jamf

Enterprise Mac Adoption

Introduction

Mac devices currently make up 27% of all devices in the enterprise (up from 24% in 2024) and continue gaining momentum. Even with growing adoption and success stories from industry-leading organizations worldwide, some IT teams still hesitate to expand support for macOS in their environments.

Often this hesitation stems from misconceptions that managing Mac is inherently more complex, that macOS does not integrate well with other platforms or that adopting it could compromise security.

In reality Apple has developed robust tools and capabilities such as Apple Business Manager, MDM framework, the Endpoint Security API and built-in security features. Together these enable IT teams to manage Mac fleets in a way that is seamless and secure. When combined with the right enterprise solution, these tools help IT teams integrate Mac confidently and efficiently alongside other platforms.

This white paper explores how organizations can overcome common challenges and successfully adopt and support Mac at scale.

Mac Adoption Steps

This white paper provides guidance and configurations tailored to the unique needs of enterprises. Compliance requirements, for example, often vary by organization, industry and region.

It focuses on best practices and key considerations for leadership to address before, during and after introducing Mac support into their environments. This approach helps minimize risk during integration while giving businesses the flexibility to adopt Mac at a pace that fits their needs.

The content is organized into three sections:

1. Key considerations for Mac adoption (BEFORE)
2. Best practices for successful deployments (DURING)
3. Ongoing management, security and support (AFTER)

"A goal without a plan is just a wish."

— Antoine de Saint-Exupéry

Key considerations for Mac adoption

1.

Adopting Mac in the enterprise isn't just a technical decision – it's a strategic one.

Support business objectives

To ensure a successful rollout, IT leaders must first align Mac adoption with broader business objectives, such as:

- improving user productivity
- enhancing security postures
- attracting/retaining top talent

Assess organizational readiness

Next, a clear path to successful Mac adoption requires leaders to **assess organizational readiness** by evaluating their:

- infrastructure
- assets/inventory
- resources (data/services)
- IT support capabilities

Streamline tools for compatibility

Integrating a **best-of-breed solution for Mac** ensures native platform support and streamlines operations. By maximizing compatibility between software and services used by stakeholders, resources used cross-platform can be used to support business success – not affect it.

Align with security and compliance

While **macOS offers strong native capability aligned with many industry standards and frameworks**, it doesn't meet all requirements on its own. Jamf builds on the macOS native capability, enabling organizations to:

- meet regulatory and industry compliance requirements
- monitor, audit and enforce compliance policies at scale
- achieve consistent protection across platforms

Implement user support and training

Supporting users effectively is a critical success factor. Providing training and smooth onboarding eases the transition for stakeholders. Additional benefits include:

- **curated support** empowers independent issues resolution
- giving IT teams room to focus on strategic tasks
- increased stakeholder productivity and error reduction

Measure performance to drive success

Understanding progress towards goals is a crucial part of every business model. It is only by assessing performance can we truly **identify risk factors and mitigate them** to achieve desired outcomes. Measuring KPIs helps to:

- track adoption success
- increase efficiency
- guides future improvements

Mac Deployment Readiness Checklist for Windows-Centric Enterprises

Before deploying Mac devices in a Windows-first environment, it's essential to create a plan that integrates Mac-specific tools and workflows into the broader technology stack. This ensures compatibility with organizational systems while supporting the unique strengths of the macOS platform and enabling smooth cross-platform operations.

1. Align Mac adoption with business objectives

- Identify how Mac supports core business goals (e.g., productivity, talent retention and security enhancements)
- Validate executive sponsorship and long-term strategy alignment
- Document measurable success metrics tied to business outcomes

2. Assess organizational readiness

- Audit infrastructure for Mac compatibility (network, identity, security, device management)
- Inventory current assets and evaluate cross-platform usage scenarios
- Review internal support capabilities for macOS troubleshooting and escalation
- Identify key services and data systems critical to Mac operations

3. Streamline tools and software compatibility

- Select a unified management solution that supports both macOS and Windows (e.g., identity provider, software distribution and security baselines)
- Ensure essential applications are available or compatible with macOS
- Standardize workflows and services for cross-platform usability
- Create app deployment and patching strategy tailored for macOS

4. Align with security and compliance frameworks

- Integrate Mac into existing security posture (EDR, VPN/ZTNA, SSO)
- Apply compliance standards (NIST, CIS, ISO) to macOS fleet
- Configure monitoring and audit policies for parity with Windows systems
- Verify encryption, authentication, and endpoint protection settings

5. Prepare user support and training programs

- Develop macOS-specific onboarding and orientation resources
- Train support staff on Apple-native tools and ticket resolution procedures
- Deploy self-service resources and knowledge base for users
- Communicate Mac benefits and support channels clearly to end-users

6. Establish performance and success metrics

- Define KPIs for Mac adoption (e.g., deployment time, user satisfaction, ticket volume)
- Monitor usage trends and cross-platform performance
- Track compliance, security incidents and system health metrics
- Use findings to iterate and improve the Mac integration roadmap

Best practices for successful deployments

2.

