Lightrun

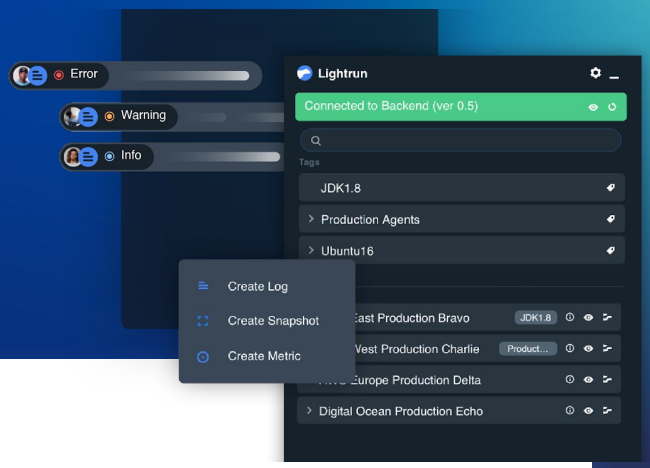
AICPA SOC 2 — AICPA Service Organization Control Reports — Formerly SAS 70 Reports

ISO

GDPR

HIPAA COMPLIANT

Security Datasheet



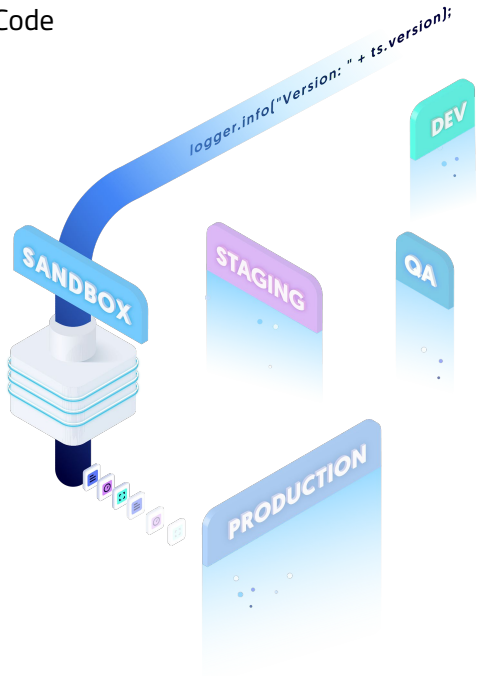
Introduction

As experienced cybersecurity engineers with strong cloud and SaaS backgrounds, the Lightrun team fully recognizes the importance of embedding security as part of the product design and delivery. This document provides a high-level overview of Lightrun's security model, architecture and primary controls. While there are no 100% bulletproof solutions, the Lightrun platform is designed with a significant investment in security from the ground up, as outlined in this document.

What Lightrun is and How it Works

Lightrun is a powerful production debugger that enables developers to securely add logs, performance metrics and traces to production and staging in real time, on demand. Lightrun eliminates the need to reproduce bugs locally or issue a new software version only for the sake of adding new logs or metrics. With Lightrun, developers and SREs gain 100% code-level observability and productivity.

Lightrun integrates directly into IDEs such as IntelliJ IDEA and Visual Studio Code via a plugin. When using the plugin to add a snapshot, Lightrun provides the stack traces, variable values and additional comprehensive details inside the snapshot, such that the execution on the server continues as usual. Meanwhile, the service owner gets the same level of insight into the code without pausing production services.



Lightrun provides enterprise-grade security and stability and is platform-agnostic, working on-prem, in the cloud, and in containers.

System Components and High-Level Architecture

Lightrun is comprised of these primary components:

	Placement	Description
 **Management Server**	SaaS or On-premises / Customer VPC	Managers manage users and configure agents and clients from a central command center. In the SaaS model the server is based on a multi-tenant, highly available and hardened CentOS 8, Java Spring Boot and a MySQL database. For on-prem, the server is provided as a Docker Image or a Helm Chart, and is based on a hardened CentOS 8 with Java Spring Boot and a MySQL database.
 **Client**	IDE plugin or Command Line Interface	Users pull or download the client plugin from a trusted source (cloud, marketplace or on-prem). In order to use the plugin, users register and create a unique account on the Lightrun Server.
 **Agent**	JAR Package / npm Package / PIP Pacakge	Lightrun's JVM agent is based on several Java 7 (or above) compatible JAR files and shared objects. Lightrun's Node.js & Python agents are npm and PIP packages, respectively. A simple package install is sufficient. The Lightrun library connects the application processes to the Lightrun Server component using a unique and dedicated API key that belongs to the tenant. The DevOps team or system administrators configure the server or service in order to run the agent on the relevant target platform (Tomcat, Jetty, Django, Flask etc).

