RELISH Platform

Technologies, Services, Security

RELISH

Proprietary & Confidential

Table of Contents

1 GENERAL INFORMATION

1.1 Definition

“AWS”	Amazon Web Services is a subsidiary of Amazon providing on-demand cloud computing platforms and APIs to individuals, companies, and governments, on a metered pay-as-you-go basis.
“Amazon CloudFront”	Is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency, high transfer speeds, all within a developer-friendly environment.
“AWS Step Functions”	Serverless function orchestrator that makes it easy to sequence AWS Lambda functions and multiple AWS services into business-critical applications. The output of one step acts as an input to the next. Each step in your application executes in order, as defined by your business logic.
“Amazon API Gateway”	Fully managed service that makes it easy for developers to create, publish, maintain, monitor, and secure APIs at any scale. APIs act as the "front door" for applications to access data, business logic, or functionality from your backend services.
“AWS Organizations”	AWS Organizations is an account management service that enables you to consolidate multiple AWS accounts into an *organization* that you create and centrally manage.
“AWS Organizations”	AWS Organizations is an account management service that enables you to consolidate multiple AWS accounts into an *organization* that you create and centrally manage.
“AWS CloudFormation”	AWS **CloudFormation** is a service that gives developers and businesses an easy way to create a collection of related AWS and third-party resources, and provision and manage them in an orderly and predictable fashion.
“AWS CloudFormation”	AWS KMS is a secure and resilient service that uses hardware security modules that have been validated under FIPS 140-2, or are in the process of being validated, to protect your keys.

1.2 Introduction

Relish bridges enterprise data systems to help teams collaborate and work where they feel the most comfortable. We are pioneers in data integration using native APIs to simplify the complex. We have done the development, so you do not have to.

This document consists of an overview of Relish's Platform which comprises a modern technological architecture to support Relish's applications in an enterprise space. In addition, the Platform includes services to maintain the uptime, security and integrity supporting any and all Relish APPs you subscribe to.

Platform Technological Features

User and Configuration Administration: Regardless of the APP licensed from Relish, at least one administration user seat will be included to support client access for:

- User creation and maintenance which may include SSO settings consistent with the client's internal network.
- APP Configurations such as Spend Solution test and production instance access or enablement of integrations with specific APIs.
- APP Monitoring such as logs of transactions processed or API messaging history

Integration and Scheduling Utilities: Nearly every Relish APP functions as a bridge between 2 or more systems with the most common end-point being the client's chosen Spend Management system. The Relish Platform, therefore, is optimized for facilitating the transfer of data through standard APIs from each of the integrated systems. Most integration actions are triggered in the system "end-points" but Relish also has a Scheduling capacity that allows for time-based triggered integrations.

Transport and Data Security: All Relish APPs sit on a robust and secure platform for the Data that is continually transferred from one system to another. Security of data in transit and data at rest is integral to the platform and therefore available for any Relish APP as needed. For more on Security Management see section 3 below.

Amazon Web Services Infrastructure: The Relish Platform is built on the Amazon Web Services infrastructure and uses tools available through the AWS ecosystem. In addition to the features above, this includes Physical Security, Disaster Recovery, Infrastructure Security and access to Monitoring and Data services as well. For more, please see Section 2 and 3 below.

Platform Services

Hosting and Uptime Service Levels: The Relish Platform and all Apps based on the platform will be maintained by Relish to support the above Features with uptime service

levels as noted in the Order Form Supplemental Terms. All hosting costs for the Relish Platform and Apps are included.

Customer Support: Support for use and configuration of the Relish Platform and Apps based on the platform are included as noted in the Order Form Supplemental Terms.

Integrated System Upgrade support: As an "Integration as a Service" provider, Relish provides 1st level support for changes that may occur among systems that are part of the Relish App solution. This support includes detection, notification, diagnosis and recommendations for addressing downtimes, changes, upgrades or sunsetting of functionality arising from integrated systems.

Relish Platform and App Evolution: The Relish Platform and Apps are provided as a software-as-a-service which may be upgraded over time. Subscription to Relish, therefore, includes upgrades and changes to the platform and apps

2 RELISH TECHNOLOGY

Relish Platform was developed as a web application exclusively, from administration to user interface, without anything to install on your servers or your computers, all any user needs is an internet browser to access all the features.

