Security Overview for LogRhythm Cloud

This document provides important details about LogRhythm Cloud and our commitment to the security, availability, and confidentiality of our customers and their data.

LogRhythm Cloud Application and Service Security

LogRhythm maintains administrative, physical, and technical safeguards as part of a comprehensive security program that is designed to:

- ensure the confidentiality, integrity, and availability of customer data.
- comply with current industry standards and all applicable laws.
- protect against misuse, threats, or hazards to the security or integrity of customer data.
- enforce compliance by the LogRhythm workforce.

This program includes rigorous industry standard design measures, secure implementation and testing, and best practices for secure deployment and maintenance. As with all LogRhythm applications, we develop LogRhythm Cloud 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.

LogRhythm Cloud Data in Transit

LogRhythm Cloud accepts logs only from LogRhythm System Monitor (SysMon) Agents. These connections are 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 and provides both your organization and LogRhythm the ability to revoke authentication at any time.

Select LogRhythm and Cloud 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 I:** LogRhythm is on target to achieve Soc 2 certification, by the end 2019, 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.
- **General Data Protection Regulation (GDPR):** GDPR 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 to reflect the requirements under the GDPR and will continue to adapt as standards evolve.

LogRhythm Cloud Data at Rest

All customer data and analytical results are secured at rest using block storage and volume encryption.

LogRhythm Cloud Data Retention

The original customer data is securely deleted from our infrastructure after it is no longer functionally useful, upon customer request, or upon the conclusion of a service relationship. LogRhythm will delete all customer data within 30 days of conclusion of a service relationship unless otherwise mutually agreed with the customer.

For ongoing LogRhythm Cloud customers, data retention is based on the Time to Live (TTL) that the customer purchased with the product. The default TTL is up to 90 days.

LogRhythm Cloud Data Availability

This solution will initially be delivered as an individually managed instance of the LogRhythm platform. As part of the offering, LogRhythm provides infrastructure monitoring on a 24x7 basis and applies the latest software level and critical patches. LogRhythm is also responsible for health monitoring, updates to the SIEM platform, and backups.

LogRhythm Cloud User Authentication and Access

Access to LogRhythm Cloud is permitted only through a browser-based console. All data accessed from the LogRhythm Platform is encrypted with TLS.

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 and 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 LogRhythm Cloud 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 who works for LogRhythm. We train and empower our employees so that 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, and continuously addresses the findings of such assessments.

Further Reading on LogRhythm Security Practices

- LogRhythm SOC 2 Certificate (*NDA required*)
- LogRhythm Data Privacy Impact Assessment (DPIA)
- LogRhythm Global End User License