Mac integration doesn't occur in a vacuum – there are multiple components that contribute to a seamless experience for all stakeholders.

Plan each step, process and workflow

Successfully adopting Mac alongside your existing enterprise begins with a well-defined plan. Mapping out each phase across the device's lifecycle – extending to processes and workflows:

- ensures cross-platform processes and workflows
- reduces risks through platform security parity
- keeps IT and Security teams functionally aligned

Automate provisioning and deployment

Provisioning allows devices to be configured out of the box. Automation eliminates manual intervention – ensuring consistent configuration of each device while simultaneously accelerating stakeholder's time to productivity. Additionally, it not only reduces the likelihood of errors but frees up IT resources for tasks befitting their skillset.

Seamless, secure integration with systems

Integrating Mac devices seamlessly and securely with your infrastructure serves to stitch together existing tools, services and equipment, resulting in centralized operations that act as the foundation for IT and business alike. Alongside integrating management, identity and security, enterprises:

- ensure consistent stakeholder experiences across platforms
- enforce policies and enable faster threat detection and response
- improve IT's support of and alignment with business objectives

Monitor devices and stay up to date with patches

Consistent monitoring and timely software updates are critical to maintaining performant, secure endpoints. A centralized management solution that supports macOS natively helps:

- establish baselines and measure compliance against benchmarks
- gather and analyze device health telemetry data in real-time
- automate patch management to remediate vulnerabilities/threats

Communicate with stakeholders and document feedback

Stakeholders are crucial to the success of Mac adoption initiatives. Regular communication keeps everyone informed and engaged throughout the deployment. Additionally, capturing feedback throughout doesn't just help identify pain points, it also drives continuous improvement through data-driven decision-making.

> *"Do the best you can until you know better. Then when you know better, do better."*
>
> – Maya Angelou

Mac Deployment Best Practices Checklist for Windows-Centric Enterprises

During the deploying of Mac devices within a Windows-first environment, align with Windows endpoints is key to minimize security gaps and ensure that compliance is not just being met but continues to be enforced holistically across the enterprise – regardless of the platform being used.

1. Plan each step, process and workflow

- Map every phase of the Mac lifecycle – from enrollment to decommission – to ensure process clarity and workflow alignment
- Define cross-platform workflows that work seamlessly across macOS and Windows environments
- Align IT and security functions to maintain platform parity and reduce risk

2. Automate provisioning and deployment

- Implement zero-touch deployment using Apple Business Manager and mobile device management (MDM) tools
- Configure automated provisioning workflows to ensure consistent device setup at scale
- Eliminate manual steps to reduce errors and free IT staff for strategic tasks

3. Integrate Mac devices securely with enterprise systems

- Connect Mac devices to core systems such as identity providers, device management and endpoint protection platforms
- Ensure consistent policy enforcement across macOS and Windows fleets
- Centralize operations for improved visibility and faster response to security events

4. Monitor Devices and Automate Patch Management

- Use tools that natively support macOS to track device health, compliance and activity in real time
- Automate software and security patch deployment to maintain up-to-date endpoints
- Establish performance baselines and measure against compliance benchmarks

5. Communicate With Stakeholders and Capture Feedback

- Keep stakeholders informed throughout the Mac deployment process with regular updates and alignment meetings
- Create feedback loops to capture user experience and operational challenges
- Use feedback to refine workflows, enhance user satisfaction and guide future improvements

Ongoing management, security and support

3.

Tighter alignment with business objectives means your technology grows and evolves lock step in support of the organization's needs.

Best practices for device management

Using mobile device management (MDM) solutions streamlines IT administration while automation reduces manual overhead. The need to maintain compliance is just as crucial for macOS as other platforms in your environment, hence why MDM acts as the critical foundation that:

- deploys secure configurations and establishes baselines
- leverages policy-based management to enforce compliance
- patches OS and app vulnerabilities, mitigating disruptive threats

Manage user identities and endpoint protection

Secure identity, configuration and endpoint management directly inform access management which is essential to protecting sensitive data across all platforms. Coupling identity and endpoint protection allows IT to implement a comprehensive security stack that allows stakeholders to focus on productivity by:

- enabling single sign-on with strong MFA across business resources
- verifying device health via telemetry before granting access requests
- upholding stakeholder privacy without compromising data security

Key strategies for maintaining Mac devices at scale

Managing Mac devices across a growing organization requires scalable processes and constant oversight. Integrating management, identity and security solutions unlock advanced automations that standardize multi-platform workflows, ensuring a stable IT environment that grows with the business.

