Mac Security Checklist

In today's evolving threat landscape, maintaining a secure Mac ecosystem in the enterprise is more critical than ever. As Macs continue to play a growing role across organizations, IT leaders must ensure they are protected at every level — from the device itself to the data it accesses — while simultaneously aligning IT and Security processes to best support business objectives.

Securing your Macs against today's sophisticated threat landscape is table stakes to protecting your enterprise data and maintaining compliance.

The following sections make up the core checklist that IT leaders need to focus on when developing a holistic security plan. One that relies on strong, foundational cores while reaping the additional benefits that only natively integrated solutions can deliver. By seamlessly integrating them, comprehensive defense-in-depth strategies, automated workflows and secure processes are enabled and empower organizations to realize:

- **Increases in productivity**
- **Boosted efficiency**
- **Upheld user privacy**
- **Greater returns on investment**

This core checklist outlines the key areas that should be prioritized in any comprehensive security strategy: device management, endpoint protection, user authentication, compliance standards and additional layered defenses. When these areas are integrated into a unified, defense-in-depth approach, organizations benefit from improved automation, stronger user privacy, enhanced efficiency and greater ROI — all while keeping a strong device and organizational security posture.

Device Management

- [ ] Use an MDM solution to enforce security policies
- [ ] Deploy secure configurations and device settings
- [ ] Install managed applications and settings
- [ ] Establish regular software update cadence
- [ ] Keep track of device inventory and user assignments

Endpoint Protection

- [ ] Install endpoint security software
- [ ] Monitor endpoint health in real-time
- [ ] Defend against in-network and on-device threats
- [ ] Quickly respond to incidents and unknown threats by leveraging AI/ML
- [ ] Stream rich telemetry data to SIEM solution for analysis

User Authentication

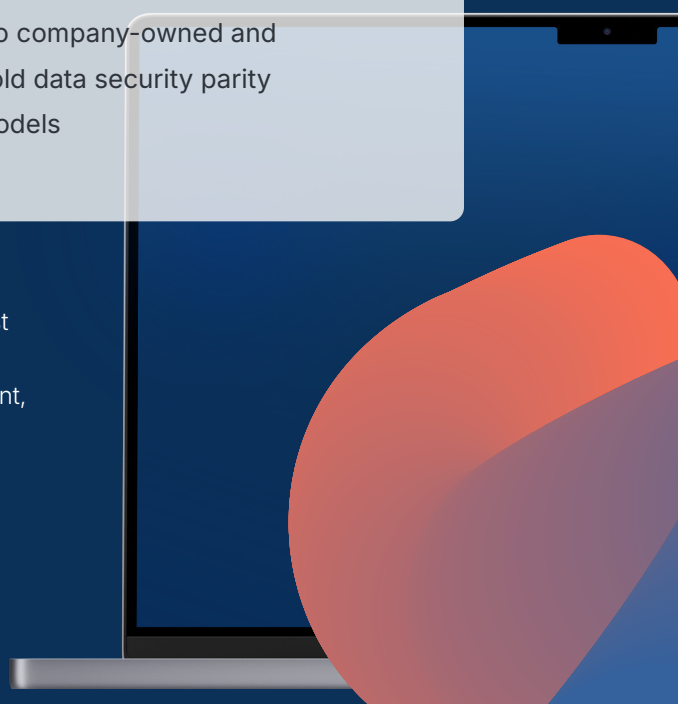
- [ ] Integrate identity and access management into security stack
- [ ] Enforce strong password policies holistically across your infrastructure
- [ ] Safeguard data with an extra layer of protection by requiring multi-factor authentication
- [ ] Maintain data integrity by encrypting data on all network connections
- [ ] Verify device and credential health with ZTNA before access to business resources is granted

Compliance Standards

- [ ] Align with industry standards and frameworks
- [ ] Create baselines tailored to acceptable risk tolerances
- [ ] Implement security policies to ensure compliance
- [ ] Conduct regular audits to measure security posture
- [ ] Continuously improve processes through iterative feedback

Additional Considerations

- [ ] Layered protections provides multiple safety nets to mitigate risks throughout your security stack
- [ ] Securely share rich telemetry data with integrated solutions to unlock advanced workflows
- [ ] Automate tasks to improve efficiency and reduce human error
- [ ] Simultaneously improve security and the user experience by implementing SSO and passwordless authentication
- [ ] Extend protections to company-owned and BYO devices to uphold data security parity across ownership models



Successfully securing Mac in the enterprise and getting them to "play nice" with other platforms requires more than just reactive defense. It demands a proactive, integrated approach to support every layer of the enterprise. By focusing on the core checklist sections above and fortifying your foundation with integrated solutions, organizations create a resilient, scalable security plan that evolves alongside the threat landscape.

The result is not only improved protection for devices and data but also measurable business benefits, like increased operational efficiency, stronger user privacy and enhanced stakeholder productivity.

As Mac continues to see increasing rates of adoption in the enterprise, aligning security strategies with industry best practices ensures your organization stays secure, compliant and ahead of the curve.

jamf

Start building a stronger security foundation today by implementing these core best practices with Jamf for Mac

www.jamf.com