jamf

5 hidden security gaps to check in your Apple fleet

Check every statement that applies, then count your total below.

1.

CONFIGURATION DRIFT

The device still checks in. The configuration is no longer the one IT intended.

- [ ] Settings on some devices may have changed since enrollment without our knowledge.
- [ ] We rely on scheduled inventory checks rather than continuous monitoring to detect configuration changes.
- [ ] No automated process exists to correct a device that has drifted from its configuration.

2.

UNPATCHED DEVICES

Most devices are patched. The exceptions create the exposure.

- [ ] We cannot verify full fleet patch coverage without manual effort.
- [ ] Devices that are offline or on different networks sometimes miss update cycles.
- [ ] We cannot easily determine how long a device has been running an outdated OS version.

3.

THREATS MDM CANNOT SEE

A device can be enrolled, reporting green and actively compromised at the same time.

- [ ] We do not have dedicated endpoint security tooling beyond MDM on our Mac fleet.
- [ ] Behavioral signals, suspicious processes or indicators of compromise are not visible in our current toolset.
- [ ] We would not know if a threat was running on a device that shows as compliant in our MDM dashboard.

4.

STALE ACCESS

Yesterday's access rights often survive today's role change.

- [ ] Access permissions are not always updated when an employee changes roles or leaves.
- [ ] Device access is not adjusted automatically when a user's status changes.
- [ ] Former contractors or reassigned employees may still have access to resources they no longer need.

5.

DISCONNECTED TOOLING

Risk often accumulates in the spaces between tools.

- [ ] Management, identity and security tools operate independently.
- [ ] A non-compliant device flagged by MDM could still pass through our identity layer without being blocked.
- [ ] A security event detected at the endpoint does not automatically trigger a response in our management platform.

Why these gaps are easy to miss

These gaps hide behind device states that look completely normal: enrolled, reporting and active. They rarely announce themselves through alerts. More often, they surface after an audit, an incident or a security review.

Your result

0-3 → **Limited exposure**

Few indicators of hidden gaps, though some blind spots may still exist.

4-8 → **Blind spots emerging**

Some gaps may already exist without obvious warning signs.

9-15 → **Multiple hidden gaps**

Several exposures may be hiding behind devices that appear healthy and compliant.

These gaps do not show up as alerts. They show up as incidents.

Filling the Gap: macOS Security identifies and shows how to close the gaps your current tools are not showing you.

jamf

www.jamf.com

Download the White Paper