Rievent System FAQ

This document addresses commonly asked questions regarding software deployment architecture, compliance, security, and business continuity at Rievent. If you have additional questions not addressed here, please ask.

Deployment

What is the software deployment model?

Rievent uses the Software as a Service (SaaS) model of software licensing and deployment. Rievent is hosted as a service and provided to customers across the Internet. Rievent is deployed as a multi-tenant software stack including application servers and a relational database system.

Where are Rievent servers located?

Rievent uses Amazon Web Services (AWS). The application servers and database servers are located in the US East AWS region data center located in Northern Virginia. Rievent also maintains a mirrored configuration in the US West (Oregon) region as part of Rievent's Business Continuity Disaster Preparedness and Recovery Plan. Rievent additionally uses Amazon Web Services including the S3 object (file) storage, CloudWatch monitoring and observability service, Route53 domain name services, AWS Identity and Access Management (IAM), and AWS Guard Duty intelligent threat detection and continuous monitoring hosted at Amazon.

Is my organization's data safe from other customers when it is running on the same servers?

Yes. The multi-tenant database architecture keeps your data segmented from other customers. Unauthorized parties cannot access your data. Customer data is uniquely identified by client ID and only accessible when access is granted by the customer. Additionally, customers can control data access by their employees using varying levels of granularity and feature permissions.

What responsibilities does the customer have to safeguard their data?

Security within the customer's organization is the responsibility of the Customer's appointed administrator. The Customer designates an administrator to serve as point of contact for all production, reporting, security, system, and training related communications with Rievent. Rievent will direct all communications referenced above through the customer administrator including any security concerns. Administrators receive training on their responsibilities. The administrator is responsible for creating client accounts. Rievent creates a customer administrator account ("top level" account) from which all other accounts are created by the customer administrator. Customers are themselves responsible for any data once extracted or saved external to the platform and should follow acceptable computer security procedures within their organization. Customers should protect and monitor the workstations and computing environments used to access Rievent services. Customers should safeguard and protect data downloaded or access via Rievent services.

Who owns the data that customers and their end-users store at Rievent?

Rievent does not own customer data. Our contract and license agreement state that you, the customer, own your data. For more information, please refer to your Rievent customer contract. Rievent won't share your data with others except as noted in our license agreement and only with your permission. Rievent keeps your data as long as you are under contract with Rievent or according to the terms of the contact. Rievent's user interfaces make accessing your data simple and accessible. Data is easily exported in Comma Separated Values (CSV) format to users with appropriate permissions.

Business Continuity

How fault tolerant is the system?

Rievent uses fault tolerance techniques including real-time data replication, geographically pre-staged remote recovery locations, and daily backups. Rievent maintains and tests internal business continuity disaster preparedness and recovery plans. Rievent maintains redundant systems with a capability to recover systems in a geographically remote pre-staged location. Rievent's database uses AWS RDS which provides high availability and failover support. In an AWS RDS Multi-AZ deployment, Amazon RDS automatically provisions and maintains a synchronous standby replica in a different Availability Zone. The primary DB instance is synchronously replicated across Availability Zones to a standby replica to provide data redundancy, eliminate I/O freezes, and minimize latency spikes during system backups.

Are systems monitored?

Rievent uses a third-party, external 24/7 electronic uptime and security monitoring service (Pingdom.com) to monitor its services and web sites, and system engineers are on call to receive alerts and respond to outages and incidents.

How and how often is data backed up?

Rievent databases are hosted on Amazon Web Services Relational Database Service (RDS) utilizing multi-availability zone mirroring replication, daily backups archived to a geographically distant emergency recovery region, and an additional full read-replica is also maintained in real time in addition to the multi-availability zone replication provided by the primary database instance. Rievent has real-time backups providing for manual and automated point of failover recovery in addition to daily backups for catastrophic failure recovery.

How does Rievent provide for business continuity in a disaster?

Rievent maintains and regularly reviews and tests an internal Business Continuity Disaster Preparedness and Recovery Plan detailing fault tolerance, backup, and recovery requirements for Rievent deployed production systems. The document outlines impact of a variety of possible failures classified by risk, including expected down time and data loss from each incident.

A disaster for the purpose of the document is any event that results in interruption of Rievent's primary business functions due to a significant facility, operating system, software, or hardware fault or cyber-attack that prevents customers from accessing the Rievent Platform. In the event of a disaster, Rievent can systematically restore, recovery, configure, and launch resources using Amazon Web Services (AWS) to ensure business continuity.

Is there a Service Level Agreement (SLA)?

Yes. Rievent's contract provides a Service Level Agreement (SLA) with a 99.9% uptime guarantee.

Software and User Integration

Identity and Access Management (IAM) and Single Sign-On?

Single sign-on between customer systems and Rievent is available using the Rievent secure Trusted Handoff Protocol. Developers register security credentials (public key) with the Rievent Platform then package and digitally sign security credentials along with user information to securely authenticate and synchronize users

with Rievent sites by passing a digitally signed and optionally encrypted JSON Web Token (JWT) (over HTTPS). Customers may also bridge or proxy from Security Assertion Markup Language (SAML) or OpenID Connect (OIDC) Identity and Access Management systems to provide seamless single sign-on. Contact Rievent for more information.

Can I integrate Rievent into my web site?

Yes. Using either Rievent Connect (embedding) or Rievent web site themes, Rievent can integrate with your existing web site to add continuing education capabilities. Additionally, web services are available.

Does Rievent offer Web Services?

