.

APPLE RELEASES AND FEATURES

1. What does your “same-day” or “day-zero” support cover on release day, and what follows later?
2. Which Apple Intelligence settings and OS 27 additions (Siri AI, Visual Intelligence, app and binary allow or deny) do you support today?
3. How are Mac apps packaged and kept updated, and how quickly?
4. Which software update controls use declarative device management, now that macOS 27 requires it?
5. If we host it ourselves, which features are cloud-only?

WINDOWS

6. Is Windows managed through Microsoft's MDM framework, your own agent, or both?
7. Is Autopilot supported, and what Entra and Microsoft licensing does it need?
8. Which Windows AI controls (Recall, Copilot app, agent connectors) can you deliver, and which need Enterprise or Education?
9. Which Windows editions and architectures (Home, Pro, Arm) are fully supported?

IDENTITY

10. Which identity providers do you document for Platform SSO, including during Setup Assistant?
11. Does our identity provider's extension support each Platform SSO feature we need?
12. Are you a generally available Intune compliance partner, and for which platforms?
13. How do your device signals reach our conditional access (Entra, Okta, Google or your own policies), and for which platforms?

ADMIN AI

14. Is your admin AI on by default, and can we turn it off completely?
15. Can it make changes, and under what approval and permissions?
16. Which model provider and sub-processors does it use, and where are UK prompts processed and stored?
17. Is our data used for training, and how long is it kept?
18. Which AI features are generally available, and which are beta or roadmap?

SECURITY AND SIEM

19. Which endpoint protection is native and which from partners, and what does it cover on each operating system?
20. Which edition includes admin audit log export, how often is it sent, and how long is it kept?
21. Is there a supported connector for our SIEM, who maintains it, and what data does it carry?
22. Which macOS compliance baselines do you provide (for example CIS, NIST or mSCP), and how are they deployed and kept current?

HOSTING AND DATA

23. Where will our data be hosted, and can we choose a UK region?
24. Do add-on products, such as EDR, identity and admin AI, process data in the same region?
25. Can an existing tenant move region later?

LICENSING AND MIGRATION

26. Is licensing per device or per user, with what minimum and term, and which edition covers our worksheet?
27. Which features are add-ons rather than included?
28. Do you support Apple's migration through Apple Business without erasing devices, in both directions?
29. Are any forced changes, such as tenant upgrades or retired features, due in the next 12 months?

SECTION 7

Licensing map

As documented in November 2026, without prices. Map your worksheet to a named edition before comparing quotes.

Microsoft 365: what includes Intune and related tools

Licence	Device management	Security and AI
Microsoft 365 Business Premium	Intune Plan 1	Defender for Business (built on Defender for Endpoint, up to 300 users; Windows, Mac, Android, iOS and iPadOS). Security Copilot is not included.
Microsoft 365 E3	Intune Plan 1. From July 2026, also Intune Plan 2, Remote Help and Advanced Analytics.	Security Copilot is not included.
Microsoft 365 E5	As E3, plus Endpoint Privilege Management, Enterprise App Management and Cloud PKI.	Security Copilot (which powers Copilot in Intune) is included for eligible E5 and E7 customers and provisioned automatically.
Other plans	Buy the Intune Suite tools separately.	Check the Defender and Purview entitlements in your agreement.

- Intune is licensed per user; Platform SSO is included in all plans. Users of a partner MDM still need an Intune licence.
- The Enterprise App Catalog (Windows only) needs a licence beyond Plan 1 or 2. STIG audit baselines need Advanced Analytics.
- Purview Endpoint DLP for AI websites needs Defender for Endpoint and E5-level Purview, and can protect Macs on any MDM.

The other four platforms

Platform	Licensing unit and term	Editions, plans and add-ons
Jamf	Per device, billed annually, 25-device minimum. Jamf for Mac and Jamf for Mobile are only available to Jamf Cloud customers.	Plans rather than single products: Jamf for Mac and Jamf for Mobile, both powered by Jamf Pro, Jamf Connect and Jamf Protect. App Installers, drawn from the Jamf App Catalog, are included with Jamf Pro Cloud. Jamf states Log Stream is available only on the Jamf Cloud Premium offering.
Iru	Quote-based and modular, “based on the solutions your organization needs, as well as the number of users and devices”, with annual commitments and a 14-day trial. Iru does not state whether the unit is per device or per user.	Six products: Workforce Identity, Endpoint Management, Endpoint Detection and Response, Vulnerability Management, Compliance Automation and Trust Center. EDR is an add-on for Mac and Windows.
Omnissa Workspace ONE	Annual subscription, per device or per user.	Editions from Mobile, Desktop and UEM Essentials up to Enterprise and Platinum. Platinum adds rugged devices, remote support, vulnerability management and advanced MFA.
JumpCloud	Per user per month, in packages, with a 30-day trial.	Packages: Device Management, SSO, Device Identity Management, Platform Essentials (300 users maximum), Platform and Platform Prime. MDM and patch management are in every package except SSO. Conditional access conditions for the User Portal and SSO apps are part of Platform Prime. The 13-month Events API for SIEMs needs Directory Insights Premium.

