

RLC Pro | Hardened

Enterprise Linux engineered for security and compliance. Pre-hardened, always current, and protected against threats that configuration hardening alone cannot stop.

Attacks on Linux infrastructure keep getting faster, more automated, and more targeted, and the systems under the most pressure are the ones carrying regulated data: payment records, patient information, financial transactions. Security teams are expected to hold a consistent hardening posture across every server and prove it to auditors. Configuration-based hardening alone leaves the gaps that matter most, because kernel exploits and memory corruption attacks operate below the visibility of the controls most organizations rely on.

RLC Pro Hardened (Rocky Linux from CIQ Pro Hardened) closes that gap. It is a secure, pre-configured, expertly supported Enterprise Linux platform with **proactive, offense-informed protection** that defends against threats before they are publicly known.

Protection, currency, and speed without the manual work



Proactive security

Hardened against entire exploit classes, including zero-days, not just published CVEs. Memory allocation and kernel runtime integrity are protected by default.



Always current

Ships the latest Rocky Linux and stays continuously patched, with accelerated mitigation for the CVEs that carry the most risk.



Protected on day one

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

Hardening that covers the whole distribution

RLC Pro Hardened is a hardened build of community Rocky Linux that protects your workloads without changing how you run them. It hardens critical system packages to neutralize entire vulnerability classes while holding performance and operational stability across the distribution. The result is fewer zero-day exposures, less time spent chasing security updates, and advanced threat detection built into the OS rather than bolted on after the fact.

Where the protection actually comes from

Every measure targets a real exploit path used in active attacks. Here is what ships in the platform and the threat each component addresses.

Capability	What it does
Privilege boundary protection	Patches and configuration changes to critical packages such as glibc strip unsafe environment variables when crossing a privilege boundary. This proactive change mitigated CVE-2023-4911 (Looney Tunables) before public disclosure.
Reduced SSH attack surface	Hardened OpenSSH removes non-essential libraries for a 54% reduction in library dependencies, shrinking the attack surface and containing the blast radius of supply-chain attacks like CVE-2024-3094 (the XZ backdoor).
Kernel exploit detection and response	Linux Kernel Runtime Guard (LKRG) detects exploitation attempts and unauthorized modifications to a running kernel and its security-critical data, filling the kernel visibility gap that EDR tools cannot reach, at roughly 2.5% overhead.
Hardened memory allocator	A secure allocator (hardened_malloc) applies advanced heap protections against use-after-free, heap buffer overflow, and double-free exploits. Proven in production at scale by GrapheneOS.
Password security	passwdqc enforces stronger password policy, accepting roughly 4x fewer weak passwords, and yescrypt hashing makes credentials about 50x slower to crack on GPUs than standard sha512crypt.
Accelerated CVE mitigation	CIQ ships patches for high-priority CVEs ahead of standard updates to shorten exposure. RLC Pro Hardened was protected against CVE-2025-4598 (systemd-coredump) while it remained unfixed in upstream EL9.
Customizable security controls	A control framework provides predefined facilities for password security and reduced exposure of local privileged programs such as SUID root. Hardened permissions persist across DNF and RPM updates.
Package validation	Every package is CIQ-verified and cryptographically signed from verified CIQ repositories. Each image ships with a checksum and an SBOM.
SIEM integration	LKRG forwards to your existing security stack over standard syslog. Run it in sensor mode for log-only operation inside your monitoring setup.

“ 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

Audit-ready images, not a remediation backlog

Regulated environments turn security work into audit work. RLC Pro Hardened ships pre-hardened, pre-remediated images mapped to the frameworks your auditors expect, including DISA STIG and CIS, with FIPS 140-3 validated cryptography. That removes the manual remediation backlog, keeps controls consistent as systems update, and gives compliance teams evidence they can hand to an assessor. CIQ provides the scripts, expertise, and support to tailor remediations to your specific requirements.

Supported frameworks:



STIG



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

An in-house Linux security team, included

RLC Pro Hardened is built by CIQ's Linux Security team, kernel and security engineers focused on kernel runtime protection, hardened memory allocation, and library attack surface reduction. Their offense-informed approach targets the exploit paths attackers actually use.

The same team backs the platform in production, with deep experience securing Linux in high-security environments across defense, finance, and critical infrastructure. Need long-term support? LTS can be added to RLC Pro Hardened for specific point releases, keeping you compliant for four additional years.

Indemnification is built in, not an upsell

RLC Pro Hardened includes protection and indemnification that move the legal and liability risk of open source software off your balance sheet. CIQ stands behind the platform and delivers the coverage that keeps your legal and compliance teams satisfied.

See it run in your environment

Teams that need an enterprise-supported, pre-hardened Linux OS can request a demo or talk through deployment options with CIQ security engineers.

✉ info@ciq.com 🌐 ciq.com/products/rocky-linux/pro/hardened/

👤 linkedin.com/company/ctrlq ✕ twitter.com/ctrlq ▶ youtube.com/c/ctrlq