Rise

Rise is an all-in-one training system with enterprise-class security

Last updated 11/16/2021

We've embedded security and resilience into Rise and throughout our operations. Our expert team uses the latest technology to make sure our infrastructure is reliable, and your data is protected. In this white paper, we'll walk you through our robust security practices.

How Rise works

Rise is a web-based, all-in-one training system that makes training easy to create, enjoyable to take, and simple to manage. Rise makes it super easy for employees to share what they know and for managers to educate their teams.

Regular security testing

We work with industry-leading security experts to conduct annual penetration tests. Objectives include validation that the Rise infrastructure and services were developed and deployed with security best practices in mind, and to obtain third-party validation that any significant vulnerabilities present in the Rise environment were identified for remediation. The ultimate goal of the assessment is to provide a clear picture of risks, vulnerabilities, and exposures as they relate to accepted security best practices, such as those created by NIST, OWASP, and/or the Center for Internet Security.

Request our annual pen testing results.

Data protection

Rise is built on enterprise-grade services to guard against external threats to data. The application is hosted on Amazon Web Services (AWS), the industry-leading provider that sets the bar for security best practices. Our in-house security engineering team uses best-in-class tools for vulnerability scanning, malicious activity detection, and blocking suspicious behavior automatically. To validate the integrity of the Rise infrastructure, a third-party professional testing organization attempted to breach the protections from the perspective of an anonymous intruder, simulating scenarios as an opportunistic, internet-based threat actor with no knowledge of the environment.

Encryption

Rise uses the most advanced encryption technology publicly available to secure data. Using PKCS (Public Key Cryptography Standard) #1 SHA-256 with 2048-bit RSA encryption, Rise encrypts data at rest as well as all network traffic into and out of AWS. In addition, the cryptographic key management process in Rise includes key rotation.

Secure authentication

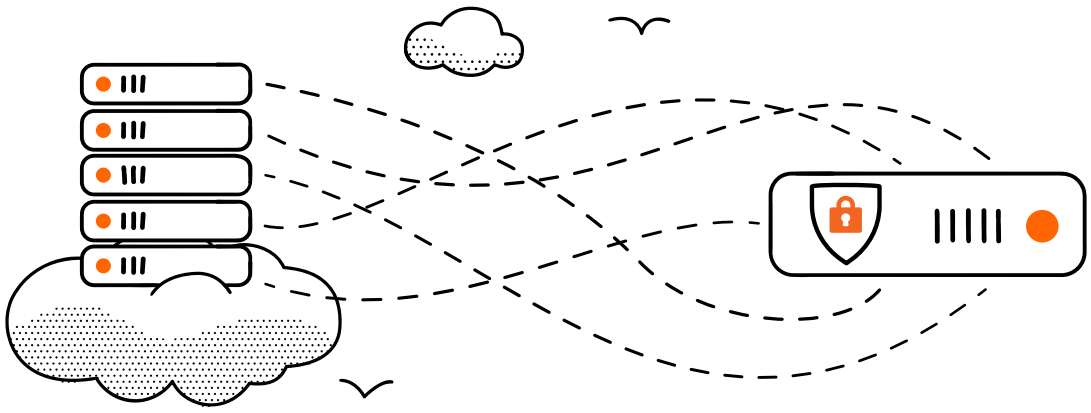
Rise does not store user credentials. Rise has strong default settings and also gives you the option to authenticate with Google or require single sign-on (SSO) powered by SAML 2.0, built on Okta.

Both our internal identity provider and Okta implement proven, common, and popular identity protocols used in enterprise identity infrastructures. In all cases, Rise user credentials are passed to providers for authentication and the provider returns a JWT. The user creates an initial password and that process requires that the user has access to their email account.

The traffic between customers and our services, including third-party services such as Okta, is all TLS 1.2 encrypted (industry standard). All customer data is encrypted at the data field level. When we use credentials supplied by Okta to authorize access to Rise, the credentials are cryptographically verified before requests are fulfilled in Rise. All passwords are hashed (and salted) securely using bcrypt.

Disaster recovery and business continuity

Rise replicates data across five separate, physically independent, and highly secure AWS locations, ensuring high availability, data integrity, and protection from local failures such as power outages and fires. We save a full backup copy of production data multiple times per day to a remote location to ensure rapid recovery in the event of a large-scale disaster. We annually test the process of recovering data from the backup location.



Trusted partners

Rise's privacy-by-design mandate ensures that only necessary data is collected, and makes it easy to see and manage your data. We partner with carefully selected industry leaders with first-rate security practices and perform annual vendor assessments to ensure ongoing adherence to industry best practices.

Stripe
(Payment processing)

Amazon Web Services
(Hosting infrastructure)

Chargebee
(Billing management)

Marketo
(Marketing automation)

Okta
(Single sign-on)

Salesforce
(Customer database)

Endpoint Security

All employee workstations are configured to run computer management software to ensure that an antivirus program is installed and conducts regular scans. In addition, computers must be up to date on the operating system with patches and all Engineering & Business Solutions computers must be encrypted at rest.

Access Control

Rise adheres to the principle of least privilege and role-based permissions when provisioning access—workers are only authorized to access data that they reasonably must handle in order to fulfill their current job responsibilities.

In addition, Rise utilizes multifactor authentication for all access to systems with highly classified data, including our production environment, which houses our customer data.

Summary

We've built our robust security infrastructure and hired skilled engineers in our commitment to protecting your data from data theft, data loss, and downtime.

Please contact us with any questions at security@rise.com or to request a copy of the Rise SOC 2 report.