



Modern, Agentless Endpoint Privilege Management

With reduced cyberinsurance cost, no productivity impact, and
no agents or additional IT resources needed to operate



Overview

Every endpoint with persistent local admin rights is a backdoor waiting to be exploited. Whether by ransomware, insider misuse, or accidental damage, unrestricted privilege equals unrestricted risk. Just one click, one bad app, or one missed alert can tank your fleet.

CISA flagged privilege escalation as one of the top exploited vectors in 2024. Yet many orgs still give users and IT staff permanent admin access. Why? Because traditional Endpoint Privilege Management (EPM) tools are clunky, agent-heavy, or kill productivity.

Unlike bloated legacy tools, Anzena is agentless, AI-native, and fast to deploy across Windows, macOS, and Linux. We enforce least privilege, enable JIT (just-in-time) admin access, and remove risky apps in real-time — all while integrating with your existing stack without slowing users down or overwhelming IT.

Why Anzena?



Just-in-Time Admin Access

Grant elevated privileges only when needed, for a limited time, with full traceability. Requests are seamless. Access is auto-revoked. Audit trails are built-in.



Frictionless User Experience

Users stay in flow. No more waiting on IT for basic installs or debug permissions. Our self-service workflows and smart approvals keep teams moving, securely.



Continuous App Risk Remediation Using Agentic AI

Spot dangerous apps that slip past your defenses. Block or uninstall based on behavior, not just signature, using intelligent scoring and flexible policies.



Save \$\$\$

- Cut licensing and operational costs by removing bloated legacy EPM tools
- Lower cyber insurance premiums by reducing attack surface



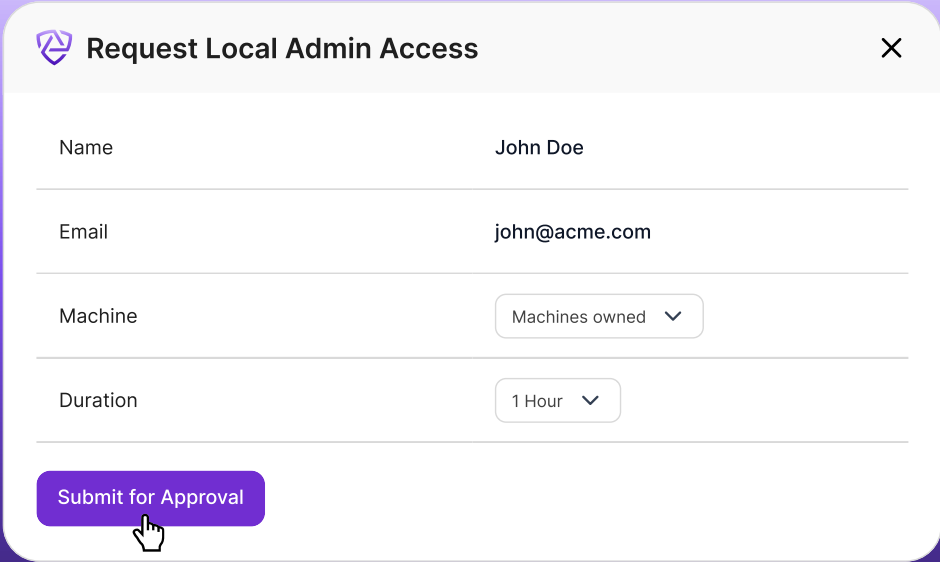
Zero Agents, Full Coverage

Anzena deploys fast and integrates with what you already use. Supports Windows, macOS, and Linux, across cloud, hybrid, or on-prem environments — all without the overhead of endpoint agents.

How It Works

Step 1: JIT Access Request

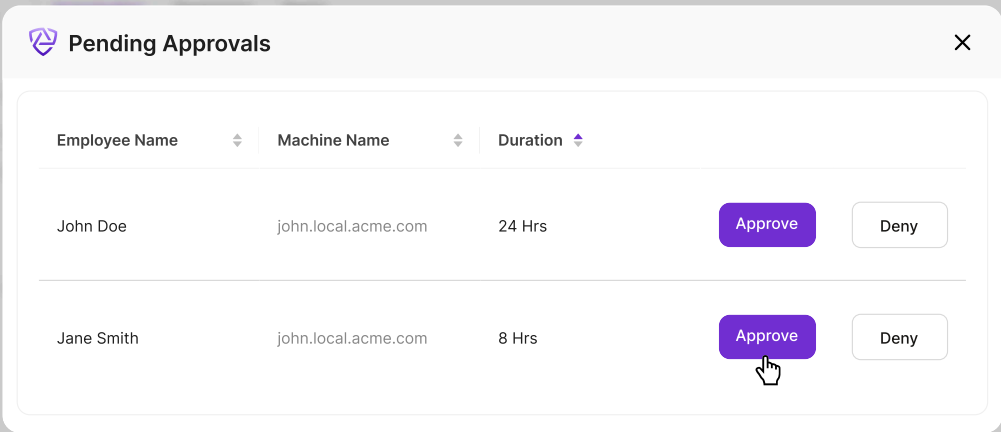
Employees request temporary admin rights through a simple, secure UI. You control when, how, and for how long access is granted.



