COMPETITIVE POSITIONING · PREPARED FOR BRAC BANK

RLC Pro | Hardened

The hardened Enterprise Linux that meets a regulated bank's security bar on the first boot, and **closes the exposures standard RHEL leaves to your team**.

Set the bar where a compliant OS stops and a hardened one begins

A production banking platform is judged on two things its operating system rarely controls on its own: how fast a critical vulnerability is closed, and what an attacker can reach if a single host is breached. A standard Enterprise Linux ships permissive defaults and leaves hardening, validation, and ongoing maintenance to your team. **RLC Pro Hardened is hardened at launch, with the defenses already configured and running.**

For a regulated bank the difference is measurable. RLC Pro Hardened boots at 96% DISA STIG and 99% CIS compliance with zero remediation, where a standard distribution starts near 45% and reaches roughly 84% only after a remediation playbook, then resets on every new deployment. FIPS 140-3 validated cryptography and runtime kernel protection are active by default. The same workloads run unchanged; the attack surface and the exposure window both shrink.

Hardened at launch, not after a playbook

Boots at 96% DISA STIG and 99% CIS with zero remediation. A standard distribution starts near 45% and reaches ~84% only after a playbook, resetting on every new deployment.

Protected during the patch gap

Runtime kernel-integrity monitoring and hardened memory defenses contain privilege-escalation and container-escape exploits before a fix ships. Critical CVEs mitigated within 30 days.

Supported in your time zone

Premium support answers SEV1 in 30 minutes, 24x7 follow-the-sun, from engineers near your region. Binary-compatible, so migration is a repository retarget.

PROOF — A LIVE CVE THAT RHEL STILL LEAVES OPEN

An attacker steals root credentials from an unhardened EL9 host in under five seconds.

systemd-coredump (CVE-2025-4598) lets a local user pull root password hashes and SSH keys from a running host almost instantly. As of CIQ's November 2025 analysis it remains **unfixed in upstream EL9**, where Red Hat rated it Medium (CVSS 4.7). RLC Pro Hardened blocks the working exploit out of the box through three independent defense layers, and the attack fails. That is the distance between a compliant baseline and a hardened one.

The platform, configured and running before you touch it

Every control below is built into the image and active on first boot, not a task left to your team. **This is the security posture a regulated bank would otherwise spend weeks assembling and re-proving on every deployment.**

Pre-hardened images

96.1% DISA STIG (446 of 468 rules; 97.6% on a subsequent scan) or 99.3% CIS at first boot with zero remediation. Fewer initial findings shorten the remediation backlog and speed approval.

Runtime kernel protection (LKRG)

Continuous kernel-integrity monitoring detects tampering and privilege-escalation exploitation with no third-party agent, and connects to your SIEM or EDR as a host sensor.

Hardened glibc, OpenSSH, and modules

A hardened glibc strips unsafe environment variables across privilege boundaries, OpenSSH ships with a reduced attack surface, and unused kernel modules are blacklisted by default.

NIST 800-171 pre-remediation

MATRIX IN DEVELOPMENT

Images ship pre-remediated for CIS, DISA STIG, and NIST 800-171 across the heaviest control families: access control, audit and accountability, configuration management, vulnerability management, and cryptographic protection.

Post-quantum cryptography

FIPS-compliant NIST post-quantum algorithms ML-KEM and ML-DSA, aligned to NSA CNSA 2.0 ahead of the 2027 transition.

DISA Vendor STIG IN PROCESS

Assessed against the DISA STIG for RHEL 9 today; an RLC Pro Hardened-specific vendor STIG is in submission and review, the primary federal credential after the DoDIN APL sunset.

Ansible Lockdown hardening playbooks

CIQ-maintained playbooks reach 96% STIG / 99% CIS in under 15 minutes when not starting from a pre-hardened image. Repeatable and fleet-deployable for new or existing systems.

