



Segura® EPM for macOS

Vendor Briefing



Our Vision



Granular Least-Privilege for macOS

Action-level elevation and sudo control for secure, productive macOS use.



Simple, Seamless User Experience

Lightweight, intuitive, and seamless for users and admins.

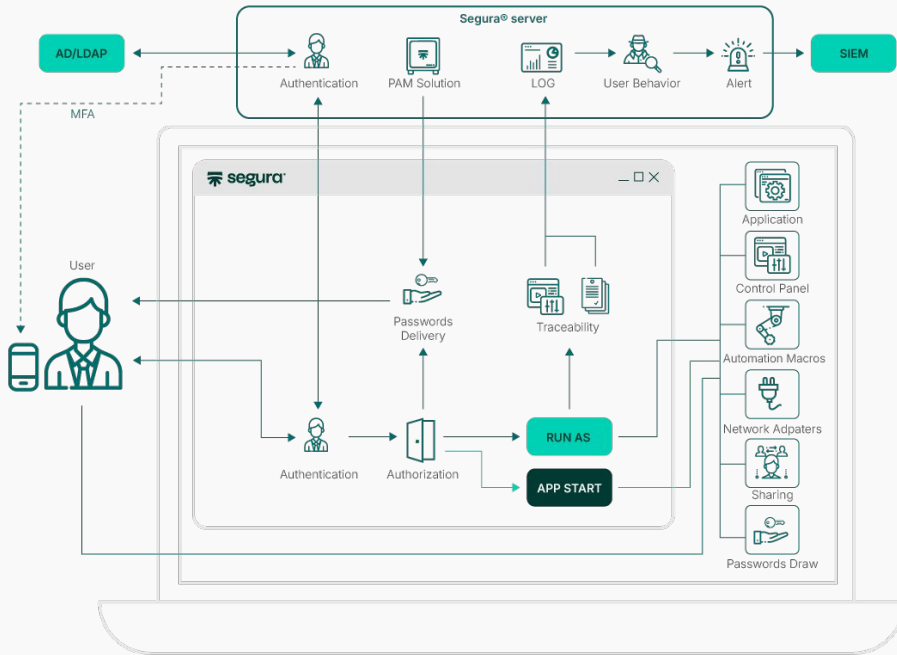


Enterprise-Grade Control & Compliance

Centralized policies, workflows, and audit visibility at scale.

EPM for macOs

Segura® can prevent privilege abuses at Mac endpoints by securely controlling privileged credentials usage.



Problem

Lack of control over privileged credentials in workstation does not allow security accountability and doesn't inhibit malicious users.

