

RONIN

ISOLATE (TRE/SDE)

< SELF-SERVICE RESEARCH COMPUTING IN A BUBBLE >



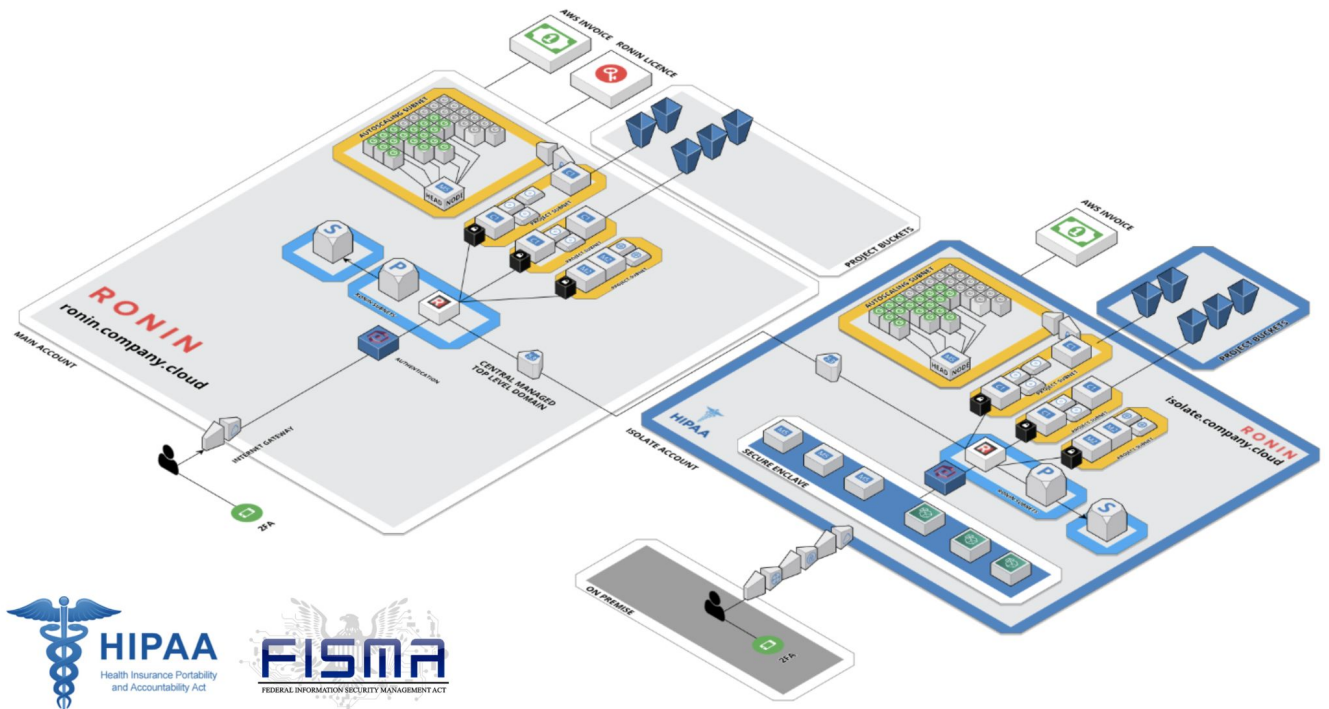
THE USER EXPERIENCE YOU LOVE, WITH THE COMPLIANCE YOU NEED

RONIN Isolate is a Trusted Research Environment (TRE) and Secure Data Environment (SDE) designed to meet the security and compliance demands of our most security-conscious customers, while providing users the same experience as **RONIN** Core. **RONIN** Isolate is configurable to be completely locked down and isolated from the outside environment to be eligible for HIPAA, FISMA and beyond.

WHY RONIN ISOLATE?

RONIN ISOLATE HELPS PROTECT YOUR SENSITIVE DATA

Supporting self-service research on AWS using protected information is challenging. **RONIN** Isolate is a research environment designed to meet the security and compliance demands of our most security-conscious customers, while providing users with an intuitive self-service platform that is as easy to work in as a laptop.



