Rescale Security Strategy Overview

Security is a vitally important topic for any cloud adopter to consider and is an area that Rescale has focused a lot of effort to ensure the most secure cloud solution available.

By taking a defense-in-depth strategy to build a multi-layered security framework, the Rescale ScaleX platform provides complete data confidentiality based on the highest standards of data encryption.

Rescale meets or exceeds industry standards, is independently audited, and conforms to assurance programs and controls. Each year Rescale is audited to ensure SOC 2 Type 2 certification, which evaluates the security, availability, processing integrity, confidentiality, and privacy of Rescale's platform, data, policies, and procedures. The platform is ITAR and EAR compliant.

Rescale's security framework in built upon four pillars

- **Data security**: job and data isolation, segmentation, encryption, redundancy, and monitoring
- **Network security**: advanced network monitoring and policy enforcement
- **User security**: enterprise IT enforced user policies
- **Secure software development**: rigorous software development process

Security FAQ

In anticipation of many common security-related questions, a list of 100+ questions and answers have been compiled. Please contact security@rescale.com to receive this document.

Rescale Security Strategy Overview

DATA SECURITY

Data security governs security of jobs running on Rescale as well as data contained within jobs, stored on the platform, and in transit to/from storage. All data is encrypted in transit and at rest. Encryption keys are isolated to the data owner and stored independently of encrypted data. Only users can access their data unless they explicitly share with colleagues or Rescale Support. Simulations always run in private, closed clusters with kernel-encrypted hard drives. ScaleX Enterprise adds multi-factor authentication for additional security. To comply with legal, privacy, and export compliance requirements, data is bound to the region in which the platform resides—the United States, Europe, Japan, or South Korea. Rescale is ITAR compliant and registered with the U.S. DDTC.

NETWORK SECURITY

Rescale data centers operate a lights-out policy requiring biometric entry authentication, ensuring an environment more secure than typical on-premise data centers. To ensure ongoing confidence in overall network security, network penetration testing is regularly carried out. Extensive firewalls control access and define connection policies for all network access points and management systems. Systems are continually monitored to ensure server security and optimal performance. The Rescale operations team manually reviews server and applications log data on a periodic basis, and annual audits are carried out by third-party firms. Automatic configuration, continuous integration testing, and deployment tools are used to keep all OS software on system servers and customer clusters up-to-date with the latest patches.

USER SECURITY

The Rescale platform implements a multi-layered set of controls and policies that ensure users are secure. These include custom firewalls for internal systems and user clusters, ensuring that secure connections are used throughout, and enabling protection against brute force and denial-of-service attacks. Rescale also offers company administrators the ability to restrict where their users can access Rescale by defining authorized IP address ranges for incoming connections. Company administrators can also enable multi-factor authentication and single-sign-on, which allows the Rescale platform to connect to the company's Active Directory authentication system, resulting in instant access to the Rescale platform.

SECURE SOFTWARE DEVELOPMENT

All software development at Rescale undergoes design, review, testing, monitoring, and ongoing maintenance. Each step of the process is also thoroughly documented for review. 100% of development is conducted in-house at our San Francisco headquarters. Development, testing, and production environments are strictly segregated. Testing is conducted at each phase prior to publishing.