jamf

Checklist: identifying security gaps

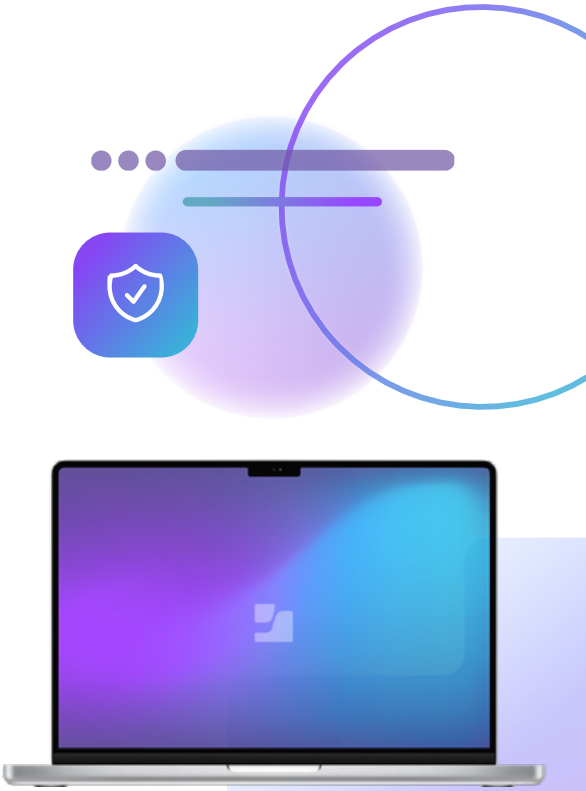
A brief guide for IT admins and SecOps teams managing Mac

Engineers, marketing professionals, executives, creative teams and more already love to use Mac at work. Mac continues to increase in popularity: the second quarter of 2025 showed a growth of 21.4% compared to Q2 of 2024 — more than any other computer vendor.

This is no surprise. After all, **employees like working with Mac**. The growth of Mac in the enterprise means more employees are using their preferred device for work, increasing their satisfaction and productivity. But what does this mean for IT and Security professionals?

Mac and Windows PCs are different. They have different operating systems, hardware strategies, architecture and design philosophies. This means that keeping them secure looks different too. Admins who've mostly worked with Windows may find gaps in their strategy, especially with a large device fleet. Since Mac — the hardware and the software — is made by Apple, admins need tools that build on and understand the Apple ecosystem.

In this checklist, we'll briefly explore strategies specific to Mac security to help you understand any potential gaps. We'll go through provisioning, identity and access, endpoint protection, and compliance, with checklists tailored specifically to the IT or Security professional.



Looking for a deeper dive? Check out our white paper:

Defense-in-depth: Closing gaps in security by integrating and layering solutions

IT admins' security gap checklist

Zero-touch deployment and device provisioning

Consider:

- Using Apple Business Manager with your mobile device management (MDM) platform
- Using Automated Device Enrollment to define payloads and restrictions
- Enforcing minimum OS version before Mac goes through Setup Assistant

User Authentication and identity provider integration

Consider:

- Integrating Platform Single Sign-On with your identity provider (IdP) and MDM
- An MDM that supports the Extensible Single Sign-on configuration
- Requiring authentication for privileged operations beyond initial login

Deploying Apple OS updates

Consider:

- Deploying automatic updates and yearly software upgrades — a different cadence from Windows devices
- Management and security vendor testing with the latest macOS version (importantly: beta testing for major releases)
- Deploying Rapid Security Responses without impacting user productivity

32% of organizations have ≥1 device with critical and patchable vulnerabilities

360 report

SecOps' security gap checklist

Alignment with compliance frameworks

Consider:

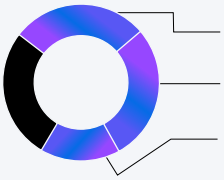
- Automate device hardening by integrating into the **macOS Security Compliance Project** (mSCP)
- Support benchmarks and baselines like **CIS Level 1 and Level 2** or **NIST 800-171**
- Implement, maintain and automate management settings to enforce specific security controls across Mac fleet

Endpoint security built for Mac-specific threats

Consider:

- Tools purpose built to block known and novel Mac-specific threats zero-day
- Implementing real-time endpoint protection that leverages built-in macOS features like XProtect, Gatekeeper and Notarization
- Threat hunting for Mac-specific malware referencing the latest expert research

Top Mac malware:

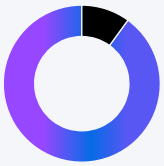


Infostealers **28.36%**

Adware **28.13%**

Trojans **16.61%**

360 report



Over **90% of cyber attacks** originate from phishing.

360 report

Streaming macOS telemetry data to existing SIEM/SOAR

Consider:

- Tools that source telemetry directly from the Endpoint Security API
- Aligning macOS telemetry to existing SIEM data models
- Tools that contextualize telemetry for immediate use
- Real-time analysis of macOS security events, like Gatekeeper bypass or when XProtect flags malware

Application installation and monitoring

Consider:

- Tools to keep third-party macOS software titles in their environments up to date
- Mac app versions and usage reporting
- Controlling app distribution channels through managed accounts and developer certificates

User and device access to company resources

Consider:

- Leveraging Apple technologies like Network Relay to enable Zero Trust Network Access
- Hardware-backed device attestation via Secure Enclave for conditional access policies
- Building Zero Trust models specific to the macOS platform

This checklist helps start your journey toward a defense in depth strategy.

jamf

www.jamf.com

Want to dive deeper?
Read our white paper.