SECTION 8

Changing platform

Changing MDM need not mean wiping every device, but it needs a plan.

DIAGRAM 5

Changing platform without wiping devices

From macOS 26, iOS 26 and iPadOS 26, an Apple capability that works with any MDM that supports it.

Can move without erasing

Organisation-owned device, OS 26 or later, enrolled through Automated Device Enrollment

→ Reassigned in Apple Business → New MDM

Needs another route

Older OS, or not enrolled through Automated Device Enrollment

→ Plan re-enrolment

Classify these devices first, so they are not a surprise mid-migration.

1. Classify devices by route
2. Build the new platform first
3. Pilot with each device type
4. Plan the access change-over
5. Move devices in waves
6. Retire the old platform

What to inventory first

- **Devices:** counts by platform and OS version, and how each was enrolled. If you are moving Macs to Intune, it supports the three most recent macOS versions.
- **Configurations:** macOS 27 no longer accepts the old software update commands, and Apple's AI controls now use declarative configurations, so older policies may need rebuilding.
- **Apps:** what is deployed, how it is packaged and how it is updated.
- **Identity:** Platform SSO, enrolment sign-in and directory sync. The MDM delivers Platform SSO settings; Managed Apple Account federation stays in Apple Business.
- **Access and compliance:** policies that depend on the current MDM. Intune accepts one compliance partner per platform.
- **Security, logging and contracts:** EDR agents, SIEM feeds, audit exports, integrations, and licence terms on both platforms.

After the move, check that security and logging data is arriving. Read Apple's migration documentation (in Sources) and your new vendor's guide first.

SECTION 9

Sources

The documents behind the facts in this guide, grouped by vendor. All were checked in November 2026.

Apple

support.apple.com/guide/deployment/migrate-managed-devices-dep4acb2aa44/web

support.apple.com/guide/deployment/platform-sso-for-mac-dep7bbb05313/web

support.apple.com/guide/deployment/apple-intelligence-declarative-configuration-dep9520d6032/web

support.apple.com/guide/deployment/depedd7d23ef/web

support.apple.com/guide/business/axmb19317543/web

support.apple.com/en-gb/148830

support.apple.com/en-gb/148828

github.com/apple/device-management (declarative configurations)

Jamf

www.jamf.com/pricing/

www.jamf.com/resources/press-releases/same-day-support-for-os-27-releases/

www.jamf.com/resources/press-releases/jamf-takes-apple-management-into-the-ai-era-at-jnuc-2026/

www.businesswire.com/news/home/20260130192806/en

community.jamf.com/release-announcements-177/jamf-pro-11-32-now-available-58792

support.jamf.com/en/articles/11024811-keeping-macs-up-to-date-with-jamf-pro

www.jamf.com/blog/introducing-blueprints/

learn.jamf.com/r/en-US/technical-articles/Jamf_Cloud_Hosted_Data_Region_Information

learn.jamf.com/r/en-US/technical-articles/Platform_SSO_for_Microsoft_Entra_ID

concepts.jamf.com/guides/device-trust-identity-and-deployment/platform-single-sign-on/psso-jamfpro-okta/

www.jamf.com/blog/macos-26-platform-sso-simplified-setup/

learn.jamf.com/r/en-US/jamf-connect-documentation-current/macOS_Login_Window_Requirements

learn.jamf.com/r/en-US/jamf-pro-documentation-current/Creating_an_Enrollment_Customization_Configuration

www.jamf.com/blog/jamf-2025-mac-management-ai-blueprints/

www.jamf.com/blog/jamf-app-installers-faq/

learn.jamf.com/r/en-US/jamf-pro-blueprints-configuration-guide/2026-04-23

media.jamf.com/documents/technical-papers/Jamf_AI_Assistant_Security_Technical_Paper_April_2026.pdf