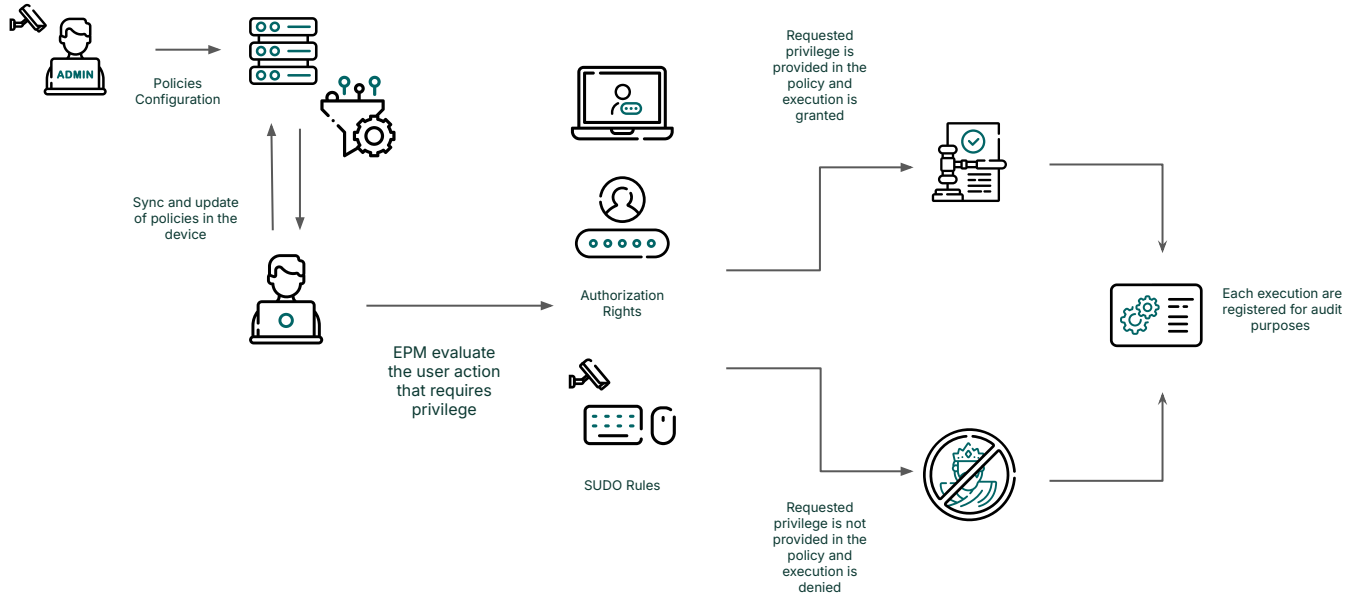
Solution

Segura® PEDM module securely manage workstation privileged credential by controlling use and creating centralized accountability.

Impact

Reduce workstation security risks.

EPM macOS - Execution Flow





Demonstration

Demonstration Scenario

EPM for macOS

1

**Access
List**

2

**Workflow
for
Executions**

3

**Session
Recording**

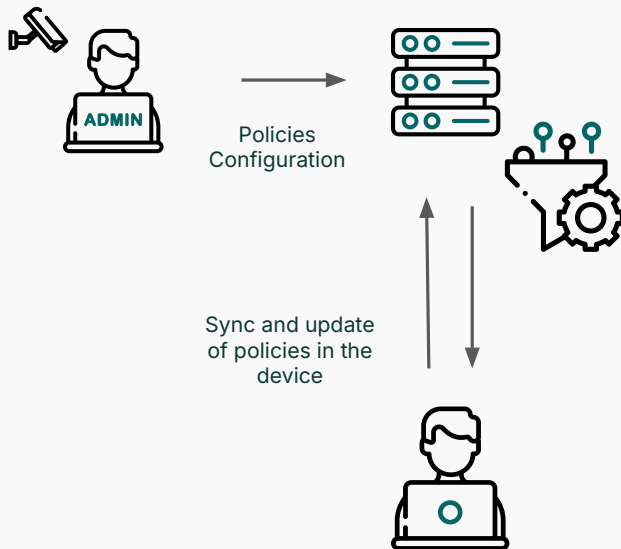
4

**Sudo
Management**

5

**Authorization
Rights**

Access Lists



Problem

Uncontrolled or unregulated application access can result in policy violations, security gaps, or compromised endpoints.

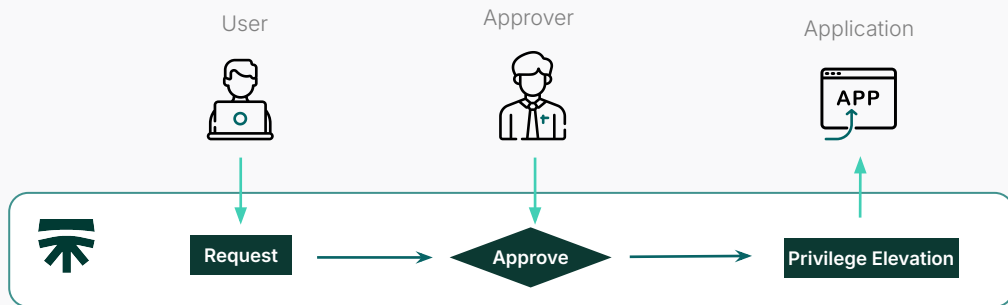
Solution

Centralizes management of allow/deny policies, defining granular access for users and machines. Automates enforcement and supports auditability.

Benefit

Blocks unauthorized actions, enforces security standards, streamlines compliance, and improves operational oversight.

Workflow for Executions



Problem

Unvalidated or unsupervised execution of sensitive actions increases risk and weakens security governance.

