jamf

Top Security Practices for Mac Management

Introduction

Evolving business operations, growing security needs and widening employee choice options continue to **fuel Mac adoption** rates in businesses by 76%. According to Computerworld, a study found "nine in 10 IT professionals praising the business advantages of Macs, iPhones, and iPads in the workplace." This is great news for employees and organizations! By diversifying the choice of technologies, employees can be their most productive when working with the hardware and software they feel most comfortable with.

From IT and Security team perspectives, any change introduces variables that potentially lead to risks if left unchecked. Luckily, risks unique to macOS can be minimized with proactive, defense-in-depth strategies that focus on delivering a comprehensive Mobile Device Management, Identity and Access and Endpoint Security solution that extends across your entire infrastructure to safeguard devices, data and users from the evolving threat landscape.

Integrating solutions opens the door for more granular security practices to maintain a baseline of endpoint health. This enforces compliance, allowing employees to remain productive while freeing up IT to develop workflows that better support business operations. In this paper we will cover critical security practices like:

- Patch & Update Management
- Threat Detection & Incident Response
- Data Protection & Encryption
- Network & Application Security

The foundation for Mac management and security

Before we get to our checklist of security practices, it's important to understand how crucial a solid foundation is with which to build your Mac management processes and workflows on. A scalable solution that doesn't offer same-day support for the latest patches for example can weaken both device and organizational security. This is often due to delays from developers in implementing support for the newest macOS version or limited support for essential features and functionality.

Mobile Device Management (MDM)

In **2024**, macOS ranked 9th out of the top 50 CVEs (Common Vulnerabilities and Exposures) identified, with a total of 508 unique vulnerabilities, making it a notable presence on the list. As of May 2025, macOS has moved up to 2nd place on the top 10 list, with **243 unique CVEs identified**, nearing 50% of 2024's total. Please note that this ranking may shift as the year progresses, so the number of CVEs and their position could change over time.

This underscores the criticality for devices to have OS and apps up-to-date. Modern features, like Declarative Device Management (DDM), enables devices to autonomously enforce settings and report changes in real time. This not only reduces the load on the MDM but simultaneously improves update speed and reliability while IT teams gain immediate visibility into key status changes.

And while MDM addresses far more than patch management, its ability to streamline operations and enhance decision-making efficiency are as essential as its ability to centrally orchestrate other crucial aspects of Mac management. Capabilities that speak directly to MDM's foundational nature include:

- Deploying secure configurations and settings
- Installing managed applications
- Executing policy-based compliance enforcement
- Maintaining current asset inventories

Identity and Access

Protecting data and ensuring that employees have access to the resources they need to stay productive may appear like two separate factors but in taking a closer look, we see that they're intrinsically linked by a common thread: permissions. According to the **Verizon 2024 Data Breach Investigations Report**, "68% of breaches involved a human element." This finding does not account for malicious insiders, focusing specifically on incidents stemming from misconfiguration of permissions (least privilege) and end-user errors relating to access credentials.

From a security perspective, this is not something that can be addressed by mandating security awareness training to spot threats and report them. To successfully navigate this and related security concerns, organizations need a solution that goes beyond enabling cloud-based identities. Such as implementing:

- Risk-aware access policies that deny access to compromised devices and accounts
- Intelligent split tunneling encrypts business traffic while upholding user privacy for non-business traffic
- Multi-Factor Authentication (MFA) enforces identity verification for resource requests

Endpoint security

Across all platforms, **malware targeting macOS** in 2024 accounted for about 11% of global malware detections. While easily behind others in terms of detections, IT nor Security teams should take this trend lightly. It's more than doubled from two years ago – and thanks to malware-as-a-service and sophisticated, AI-driven malware, threat actors increased targeting of Mac has seen **a significant rise** in infostealer malware campaigns.

In addition to other malicious code, such as trojans that attempt to bypass built-in macOS code signing protections and APTs, preventing malware is a critical necessity to defend devices against the evolving threat landscape. Additionally, there are other controls essential to maintaining strong device and organizational security postures. Such as:

- Identifying unknown threats through behavioral analytics
- Putting suspicious apps and detected threats in quarantine and removing them
- Actively monitoring, alert and report rich device health data (telemetry)
- Filtering access to risky web content, such as 0-day phishing URLs

Key security practices for Mac management

There's a lot of ground to cover in this section, so we're going to present the top security practices in a checklist format. Doing so provides the flexibility to display the necessary information for IT and Security teams to implement. This format provides IT leadership a clear, summarized view of each point, broken down into seven categories that are enabled through integration of the three foundational solutions.

