PATCH MANAGEMENT FOR REGULATED INFRASTRUCTURE

Policy-governed patching for the Linux and Unix estate you run on.

Axiler OS Patch is an on-premises patch management platform for Linux, Unix and ESXi environments, built for organizations that need policy-governed automation, audit-ready hardening, and locally delivered support.

ON-PREMISES, LINUX-NATIVE | AIR-GAP CAPABLE | 24X7 LOCAL SUPPORT

PLATFORM COVERAGE

- Enterprise Linux
- Debian-based
- SUSE Linux
- Unix (AIX)
- Virtualization (VMware ESXi)

THE PATCH LIFECYCLE, GOVERNED END TO END

01 **Discover**
Assets, packages, patch state

02 **Prioritize**
CVE mapping, severity, exposure

03 **Stage**
Repo sync, jump server, air gap

04 **Deploy**
Staged rollout, scheduled reboot

05 **Verify**
Hardening checks, drift, evidence

CORE CAPABILITIES

Policy-driven automation
Severity-based targeting, staged rollout, scheduled reboots and dependency-aware task chaining across the full lifecycle.

CIS and MBSS hardening
Pre-deployment checks and auto-hardening against CIS benchmarks and your internal MBSS baseline, with drift reporting every cycle.

Air-gapped and jump-server ready
Patch fully isolated network segments through repository synchronization and controlled staging, with no direct internet path.

RBAC, 2FA and key-based access
Role-separated administration, two-factor authentication and SSH key-based access enforced by default across the console.

Component-level rollback
Revert individual packages rather than whole systems, with full activity logging and change evidence for audit control.

Vulnerability-aware prioritization
CVE-to-patch mapping through integration with your existing scanner, so the exposure that matters gets patched first.

Central reporting and visibility
Scheduled compliance and exception reports, dynamic asset grouping and real-time patch-state visibility across the estate.

Local, mission-critical support
24x7 support delivered by Axiler's Bangladesh-based engineering team, with a defined SLA for production environments.

TECHNICAL SPECIFICATION

DEPLOYMENT	On-premises, Linux-native central management server with no Windows Server dependency.
PLATFORMS	Ubuntu, Debian, RHEL, CentOS, OEL, SUSE, Fedora, AlmaLinux, Rocky Linux, AIX, ESXi.
LICENSING	Per-instance licensing, scaled to estate size with a defined expansion model.
AUTHENTICATION	SSH key-based access, role-based access control, two-factor authentication (SSO or TOTP).
INTEGRATIONS	Vulnerability scanners (Tenable, Qualys, Rapid7); SIEM and ITSM through API.
REPORTING	Scheduled and on-demand reports, dynamic grouping, exportable formats.
SUPPORT	24x7 local support from Axiler's Bangladesh-based engineering team, defined SLA.

COMPLIANCE AND AUDIT EVIDENCE

Every cycle measures the estate against your control set before and after deployment, so compliance is proven by the patch run itself.

CIS Benchmark coverage 96%
Level 1 and Level 2 checks, auto-hardened pre-deployment.

PCI DSS 6.3.3 94%
Critical patches applied within the 30 day window.

Internal MBSS baseline 92%
Deviation flagged per host, with drift reporting each cycle.

- Signed activity log for every task and approval.
- Exception and rollback records exported for auditors.

Request a technical walkthrough

Linux, Unix and ESXi patch orchestration for regulated environments. sales@axiler.com · axiler.com

Axiler Pte. Ltd. · 111 Somerset Road, TripleOne Somerset · Singapore 238164