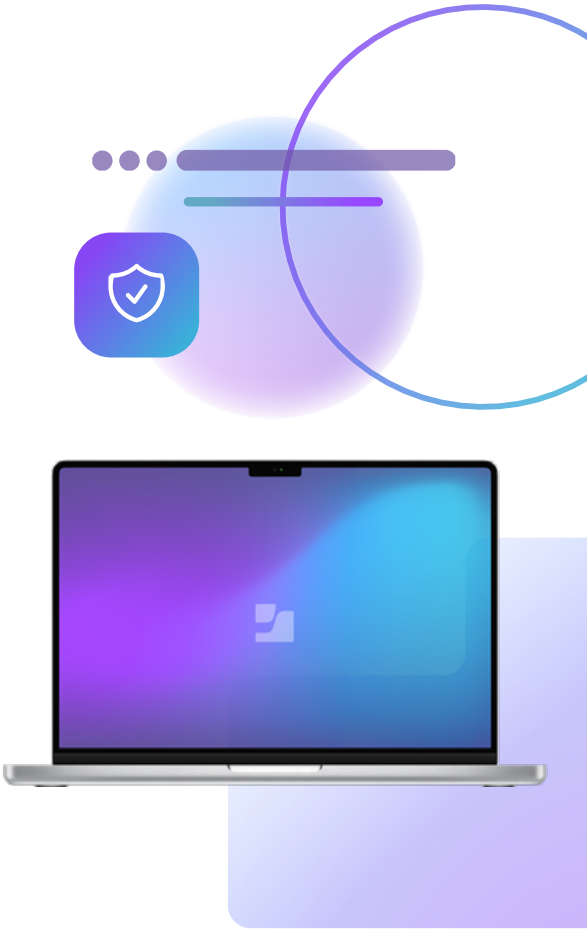
jamf

Checkliste: Suche nach Sicherheitslücken

Ein kurzer Leitfaden für IT-Admins und SecOps-Teams, die Macs verwalten

Ingenieure, Marketingfachleute, Führungskräfte, Kreativteams und viele mehr nutzen den Mac bereits gerne bei der Arbeit. Der Mac erfreut sich immer größerer Beliebtheit: Im zweiten Quartal 2025 wurde ein Wachstum von 21,4 % in Vergleich zum zweiten Quartal 2024 verzeichnet - mehr als bei jedem anderen Computerhersteller.



Das ist keine Überraschung. Schließlich **arbeiten die Mitarbeiter:innen gerne mit Macs**. Die zunehmende Verbreitung des Macs im Unternehmen bedeutet, dass immer mehr Mitarbeiter:innen ihr Lieblingsgerät für die Arbeit nutzen, was ihre Zufriedenheit und Produktivität steigert. Aber was bedeutet das für IT- und Sicherheitsexperten?

Macs und Windows-PCs sind unterschiedlich. Sie haben unterschiedliche Betriebssysteme, Hardware-Strategien, Architekturen und Design-Philosophien. Das bedeutet, dass auch der Schutz der Daten anders aussieht. Admins, die bisher vor allem mit Windows gearbeitet haben, haben möglicherweise Lücken in ihrer Strategie, insbesondere bei einer großen Geräteflotte. Da der Mac - die Hardware und die Software - von Apple hergestellt wird, benötigen Admins die nötigen Tools, die auf dem Apple Ökosystem aufbauen und dieses verstehen.

In dieser Checkliste werden wir kurz auf Strategien speziell für die Mac-Sicherheit eingehen, um Ihnen zu helfen, mögliche Sicherheitslücken zu erkennen. Wir gehen auf Nutzung, Identität und Zugang, Endpunktsicherheit und Compliance ein, mit Checklisten, die speziell auf IT- oder Sicherheitsexperten zugeschnitten sind.