Establish long-term support and maintenance

A long-term Mac strategy goes beyond initial deployment – it requires ongoing support to ensure Mac devices are managed and secured in parity with Windows endpoints.

Fortunately, integration with existing tools, like Microsoft Entra ID, Splunk and other SIEM platforms makes this process straightforward. Extending identity and security workflows to Mac allows IT to streamline operations holistically while refocusing on training practices that keep devices running smoothly and stakeholders productive.

Drive upgrades using iterative feedback

Stakeholders play a vital role in shaping how Mac environments align with productivity efficacy. Gathering feedback is essential to uncovering pain points. Also, it unlocks efficiency gains when paired with existing or novel technologies, leading to:

- increased performance with enhanced workflows
- maximized user satisfaction across the organization
- iterative improvements that drive business adoption

Ongoing Mac Management and Security Checklist for Windows-First Enterprises

After deploying Mac devices within a Windows-first environment, IT shifts to maintaining support for multiple platforms. Through careful planning (before) and thoughtful deployment (during), continued support and compliance (after) for business objectives and stakeholder productivity become the critical tasks for IT.

1. Standardize device management with MDM

- Deploy a macOS-native MDM solution to centralize configuration and compliance
- Establish secure configuration baselines aligned with Windows endpoint policies
- Use policy-based management to enforce compliance and reduce risk
- Automate patching workflows for both operating systems and applications to eliminate known vulnerabilities

2. Secure identity and endpoint access controls

- Integrate Mac devices into existing identity frameworks such as Microsoft Entra ID for unified access control
- Implement strong MFA and single sign-on for macOS users accessing business resources
- Leverage device telemetry in ZTNA workflows to evaluate macOS device health before granting access
- Ensure endpoint protection parity by enforcing antivirus, monitoring and encryption policies to macOS

3. Scale multi-platform management workflows

- Design cross-platform automation that includes macOS in workflows traditionally built around Windows
- Centralize identity, management and security platforms for a unified administrative experience
- Ensure process scalability to accommodate increasing numbers of Mac users without increasing manual workload

4. Maintain Mac devices with long-term support strategy

- Integrate Mac telemetry into your existing Security Information and Event Management (SIEM) platform (e.g. Microsoft Sentinel) to support threat detection and response
- Provide help desk training focused on macOS-specific troubleshooting and user support
- Align routine macOS maintenance schedules with Windows update cadences to standardize patch management

5. Improve operations with iterative stakeholder feedback

- Collect structured feedback from Mac users to uncover experience gaps and IT friction points
- Pair feedback insights with analytics to optimize workflows and boost device performance
- Apply findings in phased iterations to drive adoption, user satisfaction and operational efficiency

Why Mac devices?

Mac adoption in enterprises faces IT objections. With myths about cost, compatibility, management, security and expertise abound, it can be difficult to make heads or tails about making the decision to support macOS in your enterprise from a business point of view.

Key differences IT should know when deploying Mac vs. Windows

While both platforms can coexist in modern enterprise environments, Mac deployments come with unique characteristics that IT teams must plan for. Understanding these differences helps ensure a smooth rollout, strong security posture and optimized user experience, alongside management and security parity with its Windows counterparts.

What sets Mac deployments apart from Windows?

- Enrollment is identity-driven and automated through Apple Business Manager and MDM – no imaging required
- macOS supports Declarative Device Management (DDM), enabling faster, more autonomous policy enforcement by shifting control logic to the device
- OS and software updates are user-approved by default, requiring coordination to meet patching timelines
- Hardware and software are tightly integrated, minimizing variability but requiring Apple-specific tooling
- macOS prioritizes user privacy and security defaults, impacting telemetry, file access and third-party monitoring tools
- No Active Directory join required, as Mac devices can integrate via SSO, SAML and cloud identity providers
- **Lifecycle tools and provisioning workflows differ**, requiring scripting and automation strategies that are macOS native for maximum support

What to do if your organization is on the fence about supporting Mac?

Whether you're an IT leader building a case for Mac adoption or a new-to-macOS MacAdmin, reviewing the **5 common IT objections to Mac in the enterprise** helps separate fact from fiction. By tackling these concerns head-on, you'll gain a clearer understanding –supported by data and real-world successes – of why adopting and supporting Mac is far easier than it seems.