Hardened memory allocator

hardened_malloc, the default for root-owned processes, mitigates heap overflow, use-after-free, double-free, and heap-metadata corruption, and zeroes freed memory to prevent data disclosure.

FIPS 140-3 validated cryptography

FIPS mode and the FIPS:STIG policy enabled at first boot on select builds, with CMVP-validated modules today (OpenSSL, NSS, GnuTLS, Libgcrypt, Kernel Crypto API). Ahead of the 21 Sep 2026 FIPS 140-2 sunset.

Extended audit trail

The default auditd configuration is extended to capture commonly-missed events: kernel module loads, privileged command execution, and discretionary access control (xattr) changes.

Binary compatibility and long-term support

1:1 binary-compatible with Enterprise Linux; existing application stacks deploy with minimal modification. Select minor versions carry four to eight years of long-term support.

On a standard distribution, every line above is a task your team owns: applied by hand, validated, and re-proven on every new deployment. **RLC Pro Hardened ships them done, and keeps them that way.**

The exploits this stops, and the ones RHEL leaves open

Hardening earns its place by stopping real attacks before a patch exists. The hardened modules neutralize documented, high-severity CVEs out of the box.

Protected by	Documented CVEs neutralized
LKRG + sysctl hardening	Dirty Pipe (CVE-2022-0847, 7.8), Dirty COW (CVE-2016-5195, 7.8), OverlayFS privilege escalation (CVE-2023-0386, 7.8), Netfilter use-after-free (CVE-2024-1086, 7.8), and the runc container escape (CVE-2024-21626, 8.6), plus 14 further kernel exploit CVEs across io_uring, nftables, and pipe.
Hardened glibc + packages	Looney Tunables (CVE-2023-4911, 7.8), Baron Samedit / sudo (CVE-2021-3156), and the glibc iconv overflow (CVE-2024-2961, 8.8).
hardened_malloc	Use-after-free (CWE-416), heap buffer overflow (CWE-122), and out-of-bounds write (CWE-787).

The patch gap is where banks get hurt

CIQ mitigates critical vulnerabilities within 30 days of a fix becoming available, coordinates patching across all supported variants, and provides interim mitigations where a kernel update cannot be applied immediately. Where the upstream vendor under-rates or declines to fix a vulnerability, CIQ maintains its own repository, re-scores against CVE.org severity, patches what its customers need, and contributes the fix back upstream. On CIQ's own measurement it publishes fixes roughly 50% faster than Red Hat and Ubuntu. The community Rocky build cannot do this; it waits on the upstream cycle.

Built from how systems are attacked, not a checklist

The hardening is built around real exploitation rather than audit checkboxes. That is why named, high-severity exploits are contained out of the box, before a patch exists. A passing compliance scan confirms a configuration; it does not stop the exploit.

The exposure window is the real risk

Compliance proves a posture at a point in time. RLC Pro Hardened narrows the window between disclosure and fix, contains what a breach can reach in the meantime, and verifies continuously that nodes have not drifted out of compliance.

~50% faster
Fixes published vs. Red Hat and Ubuntu, on CIQ's own measurement

30-day SLO
Committed mitigation window for critical CVEs, across all variants

19+ CVEs
High-severity kernel exploits stopped out of the box

Requirements to write into the RFP

Each statement below is accurate to RLC Pro Hardened and difficult for a standard RHEL bid to satisfy. Every line maps to a control a bank's security team or auditor can verify. **Write the requirement, and the field narrows on its own.**