Möchten Sie noch tiefer einsteigen? Dann sehen Sie sich unser Whitepaper an

Defense-in-Depth: Schließen von Sicherheitslücken durch Integration und Schichtung von Lösungen

Checkliste der Sicherheitslücken für IT-Admins

Zero-Touch-Bereitstellung und Gerätenutzung

Sie sollten Folgendes berücksichtigen:

- Verwendung des Apple Business Managers mit Ihrer Plattform für das Mobile Device Management (MDM)
- Automatisierte Geräteregistrierung zur Definition von Payloads und Beschränkungen
- Erzwingen einer Mindestversion des Betriebssystems, bevor der Mac den Einrichtungsassistenten durchläuft

Nutzerauthentifizierung und Integration von Identitätsprovidern

Sie sollten Folgendes berücksichtigen:

- Integration der Plattform Single Sign-On mit Ihrem Identitätsprovider (IdP) und MDM
- Ein MDM, das die Konfiguration für Extensible Single Sign-on unterstützt
- Für privilegierte Operationen ist eine Authentifizierung nach der Erstanmeldung erforderlich

Bereitstellung von Apple OS Updates

Sie sollten Folgendes berücksichtigen:

- Bereitstellung automatischer Updates und jährlicher Software-Upgrades - ein anderer Zeitrahmen als bei Windows-Geräten
- Management- und Sicherheitsanbietertests mit der neuesten macOS Version (wichtig: Betatests bei größere Versionen)
- Bereitstellung schneller Sicherheitsmaßnahmen ohne die Produktivität der Nutzer:innen zu beeinträchtigen

32 % der Organisationen haben ≥1 Gerät mit kritischen und patchbaren Schwachstellen

360-Bericht

SecOps-Checkliste für Sicherheitslücken

Angleichung an Compliance Frameworks

Sie sollten Folgendes berücksichtigen:

- Automatisierte Härtung von Geräten durch Integration in das **macOS Security Compliance Project** (mSCP)
- Unterstützung von Benchmarks und Baselines wie **CIS Level 1 und Level 2** oder **NIST 800-171**
- Implementierung, Aufrechterhaltung und Automatisierung von Verwaltungseinstellungen zur Durchsetzung spezifischer Sicherheitskontrollen in der gesamten Mac Flotte

Endpunktsicherheit für Mac-spezifische Bedrohungen

Sie sollten Folgendes berücksichtigen:

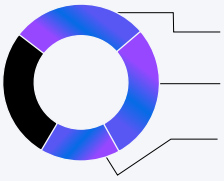
- Speziell entwickelte Tools zur Abwehr bekannter und neuer Mac-spezifischer Zero-Day-Bedrohungen
- Implementierung eines Endpunktschutzes in Echtzeit, der integrierte Funktionen von macOS wie XProtect, Gatekeeper und Notarisierung nutzt
- Bedrohungssuche nach Mac-spezifischer Malware unter Berücksichtigung neuester Expertenforschung

Streaming von macOS-Telemetriedaten an bestehende SIEM/SOAR

Sie sollten Folgendes berücksichtigen:

- Tools, die Telemetriedaten direkt von der Endpoint Security API beziehen
- Anpassung der macOS-Telemetriedaten an bestehende SIEM-Datenmodelle
- Tools, die Telemetriedaten für die unmittelbare Nutzung kontextualisieren
- Echtzeitanalyse von macOS-Sicherheitsereignissen, wie z. B. Gatekeeper-Umgehung oder Malware-Erkennung durch XProtect

Die häufigste Mac-Malware:

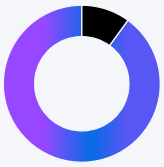


Infostealers **28,36 %**

Adware **28,13 %**

Trojaner **16,61 %**

360-Bericht



Über **90 % der Cyberangriffe** gehen auf Phishing zurück.

360-Bericht

Installation und Überwachung von Apps

Sie sollten Folgendes berücksichtigen:

- Tools, um macOS-Software von Drittanbietern in ihren Umgebungen auf dem neuesten Stand zu halten
- Mac App-Versionen und Berichte über die Nutzung
- Kontrolle der App-Vertriebskanäle über verwaltete Konten und Entwicklerzertifikate

Zugang für Nutzer:innen und Geräten zu Unternehmensressourcen

Sie sollten Folgendes berücksichtigen:

- Nutzung von Apple Technologien wie Network Relay, um Zero-Trust-Netzwerkzugriff zu ermöglichen
- Hardwaregestützte Geräteattestierung über Secure Enclave für bedingte Zugriffsrichtlinien
- Aufbau von Zero-Trust-Modellen speziell für die macOS Plattform

Diese Checkliste hilft Ihnen, eine Defense-in-Depth-Strategie zu entwickeln.

jamf

www.jamf.com/de/

Möchten Sie tiefer eintauchen?
Lesen Sie unser Whitepaper.