Zuora Technical Operations | 2021

Zuora Technical Operations & Security

Confidentiality

This document contains confidential Zuora information. This document is intended solely for use by internal Zuora personnel, Zuora business partners, Zuora customers, and Zuora prospective customers that have completed a non-disclosure agreement with Zuora.

Unauthorized use, reproduction or distributions of this document, in whole or in part, is strictly prohibited.

Disclaimer

The information contained herein is believed to be accurate at the time of issue; no liability can be accepted for any inaccuracies. The reader is reminded that changes may have taken place since issue.

This policy is provided for informational purposes only. Zuora reserves the right to modify this policy at any time.

Table of Contents

Introduction

Zuora, Inc. was started to help businesses move to the Subscription Economy. Today's subscription businesses require speed and flexibility to launch new products to market, automation to eliminate manual processes, and key metrics to make accurate business decisions. Zuora's founders built Zuora from the ground up as a SaaS platform to ensure that Zuora customers achieve rapid time to market and lower TCO (total cost of ownership) with a billing and subscription management platform that continues to innovate, scale and evolve on an ongoing basis.

Zuora delivers its products on a reliable, battle-tested and proven platform that is mission critical to over 950+ customers, including companies such as HBO, Symantec, Toshiba, Zillow, NCR, and Vivint.

This document describes how Zuora operates its platform, from an infrastructure, development, and security perspective. Zuora customers and partners can use this document as a guide to Zuora's technology policies, and as a reference for information about the architecture and performance of Zuora's platform.

This document applies to both Zuora Central and Zuora RevPro. Topics covered include:

- Capacity, response times, and scalability
- Private and public data center locations
- Release timing and processes
- Newest innovations, such as the reinvention of existing functionality as microservices
- Backup policies and schedules
- Organization-wide security practices
- Compliance, including PCI and SOC compliance

The Zuora Technical Operations team can provide further information and guidance if needed. In particular, as part of a thorough evaluation of Zuora, prospective customers should expect to have a direct conversation with a Zuora Technical Operations team member to gain a complete understanding of the quality of Zuora's platform and ensure that any queries are fully addressed.

Zuora's platform is centered on leveraging industry leading technologies and best practices, along with constant innovation to deliver a market leading solution that is superior not just in product features, but also in core scalability, performance and security. Coupled with Zuora's unique partner ecosystem and open APIs, we believe that Zuora offers the strongest and most flexible platform in the industry today.

To learn more about Zuora, visit http://www.zuora.com.

Technology Group and Culture

Zuora has over 200 technologists, located across the US, Europe, South America, and APAC.

The technology group is actively engaged with Zuora customers and partners via the Zuora Community. One of the most well-received outreach activities is the Engineering Blog, in which Zuora technologists showcase the innovative projects and solutions that they are working on.

The Engineering blog is located at http://engineering.zuora.com/

The technology group also has regular hackathons, which frequently result in new capabilities and technologies being added to Zuora's products, as well as enhancements to the way that teams collaborate within Zuora.

Performance

Transaction Capacity

Zuora Central

Zuora currently manages almost 250 million subscriptions across the entire Zuora customer base. Through their API calls, customers currently run 50+ million queries per second against Zuora's 50+ TB primary storage platform.

As a representative example, a typical high volume Zuora customer has:

- 1.7 million accounts
- 3 million subscriptions
- 2 million invoices per bill run

Transactions that flow through Zuora's infrastructure are of two types:

- **Synchronous** - Includes real-time creation of new subscriptions, new accounts, and changes to existing subscriptions.

- **Asynchronous** - Includes batch invoice generation, payment collection, and invoice exports.

Zuora's platform has been architected with large amounts of standby capacity to accommodate growth, and is benchmarked to scale to levels much higher than current usage rates. The average monthly usage rate is 30% of benchmarked capacity.

The following table gives a snapshot of the current usage rates for different types of transaction. Actual transaction capacity varies with the type of transaction.

Transaction Type	Current Usage Rate
All synchronous transactions	Zuora processes an average of 2.5 billion to 3 billion transactions per month, with approximately 80 million to 90 million transactions per day. The US Production environment is benchmarked to process 2700+ synchronous transactions per second across all tenants.
Create subscription	Zuora customers create an average of 7.5 million new subscriptions per month.
Amend subscription	Zuora customers amend an average of 1 million subscriptions per month.
All asynchronous transactions	Zuora processes an average of 150 million to 160 million transactions per month.
Generate invoice	Zuora customers generate an average of 13.8 million invoices per month. During 2017, Zuora customers invoiced a total of $23 billion USD.
Collect payment	Zuora customers collect an average of 11.3 million payments per month.
Bill run	Zuora bill runs process around 1.1 billion accounts every month. 50% of tenants achieve or exceed an average billing rate of 70 thousand invoices per hour per thread. Zuora can assign additional threads to tenants if required. This enables near-linear scaling of bill run performance.