HOW DOES **RONIN** ISOLATE DIFFER FROM **RONIN** CORE?

The main characteristic of **RONIN** Isolate in contrast to our flagship product **RONIN** Core is that **RONIN** Isolate is deployed in an AWS account that is, by default, isolated from the outside world. All AWS resources must be accessed through a secure enclave. By default the secure enclave will contain Amazon workspaces for the users to access the environment. These can be restricted to IP addresses, approved devices, transit gateway connections and more..

RONIN Isolate additionally provides a configurable baseline of policies, controls and guardrails required to best position your organization to meet both regulatory and institutional IT security requirements.

- ✓ Restricted Access via Secure Enclave
- ✓ Machine Restricted Storage Keys
- ✓ Data Encrypted in Transit and at Rest

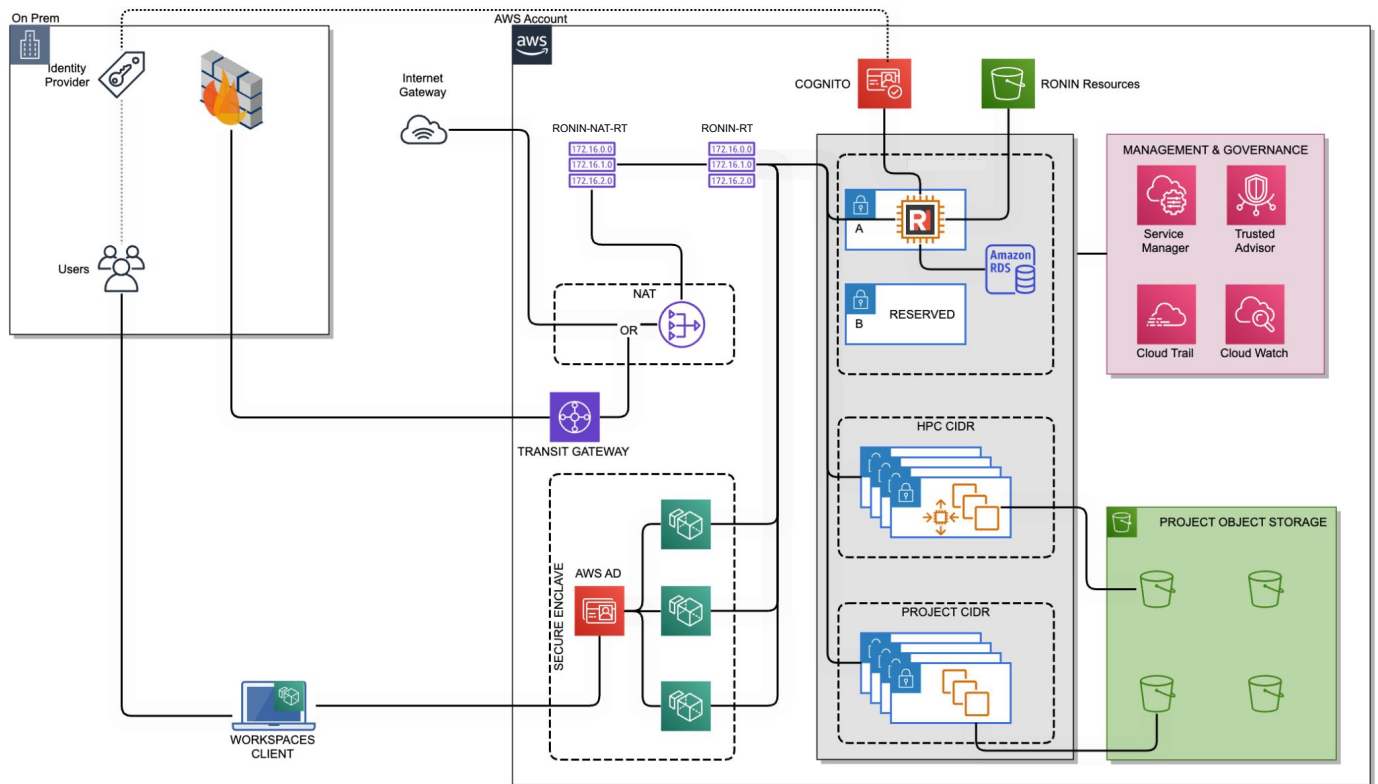
- ✓ Comprehensive Logging and Auditing
- ✓ Custom Network Isolation Rules
- ✓ All the features of **RONIN** Core