Device Enrollment and Provisioning

- Secure, Zero-Touch device deployments with MDM enrollment
- Automated system setup, including managed app and configuration provisioning
- Enforce company-wide standards and security policies across all ownership levels: company-owned and BYOD

Endpoint Protection and Compliance

- Harden macOS security settings (FileVault, Gatekeeper, XProtect)
- Tailor on-device and in-network threat prevention with customized analytics
- Generate security guidance to configure endpoints with desired compliance level to create customized security baselines based on industry frameworks and standards

Identity and Access Management (IAM)

- Establish role-based access controls (RBAC) for least privilege access
- Minimize credential risks by implementing SSO and passwordless authentication
- Verify device and credential health with Zero Trust Architecture

Patch and Update Management

- Streamline OS and application updates to mitigate known vulnerabilities automatically
- Track telemetry data and share it securely with integrated solutions in real-time
- Ensure compliance is upheld through automated, policy-based remediation workflows that are triggered when non-compliance is detected

Threat Detection and Incident Response

- Leverage ML to automate threat intelligence gathering and analysis, as well as provide data-driven guidance and recommendations
- Resolve incidents quickly with seamless Endpoint Detection and Response (EDR) tools
- Augment threat hunting investigations and automate remediation with AI and policy-based workflows

Data Protection and Encryption

- Enforce FileVault encryption and automate key collection by securely storing and updating recovery keys within device records
- Holistically extend Zero Trust Network Access (ZTNA) across your infrastructure, verifying device and credential health before granting access to protected business resources
- Ensure data remains stored on protected volumes and restrict unauthorized sharing or copying to unsanctioned location with Data Loss Prevention (DLP)

Network and Application Security

- Enforce security across networks with always-on encryption of all network connections and managing Firewall policies
- Managing third-party app permissions and macOS security baselines
- Segment network traffic, preventing network-based attacks (Man-in-the-Middle), by routing each resource request through its own microtunnel

Jamf works! Real outcomes from the field

Gaining efficiency by reducing device provisioning times

"We save upwards of a day per laptop, as compared to provisioning manually."

– product owner, digital e-signature and document automation platform.

Organizations adopting Mac are realizing **measurable efficiency gains** and enhanced security postures.

Focus more on innovation and less on repetitive tasks

"Today we spend ten minutes per machine: it's a great time-saver."

– manager of information technology, financial management and accounting platform

Demonstrate the **tangible time savings and resource optimization** achieved through automated, zero-touch deployment workflows.

Keep data safe and users productive with comprehensive risk mitigation

"The real-time threat detection, compliance monitoring and centralized policy enforcement functionalities have proven instrumental in safeguarding our assets and ensuring regulatory compliance."

– manager of information technology, digital public library

Leverage Mac management to **strengthen security** and regulatory compliance, emphasizing the impact of real-time threat detection and centralized policy enforcement.

Enforce organizational compliance throughout the device lifecycle

"This structure not only met but also supported compliance with stringent standards like SOC 2, Type II, ISO and HIPAA. This illustrates Jamf's capability to reinforce organizational security and ensure compliance with critical industry regulations."

– senior manager of information technology, digital health company

Proactively improve compliance benchmark alignment and **implement security baselines** based on industry-accepted standards and frameworks.

Conclusion

As Mac adoption in the enterprise continues to grow, organizations must prioritize a proactive, integrated approach to managing and securing their Mac fleet. The evolving threat landscape and increasing complexity of work environments, including hybrid and remote workforces, benefit greatly from a security strategy with a clear focus that aligns with and supports business operations yet is flexible enough to meet stakeholders where they are.

This requires more than a one-size-fits-all solution.

Rather, it needs a multi-layered solution that natively supports Mac throughout each phase of the device and app lifecycles. Starting by establishing a strong foundation with Mobile Device Management (MDM), Identity and Access Management (IAM) and Endpoint Security. From there, businesses can confidently support user choice without having to choose between compromising security or impacting user privacy.

In simple terms:

- **Devices are compliant**
- **Data is secure**
- **Users are protected**

This paper has outlined the essential security practices required to maintain endpoint integrity and ensure regulatory compliance. This grants Security teams the tools to respond swiftly to threats and freeing IT teams to focus on innovation while delivering top-notch support to stakeholders. Additionally, employees are empowered to be their most productive without interruptions to their workflows.

When solutions work together seamlessly, organizations achieve a secure, scalable Mac ecosystem that operates alongside Windows PCs, balancing and promoting productivity, usability and protection — paving the way for innovation and resilience wherever you work.

Key takeaways

Mac adoption in business has grown by **76%** driven by employee choice and productivity benefits.

Endpoint security for macOS is more critical than ever amid rising malware threats, including infostealers and AI-powered malware.

90% of IT professionals recognize the business advantages of using Apple devices in the workplace.

Zero Trust Architecture and automation play pivotal roles in maintaining compliance, detecting threats and reducing response times.

Integrating foundational solutions enables automation and streamlines compliance with minimal user disruption.

68% of breaches involve a human element, making permissions and access controls a top priority.

Comprehensive solutions must include MDM, Identity and Access Management (IAM) and Endpoint Security.

IT and Security teams must adapt to new variables introduced by Macs, requiring integrated, defense-in-depth strategies to mitigate risk.

A comprehensive and integrated Mac security strategy allows organizations to scale securely while maximizing user productivity.

A defense-in-depth strategy is essential to minimize macOS-specific risks across the organization.

jamf

www.jamf.com

Try Jamf for Mac.