Security Overview for LogRhythm CloudAI

This document provides important details about LogRhythm CloudAI and our commitment to the security and privacy of our customers and their data.

CloudAI Application and Service Security

LogRhythm operates a comprehensive software security program to ensure that CloudAI and our full software portfolio comply with our policies, standards, and controls. This program includes rigorous design standards, secure implementation and testing, and standardized practices for secure deployment and maintenance. As with all LogRhythm applications, we develop CloudAI with modern and memory-safe programming languages. Security is ensured during the solution delivery lifecycle through continuous static code analysis, manual security reviews, and regular independent penetration tests.

CloudAI Data in Transit

CloudAI accepts metadata (but not raw logs, which aren't used in any manner) from your LogRhythm Platform's data indexing layer and surfaces data and visualizations through your platform management layer. This connection is protected with unique X.509 certificates and AES encryption (TLS 1.2). Mutual authentication helps ensure that data in transit is available only to your intended recipients. Moreover, it provides both your organization and LogRhythm the ability to revoke authentication at any time.

CloudAI Data at Rest

CloudAI streamlines product delivery and updates by storing metadata in a world-class, multi-tenant cloud service that complies with SOC 2 Type II. Data is segregated by account and stored in logically separated areas of the file system, enhancing data protection. Additionally, non-live customer metadata and analytical results are secured at rest using block storage and volume encryption provided by our PaaS technology partner.

CloudAI Analysis of Anonymized Data

To enable analysis and learning across CloudAI's global deployment footprint, LogRhythm may collect and maintain information from customer environments to generate threat models that benefit the broader customer base. These models are anonymized per applicable law.

CloudAI Data Retention

CloudAI stores metadata to allow the recalculation of anomaly reports across new timespans. The original metadata is securely deleted from our infrastructure after it is no longer useful, upon customer request, or upon the conclusion of a service relationship. Anonymized data, described in the previous section, is retained indefinitely to support the accuracy of CloudAI.

CloudAI User Authentication and Access

LogRhythm provides access to CloudAI through your LogRhythm platform, giving you flexible control over who in your company can access CloudAI dashboards and data. All summary data accessed from the LogRhythm Platform is encrypted with TLS over HTTPS.

Select LogRhythm and CloudAI Standards, Compliance, and Certifications

LogRhythm is committed to integrating security into our organizational management and technical processes. This is also the foundation for our compliance with industry standards, including:

- **SOC 2 Type II:** LogRhythm has achieved SOC 2 Type II certification of our organizational security, availability, process integrity, and confidentiality processes, providing assurance about the systems we use to protect customer data.
- **Privacy Shield:** The EU-US and Swiss-US Privacy Shield Frameworks were designed by the U.S. Department of Commerce, European Commission, and Swiss Administration to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the European Union and Switzerland to the United States.
- **TrustArc**: TrustArc performs third-party assessment and verification of EU-US & Swiss-US Privacy Shield Compliance.
- **General Data Protection Regulation (GDPR):** With an enforcement date of May 2018, the EU General Data Protection Regulation (GDPR) will replace the Data Protection Directive 95/46/EC. It is designed to harmonize data privacy laws across Europe, to protect and empower EU citizens with data privacy, and to reshape the way organizations across the region approach data privacy. We have adapted our security and privacy controls in anticipation of GDPR and will continue to adapt as standards evolve.

LogRhythm Operational Security Practices

LogRhythm applies security best practices and technologies to safeguard our employees, data, products, and infrastructure. Our comprehensive operational security program applies policies, standards, and processes based on the ISO 27001 framework and NIST 800-53 standard.

- **Information Security Policies:** We maintain, regularly review, and update internal information security policies, including incident response plans.
- **Data Centers and Service Providers:** We screen all service providers that handle customer data and bind them under contract to meet appropriate confidentiality and security obligations. These vendors offer SOC 2 Type II reports and provide expected physical security protections.
- **Access Controls:** We apply a need-to-know/least-privilege-necessary standard for access to sensitive data in our databases, systems, and environments.
- **Audit Logging:** We maintain and monitor audit logs for our services and systems.
- **Vulnerability Management:** We continuously scan CloudAI for vulnerabilities and we conduct regular, independent penetration tests.
- **Employee Background Screening:** We conduct background checks on all prospective LogRhythm employees.
- **Security Awareness Training:** Security is the responsibility of everyone working for LogRhythm. We train and empower our employees so they can identify security risks and take action to prevent incidents.

LogRhythm Incident Management

LogRhythm operates its own Security Operations Center (SOC) and Incident Response (IR) team. Together, they ensure that we are protected from and can detect and respond to a broad set of threats, including those commonly targeted at our industry and company profile. These teams monitor our core security infrastructure (which includes best-of-breed protection, detection, and response capabilities at the user, network, and endpoint levels) for operational and security events. LogRhythm also conducts regular security assessments and penetration tests, addressing findings as appropriate.

Further Reading on LogRhythm Security Practices

- LogRhythm SOC 2 Certificate*
- SIG Lite Questionnaire Response*
- LogRhythm Global End User License

*NDA required

©2017 LogRhythm Inc.