Response Times

Zuora Central

Response times vary based on a number of factors, including (but not limited to) the type and shape of the call, concurrent load on Zuora's platform, and the complexity of the data in the tenant.

Most API operations have sub-second response times, ranging from 5 ms to 300 ms. Some API operations perform more intensive actions or involve Zuora third parties in the workflow. These API operations have response times that can range from under a second to 3 seconds.

The API operation that Zuora services the most every month is the Zuora Object Query Language (ZOQL) query operation. Response times to ZOQL queries average around 40 ms.

Infrastructure and Architecture

Data Center Locations

Zuora Central runs on a hybrid Public/Private cloud deployment model.

Private Data Center Locations

Zuora has two state of the art private data centers in the US:

- **Primary Data Center** - Switch (Las Vegas)
  Tier 4+ certified data center
  Notable client: Google

- **Secondary Data Center** - CoreSite (San Jose)
  Telco grade data center
  Notable client: Facebook

The private data centers are fully synchronized and located in separate disaster zones. Zuora maintains a warm standby stance, with the secondary data center able to take over full service capacity.

The private data centers use:

- Fully redundant Tier 1 network carriers. The primary data center has 17 different network carriers in use by Zuora. The secondary data center has 2 network carriers in use by Zuora.

- Fully redundant Juniper switching and routing equipment.

- Web and application firewalls to defend against attacks.

- Akamai CDN for static and dynamic content acceleration.

The throughput of the private data centers is 1 Gbit/s North-South and 40 Gbit/s East-West, over InfiniBand. The average latency for the US Production environment across the whole world is 128 ms. From North America, the average latency of the US Production environment is 70 ms. From Europe, the average latency of the US Production environment is 186 ms.

Public Data Center Locations

Zuora also operates parts of its service from Amazon Web Services (AWS) regions around the world.

In July 2017, Zuora launched a data center located within the EU and hosted completely in the cloud. The EU data center currently supports the Zuora Production and Sandbox environments, the Zuora REST API, and all Zuora products.

The EU data center is completely isolated from other data centers; no customer data is replicated between the US and the EU. This provides data residency assurances for Zuora customers that operate in the EU. The current location of the EU data center is Germany.

The EU data center follows the same customer onboarding process and release schedule as the US data centers. For security, usability, and ease of implementation, Zuora provides a separate login page for tenants in the EU data center.

See the Zuora Knowledge Center for more information:
https://knowledgecenter.zuora.com/BB_Introducing_Z_Business/Zuora_Data_Centers

Communication Between Private & Public Data Centers

Our private data centers use a combination of direct and WAN based connectivity to provide the optimal path between resources deployed in our data centers and third party cloud providers. In order to maintain consistent resource separation, Zuora uses a combination of overlay network technologies in both our private data centers and our third party cloud deployment.

Zuora RevPro

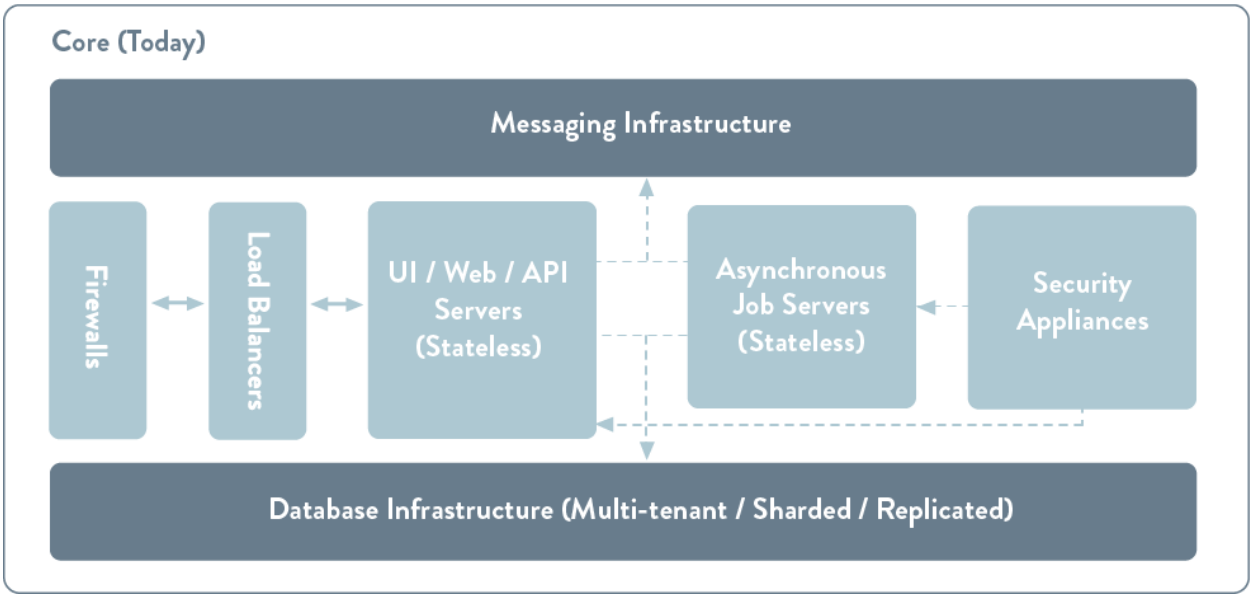
Zuora RevPro runs on a Public cloud deployment model, with all services built on AWS.

