TuxCare

Datasheet

Always-On Security
for Financial Systems That Can't Pause

Financial services infrastructure doesn't get to take a break. Transactions run continuously, markets move in real time, and regulatory expectations **never skip a beat.**

In an industry where a single minute of downtime is measured in millions, infrastructure must be as resilient as the markets themselves – which, today, brings you to **TES**.

TuxCare Enterprise Support

TES delivers the security, compliance, and support that helps financial institutions protect and maintain Linux-based systems without compliance lapses, downtime, forced upgrades, or vendor lock-in. By simplifying compliance, providing access to experts, removing reboot-driven disruption, and extending the life of critical platforms, TuxCare turns community-powered, RHEL-compatible Linux into stable, enterprise-grade financial infrastructure.

Built for Regulated, Always-On Financial Environments

Financial organizations operate under constant pressure – market hours, customer expectations, audits, and regulatory scrutiny all collide on the same systems. TuxCare is designed for institutions running a mix of modern and legacy Linux environments, where stability matters as much as security and where outages or rushed migrations carry real financial risk.



The result: continuous protection, predictable operations, and fewer trade-offs between uptime and compliance.

Financial Systems We Support

TuxCare secures Linux systems across the financial stack, including:

Transaction and settlement systems	Market and risk platforms	Customer-facing and and API-driven services	Long-lived analytical systems
Core banking platforms, payment gateways, authorization services	Trading engines, pricing systems, risk and exposure analysis	Mobile banking applications, customer portals, fintech APIs	Claims processing, actuarial models, historical data platforms

These systems stay online, patched, and compliant – even during peak usage and market hours.

Compliance that Keeps Pace With Security

Audit-Ready Patching for Regulated Workloads

Financial compliance frameworks demand timely remediation and traceability. TuxCare aligns patching workflows with regulatory expectations, such as PCI DSS

What are the built-in advantages?

- Detailed vulnerability documentation and traceable patch history
- Clear evidence for auditors – no manual log chasing
- Reduced audit prep time and compliance overhead

Security updates activate immediately, closing exposure windows instead of extending them until the next reboot.

FIPS-Friendly Cryptographic Modules that You Can Rely on Long Term

Financial systems often outlive upstream support timelines, but encryption requirements don't expire.

TuxCare provides access to FIPS-validated cryptographic modules across supported Linux releases, helping organizations maintain regulator-recognized data protection on both modern and legacy platforms.

Expert Support that Eliminates Technical Roadblocks

Bridging the Gap Between Open Source Freedom and Enterprise Reliability

For organizations running community distributions like Rocky Linux or AlmaLinux, the lack of a traditional vendor safety net can be a significant hurdle. TES provides the 24/7 expert "backstop" needed to run your community-powered Linux OS with the same confidence as a proprietary commercial OS – delivering enterprise-grade support so that you can stay on the community distro you love.



What Teams Gain:

Expedited 24/7 break-and-fix support, covering:

- Consultation on installation and migration issues between OSs of the same major version
- Package update issues
- OS bug troubleshooting
- Kernel crash issues
- Hardware support requests

Enterprise-grade support for your distro and a range of open-source applications, covering:

- Application support and configuration assistance
- Design and architecture review
- Data storage and backups
- KernelCare or Extended Security Updates setup/update issues

Remove the Operational Cost of Reboots

Rebootless Live Patching for the Kernel and Critical Components

Traditional patching forces financial teams to choose between security and availability. **TuxCare removes that choice by loading security fixes directly into memory while systems keep running – no restarts, no maintenance windows, no service interruptions.**

What this eliminates:

- Interrupted transactions or trades
- Downtime during market hours
- Delayed patch activation waiting on reboots

What teams gain:

- Rapid CVE remediation as vulnerabilities are disclosed
- Continuous uptime for always-on financial services
- Fewer change windows and operational escalations



Why Financial Institutions Choose TuxCare

Organizations running Linux as critical financial infrastructure choose TuxCare because it removes friction from security and compliance:

- Rebootless patching for always-on environments
- FIPS-validated cryptographic modules across supported releases
- PCI DSS–aligned, audit-friendly patching workflows
- Clear, traceable patch history for regulators and auditors
- Lifecycle extensions for legacy but business-critical systems
- Predictable pricing, transparent SLAs, no per-node lock-in
- 24/7 expert Linux support and hardening guidance

Secure Your Financial Linux Stack – Without Slowing It Down

TuxCare helps financial institutions protect critical systems while preserving uptime, operational stability, and open-source flexibility.

Reduce audit pain. Eliminate downtime risk. Keep security controls active without forcing disruptive change.



Learn more about TuxCare Enterprise Support for Financial Services at:

tuxcare.com/use-case/finance

Certifications

FIPS 140-1 140-2 · AICPA SOC · PCI DSS Level 1 Service Provider · EU GDPR Compliant · CCPA · SAM

Awards

2021 IT World Awards Information Technology Cyber Security · AVA Digital Awards Platinum Winner · Cyber Security Excellence Awards Winner 2023 · 2022 Stevie Winner Gold · Gold · Bronze 2023 Stevie Winner

Follow TuxCare on Social Media

+1 (800) 231-7307 sales@tuxcare.com