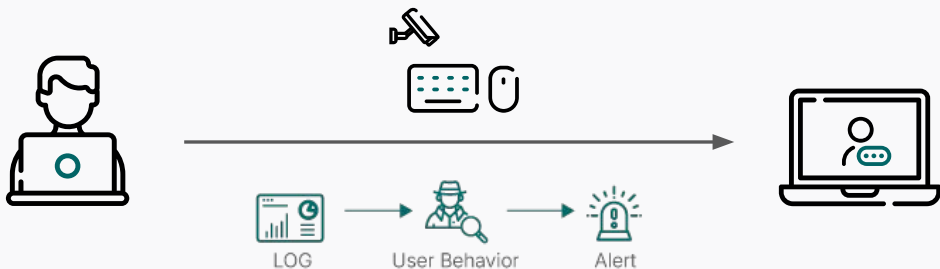
Solution

Implements automated multi-level approval workflows for critical operations, requiring justification and customizable policy checks before execution.

Benefit

Guarantees compliant, auditable processes and enables scalable enforcement of least-privilege principles.

Session Recording



Problem

Missing or incomplete activity records prevent thorough audits, hinder incident investigations, and reduce compliance effectiveness.

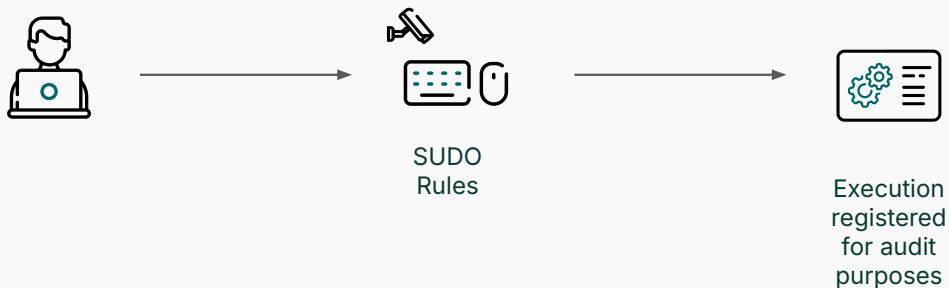
Solution

Missing or incomplete activity records prevent thorough audits, hinder incident investigations, and reduce compliance effectiveness.

Benefit

Enables precise audit trails, reconstructions, and proactive risk mitigation through high-fidelity records.

Sudo Management



Problem

Uncontrolled privileged command execution via sudo can cause security breaches or unintentional system changes.

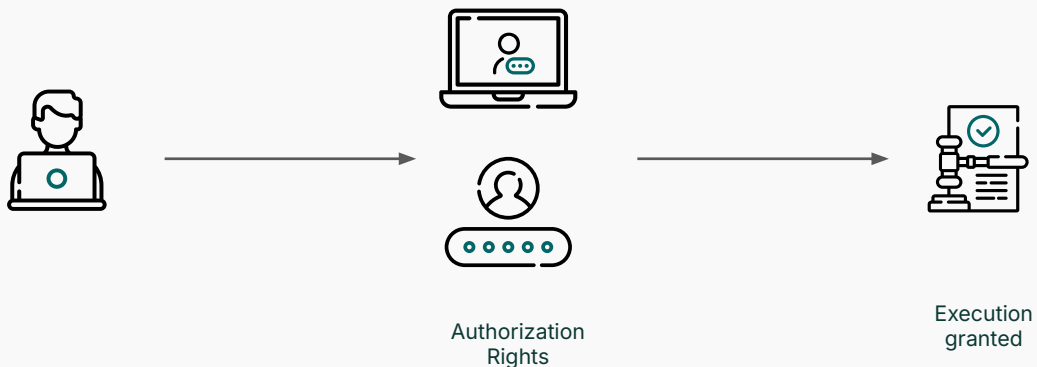
Solution

Centralizes sudo command controls, restricting, monitoring, and logging privileged activities in accordance with policy.

Benefit

Reduces privileged risks, enforces fine-grained controls, and improves command accountability.

Authorization Rights



Problem

Excessive administrative rights create unnecessary risk and dependency on privileged accounts for routine tasks.

Solution

Grants users only the rights they need, with automated provisioning and revocation, minimizing standing privileges.

Benefit

Increases security, accelerates workflows, and enforces least-privilege access at scale.

Why Segura® EPM for macOS?

- 1** Recognized and industry-awarded User Experience (UX)
- 2** Least-privilege: per-permission elevation with sudo governance
- 3** Automated trust: JIT approvals and granular authorization rights
- 4** Unified compliance: access lists, session recording, centralized audit logs



Customer Cases



Large Digital Payments Fintech

Company with a market value of over USD 1 billion.