www.jamf.com/products/jamf-protect/

learn.jamf.com/r/en-US/jamf-protect-documentation/Data_Collection_Options

support.jamf.com/en/articles/10932419-compliance-benchmarks-faq

developer.jamf.com/jamf-pro/docs/webhooks-1

developer.jamf.com/jamf-pro/docs/jamf-log-stream

splunkbase.splunk.com/app/6912

Microsoft

learn.microsoft.com/intune/fundamentals/ref-supported-platforms

learn.microsoft.com/intune/fundamentals/architecture

learn.microsoft.com/intune/fundamentals/planning-guide

learn.microsoft.com/intune/whats-new/

learn.microsoft.com/intune/device-security/compliance/third-party-partners

learn.microsoft.com/intune/device-configuration/settings-catalog/configure-platform-sso-macos

learn.microsoft.com/intune/device-configuration/settings-catalog/configure-platform-sso-during-enrollment

learn.microsoft.com/intune/app-management/deployment/enterprise-app-management

learn.microsoft.com/intune/configmgr/comanage/overview

learn.microsoft.com/intune/privacy/data-handling/data-storage-processing

learn.microsoft.com/intune/device-security/security-baselines/configure-baselines

learn.microsoft.com/intune/governance/integrate-azure-monitor

learn.microsoft.com/intune/governance/monitor-audit-logs

learn.microsoft.com/intune/copilot/

learn.microsoft.com/copilot/security/security-copilot-inclusion

learn.microsoft.com/copilot/security/faq-data-compliance

techcommunity.microsoft.com/t5/intune-customer-success/microsoft-intune-and-apple-os-27-new-settings-support-and/ba-p/4559764

learn.microsoft.com/windows/client-management/manage-recall

learn.microsoft.com/windows/client-management/manage-windows-copilot

learn.microsoft.com/windows/client-management/mdm/policy-csp-windowsai

learn.microsoft.com/windows/configuration/policy-based-inbox-app-removal/policy-based-inbox-app-removal

learn.microsoft.com/troubleshoot/microsoft-365/purview/data-loss-prevention/diagnose-paste-to-supported-browser-issues

learn.microsoft.com/defender-endpoint/microsoft-defender-endpoint

learn.microsoft.com/defender-vulnerability-management/tvm-supported-os

learn.microsoft.com/defender-xdr/configure-siem-defender

learn.microsoft.com/azure/sentinel/data-connectors-reference

learn.microsoft.com/graph/api/resources/intune-graph-overview

Iru

iru.com/newsroom/kandji-now-iru

docs.iru.com/en/iru/platform-overview/upgrade-to-iru

docs.iru.com/en/iru/platform-overview/iru-overview

www.iru.com/pricing

www.iru.com/updates/all

docs.iru.com/en/endpoint/library/managed-os/configure-managed-os-for-macos

docs.iru.com/en/endpoint/library/auto-apps/auto-apps-overview

docs.iru.com/en/endpoint/library/library-items-profiles/configure-the-platform-sso-with-microsoft-entra-id-library-item

docs.iru.com/en/endpoint/integrations/okta-desktop-password-sync/deploy-okta-desktop-password-sync-and-platform-single-sign-on

docs.iru.com/en/endpoint/library/passport/configure-the-passport-library-item

docs.iru.com/en/endpoint/enrollment/configure-require-authentication-for-enrollment

docs.iru.com/en/endpoint/integrations/okta-device-trust-main/okta-device-trust-integration-setup

docs.iru.com/en/endpoint/settings/windows-integrations/configure-windows-autopilot

docs.iru.com/en/iru/requirements/using-iru-on-enterprise-networks

docs.iru.com/en/endpoint/library/library-items-profiles/configure-the-restrictions-library-item

docs.iru.com/en/iru/iru-ai/iru-ai-overview

docs.iru.com/en/endpoint/endpoint-detection-response-edr/endpoint-detection-and-response-edr-overview.md

docs.iru.com/en/endpoint/vulnerability-management/vulnerability-management-overview.md

www.iru.com/updates/2026/02/updated-cis-blueprint-templates-and-parameters

docs.iru.com/en/endpoint/integrations/security/amazon-s3-activity-log-integration.md

docs.iru.com/en/endpoint/api/iru-api-overview.md

www.elastic.co/docs/reference/integrations/iru

Omnissa

omnissa.com/official-launch-pr

itbrief.co.uk/story/omnissa-appoints-amit-singh-as-chief-executive-officer

www.omnissa.com/products/workspace-one-unified-endpoint-management/

www.omnissa.com/apple/

techzone.omnissa.com/resource/enforcing-macos-security-compliance-project-baselines-workspace-one-operational-tutorial