Scalability

Zuora Central

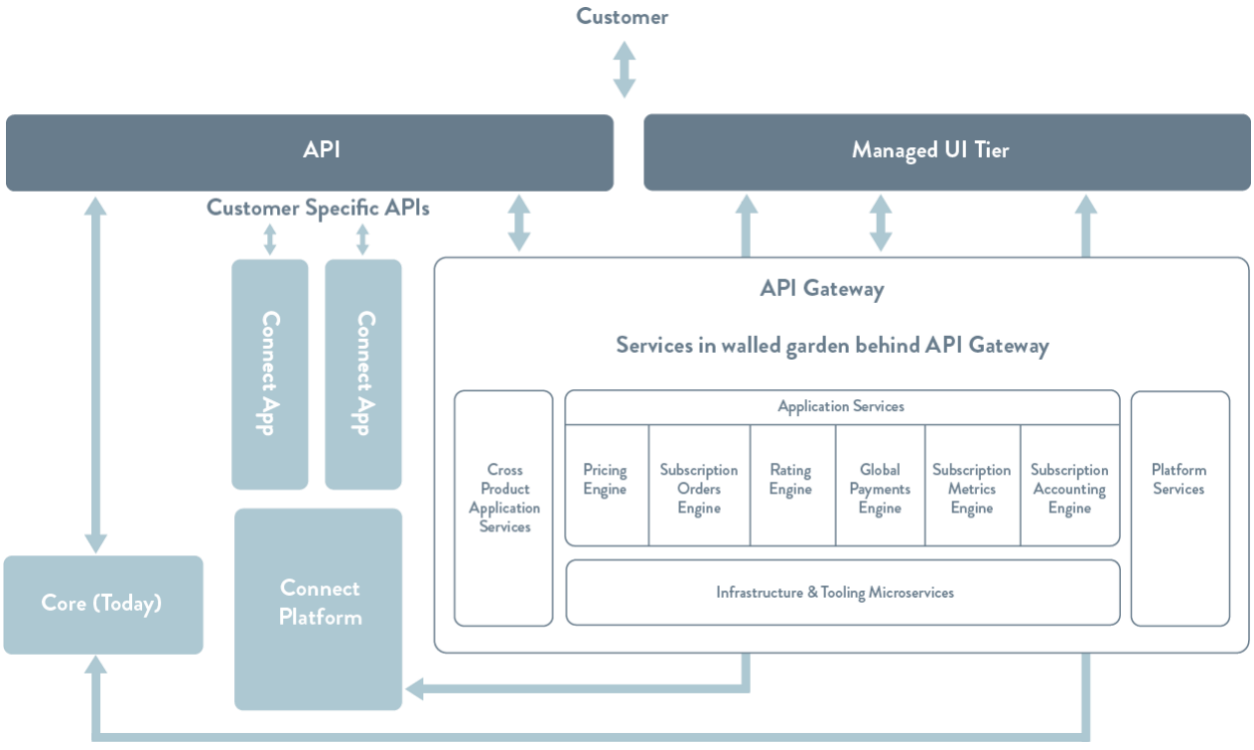
Zuora's platform has been architected from the ground up to scale horizontally and vertically. The platform is designed to scale horizontally at the application level, the messaging infrastructure level, and the database level. The following diagram illustrates the architecture of Zuora's cloud infrastructure (this includes our transition to microservices):

Today



Future State (Microservices)