A modal form titled "Request Local Admin Access" with a close button (X) in the top right corner. The form contains four input fields: "Name" with the value "John Doe", "Email" with the value "john@acme.com", "Machine" with a dropdown menu showing "Machines owned", and "Duration" with a dropdown menu showing "1 Hour". At the bottom of the form is a purple button labeled "Submit for Approval" with a hand cursor icon pointing to it.

Step 2: Approval + Enforcement

Approve requests manually or set up rules for automatic access. Optional workflows and policy logic help balance security with speed

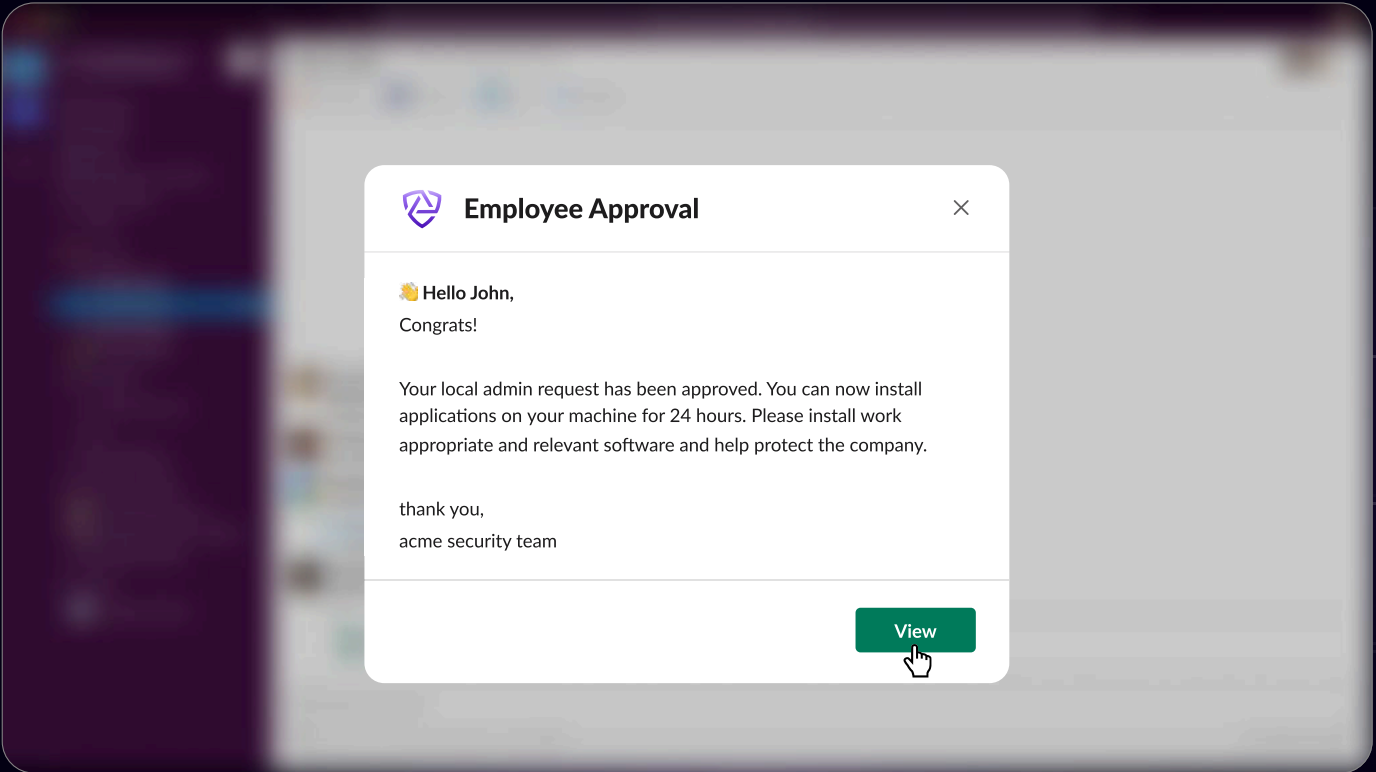


A modal titled "Pending Approvals" with a close button (X) in the top right corner. It displays a table of pending requests. The table has three columns: "Employee Name", "Machine Name", and "Duration". Each row has two buttons: "Approve" (purple) and "Deny" (white). A hand cursor icon is pointing to the "Approve" button for the second row.

