:RESOLVER

ENTERPRISE-LEVEL DATA SECURITY WITH AMAZON WEB SERVICES

INTRODUCTION

The security and privacy of your data is extremely important to both of us. We provide enterprise-level security and privacy that satisfies the most demanding security-sensitive organizations through a comprehensive program that meets the requirements of AICPA SOC 2 Trust Service Principles.[1]

Resolver's cloud software applications are deployed on Amazon Web Services (AWS), one of the most flexible and secure cloud computing environments available. With AWS, we provide our customers with advanced cloud infrastructure and application services in a secure and rapid fashion.

[1] *https://aws.amazon.com/compliance/soc-faqs/*

INFRASTRUCTURE

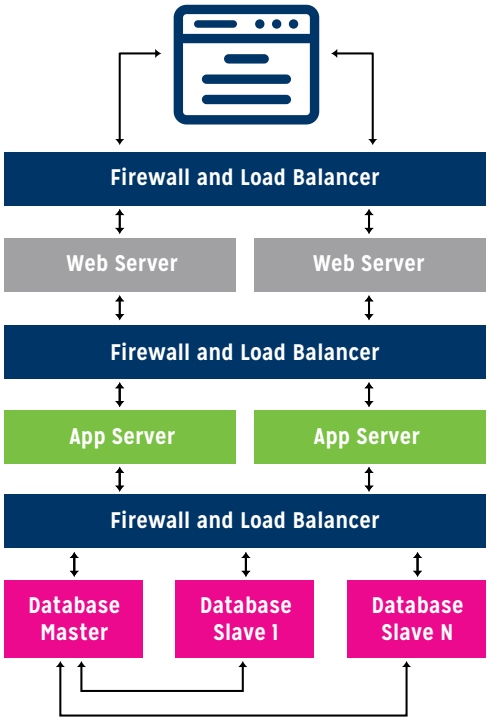


Figure 1: Resolver's Multi-Tiered Architectural Approach

Resolver's cloud infrastructure is housed in AWS's data centers and is designed to satisfy the requirements of the most security-sensitive customers. The AWS infrastructure has been designed to provide the highest availability while putting strong safeguards in place regarding customer privacy and segregation.[2]

Resolver uses a multi-tiered architectural approach, as shown in Figure 1.

Availability

Resolver's hosted service level commitment for availability is 99.9% as measured monthly and is both local and geo applied.[3]

AWS builds its data centers in multiple geographic regions as well as across multiple Availability Zones within each region to offer maximum resiliency against system outages. AWS designs its data centers with significant excess bandwidth connections so that if a major disruption occurs there is sufficient capacity to enable traffic to be load-balanced to the remaining sites, minimizing the impact on you.[4]

Scalability

AWS provides automatic horizontal (adding more machines) or vertical (adding more power [CPU/RAM] to your existing machine) expansion to meet your changing business needs with ease.

Server regions

As a Resolver customer, you choose the region in which your servers are located. We currently offer server locations in the US, Europe, and Canada.[5] As a Resolver customer, you are free to choose the region that best suits your unique needs.

24x7 monitoring and protection

AWS infrastructure is protected by extensive network and security monitoring systems. In addition, AWS infrastructure components are continuously scanned and tested. Access to the AWS production network is monitored by the Resolver DevOps team. The AWS production network is segregated from the Resolver corporate network and requires a separate set of credentials for access, consisting of SSH public-key authentication through a secure and hardened host using a MFA token.

[2] *https://aws.amazon.com/security/platform/*
[3] *99.9% as measured monthly excluding scheduled and planned maintenance.*
[4] *https://aws.amazon.com/security/platform/*
[5] *https://aws.amazon.com/about-aws/global-infrastructure/*

CERTIFICATIONS AND AUDITS

AWS provides certification reports that describe how the AWS infrastructure meets the requirements of an extensive list of global security standards, including:

- ISO 27001
- ISO 27018
- PCI Data Security Standards (DSS) Level 1
- SOC
- FedRAMP
- the Australian Signals Directorate (ASD) Information Security Manual
- the Singapore Multi-Tier Cloud Security Standard (MTCS SS 584)

For more information about the security regulations and standards with which AWS complies, see the AWS compliance webpage. [6,7]

Health Insurance Portability and Accountability Act (HIPAA)

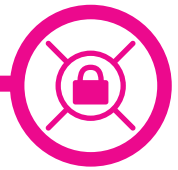
AWS enables covered entities and their business associates subject to the U.S. Health Insurance Portability and Accountability Act (HIPAA) to leverage the secure AWS environment to process, maintain, and store protected health information.[8]

Personally Identifiable Information (PII) Protection

AWS infrastructure is ISO 27018 certified, meaning AWS follows best practices for cloud security.

[6] *https://aws.amazon.com/compliance/pci-data-privacy-protection-hipaa-soc-fedramp-faqs/*
[7] *https://aws.amazon.com/security/platform/*
[8] *https://aws.amazon.com/compliance/*

DATA SECURITY



Resolver encrypts data at rest and in transit using commercial methods for all product lines. Resolver performs monthly, quarterly, and annual security assessments that incorporate a Resolver hosted platform penetration test utilizing industry standard software, reviews of security policies, and practices.

