WHITEPAPER

Security at CloudLinux, Inc.

CloudLinux OS and Imunify Security

As of January 1st, 2022

Content

Introduction

Since its founding in 2009, CloudLinux has become a leader in specialized hosting of OS providers. CloudLinux is on a mission to make Linux secure, stable, and profitable. We have spent more than 500 combined years working on Linux, and are changing how hosting companies and data centers use this technology we love by bringing it to millions of their customers. With more than 500,000 product installations and 4,000 customers, CloudLinux combines in-depth technical knowledge of hosting, kernel development, and open source with unique client care expertise.

CloudLinux OS product family now includes CloudLinux OS Shared, CloudLinux OS Shared Pro and CloudLinux Solo. Each product caters the needs of the customers from small VPS owners to hosting companies.

CloudLinux expanded to include Imunify360, Linux server malware protection. Imunify Security is a set of security solutions tailored to hosting providers and VPS owners. The goal of Imunify Security is to keep servers protected from different malicious attacks, bad bots, malware and many more. Imunify360, a flagman of Imunify Security, is a combination of antivirus, Firewall, WAF, PHP Security Layer, Patch Management, Domain Reputation with easy UI and advanced automation.

CloudLinux Inc. solutions - Imunify360 & CloudLinux OS - now address the needs of WordPress, Shared, Dedicated, VPS hosting by offering optimization & security of the server.

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

Organizational security

Security policies and training

CloudLinux's employee security practices apply to full- and part-time employees and contractors who have access to CloudLinux'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 CloudLinux, a former employee's access to CloudLinux systems is removed immediately by the IT department using a standardized procedure, including disabling all accounts.

CloudLinux's security program and team

CloudLinux employs a team of security professionals—comprising in-house employees—who oversee and run CloudLinux'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 CloudLinux'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 CloudLinux's applications may request to do so and should contact their CloudLinux 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 CloudLinux 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

CloudLinux 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 CloudLinux. Critical patches are applied as soon as reasonably possible according to CloudLinux's Patch Management Policy.

Security monitoring

CloudLinux 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 CloudLinux 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

CloudLinux 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 CloudLinux's 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 CloudLinux's Compliance team.

Secure software development

CloudLinux'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. CloudLinux 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. CloudLinux'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

CloudLinux 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). CloudLinux 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 CloudLinux and is reviewed and tested annually.

Organizational security

Third-party vendors

CloudLinux 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, CloudLinux executes a due diligence program and evaluates the vendor's security posture. CloudLinux 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

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

Protecting customer data

Authorizing employee access

Access to all CloudLinux internal systems requires employees to authenticate via a single-sign-on system with mandatory multi-factor authentication. CloudLinux adheres to the principle of least privilege. Requests to access internal systems are documented, reviewed, and approved by the respective managers and service owners. CloudLinux 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 CloudLinux 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. CloudLinux's Security team collects device logs and monitors workstation alerts.

Legal compliance

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

Customer data privacy

CloudLinux respects the privacy of user data, as specified in CloudLinux's Privacy Policy. Committed to the GDPR principles, CloudLinux never collects personal data without a lawful basis, limits the amount of collected and processed data, and deletes the data when it is no longer needed for the services outlined in CloudLinux's Privacy Policy (e.g., to provide and improve our services). Users can request a list of their personal data used in our services.

Protecting customer data

CloudLinux users can remove their personal data from CloudLinux's systems at any time by logging into their account, accessing the Settings page, and then deleting their account. Enterprise customers can contact their account representative for deletion. CloudLinux has a set of policies and technical controls that prevent employees from accessing customer data that is stored or processed by CloudLinux systems. Access to production systems is restricted to dedicated engineers who develop these systems and ensure their reliability and uptime. Production systems that work with user data are deployed in a separate infrastructure isolated from all other CloudLinux systems. Where appropriate, CloudLinux uses private keys and restricts network access to particular employees.

Processed and stored data

Information that users save in CloudLinux is stored by CloudLinux so users can access it again when desired. Information is stored until it is deleted by the user through CloudLinux. CloudLinux services access only that type of information that is necessary for provision of the rendered services.

Data retention and disposal

Customer data is deleted immediately from production services upon user deletion. CloudLinux deletes user's information from backups in 60 days after its removal from servers. CloudLinux's hosting service provider is responsible for ensuring that the removal of data from disks is performed in a responsible manner before they are repurposed.

Account deletion

Customers have the ability to end their CloudLinux 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. CloudLinux 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 CloudLinux infrastructure in the cloud.

Core infrastructure

All CloudLinux 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 CloudLinux'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 CloudLinux infrastructure are protected by up-to-date encryption protocols, including TLS 1.2.
- CloudLinux customer data is encrypted at rest using LUKS aes-xts-plain64 encryption.
- Passwords are stored in encrypted databases with applied bcrypt hashing.

Each CloudLinux user's data is segregated logically from other users' data. A user must be logged in to their CloudLinux 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 CloudLinux support or your CloudLinux account executive if you have any questions regarding CloudLinux's security.