To further improve scalability, the Zuora platform is currently undergoing a microservices-based re-architecture. Some of the re-architecture has already been completed. The following diagram resembles the target architecture after the re-architecture has been completed. Please see Development Practices section for more information:



The following table describes how Zuora uses resources to ensure that the platform is scalable at all levels:

Infrastructure	Description
Network equipment	Zuora uses Juniper and Mellanox network equipment.
Web server and load balancers	Zuora uses SuperMicro high-capacity web servers. All web servers are horizontally scalable and are configured in a redundant manner for high availability (HA). Software load balancers route traffic to multiple servers.
Application servers	Zuora uses SuperMicro high-capacity application servers. One set of application servers handle UI and API traffic. UI and API processing is stateless, multi-threaded, and configured with large Java heaps. Other application servers process batch and asynchronous transactions. These back end servers are re-entrant, highly multi-threaded, and configured with large Java heaps. These back end servers also segregate higher priority from lower priority processing.
Messaging	Zuora uses ActiveMQ Broker to implement a publish-subscribe model. ActiveMQ Broker is set up in an active-passive configuration for quick failover and HA.
Storage layer	Zuora uses high-performance Oracle SAN for the storage layer.
Database servers	Zuora uses a Percona MySQL database running on local SSDs. All database servers are horizontally scalable. Sharding separates multiple tenant groups. The database servers are set up in a master-slave configuration for HA, with read-only slaves used to offload query workloads. Zuora also uses an ActiveMQ database for persistent messaging in the event of failover recovery.
Encryption	Zuora encrypts sensitive data such as credit card data are encrypted using 256 bit Advanced Encryption Standard (AES-256) and keys managed by Hardware Encryption Module (HSM).

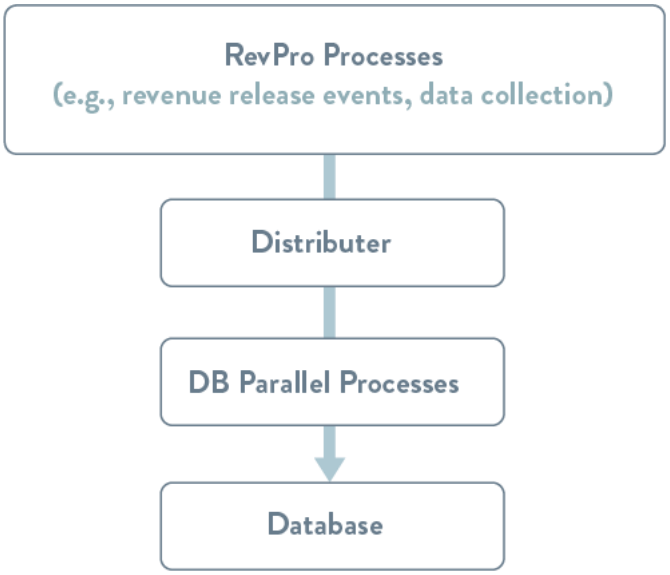
Zuora RevPro

The following table gives representative examples of how Zuora RevPro scales with transaction volume:

Use Case	Input	Output	Time Taken
Representing orders rateable over 1 year, without allocations	600,000 transaction lines	7 million accounting schedules created	20 minutes
Representing orders rateable over 3 years, with allocations	600,000 transaction lines	48 million accounting schedules created	55 minutes

The transaction counts provided above represent a single batch of transactions. Zuora RevPro can process multiple batches of transactions in parallel. The number of accounting schedules generated and the time taken will vary based on the use cases being addressed.

Zuora RevPro supports parallel processing for extra-large transaction volumes. The following diagram illustrates the parallel architecture:



Release Processes and Development Practices

Release Processes

Zuora Central

Zuora updates its platform on a regular basis, in accordance with established release processes. Zuora performs releases with zero downtime.

Most parts of the platform are subject to a monthly release cycle, with each monthly release identified by a sequential number. For example, the January 2018 release was numbered R220 and the February 2018 release was numbered R221. Some parts of the platform, such as functionality provided by microservices (see below), are updated on a different schedule and use a different versioning scheme.

For each monthly numbered release, Zuora deploys platform updates to the Zuora Sandbox environment around 1 week before the Zuora Production environment. Zuora tests all platform updates before deploying the updates to the Zuora Sandbox environment; the period between deployment to the Zuora Sandbox and Production environment enables Zuora customers to preview and prepare for release.

As an additional step to help customers prepare for releases, Zuora publishes release information in advance of each release. The release information includes feature highlights and expected deployment dates for the Zuora Sandbox and Production environments. To view the latest release information, visit the Zuora Knowlegde Center at https://knowledgecenter.zuora.com/AA_Whats_New/AA_Zuora_Release_Notes. The Zuora Knowledge Center also contains information about previous releases dating back to December 2009.