Requirement to specify	RLC Pro Hardened	Standard RHEL
Runtime kernel-integrity monitoring for tampering and privilege escalation, no agent required	✓ Included (LKRG); feeds SIEM / EDR	✗ Not offered
Pre-hardened image meeting DISA STIG and CIS at first boot with zero remediation	✓ 96% STIG / 99% CIS at first boot	✗ ~45% at install; ~84% only after a playbook, resets each deploy
FIPS 140-3 validated cryptography enabled by default	✓ FIPS mode + FIPS:STIG at first boot	✗ Manual enablement
Post-quantum readiness aligned to NIST and CNSA 2.0	✓ ML-KEM and ML-DSA supported	✗ Not addressed
Hardened core packages against memory-corruption and privilege-boundary attacks	✓ hardened_malloc, glibc, OpenSSH; modules blacklisted	✗ Standard packages
Extended audit trail capturing commonly-missed security events	✓ Module loads, privileged commands, xattr changes	✗ Default auditd
NIST 800-171 pre-remediated image across the heaviest control families	✓ Shipped pre-remediated	✗ Manual remediation
Critical CVEs mitigated within a committed window, including those upstream will not fix	✓ 30-day SLO; CIQ-maintained repo	✗ Tied to upstream cycle
Continuous compliance with drift detection across the fleet, not a point-in-time scan	✓ Enforced and verified continuously	✗ Manual or third-party tooling
SEV1 support response with engineers in the bank's time zone	✓ 30-min SEV1 (Premium), 24x7	✗ Varies by plan and region

Migration is straightforward. RLC Pro Hardened is 1:1 binary-compatible with Enterprise Linux, so the move is a repository retarget rather than a reinstall: existing application stacks deploy with minimal modification, there is no downtime, and it runs alongside your current RHEL during the transition. Select minor versions carry four to eight years of long-term support.

Complete the solution: continuous enforcement with Ascender Pro

RLC Pro Hardened secures and hardens the host. **Ascender Pro, CIQ's commercially supported automation platform, enforces that posture across the entire fleet and proves it continuously** — an option that completes the solution rather than a separate stack to assemble, running your existing Ansible playbooks unchanged.

Enterprise Ansible automation

Web UI, role-based access control, workflow orchestration, and AES-256 encrypted credential management with HashiCorp Vault and CyberArk integration. Existing Ansible playbooks run unmodified.

Fleet-scale enforcement of the hardening

Deploys the hardening playbooks across the estate and continuously verifies every node matches its intended state, so first-boot compliance holds over time rather than drifting.

Built-in observability and compliance

Searchable job history, configuration drift detection, CVE and errata tracking by host and package, exportable compliance reporting, and read-only self-service access for auditors.

No separate logging tier

Audit-grade observability is native, removing the need for a separate logging platform (commonly Splunk) and the recurring cost that comes with it.

Stability where AWX falls short

AWX has had no stable release since 2024 and carries a backlog of unpatched vulnerabilities. Ascender Pro ships version-locked, tested releases with a managed upgrade path, commercial support and SLAs, and indemnification available.

Proven outcomes

Documented customer results include VM provisioning cut from six weeks to eight minutes, and onboarding from eighteen months to two weeks.

Support that matches a bank's operating reality

Premium

24x7 follow-the-sun, with a 30-minute response on SEV1 issues, from engineers near your region across the Middle East, India, and Japan.

Standard

Local business-hours coverage, 8am to 6pm in your time zone, with a one-hour response on SEV1 issues.

Access and escalation

CIQ portal, web, email, and ticketing, with dedicated Slack channels for premium customers and escalation calls as needed.

Support is commercial and backed by SLAs, with indemnification available and no vendor lock-in. The customer-success engineer who knows your environment handles your tickets, so escalations do not start from zero.

Across every alternative Enterprise Linux, **RLC Pro Hardened is the only option that ships runtime kernel protection, FIPS 140-3 cryptography, and DISA STIG and CIS hardening active at first boot, with critical CVEs mitigated on a committed schedule.** Paired with Ascender Pro, that posture is enforced and proven across the entire fleet. Standard RHEL and the other distributions leave that work to your team to build, validate, and maintain on every deployment.

Next step: CIQ engineering is available for a technical deep-dive and a proof-of-concept on your environment.
info@ciq.com · ciq.com/products/rocky-linux/hardened/