Rievent's customers have a number of secure web service endpoints available for their developers to use to automate or integrate Rievent services. For example, customers may use web services to query the course catalog, query end user's course history and transcripts, query and modify production status, query participation record queries, and submit exam results.

Information Security/ Compliance

Rievent follows industry best practices for information security.

What standards does Rievent follow for information security?

Rievent uses the U.S. Department of Commerce National Institute of Standards and Technology (NIST) Cybersecurity Framework to guide its security practices. The Framework is voluntary guidance, based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk. The Framework is the go-to resource for Rievent when evaluating and developing security practices and software standards. NIST SP-800-53 Rev. 4 & 5 is Rievent's primary security and privacy control specification and overrules any conflicting or older standards.

Is Rievent Payment Card Industry Data Security Standard (PCI DSS) complaint?

Yes. Rievent has completed the Payment Card Industry (PCI), Data Security Standard (DSS), Self-Assessment Questionnaire A and Attestation of Compliance. Rievent is a card-not-present (ecommerce) provider, all card processing is fully outsourced with no electronic storage, processing, or transmission of cardholder data on within Rievent software or systems. Rievent is integrated with PayPal and Authorize.Net as e-commerce processors.

Is Rievent HIPAA / HITRUST Common Security Framework (CSF) Compliant?

HIPAA and HITRUST CSF are not required for continuing education as long as no patient information is included in learning activities. Rievent has not completed HIPAA nor HITRUST reviews. Rievent is not a health care provider nor covered entity under HIPAA and does not create, maintain or transmit PHI. However, Rievent would meet most HIPAA and HITRUST technical, privacy, and security standards.

Are Service Organization Controls (SOC) reports available?

Rievent is hosted at Amazon Web Services. Service Organization Controls (SOC) reports (SSAE 18 and ISAE 3402 standards), ISO, and additional reports are available from Amazon. Rievent has not undergone a SOC 2 audit.

Do you perform penetration tests of your infrastructure?

Yes. Rievent uses a third-party to conduct monthly penetration tests of production and production support systems.

Can customers perform penetration tests against Rievent?

Yes. Customers may be billed for support and disruption of services caused by penetration tests. Prior permission must be requested, and services may be terminated by active security and threat detection systems and security personnel. Additional fees may apply.

Is there an employee information security policy that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy?

Yes. All employees review and sign the "Corporate Computer Security,

Data Privacy, and Acceptable Use Policy" at least annually. Employees receive a security briefing upon hire. The policy is reviewed annually. The policy details acceptable use, server access rights and requirements, data access and transmission, physical security, workstation security, email and cloud computing security, network security, password and private key security, vulnerability risk assessment, social engineering threats, and intrusion/data corruption/unauthorized user incident response.

Are systems in place to monitor for security breaches?

Yes. Software monitors Rievent systems for changes to key operating system files. Customers will be notified if a breach occurs. Active attack monitoring software will automatically block bruit force attacks.

Are networks secured with firewalls?

Yes. Rievent is deployed within an AWS Virtual Private Clouds (VPC) and access control groups are used to limit and control traffic in, out, and within the network.

Are Operating systems and software updated?

Yes. Rievent applies patches to operating systems and monitors for security advisories. Systems are upgrade with each Rievent software release or on an as needed basis based on the threat level of a discovered vulnerability.

Accessibility Compliance

Is Rievent software Section 508 compliant?

Yes. Rievent meets accessibility requirements. The Rievent VPAT™ Accessibility Conformance Report (WCAG edition) is available upon request. Rievent meets or exceeds W3C Web Content Accessibility Guidelines (WCAG) 2.1 Level A and Level AA success criteria.

A Voluntary Product Accessibility Template (VPAT™) explains how information and communication technology (ICT) products conform to the Revised 508 Standards for IT accessibility.

Privacy Compliance

Does Rievent have a Privacy Policy?

Yes. We've developed a Privacy Policy that covers how Rievent products and services collect, use, disclose, transfer, and store end user and customer information. The policy is available at the bottom of Rievent product web pages.

What is the customer's responsibility for protecting end-user and employee privacy?

Rievent's products and services are frequently embedded within our customers' websites, or Rievent hosts sites for our customers with their branding and website wrappers. Our customers share the responsibility to maintain and respect the privacy of end users and its employees and follow federal, state, and international law as applicable.

What privacy standards, laws and regulations does Rievent follow?

Rievent conforms to United States and international privacy consumer and Internet privacy laws, a shared responsibility with our customers. Rievent follows US federal and state data breach notification laws (in coordination with customers), disposal of records laws, personal information handling and security requirement laws, social security number restrictions (Rievent will not store or collect SSNs), identity theft protection laws, and data security measures as required by law.

Rievent conforms to the following privacy standards and laws:

International

- European Union General Data Protection Regulation (GDPR). Rievent and Rievent's customers share privacy compliance responsibility; Under GDPR, Rievent is a Data Processor, customers are Data Controllers.

Federal

- United States Federal Trade Commission's Fair Information Practices (US FTC FIP)
- Federal CAN-SPAM act

State

- California Consumer Privacy Act of 2018 (CCPA)
- California Online Privacy Protection Act of 2014 (CalOPPA)
- Rievent complies with additional states' laws, with CCPA and GDPR providing comprehensive guidelines exceeding or including requirements of other states in most cases.

Next Steps

Can I learn more about security and business continuity at Rievent?

Rievent would be happy to share more security details with our current and potential customers. Rievent's security procedures require that customers sign a non-disclosure agreement prior to receiving more detailed information. Requests for detailed security information must be authenticated. If you have specific questions, please ask.