Employee Name	Machine Name	Duration	Approve	Deny
John Doe	john.local.acme.com	24 Hrs	Approve	Deny
Jane Smith	john.local.acme.com	8 Hrs	Approve	Deny

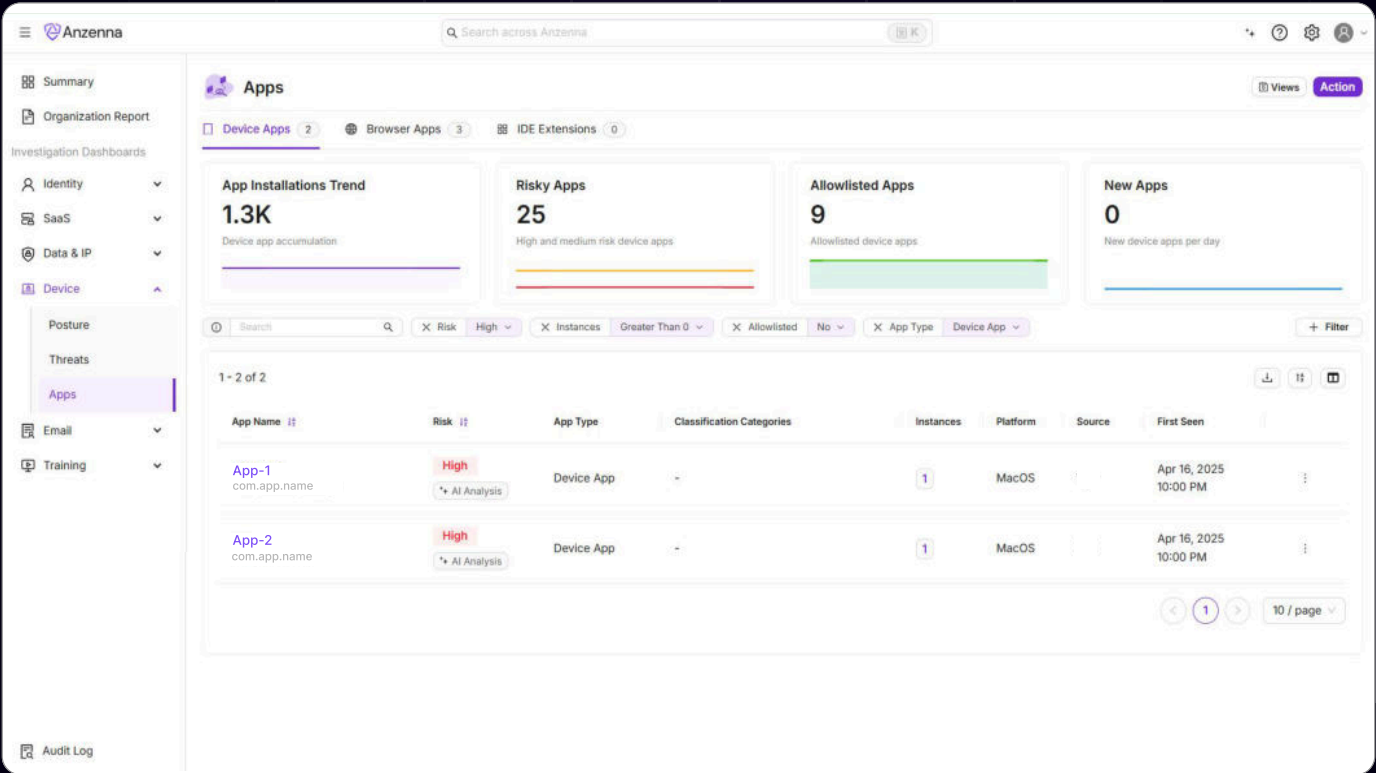
Step 3: Notification

Users receive admin rights for a defined period. Once the clock runs out, access is revoked automatically — no follow-up needed.



Step 4: Monitor & Remediate

Anzenna monitors & removes risky applications and unusual privilege use using AI. High-risk software can be flagged, blocked, or removed based on your policies.



Built for Your Environment

- OS Coverage: Full support for Windows, macOS , and Linux
- MDM-Driven: Leverages your existing MDMs, EDRs & Identity systems – no need to rip and replace
- Exception Handling: Allow permanent admin access for designated user groups
- Future-Ready App Control: Move beyond uninstall – enforce automatic run/block policies based on hash, publisher, path, and more

Benefits

- Replace brittle legacy EPM tools with a faster, AI-native solution
- Enable secure self-service admin access during critical moments (e.g., dev installs, debugging)
- Proactively reduce insider risk and ransomware exposure
- Monitor post-install app behavior and enforce dynamic compliance

Let's Talk

Anzenna is purpose-built for fast-moving IT and security teams that care about safety, speed, and user experience. Whether you're scaling your fleet, tightening controls, or prepping for audit, we'd love to show you how we fit in.



Reach out at sales@anzenna.com