Does your Mac fleet need an EDR?

Five inputs and deployment cost.

1. Fleet shape. Who uses the Macs, and what runs on them. Twenty developer laptops pose a different problem from two thousand student devices.

---

2. Obligations. Essential Eight target, contract clause, cyber-insurance requirement, customer security review. Note the maturity level if one is already set.

---

3. Incident history. What has actually happened, including incidents you suspected but could never prove.

---

4. Existing coverage. Tick what you run. Note what it really does, not what you assumed.

- ☐ Compliance checks. MDM asking “is the setting on?” A status, not a record of what ran.
- ☐ Point-in-time queries. osquery asking “what is on the Mac right now?” A snapshot.
- ☐ Application control. “Should this binary run?” Its decisions, not what an allowed binary did next.
- ☐ Continuous monitoring and response. Retained events, rules over them, and something that can act.

Everyone already has XProtect: free, always on, and including behavioural detection of unknown malware. But Apple owns the logic, and there is no record you can search. Nobody chose it, so don't count it as coverage you added.

Honest gaps: _____

5. Who answers the alert at two in the morning? A name, not a team. Which hours? What gets escalated? What happens when nobody is available? If the name is yours, a product that generates alerts is buying you a second job. That may still be the right call. Just count your own time as part of the cost, and consider a managed service.

Deployment cost. Day one user experience and help desk load. Battery and performance. Alert noise, especially on developer Macs. Getting it off cleanly if you change your mind.

If the answer is yes, or probably

Ask these, then listen for specifics: lists, limits, failure modes. If the answer stays at the level of the user interface, keep asking.

1. What macOS activity do you actually see, and where are the gaps?
2. Which operations can you block before they happen, and what is the performance cost?
3. Can we inspect and tune the detections that will alert our team?
4. What does deployment cost in macOS permissions, performance, noise and removal?

Follow-up: can detection content be exported, and in what format?

If the answer is not yet

Defensible if your risk is low, existing controls cover the likely paths, and nobody has time to deal with the alerts. If the only problem is who would run it, consider a managed service.

- Pilot application control. Use audit or monitor mode where available; check what the current macOS release provides.
- Enforce the MDM baseline you already claim.
- On osquery, enable evented collection. Test the overhead before rollout.
- Retain events centrally, make sure you can query them later, and verify the retention.
- Write down what would change this answer: a new maturity target, more sensitive data, an incident, or a team who could run it.

Review date: _____

Companion to the talk “Does Your Mac Fleet Need an EDR? A Field Guide for Mac Admins” by Victor Lyuboslavsky.