TL;DR the sections below include key takeaways of the benefits to organizations of managing and securing Mac alongside Windows in multi-platform environments.

Security

- Establishing a consistent security baseline ensures uniform protection standards, reduces complexity and maintains compliance across the entire device fleet.
- Deploying compatible apps from trusted sources streamlines software distribution while keeping applications secure and up to date.
- Real-time monitoring and telemetry analysis standardizes the view of device health, making it easier to detect risks, enforce policies and respond to threats quickly.

Productivity

- Streamlining Mac provisioning through zero-touch deployment ensures they're ready to use and compliant right out of the box.
- Implementing Zero Trust architecture blocks compromised devices and reduces risk of credential misuse from accessing protected enterprise resources.
- Uphold and ensure a standardized, seamless user experience regardless of the device type, OS platform or ownership model used.

Employee satisfaction

- Minimize stakeholder downtime through proactive management of device inventory and repair requests throughout the device's lifecycle.
- Curating a Self Service app catalog allows stakeholders to address common issues, such as app installs or password resets, themselves without impacting IT.
- Attract and retain top talent by accommodating employee programs, empowering them to do their best work with the platform they feel most comfortable with.

Usability

- Achieve a comprehensive, holistic approach to access control and threat protection by unifying endpoint security and IAM.
- Support lifecycle efficiency and device uptime through continuous management of device inventory and service needs.
- Unlock new capabilities and develop enhanced workflows to better support business continuity through integration with tools and solutions.

ROI/TCO

- **Reduce Mac management and device support costs** by one-third compared to Windows endpoints
- **Increase employee productivity by 3.5%** with greater device performance and reliability
- Grow residual value after an average of four years of use, **from 15% to 30%** by adopting Mac over PCs

Top 5 actions IT leaders should prioritize when adopting Mac into a Windows-first enterprise environment

1.

Establish platform parity through unified management

Integrate Mac-specific solutions with existing identity, MDM and security platforms to ensure consistent oversight and policy enforcement across macOS and Windows. Taking an integrated, best-of-breed approach helps maintain parity, reduce complexity and deliver a cohesive experience for both users and administrators.

2.

Automate provisioning and zero-touch deployment

Use Apple Business Manager together with an Apple-specific MDM solution like Jamf to automate device enrollment, configuration and policy application from the moment Mac devices are activated. This automation eliminates manual errors, accelerates time to productivity and enables scalable, consistent deployment tailored for macOS across the organization.

3.

Align macOS security with enterprise standards

Extend core security practices – like MFA, Mac specific endpoint protection, patch management and compliance monitoring – to include macOS with the same rigor as Windows. This protects sensitive data, ensures regulatory compliance and helps maintain a strong security posture regardless of device type.

4.

Prepare support infrastructure and end-user training

Train IT support teams on macOS-specific tools and empower users with onboarding and self-service resources. Proactive support reduces ticket volume, improves user satisfaction and helps stakeholders navigate the platform confidently without productivity loss.

5.

Continuously monitor, measure, and iterate

Monitor Mac health, compliance status, and user feedback using native tools and integrated solutions. Iterative improvement based on real-time data and stakeholder input allows IT to adapt quickly, optimize workflows and drive long-term adoption success.

Conclusion

Though a common misconception, Mac adoption in the enterprise is not a niche initiative – it's a strategic opportunity to modernize infrastructure, empower employees and strengthen security postures across platforms. With thoughtful, intentional planning, adopting best practices and leveraging the right solution, organizations can seamlessly integrate Mac alongside Windows while achieving compliance parity across the infrastructure – all without increasing complexity.

A consistent, scalable management and security approach supports business agility and stakeholder satisfaction while reducing total cost of ownership and maximizing return on investment. The road to successful Mac adoption isn't paved with compromise – it's built on clear communication with stakeholders, secure integration of tools and a thoughtful, holistic vision of the business environment. With the right foundation in place, your organization can unlock the full value of supporting Mac at scale.

Key points of cross-platform support

- Align Mac adoption with business goals to drive value and stakeholder support.
- Integrate Mac-specific tools and policies into the broader IT strategy to streamline management and security.
- Automate provisioning, patching and updates to reduce risk and IT overhead.
- Implement Zero Trust by integrating existing identity provider and endpoint security.
- Provide user training and self-service tools to improve productivity and satisfaction.
- Drive continuous improvement by collecting feedback and monitoring fleet health.
- Reduce TCO and align long-term strategies that support business objectives.

Tomorrow's success is built upon today's foundation.

Try Jamf