All Lightrun system components undergo a strict hardening process prior to delivery to help reduce security risks or avoid the introduction of vulnerabilities to customer environments. All code libraries are scanned for vulnerabilities as are the Docker images, operating systems and other system components.

Data Flow Diagram

For on-prem, the Lightrun server can be placed in any network segment or location per customer preference

International Security Compliance Program (ISO27001, SOC2, HIPAA)

Lightrun is audited for compliance with ISO 27001 and SOC 2 Type II on an annual basis. Our security policies are approved by Lightrun management at least annually and communicated to employees on a regular basis as part of the security awareness program, which covers various types of security-related training modules. In some cases, Lightrun may process basic personal data relating to data subjects in the EU (full name, business email). Where applicable, Lightrun can meet HIPAA requirements via a Business Associate Agreement.

Agile Deployment Models: SaaS or On-premises or the Customer's Private Cloud

SaaS model: Lightrun hosts the server components in the highly-secure and available AWS environment, based on hardened virtual servers and services. Lightrun's Engineering and DevOps teams are responsible for the ongoing maintenance and uptime of the environment.

On-premises: Lightrun is installed within your organizational network or through a private cloud, via Docker or Kubernetes. The customer's IT or DevOps team is responsible for the ongoing maintenance, as is the case for any other internal/local resource. In addition, all of the customer's existing organizational security controls and policies automatically apply to all of Lightrun's components.

Lightrun has No Access to Your Source Code

Lightrun utilizes the developers' existing IDE and therefore the customer's source code does not leave its infrastructure. Only the customer has access to the source code, at all times. The Lightrun architecture ensures that the customer manages the code and the Lightrun components end-to-end, effortlessly. The Lightrun Sandbox ensures no changes to the application state, and the thresholds it enforces cap usage overhead.

Encryption - in transit and at rest

The communication between all Lightrun components and the Management server is always established over industry-standard TLS 1.2 encrypted channels. Certificate pinning is utilized both in the agent and the client.
SaaS - All customers' data hosted in AWS is encrypted using Amazon's AES-256 encryption algorithm and stored on Elastic Block Store (EBS) storage and Relational Database Service (RDS) databases.

On-Prem - All customers' data is stored in a self managed Database. We strongly recommend to encrypt the database using industry standards.

Key Management

In our SaaS solution Encryption keys are managed using Amazon's Key Management Service (KMS). Access to KMS is restricted by role and strictly managed. Access to the actual keys is not allowed. Encryption keys are customer-specific and are unique for each customer/tenant. The customer does not have access to the KMS nor to managing the keys in the Lightrun hosted service environment.
Encryption keys are rotated on an annual basis.
On-Prem - We strongly recommend to manage the encryption keys using industry standards.

Authentication and Access Management

Only registered, authenticated and authorized users are able to access and leverage Lightrun. Identity is managed based on a self-service registration process in which a unique username and password are created for each user. Lightrun uses an Identity and Access Management framework and enforces strict password policy with a minimum length of 8 characters and full complexity. The passwords are securely stored, hashed and salted - In accordance with NIST requirements. Once the client plugin has been installed, users undergo are authenticated before it is enabled.

Role Based Access Control (RBAC) and Single Sign-on

Lightrun provides several types and levels of roles to help support granular management and segregation of duties. These roles introduce various permission levels, ranging from System Administrator (the highest level), through the more restricted roles of Manager and Standard User. In addition, Lightrun supports Google Login and Single Sign On (SSO) module (both SAML and OpenID Connect) to help customers leverage their existing organizational
directory and repository.