2.1 Relish Platform

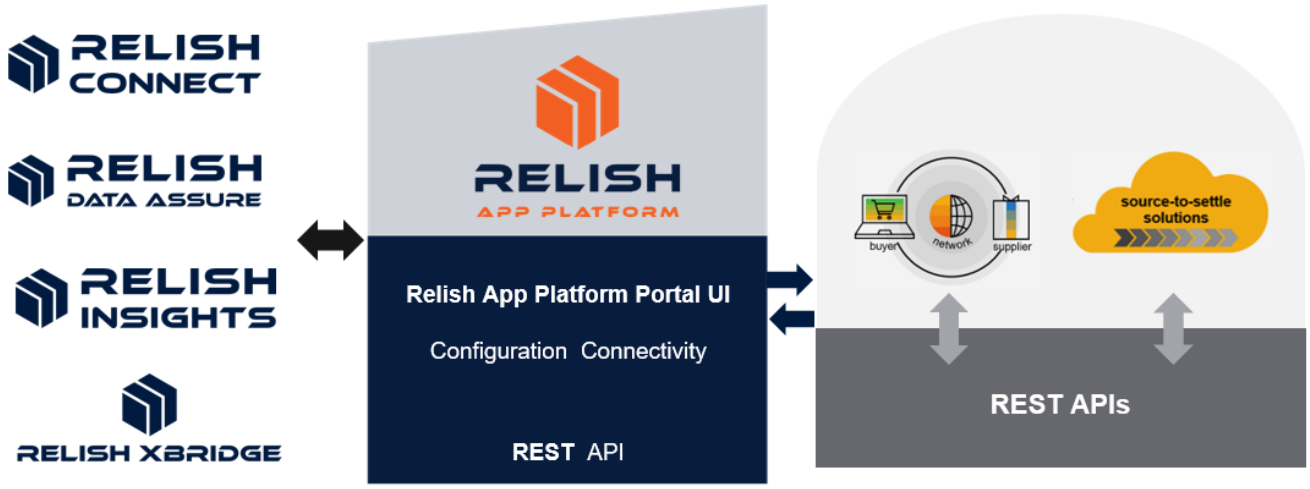


Figure 1 - Relish Platform

Our solution is developed using Amazon Web Services (AWS) which provides the hardware and infrastructure to support Relish applications. AWS was launched in July 2002 and is the most popular on demand infrastructure for commodity computing and virtual secure storage on the planet.

The Relish platform does not require special technical administration of the application and/or databases. It is designed as a multi-tenant application based on a micro-service architecture and built using serverless AWS services.

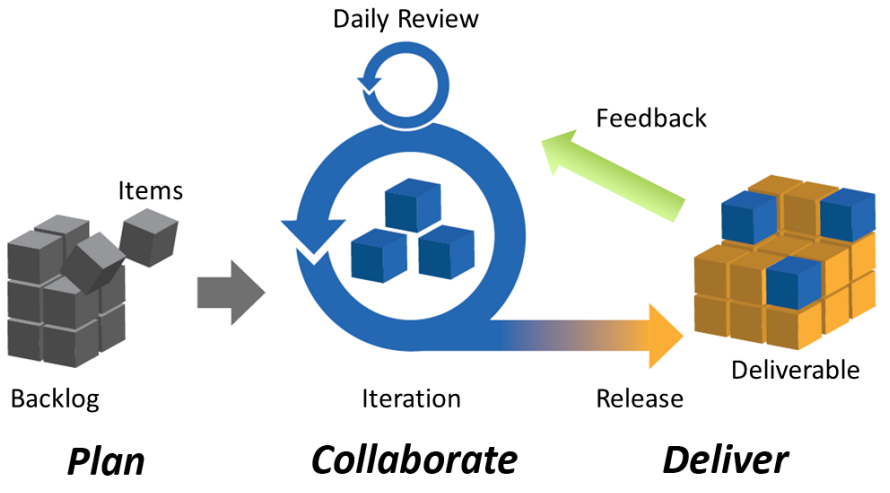
2.2 Software Architecture

The Relish Platform managed and deployed using AWS CloudFormation and it consists in 3 main components: Connector, Scheduler, Web Application.

This architecture allows flexible and loosely coupled services, which means that we can easily add and modify different connectors independently, and by using AWS serverless services we can scale based on workload while keeping costs down.