If an issue is identified during the period between deployment to the Zuora Sandbox and Production environment, Zuora deploys revised platform updates to the Zuora Sandbox environment. If a critical issue is identified after deployment to the Zuora Production environment, Zuora performs an expedited release to address the issue. During an expedited release, Zuora typically deploys platform updates to the Zuora Production environment within 24 hours of deploying to the Zuora Sandbox environment.

Each time Zuora updates its platform, Zuora deploys the same updates across data center locations. Zuora typically deploys updates to the EU data center 3 hours before the US data centers.

Microservices

Microservices use the same staged deployment process as the core, that is to an internal staging environment, followed by our APISandbox environment, and finally the Production environment. Microservice release schedules, however, differ from the core in that deployments of new releases happen continuously through a streamlined CICD pipeline, whereas the core has a more defined, monthly release cadence/schedule

Zuora RevPro

Zuora RevPro performs product releases with zero downtime. Each product release is available for preview in a sandbox environment prior to the production release. Additionally, release notes are published ahead of each product release.

Zuora RevPro adheres to the following maintenance practices:

- All Zuora RevPro product releases are regression tested and are backwards compatible.
- Critical security updates are applied as soon as a resolution is available.
- Quarterly maintenance releases include application bug resolutions and security updates.
- Zuora RevPro customers are notified in advance of any planned maintenance downtime.

Development Practices

Zuora Central

Zuora is currently transitioning its platform to a service-based architecture, with all new services being built on AWS. Services running out of US regions integrate with the existing private data centers in the US, and services running out of EU regions integrate with the AWS-based datacenter in the EU.

In addition to delivering new services on AWS, Zuora is "reinventing" existing functionality as microservices. This initiative enables Zuora to:

- Leverage modern technology stacks and ensure future scalability.
- Increase the velocity and agility with which existing teams operate.
- Reduce the size of Engineering teams and empower Engineering teams to own their services from design to deployment.
- Make team interactions more API driven.

As of today, around 20% of existing functionality has been reinvented.

As part of the reinvention, the Operations and Security teams are moving to a model of supporting Engineering teams securely via tooling and services that assist the Engineering teams in configuring, deploying, and operating their own services.

Redundancy and Disaster Recovery

Zuora Central

Zuora maintains sub-second data replication for services across all datacenter facilities. Zuora's goal is to maintain a 15 minute recovery point service (RPO) with 4 hour recovery time objective (RTO). To achieve this goal:

- Hourly backups for a rotating 7-day window are stored onsite and offsite. Data is stored onsite and offsite in a PCI compliant manner.
- Backups consist of point-in-time snapshots and full database archives.
- Services are deployed across Zones and Regions where possible.
- Mock failover exercises are performed annually.

