

RLC Pro | Hardened + Ascender Pro

A pre-hardened Enterprise Linux base and the automation that enforces it, proves it, and keeps it that way. Compliance as a closed loop, not a backlog.

Regulated infrastructure carries two obligations that are usually treated as separate projects. You have to hold a consistent hardened posture on every server, and you have to prove that posture to an auditor on demand. Configuration hardening alone leaves the gaps that matter most, because kernel exploits and memory corruption operate below the controls most teams rely on. The automation meant to enforce hardening is often the least maintained platform in the estate, and the record of what it changed sits in a database that was never built to be searched, or gets forwarded into Splunk at a per-gigabyte ingest bill.

Hardening and proof are one problem, solved as one loop

RLC Pro Hardened is the secure base: a pre-configured, pre-remediated Enterprise Linux platform that neutralizes entire exploit classes and ships mapped to the frameworks your auditors expect. Ascender Pro is the engine that enforces and proves it: hardened, commercially supported Ansible automation with Ledger Pro, a native audit layer that records every change down to the file and correlates it against live CVE data. The hardened image sets the baseline. The automation holds the fleet to it and produces the evidence. Neither half leaves a gap for the other to cover.



Hardened on day one

A pre-hardened OS removes the manual work of securing a fleet server by server. Coverage starts the moment you deploy.



Enforced at fleet scale

Ascender automates remediation across the estate on the same Ansible engine you already run, proven from dozens of nodes into the hundreds of thousands.



Provable, continuously

Ledger Pro turns every change into a searchable audit trail tied to the job, the user, and the host, ready to hand to an assessor.

From hardened image to provable compliance, in one loop

The two products close a loop that manual processes leave open. The hardened image defines what a compliant system looks like. Automation drives the fleet to that state and keeps it there. The audit layer proves it held, and feeds the next remediation. Each stage hands the next exactly what it needs, with no remediation backlog accumulating between them.



01

Harden

RLC Pro Hardened ships pre-remediated images mapped to DISA STIG and CIS, with FIPS 140-3 validated cryptography. LKRG, hardened_malloc, and a reduced OpenSSH attack surface protect the kernel and memory below where EDR can see.



02

Enforce

Ascender Pro automates STIG and CIS remediation and configuration across the fleet on the Ansible engine you already run. Federated inventory routes each job to the right location; nested workflows chain full provisioning sequences.



03

Prove

Ledger Pro records what actually changed, to the file, tied to job, user, and host, and correlates every package against Enterprise Linux errata and CVE data. Query exposure by host, errata, CVE, or package through the API.



The loop closes itself: from "which hosts are exposed" to "patched and proven"

Query a CVE and Ledger Pro returns every affected host and the exact vulnerable packages. Hand that to an Ascender playbook and it patches only those packages, only on those hosts, and leaves everything else untouched. Drift works the same way in reverse: run the RLC Pro Hardened baseline nightly in check mode, and Ledger Pro records precisely what fell out of compliance without changing a thing. The hardened image is the standard the fleet is measured against, every night.

RLC Pro Hardened secures the base

- Privilege-boundary protection in glibc mitigated Looney Tunables (CVE-2023-4911) before public disclosure
- Hardened OpenSSH cuts library dependencies 54%, containing supply-chain blast radius like the XZ backdoor
- LKRG detects kernel exploitation at roughly 2.5% overhead and forwards to your SIEM over syslog
- Accelerated CVE mitigation covered systemd-coredump (CVE-2025-4598) while it stayed unfixed in upstream EL9

Ascender Pro enforces and records it

- One per-node license covers the controller and Ledger Pro, with every component included
- A continuously hardened container: CVEs tracked and prioritized, dependencies cut from ~1,900 to ~1,500
- Every change streamed in real time with a full diff; one deployment holds over two million package records
- Controller keeps a working window of weeks; Ledger Pro keeps the searchable history for a year

Audit-ready, not audit-burdened

Regulated environments turn security work into audit work. RLC Pro Hardened removes the manual remediation backlog by shipping images already mapped to the frameworks assessors expect. Ascender Pro removes the second tax: because the audit trail is native, you stop forwarding every Ansible callback on every host into Splunk just to keep a compliant record. Keep Splunk for security analytics and cross-source correlation, and stop paying its per-gigabyte ingest to log your own automation.

6 wks → 8 min

VM provisioning time

Financial services customer

18 mo → 2 wks

Customer onboarding at 300–600 VM scale

Healthcare services customer

180,000

Nodes in production, 400K jobs per month

Large enterprise customer

Mapped to the frameworks your assessors expect

Pre-hardened, pre-remediated images come mapped to DISA STIG and CIS, with FIPS 140-3 validated cryptography. That gives compliance teams evidence they can hand to an assessor, and CIQ provides the scripts, expertise, and support to tailor remediations to your specific requirements.

Release	FIPS 140-3 status	
9.6 LTS	Validated	FIPS 140-3 Inside, Cert #5117, #5116, #5113, #5095
10.2	In progress	Available as an option, FIPS 140-3 validation underway

Our engineers spent most of their time chasing vulnerabilities, patching, and preparing for audits across dozens of servers. With RLC Pro Hardened, it's like having an additional team of Linux security experts on staff.

Financial services firm

One vendor stands behind the whole loop

RLC Pro Hardened is built by CIQ's in-house Linux Security team, kernel and security engineers whose offense-informed approach targets the exploit paths attackers actually use. The same team backs the platform in production, with deep experience securing Linux across defense, finance, and critical infrastructure. Ascender Pro is the commercially supported, hardened build of the open-source Ascender project, backed by the same commitment to keep the platform current.



Adopt without re-platforming

Ascender is API-compatible with AWX, so existing integrations keep working. Migration is a database backup and a script; one customer moved 180,000 nodes by changing the image names in the manifest they already had. Move workloads incrementally, on your schedule.



Long-term support and indemnification

LTS can be added to RLC Pro Hardened for specific point releases, keeping you compliant for four additional years. Indemnification is built in, moving the legal and liability risk of open source off your balance sheet, not sold as an upsell.



Deploys where you already run

Ascender runs on RKE2, K3s, AKS, or EKS with a guided installer, fully air-gapped from the CIQ depot, or reaching isolated networks through external nodes. RLC Pro Hardened ships as AWS, Azure, and GCP images alongside on-prem.

Secure the base, automate the enforcement, prove the result. One loop, one vendor, evidence an auditor will accept.

✉ info@ciq.com

🌐 ciq.com/products/rocky-linux/pro/hardened/

🌐 linkedin.com/company/ctrlq

✕ twitter.com/ctrlq

▶ youtube.com/c/ctrlq