RONIN ISOLATE FEATURES

A SECURE ARCHITECTURE

RONIN Isolate is installed within your organization's AWS account (“self-hosted”). It is not Software as a Service (SaaS). This self-hosted deployment model provides your organization complete visibility and control over every aspect of the underlying AWS infrastructure and also means data never needs to leave your custody or be copied to a third party.

RONIN Isolate creates an Amazon Virtual Private Cloud (VPC) service, which allows RONIN to launch AWS resources in a virtual network. To isolate this VPC from public network access, it must be connected to your secure enclave and a NAT gateway. RONIN Isolate is architected to only allow access to the resources from the secure enclave. Machines created in **RONIN** have no inbound network connectivity except through the secure enclave. Outbound traffic goes via the NAT gateway and can be directed to an internet gateway, Firewall, or transit gateway to go via your on prem firewalls.



RONIN ISOLATE FEATURES

LOGGING AND AUDITING

RONIN Isolate also helps customers address compliance requirements related to in-depth auditing capabilities. **RONIN** Isolate supports granular protection of data by user and machine to limit data access according to the principle of least privilege and separation of duties. Every action that a user makes within **RONIN** Isolate is logged and can be audited.

Together, **RONIN** Isolate logging for UI actions and AWS CloudTrail logging for AWS infrastructure actions provide clear audit trails for who accessed data, when they accessed it, who created which machines, who created keys, and who granted access to machines and keys. These audit trails support HIPAA regulations for monitoring and auditing use of electronic protected health information (ePHI) or identifying accidental exposure.



ENCRYPTION

Within the environment, **RONIN** Isolate ensures that all data is encrypted at rest and in transit to meet industry standard best practice guidelines defined by the CIS (Center for Internet Security). All access within **RONIN** Isolate private networks is encrypted in transit through the use of SSH and HTTPS protocols only.

All data that is stored on drives or S3 buckets created with **RONIN** are encrypted at rest and bucket policies are enforced to ensure object access is only available to allowlisted machines within **RONIN** Isolate private subnets over internal HTTPS.



BACKUP AND DISASTER RECOVERY

Institutions and projects often require fine-grained control over data backup and disaster recovery mechanisms to trade off cost versus risk. **RONIN** Isolate automates complex security capabilities such as access key regeneration and backup of data, machines and clusters to highly durable storage. These features support implementation of policies that minimize risk of accidental loss and a variety of automated or non-automated backup procedures.



RONIN ISOLATE FEATURES

ADDITIONAL AWS ACCOUNT SECURITY BEST PRACTICES

Because **RONIN** Isolate is installed within your organization's AWS account, the shared responsibility model established between AWS and the customer applies. **RONIN** configures the organization's account to be in the best position for addressing security and compliance requirements; however, organizations may tighten or relax constraints to serve their needs.

AWS provides multiple services to implement additional security controls that **RONIN** Isolate is fully compatible with including:



AWS Trusted Advisor: an AWS service that can perform checks (dependent upon your AWS Support Plan) to help with security based on AWS best practices.


AWS GuardDuty: a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts, workloads, and data stored in Amazon S3.

If you have questions about how **RONIN** Isolate can provide a secure research environment, please contact us to discuss your specific requirements.

DON'T BE SHY..

CONTACT US TO GET UP AND **RONIN**.

 [HTTPS://RONIN.CLOUD](https://ronin.cloud)

 CONTACT@RONIN.CLOUD

OR STALK US...

