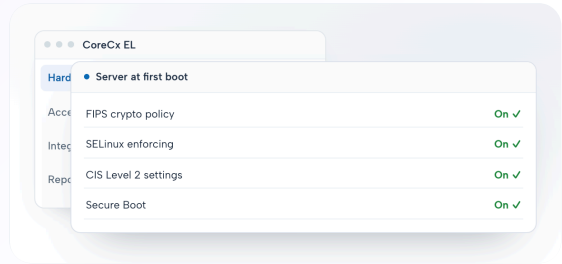




CoreCx EL

The hardened operating system every CoreCx product runs on, secure from the first boot.

An enterprise Linux built for regulated sites. FIPS mode, SELinux, Secure Boot and CIS Level 2 settings are on before the first login, updates are signed and checked for vulnerabilities, and one command prints the evidence your auditor asks for. Install it on-premise on physical servers or any leading hypervisor, air-gapped if you need, or in your own cloud.



- ✓ Hardened from first boot
- ✓ Locked-down access
- ✓ Tamper-evident by design
- ✓ On-premise or your own cloud

FIPS mode

Crypto

CIS Level 2

Benchmark

Installer or virtual appliance

Delivery

Into the 2030s

Support

What CoreCx EL does for you

Hardened from first boot

FIPS mode with the FIPS crypto policy, SELinux enforcing, Secure Boot through a signed boot chain and CIS Level 2 settings are applied before anyone signs in. Kernel settings are hardened, unused kernel modules are blocked, and full-disk encryption is offered at install.

- FIPS mode
- SELinux enforcing
- Secure Boot
- Disk encryption option

Locked-down access

Only management access is open on the firewall, and every other port is closed. Remote root sign-in is off, sign-in attempts are limited with a legal banner, and key-only sign-in is one setting away. Accounts lock for 15 minutes after five failed attempts, passwords need 14 characters across four character types, and idle sessions close after 15 minutes.

- Management-only firewall
- Account lockout
- Strong passwords
- Idle session timeout

Tamper-evident by design

Audit rules aligned to CIS and STIG are locked, so nobody can switch them off without a reboot. A daily integrity check compares system files against their install baseline, unknown USB devices are blocked, and the system journal is kept on disk with a fixed size cap.

Locked audit rules Daily integrity check USB device control
Persistent journal

Compliance you can print

One command checks every control and prints a PASS, WARN or FAIL report for your auditor. Every CoreCx product team runs the same check after installing, so a new failure is treated as our defect, not your problem.

Hardening report PASS, WARN and FAIL
Checked by every product

Install anywhere in minutes

An offline installer for physical servers and any leading hypervisor, or a ready virtual appliance with a first-boot wizard or unattended setup. Every copy creates its own machine identity, host keys, USB policy and integrity baseline, so no two servers share secrets.

Offline installer Virtual appliance Unique identity per server
Automatic secure disk layout

Current while air-gapped

Updates come from a signed CoreCx repository and can be carried to offline sites as files. Every build passes a vulnerability gate before release, with long-term support into the 2030s.

Signed repository Offline updates Vulnerability gate
Long-term support

What is hardened before the first login

No scripts to run and no checklist to follow. These controls are on from the first boot, on every server.

Cryptography

FIPS mode with the FIPS system-wide crypto policy.

Access control

SELinux enforcing for every service.

Boot and disk

Secure Boot through a signed boot chain, with optional full-disk encryption.

Network

Management access only. Every other port is closed.

Accounts

Lockout after five failures, 14-character passwords, password history and a 15-minute idle timeout.

Audit

CIS and STIG-aligned audit rules, locked until the next reboot.

Integrity

Daily file integrity check against the install baseline. Unknown USB devices are blocked.

Kernel and storage

Hardened kernel settings, unused modules blocked, restricted disk mounts and core dumps off.

Works with what you run

Every CoreCx product Physical servers
Leading hypervisors Bring your own cloud
Air-gapped sites

Security, built in

- ✓ FIPS mode and FIPS crypto policy
- ✓ SELinux enforcing and Secure Boot
- ✓ CIS Level 2 settings and STIG-aligned audit rules
- ✓ Management-only firewall and account lockout
- ✓ Daily file integrity check and USB control
- ✓ Signed updates with a vulnerability gate

Specifications

Crypto	FIPS mode
Benchmark	CIS Level 2
Delivery	Installer or virtual appliance
Support	Into the 2030s
Deployment model	On-premise, air-gapped or bring your own cloud
Installation	Signed, offline installer

From box to hardened server

STEP 1

Choose the format

An offline installer for physical servers and any leading hypervisor, or a ready virtual appliance.

STEP 2

Answer a few questions

A first-boot wizard sets the name, network and administrator, or you supply the answers unattended.

STEP 3

Hardened on first boot

Every control switches on, and the server creates its own identity, host keys and integrity baseline.

STEP 4

Prove it and build on it

Run the hardening check, keep the report for your auditor, then install your CoreCx products.

Where CoreCx EL makes the difference

Pass the host hardening audit on day one

Appliances arrive on a generic Linux that fails the CIS checklist and needs weeks of hardening.

OUTCOME

Hardening report printed, not performed.

Stay patched in an air-gapped site

Air-gapped sites fall months behind on patches because updates need the internet.

OUTCOME

Current without a connection.

See CoreCx EL on your own infrastructure.

Book a demo, or ask our product team for the architecture pack and a sizing.

corecx.ai

contact@corecx.ai