techzone.omnissa.com/resource/provisioning-enrolling-and-onboarding-windows-devices-workspace-one-uem

techzone.omnissa.com/managing-updates-windows-devices-workspace-one-operational-tutorial

status.workspaceone.com/incidents/hkf59gm5t6hz

itbrief.co.uk/story/omnissa-adds-windows-server-management-to-workspace-one

docs.omnissa.com/macOS-Device-Management-VSaaS/PSSODuringADE

techzone.omnissa.com/resource/managing-apple-intelligence-macos-and-ios-workspace-one-uem

www.omnissa.com/newsroom/news/omnissa-one-amer-2026-elara-press-release/

www.omnissa.com/insights/blog/work-smarter-omni-now-ga/

docs.omnissa.com/OmnissaAIPolicy/aipolicy

docs.omnissa.com/Intelligence/IntelSupportedDataCategories

docs.omnissa.com/WorkspaceONE-MobileThreatDefense-VSaaS/MTD-Overview

techzone.omnissa.com/blog/intelligence-use-case-vulnerability-management-and-remediation

docs.omnissa.com/TroubleshootingandLoggingGuide-V2410/SyslogIntegration

docs.cloud.google.com/chronicle/docs/ingestion/default-parsers/airwatch

developer.omnissa.com/workspace-one-uem-apis/

JumpCloud

jumpcloud.com/pricing

jumpcloud.com/support/agent-compatibility-system-requirements-and-impacts

jumpcloud.com/support/get-started-android-emm

jumpcloud.com/support/support-for-apple-operating-systems-2026

jumpcloud.com/support/create-a-ddm-based-macos-patch-policy

jumpcloud.com/support/get-started-patch-management

jumpcloud.com/support/jumpcloud-eu-data-center-faq

jumpcloud.com/blog/intune-competitor

jumpcloud.com/support/device-password-sync

jumpcloud.com/support/configure-an-sso-extension-policy-for-macos

jumpcloud.com/support/establish-okta-device-trust-with-jumpcloud

jumpcloud.com/support/integrate-with-apple-business-manager

jumpcloud.com/support/get-started-conditional-access-policies

jumpcloud.com/support/create-a-mac-policy-to-restrict-apple-intelligence

jumpcloud.com/support/users-understand-saas-management

jumpcloud.com/support/get-started-ai-powered-features

jumpcloud.com/support/get-started-ai-admin-assistant

jumpcloud.com/blog/jumpcloud-supports-eu-data-protection

jumpcloud.com/support/crowdstrike-integration

jumpcloud.com/support/integrate-with-sentinelone

jumpcloud.com/support/directory-insights

jumpcloud.com/support/siem-integration-in-directory-insights

jumpcloud.com/support/system-insights

www.elastic.co/docs/reference/integrations/jumpcloud

Identity providers

help.okta.com/oie/en-us/content/topics/oda/macos-pw-sync/about-psso.htm

help.okta.com/oie/en-us/content/topics/oda/macos-pw-sync/configure-macos-psso-intune.htm

support.okta.com/help/s/article/mdm-compatibility-with-okta-device-integrations

help.okta.com/oie/en-us/content/topics/identity-engine/devices/device-assurance.htm

help.okta.com/oie/en-us/Content/Topics/identity-engine/devices/integrate-third-party-mdm.htm

knowledge.workspace.google.com/admin/devices/set-up-third-party-partner-integrations

Other

www.computerworld.com/article/4077093/kandji-becomes-iru-opens-mdm-windows-android.html

www.elastic.co/docs/reference/integrations/jamf_protect

docs.cloud.google.com/chronicle/docs/ingestion/default-parsers/ingest-jamf-logs

HOW WE HELP

Talk it through with us

We deploy and manage Jamf and Microsoft Intune every day, often together. If you are choosing an MDM or reviewing the one you have, we can work through your devices, identity and data requirements, this worksheet and the vendor answers with you, and set out the options.

CALL

+44 20 7550 9103

EMAIL

info@postremoit.com

WEB

postremoit.com

LONDON HEAD OFFICE

Level 24, One Canada Square
Canary Wharf, London E14 5AB

POSTREMOIT

Postremo IT Limited. Choosing an MDM in 2026, November 2026 edition. Product names belong to their owners. Based on vendor documentation checked in November 2026; products change often, so confirm details with each vendor before you decide.