2.3 Agile Development Methodology

Relish's development process is based on the **Agile methodology** with its **iterative approach** to software development and assessment. This embeds Quality Assurance directly into the ongoing development process sooner than with a more traditional approach.
Agile software development is a set of software development methods based on iterative and incremental development, where requirements and solutions evolve through collaboration between self-organizing, cross-functional teams. It promotes adaptive planning, evolutionary development and delivery, a time-boxed iterative approach, and encourages rapid and flexible response to change. It is a conceptual framework that promotes foreseen interactions throughout the development cycle.



Agile Project Management: Iteration

For Major releases we add a project-level QA process that is in addition to the continual QA used for interim releases. We have implemented a comprehensive series of quality checks based on the ISO 25000:2014 standard.

Our development environment is based on OWASP best practices. The Open Web Application Security Project (OWASP) is an open-source application security project. The OWASP community includes corporations, educational organizations, and individuals from around the world. This community works to create freely available articles, methodologies, documentation, tools, and technologies.

3 Security Management

3.1 Physical Security

With Amazon.com providing the physical hosting infrastructure through their EC2 service, Amazon enforces physical security through a variety of methods as covered in their Security Whitepaper.

3.2 Transport Security

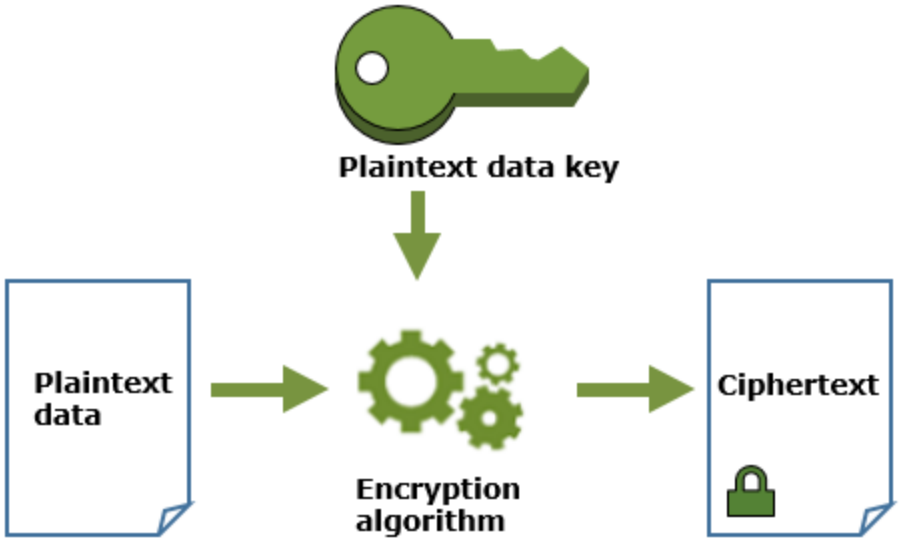
All communications between the web server and the clients (i.e., over the Internet) are encrypted. Access to Relish's on-demand applications and services is only available through secure sessions (https) and only available with an authenticated login and password. Relish uses HTTP over Transport Layer Security (HTTPS) for communication. Passwords are never transmitted or stored in their original form, so they are never compromised by third parties.

The Transport Layer Security (TLS) protocol is the industry standard method for protecting communications on IP networks, such as the Internet. TLS provides data encryption, server authentication, message integrity, and optional client authentication for TCP/IP connections. For encryption, TLS uses RSA Data Security, which is the most commonly used encryption and authentication algorithm. For more information, see RSA's website, www.rsa.com.

3.3 Application Security

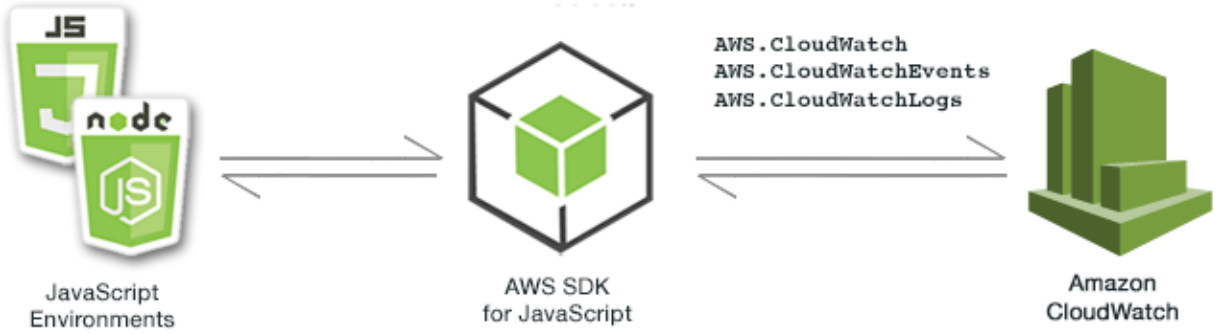
Application security governs end-user access to the online services and information on the Relish platform. Relish uses unique user IDs and passwords as the primary means of user authentication and access control. IDs and Passwords are case-sensitive. Passwords are stored hashed using the Auth0 service.