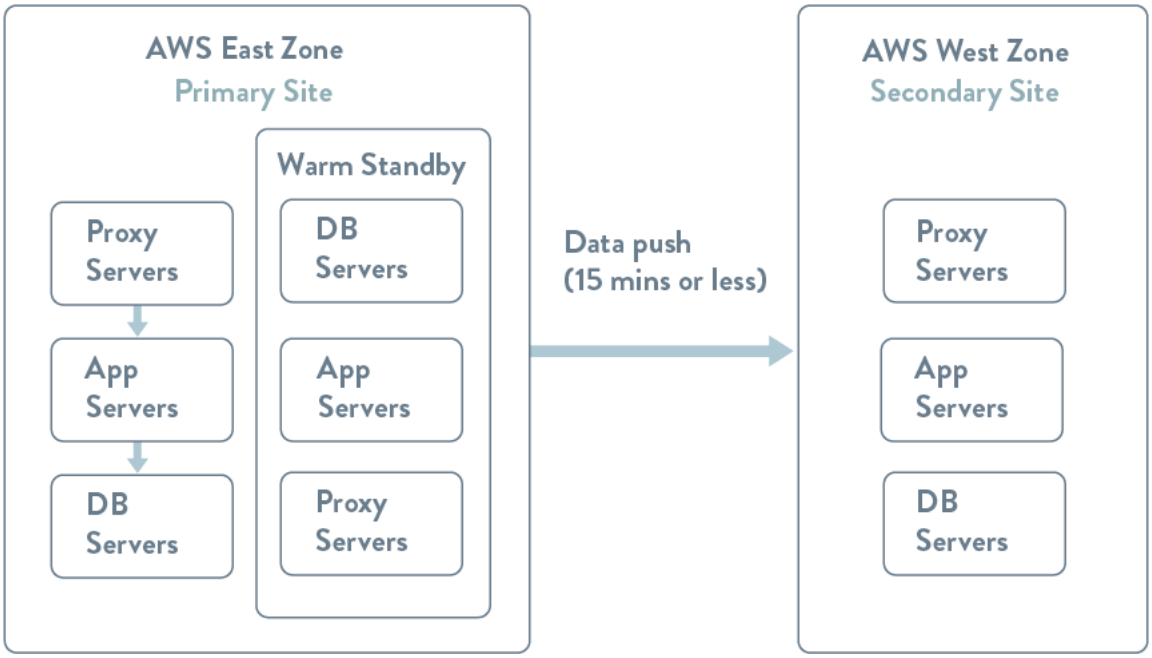
Zuora RevPro

Zuora RevPro is designed for 24/7 reliability. Over the past 8 quarters, Zuora RevPro has maintained an uptime of 98.98%.

To achieve resiliency and business continuity:

- Zuora RevPro has a warm standby environment in the AWS West Zone in case of a production failure.
- Zuora RevPro has a disaster recovery site in the AWS East Zone. At minimum, data is replicated every 15 minutes.
- 17-point system and database checks are performed every 10 minutes to ensure performance and availability.
- Backups are performed daily.
- Capacity analysis is performed every quarter to identify bottlenecks.

The following diagram illustrates Zuora RevPro's infrastructure:



Security and Compliance

Security Measures and Features

Zuora Central

Zuora recognizes that security is critical and strongly believes that security is everyone's responsibility. Zuora staff and partners practice dozens of security measures to ensure that Zuora transaction data is secured everywhere it goes.

Zuora maintains systems, applications, and services in compliance with PCI and industry standards. The following measures protect Zuora's systems and data:

- Zuora follows all industry-standard security practices to ensure information safety for Zuora customers and partners. Zuora staff and partners adhere to security policies and practices designed to keep data safe.

- Zuora leverages strong encryption technologies to protect the confidentiality and integrity of data everywhere it goes. Zuora also implements state of the art technologies such as firewalls and intrusion detection to deter and detect any malicious or unauthorized system activity.

- Zuora's software is developed using industry-standard security best practices.

- Zuora's systems are housed in secure environments and are monitored around the clock by Zuora security staff.

- Zuora continues to explore and evaluate advances in security technology and practices.

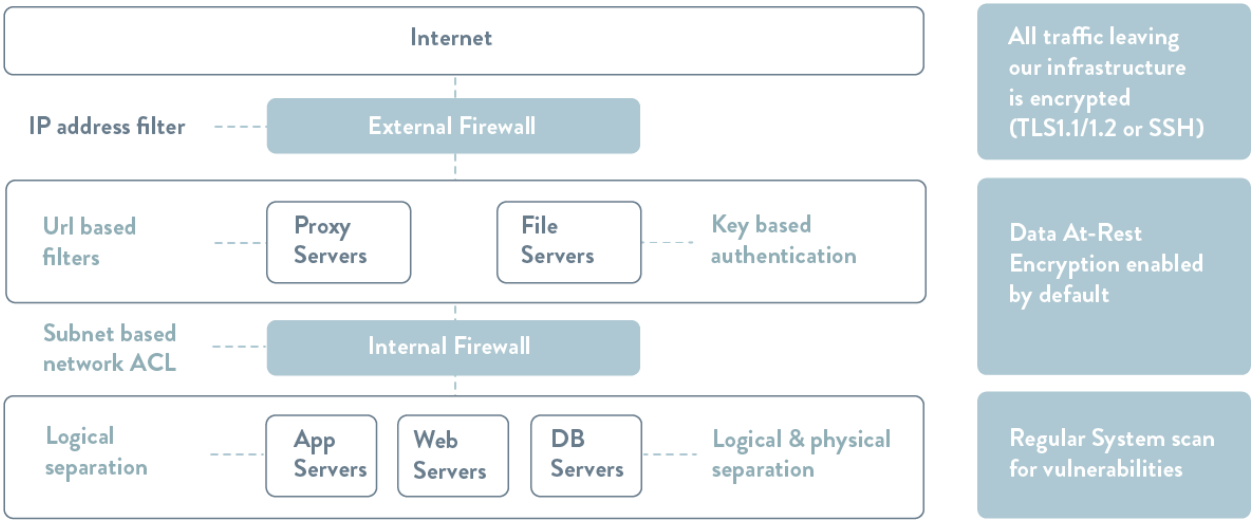
The following table describes how Zuora puts these measures into practice:

Security Category	Description
Network security	The Production environment is separated from all non-production environments. Three-factor authentication is required for remote access to the Production environment. Host-based intrusion detection systems run on all production systems, providing an additional layer of security. Firewall and network security segregate systems and applications based on established security rules.
Application security	Sensitive data such as credit card data are encrypted using 256 bit Advanced Encryption Standard (AES-256) and keys managed by Hardware Encryption Module (HSM). Application security testing is conducted on a continuous basis to review for OWASP.
Vulnerability management	Log monitoring systems watch for security events in critical systems. Zuora staff are alerted to suspicious activities in real time. Rapid 7 Internal and External network scans are conducted on a weekly basis. WhiteHat Security application scans are conducted on a continuous basis. A third-party penetration tester conducts web application penetration testing. Zuora monitors CVE, NIST, and vendor vulnerability lists. On a monthly basis, critical vulnerabilities are reviewed and patched in a time frame commensurate with risk.

Zuora RevPro

Zuora RevPro supports single sign-on via SAML 2.0. After SAML is enabled, Zuora RevPro customers can enable and disable user access to Zuora RevPro from within their own systems. However, Zuora RevPro does not currently provide a user management API. This means that customers must manually add new users and remove old users from within Zuora RevPro.

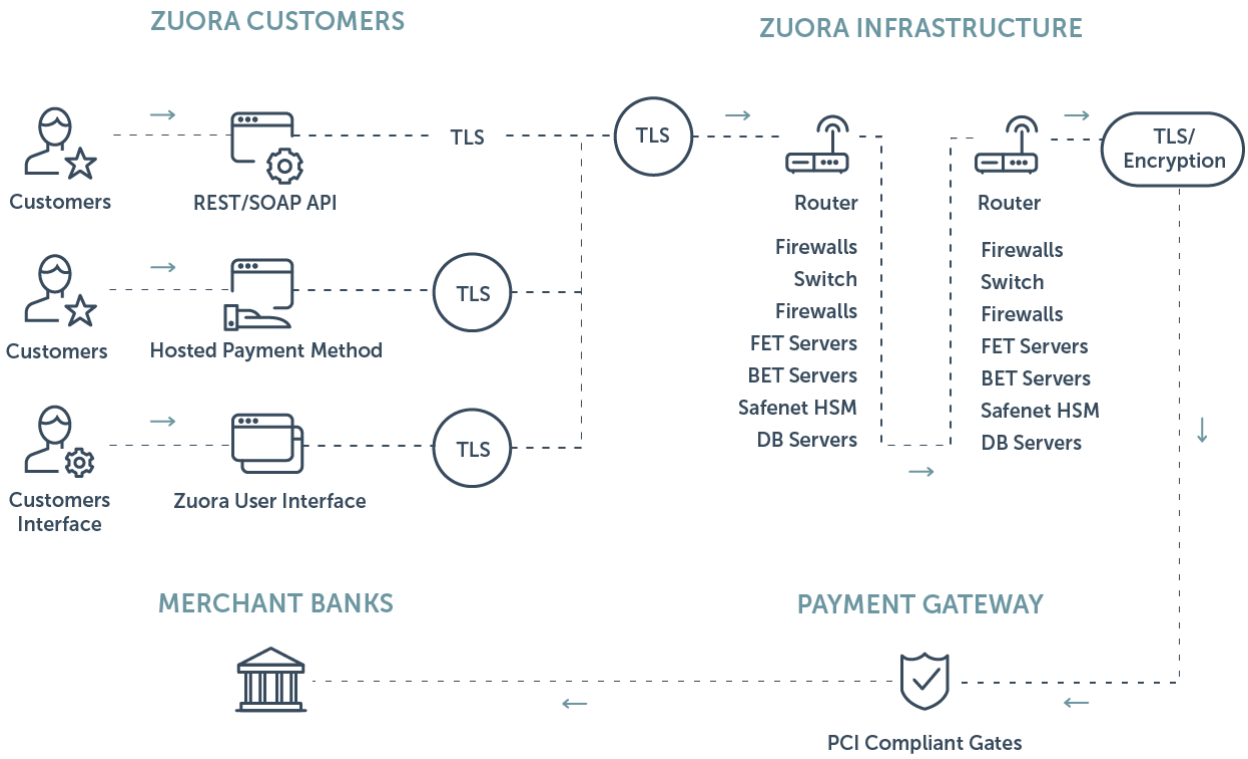
Zuora also takes measures to prevent malicious access to RevPro. The following diagram illustrates the firewalls that are set up at key network nodes:



Data Security

Zuora Central

The following diagram illustrates the flow of data through Zuora's infrastructure, from Zuora customers to payment gateways and merchant banks:



Data originates externally from Zuora customers and their direct customers. From there, the data reaches Zuora over TLS using one of the following primary channels:

- **Zuora API** - The Zuora REST API is accessible at https://rest.zuora.com (US Production environment) and https://rest.eu.zuora.com (EU Production environment). For existing Zuora customers with a tenant in the US Production environment, the legacy Zuora SOAP API is accessible at https://www.zuora.com/apps/service. The REST API and SOAP API both accept sensitive data encrypted with industry-standard TLS encryption.

- **Zuora Hosted Payment Method** - The Zuora Hosted Payment Method interface enables merchants to submit payment data to Zuora using direct POST over TLS. Alternatively, a payment method page can be embedded in an iframe, with payment data submitted directly from the customer's browser to Zuora over TLS.

- **Zuora Administrators** - The Zuora Administrator web interface is accessible at https://www.zuora.com/apps/newlogin.do (US Production environment) and https://eu.zuora.com/apps/newlogin.do (EU Production environment). The web interface enables administrators in Zuora customer organizations to configure Zuora settings. Not cardholder data is transmitted or accessed over this channel.

From these encrypted input channels, data enters the Zuora system. Data is then further stored, processed, and transmitted as follows:

- Cardholder data is encrypted with TLS when in transit over Zuora managed devices, including network devices and load balancers.

- Cardholder data is processed within logically and physically secured Frontend Tomcat (FET) and Backend Tomcat (BET) servers.

- Cardholder data is encrypted using 256 bit Advanced Encryption Standard (AES-256) and HSM managed keys when stored on internal hardened database servers

- To support the secure transfer of cardholder data into and out of the Zuora CDE (cardholder data environment), all files are required to be encrypted using PGP asymmetric encryption with an RSA bit size of 3,072 bits or equivalent. All files are also required to be transferred using the SFTP encrypted file transfer protocol.

- Strong asymmetric private keys are generated and armored with symmetric encryption. Key encryption keys are retained in a separate location.

- A Secure Migration Policy governs access and controls for data migration activities.

To process payments, cardholder data is encrypted using TLS or equivalent encryption technology when transmitted to PCI-compliant payment gateway providers. Each Zuora customer has a choice of payment gateways to use to connect to their merchant bank. Zuora leverages secure interfaces of the PCI-compliant payment gateway when transmitting data to that gateway. All transactions are processed using the Merchant ID of the Zuora customers.

Payment gateways then transmit cardholder data using secure interfaces to the merchant bank for settlement. Merchant banks are directly responsible for PCI compliance. Payment gateways are obligated to maintain their PCI compliance annually. Each Zuora customer chooses their own merchant bank and each merchant is responsible for transaction settlement directly with their respective merchant bank.

Compliance

Zuora Central

Zuora maintains the following types of compliance and certification:

- PCI DSS Level 1 Compliance
- SOC 1 (SSAE18 and ISAE 3402) Type 2 Compliance
- SOC 2 Type 2 Compliance
- SOC 3 Compliance

- ISO 27001 Certification
- ISO 27018 Certification
- HIPAA (Business Associate) Compliance
- EU-U.S. Privacy Shield
- Swiss-U.S. Privacy Shield
- TrustArc platform assessment (previously TRUSTe)

The latest compliance reports can be provided upon request under a mutual non-disclosure agreement.

Zuora RevPro

Zuora RevPro maintains the following types of compliance:

- SOC 1 (SSAE18 and ISAE 3402) Type 2 Compliance
- SOC 2 Type 2 Compliance
- ISO 27001 Certification
- ISO 27018 Certification
- EU-U.S. Privacy Shield
- Swiss-U.S. Privacy Shield
- TrustArc platform assessment (previously TRUSTe)

Support

Zuora provides 24/7 support coverage for Zuora Central and Zuora RevPro across multiple channels, including online portals, email, and phone. Zuora employs full-time support representatives with domain and technical expertise.

Zuora customers, partners, and employees can use the Zuora Community to:

- Find answers and share expertise
- Submit and vote on product ideas
- Collaborate globally and in regional user groups
- Subscribe to product release and service notifications

The Zuora Community is located at https://community.zuora.com/.

The Zuora Global Support portal is located at https://support.zuora.com. For Zuora RevPro support, visit https://support.leeyo.com/support/login.

Other support resources include:

- Zuora Knowledge Center - https://knowledgecenter.zuora.com/
- Zuora Developer Center - https://www.zuora.com/developer/