Monitoring & Incident Response

Critical infrastructure components and services within Lightrun generate logs and audit trails. Alerts are generated based on severity and addressed by the relevant stakeholder or team within Lightrun.

Read-Only Guarantee & PII Redaction

Lightrun recognizes the importance of the audit & compliance requirements for application integrity in production services that our enterprise customers are facing.

It's important to remember that - at its core - Lightrun can be considered a real-time data collection platform, allowing developers to define the information that needs to be gathered from the live application in runtime. This is the same as other APM/logging solutions such as Datadog, Elastic, Splunk, and more - where actions taken by the solution are, by design, read-only.

Furthermore, Lightrun is the only player in the field with a configurable, proprietary and patent-pending **agent sandbox** that ensures all Lightrun actions are indeed **read-only**. Unlike traditional debuggers, Lightrun guarantees that the code state is never modified, that process behavior and flow remain unchanged, and that running processes are never stopped or interrupted.

In addition, Lightrun has a capping mechanism that ensures that your performance footprint thresholds (CPU, memory & network) are maintained.

Lightrun also supports file and function level blocklists, which allows the system administrators to restrict access to certain resources or use the Personal Data Fencing feature to restrict access to certain types of PII or sensitive data. As an additional security best practice, the Lightrun agent files can and should be placed in a path with read-only permissions, thereby further reducing risk.

Lightrun SaaS Security Model

1. Lightrun leverages the native, advanced security capabilities of AWS such as Trusted Advisor, Security Hub, Guard-duty, and Cloud-trail to protect the environment, monitor anomalies and help ensure cloud workloads are hardened and protected.

2. Customer Segregation - Each customer is provisioned with a unique ID and URL (e.g. app.Lightrun.com/company/customerX). All actions and activities within Lightrun are based on that unique identifier. The Lightrun platform was designed with strict customer segregation and multi-tenancy enforcement. In addition, this scenario is specifically tested in Lightrun's routine penetration tests.

3. Encryption - Lightrun uses encrypted storage on AWS, using AES256.

4. Ongoing vulnerability assessments - Lightrun conducts several types of routine vulnerability scans to help proactively identify deviations from the security baseline and policy.

5. Penetration tests - Lightrun performs application and infrastructure penetration tests using independent security firms to help proactively detect vulnerable code, applications or systems. In addition, subject to prior coordination and approval in writing, Lightrun encourages its customers to conduct their own security tests against the Lightrun Cloud environment.

6. High availability - Lightrun's AWS infrastructure was designed and implemented under high availability principles, meaning that critical components can handle failure with minimal service disruption or data loss, and seamlessly recover from such failure.

7. Backup and Restoration - Lightrun's critical components and servers are backed up on a daily basis. Restoration tests take place periodically and is audited as part of our ISO27001.

Physical Security

Access to Lightrun facilities is restricted to authorized staff. Data center security is fully controlled by Amazon, as the providers of Lightrun's hosting facilities and infrastructure. All data centers include multiple top-tier security controls, such as biometric identification, cameras, vehicle barriers and advanced intrusion detection systems. For more details, see:
https://aws.amazon.com/compliance/data-center/controls/

Secure Product Development Lifecycle

Lightrun invests significant efforts to help ensure its product and system components are well protected and in alignment with the security industry's best practices. Once a year, critical components within the Lightrun product undergo a Secure Design Review. In addition, all system components undergo security penetration tests on a regular basis by an independent third party, and the source code is scanned with static code analysis tools to help proactively identify potential security vulnerabilities. The Lightrun internet-facing components undergo vulnerability scans on a daily basis to help proactively identify potential issues.

Audit Trail and Logs

Lightrun activity, actions and changes are logged and can be audited by the customer administrators. In addition, Lightrun provides easy integration with SIEM and security monitoring platforms.

Lightrun

Lightrun is the first to bring "shift left" observability, giving developers deeper insights into running applications with the richest set of observability pillar tools for troubleshooting applications directly from within the IDE.

Lightrun simplifies every aspect of incident resolution. Lightrun is ISO-27001 certified and is proud to have some of the most innovative technology companies in the world as customers, including Taboola, Sisense, Tufin and more.

CONTACT US: Lightrun.com/contact