All other sensible data (API keys and other parameters) is stored and managed using AWS Key Management Service (KMS), AWS KMS is a secure and resilient service that uses hardware security modules that have been validated under FIPS 140-2, or are in the process of being validated, to protect your keys.



3.4 Monitoring Services

Relish uses Amazon Elasticsearch Service to stream data from Amazon CloudWatch and centralize its monitoring service providing a maximum alerting capability. It monitors all traffic, processes system messages and alerts, application status, transaction status, etc.



3.5 Database Security

Databases are partitioned for each customer so that the data for different customers does not co-mingle. Database infrastructure is completely segregated from the Application servers and the Internet via firewalls. Only application servers can query the database using strong authentication.

3.6 Disaster Recovery Program

Relish's Disaster Recovery Plan (DRP) outlines the policies and procedures that the company will use for technology disaster recovery. The goal of this plan is to outline the key recovery steps to be performed to critical technology platforms and telecommunications infrastructure after a disruption to protect the company's intellectual property as well as our clients' data and ability to operate without significant disruption.

3.7 Infrastructure Security

Relish uses AWS Service Control Policies to manage an AWS organization hierarchy that allows to control access and set boundaries to its different instances.

3.8 Security Policies and Standards

The following list of documents are maintained and updated to support the various security standards that Relish is a part of. Depending on the need or context, Relish may provide the latest versions or otherwise show their contents to aid in assessments and security discussions.

3.8.1 Exercise Documentation

- Business Impact Analysis
- AWS Risk Assessment

3.8.2 Policy Documentation

- Access Control Policy
- Audit and Accountability Policy
- Awareness and Training Policy
- Configuration Management Policy
- Contingency Planning Policy
- Identification and Authentication Policy
- Incident Response Policy
- Incident Response Plan
- Maintenance Policy
- Media Protection Policy
- Personnel Security Policy
- Physical and Environmental Protection Policy
- Planning Policy
- Program Management Policy
- Risk Assessment Policy
- Assessment, Authorization, and Monitoring Policy
- Systems and Communication Protection Policy
- System and Information Integrity Policy
- Systems and Services Aquisitions Policy

- Data Privacy Program
- Individual Participation Policy
- Privacy Authorization Policy

3.8.3 Standard Documentation

- Acceptable Use Standard
- Access Control Standard
- Anti-Malware & Anti-Virus Standard
- Asset Management Standard
- Audit & Assessment Standard
- Backup Management Standard
- Bring Your Own Device (BYOD) Standard
- Change Management Standard
- Configuration Management Standard
- Data Encryption Standard
- Data Retention Standard
- Incident Response Standard
- Information Classification Standard
- Information Security Exception Management Standard
- Logging & Monitoring Standard
- Media Destruction & Disposal Standard
- Network Device Management Standard
- Password Management Standard
- Physical Security Standard
- Remote Access Standard
- Risk Assessment & Management Standard
- Secure Software Development Lifecycle (SDLC) Standard
- Security Awareness Standard
- Vendor Management Standard
- Vulnerability Management Standard
- Wireless Networking Standard

4 Revision and Review

This log is updated each time this document is updated. The log identifies the version number, the date the version was completed, the author of the changes, and a brief description of the changes.

Version	Date	Author	Description
1.0	12/12/2019	IT Development	First version of the document.
1.1	06/01/2020	Security	Added Security management section
1.2	01/04/2021	Security	Added sections: 4.5 Database Security. 4.6 Disaster Recovery Program Minor changes to the document.
2.0	11/3/2021	Solution Mgmt	New Version based on Technical_Environment document but that applies across all Relish APPs and regardless of other integrated systems. Added descriptions of Platform technologies and services.