Situation

- ✓ Engineering organization with a large portion of developers on macOS.
- ✓ **Fleet size: 2,200+ macOS workstations.**
- ✓ Strong audit and compliance requirements around endpoint privilege management.
- ✓ Developers historically relied on local admin to perform day-to-day tasks.

Problem

No effective macOS privilege-elevation governance, **creating audit gaps and operational risk;**

Needed granular, per-action elevation (e.g., at command/app level) to preserve developer productivity while enforcing least privilege;

Required a structured way to map applications and commands to meet compliance expectations.

Solution

Deployed Segura EPM for macOS to **control sudo and provide granular, policy-based privilege elevation per action;**

Removed standing local admin; established policies that map approved applications and commands for authorized elevation;

Prioritized granular elevation capabilities on macOS specifically to meet this client's requirements;

Results

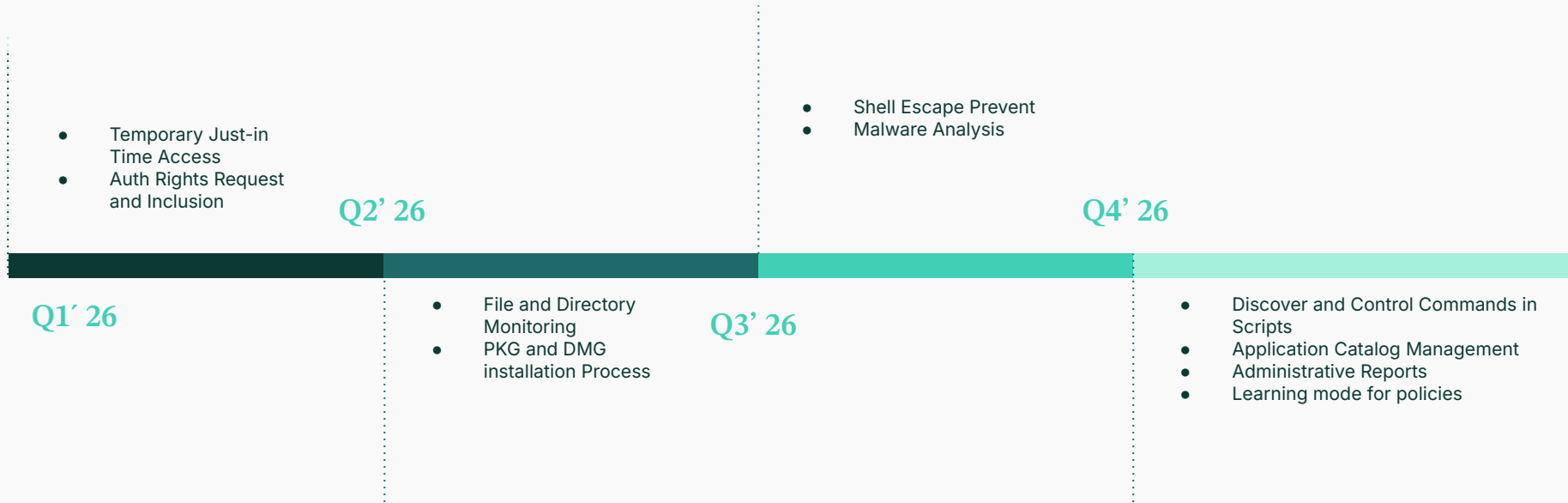
Revoked administrator access across the macOS fleet while enabling controlled, auditable elevation;

Established a sustainable culture of **privilege control through mapped apps/commands and clear policies;**

Passed a security audit, meeting critical compliance requirements;

The macOS EPM deployment was decisive for deal win.

Roadmap* for EPM macOS



* All dates and features listed in this document are an estimation of what we see coming in the next releases, and it may change according to segura's strategy. This Roadmap is valid until Q2/2026 - After this date ask for an updated version

A person in a dark suit is seen from the side, sitting at a table and typing on a silver laptop. The laptop screen shows a blurred image of a tree. In the background, another laptop and the hands of other people are visible, suggesting a meeting or collaborative work environment. The overall lighting is dim, with the laptop screen providing a focal point of light.

Briefing EPM macOS

analystrelations@segura.security

Segura® is a comprehensive identity security platform that gives your organization everything it needs to control privileged access and protect digital identities—quickly, easily, and securely. Globally recognized by Gartner, KuppingerCole, and Frost & Sullivan, Segura® stands out for its innovation, reliability, and exceptional customer experience.



Futureproof
Identity
Security

segura.security