ACCESS MANAGEMENT

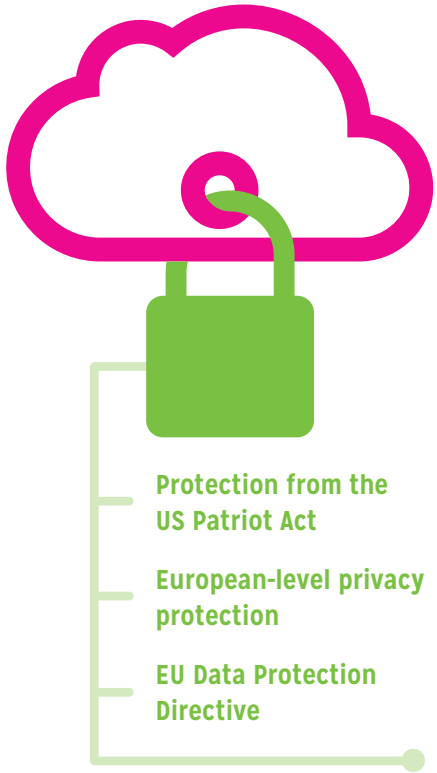
Our access to your data is strictly controlled and limited to authorized personnel, and only for the purposes of delivering and supporting Resolver's services. Access to production systems is limited to a small segregated Resolver staffed DevOps team. Access controls ensure that users cannot access information unless they are authorized to do so. All Resolver's Hosted Platforms resources, systems, and applications have access controls implemented.

All Resolver employees receive security training on Resolver's security and privacy policies and procedures. Security training is an on-going activity at Resolver. Periodic security reminders keep full time and contract team members up to date with potential new threats. The frequency and form of these reminders vary and include matters such as security-related notices, emails, and verbal communication.

BACKUPS

Everything in our AWS hosted facilities is backed up in real time and kept for 24 hours. Resolver also takes and keeps full nightly images of our servers. In a disaster recovery scenario, data will automatically adjust to make itself available. Please contact Resolver for further details about our disaster recovery procedure.

PRIVACY



Privacy is important to Resolver. As a Canadian-based company, we offer customers European-level privacy protection. Canada's privacy laws meet European Union (EU) requirements and provide US organizations with protection against the US Patriot Act.

Protection from the US Patriot Act

If you buy a cloud-based application from a US-based company, or a company whose data centers are located in the US, the US Patriot Act may permit US authorities to legally access your data without permission and without notice.

As a Canadian-based company providing cloud-based applications, we are able to provide our US customers an extra level of protection from the Patriot Act. The FBI or any other agency would have to obtain an injunction or subpoena against Resolver. We are not obligated to provide access to a customer's data without informing our customers of the request from the US agency. Effectively, with a US-based cloud service, that cloud service would have to comply to data requests without injunction or subpoena. A company would never have to inform its customers of the request.

All the while, a US customer's data is still located in the US, but it is without a US-based address or location (which is the definition of cloud-based offerings as differed from colocation or hosted services).

By purchasing non-US-based cloud services from Resolver, US-based companies are better able to protect their data from the US Patriot Act with Canada's strong privacy laws.

EU-based companies using Resolver applications on Resolver's EU servers will be better protected from the US Patriot Act by EU privacy laws.

European-level privacy protection

Europe's privacy laws are significantly more focused in the rights of individuals than those in the US. Currently Canada's personal information privacy laws are comparable, if not equivalent, to EU privacy laws.

EU-based customers choosing Resolver's application services can be confident that their EU privacy obligations are being complied with. By choosing Resolver's EU-based servers, your data will be protected by EU privacy laws. By choosing Resolver's Canadian-based servers, your data will be protected by Canadian privacy laws. This can be quite advantageous to US-based companies that would like their data to be protected by the strong privacy laws in Canada and the EU.

EU Data Protection Directive

AWS is in compliance with the EU Data Protection Directive (Directive 95/46/EC), protecting processing of individuals personal data and the free movement of such data.[10]

[10] *https://aws.amazon.com/compliance/eu-data-protection/*

NEW RELEASES

New product releases are automated and managed by Resolver, however, special accommodations can be made when required.

SUPPORT

Resolver premium support is available 24 hours a day, 7 days a week.

Online:
Create a ticket

Phone:
Speak to a support representative

APPENDIX: ADDITIONAL INFORMATION

For more information on AWS compliance and security, please explore the links below:

AWS Cloud Security:
https://aws.amazon.com/security/

AWS Compliance:
https://aws.amazon.com/compliance/

AWS PCI:
https://aws.amazon.com/compliance/pci-dss-level-1-faqs/

AWS HIPPA:
https://aws.amazon.com/compliance/hipaa-compliance/

AWS SOC:
https://aws.amazon.com/compliance/soc-faqs/

AWS Data Privacy:
https://aws.amazon.com/compliance/data-privacy-faq/

ABOUT RESOLVER:

Resolver is the risk backbone for over 1000 of the world's largest organizations, providing software that takes the uncertainty from risk based decisions. Its integrated platform supports application areas including Decision Making, Internal Control, Internal Audit, Compliance Management, Enterprise Risk Management and Incident Management. Resolver's team members are experts in all areas related to risk, supporting users located across more than 100 countries. Resolver has offices in North America, United Kingdom, the Middle East, and Australia.

:RESOLVER

888.891.5500 | RESOLVER.COM