

Enabling Secure Trusted Research Environments for Biomedical Research at a Leading US Academic Medical Center

Executive Summary

The customer is one of the nation's premier academic medical centers, supporting hundreds of researchers conducting studies involving protected health information (PHI), clinical datasets, genomics, medical imaging, and other highly sensitive research data.

As research programs expanded across multiple departments and business units, the institution required a modern cloud platform that would enable researchers to leverage AWS while maintaining strict institutional security policies and governance requirements.

The institution sought a Trusted Research Environment (TRE) that would provide secure, isolated research workspaces while ensuring sensitive data remained protected throughout its lifecycle—from data ingestion to researcher collaboration and controlled data export.

Relevance Lab partnered with the academic medical center to deploy a customized implementation of Research Gateway that provided secure research environments, automated governance workflows, and simplified administration across the organization.

Business Challenge

The institution needed to provide researchers with scalable cloud-based research environments while satisfying stringent institutional security, compliance, and operational requirements.

Several key challenges had to be addressed:

Challenge 1: Secure Research Workspaces

Challenge 2: Standardized Computing Environments

Challenge 3: Controlled Data Movement

Challenge 4: Role-Based Governance

Challenge 5: Scalable Administration

At a Glance

Industry

Healthcare & Life Sciences

Solution

Secure Trusted Research Environment (TRE) Platform

Platform

Relevance Lab Research Gateway on AWS

Primary Goals

Secure Research Computing, Governance, Compliance, Data Protection

Research Areas

Clinical Research, Biomedical Research, Population Health, Genomics, AI/ML

Key Capabilities

Secure Research Workspaces, Data Ingress/Egress Governance, Research Project Management, Cost Monitoring

Compliance Focus

HIPAA-Aligned Security Controls, Controlled Data Access, Institutional Governance



Challenge 1

Secure Research Workspaces

Research workspaces needed to be deployed within AWS while remaining accessible only from the institution's corporate network. Direct Internet access to research desktops was prohibited, ensuring that sensitive research data remained within the institution's secure environment.



Challenge 2

Standardized Computing Environments

Research IT required every workspace to conform to institutional standards. Researchers needed Windows Server and Red Hat Enterprise Linux desktop environments with mandatory enterprise software—including CrowdStrike security agents—and licensed research applications such as SAS pre-installed and centrally managed.



Challenge 3

Controlled Data Movement

Research data could not be freely imported into or exported from research environments. All ingress and egress activities required institutional approval, complete auditability, and enforcement of approved data handling policies to prevent unauthorized movement of sensitive information.



Challenge 4

Role-Based Governance

The platform needed to support multiple organizational roles with clearly separated responsibilities.

Research administrators required the ability to onboard AWS accounts, create projects, configure research environments, and manage institutional settings. Researchers and Project Owners needed self-service capabilities within the boundaries established by institutional governance.



Challenge 5

Scalable Administration

As the number of research programs increased, the institution required a solution that minimized manual administration while maintaining centralized governance, consistent security controls, and cost visibility across departments.

The objective was to create a secure, scalable, and researcher-friendly cloud platform that accelerated scientific discovery without compromising compliance or institutional governance.



Solution

Secure Trusted Research Environment on AWS

Relevance Lab deployed Research Gateway as a private institutional research platform accessible exclusively from the customer's network.

The solution combined secure infrastructure provisioning with automated governance workflows to provide researchers with compliant, self-service research environments.

Private Research Portal

Research Gateway was deployed as an internal application accessible only from within the institution's network.

Researchers could securely request and manage cloud resources without exposing administrative services to the public Internet.

Trusted Research Environment

Each research project received isolated cloud workspaces with centrally managed security controls.

Key capabilities included:

- Windows Server Remote Desktop environments
- Red Hat Enterprise Linux Remote Desktop environments
- Standardized institutional software images
- Mandatory CrowdStrike endpoint protection
- Centrally managed software updates
- Licensed research applications including SAS
- Secure project storage
- Identity-based access controls

Governed Data Ingress and Egress

Research Gateway implemented approval-driven workflows governing all movement of research data.

A dedicated Data Administrator role was introduced to oversee institutional data governance.

Responsibilities included:

- Managing institutional Data Libraries
- Creating and administering research studies
- