TuxCare
We Take Care of Linux

WHITEPAPER

Security at TuxCare.

TuxCare Security

Content

Introduction	3
Organizational Security	4
Protecting customer data	9
Architecture overview	11
Conclusion	12

Introduction

TuxCare is a live patching and Linux security innovator offering affordable cybersecurity solutions that make enterprise-grade support available to organizations of all sizes, in any industry. Before spinning off to become an independent organization, TuxCare was part of CloudLinux – a leader in Linux security innovation that has been continually increasing cybersecurity, stability and availability of Linux servers and devices since 2009.

Our flagship live patching solution, KernelCare Enterprise, was launched in 2014, enabling automated patch deployment without reboots or downtime – and has grown substantially since then. Based on customer demand, we've added integrations to popular vulnerability scanners, reporting and automation tools, and an improved ePortal patch server to apply rebootless patches to servers that don't have access to the internet.

In this document, we aim to explain our high-level system architecture and our approach to security.

Organizational security

Security policies and training

TuxCare's employee security practices apply to full- and part-time employees and contractors who have access to TuxCare's internal systems. Before gaining access to internal systems, all employees must pass background checks, pass and sign-off onboarding information security awareness training and sign a contract with Non-Disclosure agreement. All employees are required to complete privacy and security training annually. The training covers a wide range of privacy and security topics, including acceptable data use, phishing and social engineering, use of company-owned and personal devices, best practices to prevent malware, requirements around physical security, and incident reporting. Upon termination of work at TuxCare, a former employee's access to TuxCare systems is removed immediately by the IT department using a standardized procedure, including disabling all accounts.

CloudLinux's security program and team

TuxCare employs a team of security professionals—comprising in-house employees—who oversee and run TuxCare's security program. This team supports the three pillars of our security program through a variety of initiatives and best practices:

- Product security
  - Train developers on secure application development practices and other best security practices
  - Provide design and code reviews for detection of possible security flaws
- Infrastructure and operations security
  - Manage firewalls, website certificates, and other pieces of security infrastructure
  - Gather security-relevant logs and maintain tools for log analysis
  - Provide a platform for secure deployment, monitoring, and patching of CloudLinux's production services

Organizational security

- Manage endpoint-device-protection tools and services
- Coordinate external penetration testing
- Conduct ongoing vulnerability assessments
- Respond to security incidents

- Compliance and risk management
  - Coordinate audits and maintain security certifications
  - Develop and maintain TuxCare's information security management system
  - Respond to customer inquiries
  - Review and qualify vendor security posture
  - Coordinate BCP/DRP activities
  - Manage privacy program

Penetration testing

Customers wishing to conduct their own penetration tests of TuxCare's applications may request to do so and should contact their TuxCare account representative. A third party is engaged quarterly to conduct an external network penetration test. The findings from the third-party security assessments are reviewed by the Security team, categorized by their severity, and tracked to resolution.

Organizational security

Vulnerability assessment

CloudLinux's Security team performs vulnerability assessments of TuxCare services as follows:

- Services before deployment to production are verified with a software composition analysis (SCA) service.
- Infrastructure is scanned continuously using the following security tools, such as Nessus.
- Public-facing web services are scanned continuously by web-application scanners.
- Post-release vulnerability assessments are performed by various vulnerability-management solutions.

Patch management

TuxCare regularly applies security patches to service infrastructure. The IT team subscribes to regular feeds and channels dedicated to notifications of critical updates for the asset types used at TuxCare. Critical patches are applied as soon as reasonably possible according to TuxCare's Patch Management Policy.

Security monitoring

TuxCare uses a set of instruments and processes for the detection of malicious, suspicious, or otherwise illegitimate actions within its own infrastructure, services, and applications. The company logs and retains administrative access, use of privileged accounts, and system calls on service critical servers in TuxCare environments. Analysis of these logs is automated when practical to detect potential issues and alert responsible personnel. Access to audit logs is restricted to the limited number of personnel who require this access to conduct their duties.

Organizational security

Incident management

TuxCare executes procedures for incident management that minimize downtime, service degradation, and security risks to customers and internal users. Security events are identified and communicated to TuxCares Security team through established channels. The Security team then defines the type of event, establishes its severity, and responds to it according to the approved service-level agreements (SLAs) based on industry best practices. Security events that may impact privacy are subject to additional analysis and response by TuxCare's Compliance team.

Secure software development

TuxCare's engineering teams use industry-leading managed services for roles and access policies, account management, certificate management, encryption and key management, secrets management, security logs collection and monitoring, firewalls, and network access lists. All code is checked in a version control system. Code changes undergo peer review and automatic integration testing. TuxCare applications, libraries, and other development artifacts are automatically scanned for known vulnerabilities, and fixes are applied promptly. Every development team has a regular cadence of security check-ins with the Security team and Infrastructure team, which is responsible for providing an optimal infrastructure toolkit to help engineers focus on product development. TuxCare's services are designed, developed, deployed, and tested against known security vulnerabilities, including those listed by the Open Web Application Security Project (OWASP). Guidelines for secure development and testing are maintained and communicated to all engineers.

Disaster recovery

TuxCare uses services deployed by its cloud hosting providers to distribute production operations across multiple availability zones located worldwide (Chicago and Miami in the United States, Germany and Poland in the European Union area). TuxCare has a Disaster Recovery Plan (DRP) to guide teams to recover after disruptions caused by unexpected events in compute capacity, applications, infrastructure, or data. The DRP is maintained by dedicated teams at TuxCare and is reviewed and tested annually.

Organizational security

Third-party vendors

TuxCare relies on a number of third-party vendors for specific services and functions, such as hosting our servers, email communication, customer support services, and analytics. Prior to using a third-party vendor, TuxCare executes a due diligence program and evaluates the vendor's security posture. TuxCare validates that personal information is removed from third-party systems after there is no longer any legal basis for its storage. Selected third parties are subject to continuous monitoring by a vendor-risk-management service.

Business model

TuxCare does not sell or rent users' personal data or share personal data with third parties to enable them to deliver advertisements. TuxCare only makes money by offering a paid product to consumers and businesses.

Protecting customer data

Authorizing employee access

Access to all TuxCare internal systems requires employees to authenticate via a single-sign-on system with mandatory multi-factor authentication. TuxCare adheres to the principle of least privilege. Requests to access internal systems are documented, reviewed, and approved by the respective managers and service owners. TuxCare management systematically reviews employees' access to the systems that hold or process customer data and revokes access if access is no longer needed to perform specific work tasks.

Endpoint protection

All TuxCare workstations are required to run endpoint-management software that enforces secure configurations, password rules, and encryption. It also facilitates a lock-when-idle function and allows for control to be taken remotely if a device is compromised or lost. Employee workstations run monitoring agents from an industry-leading vendor BitDefender to detect possible malware and suspicious behaviors. TuxCare's Security team collects device logs and monitors workstation alerts.

Legal compliance

TuxCare complies with the EU General Data Protection Regulation (GDPR) for the collection, use, and retention of personal information. For more detail, see TuxCare's Privacy Policy available at our websites. TuxCare employs a dedicated Compliance Officer with extensive expertise in data privacy and security. This professional reviews TuxCare product offerings and processes for compliance with applicable legal and regulatory requirements.

Protecting customer data

Account deletion

Customers have the ability to end their TuxCare subscription at any time. As in accordance with the Privacy Policy, the user's personal data is deleted from the internal and external services when the customer deletes their account. TuxCare may maintain the user's personal data for as long as reasonably necessary for legitimate business interests, including tax and audit purposes, and to comply with legal obligations.

Architecture overview

In this section, we'll explain how user data is transferred, stored, and processed securely by TuxCare infrastructure in the cloud.

Core infrastructure

All TuxCare server-side infrastructure is hosted in industry-leading secure data centers: Hivelocity located in Tampa, Florida and Hetzner located in Germany in the European Union area. The research and development infrastructure is located in Atman datacenter, Poland, European Union area. All components that process user data operate in TuxCare's private network inside our secure cloud platform.

Data encryption and isolation

Data is encrypted in transit and at rest:

- Connections between clients and the back-end TuxCare infrastructure are protected by up-to-date encryption protocols, including TLS 1.2.
- TuxCare customer data is encrypted at rest using LUKS aes-xts-plain64 encryption.
- Passwords are stored in encrypted databases with applied bcrypt hashing.

Each TuxCare user's data is segregated logically from other users' data. A user must be logged in to their TuxCare account—and any client request must be authenticated and authorized—in order for the user to access their data.

Conclusion

We know that security is of the utmost importance to you, and keeping data secure is a responsibility we take incredibly seriously.

Please contact TuxCare support or your TuxCare account executive if you have any questions regarding TuxCare's security.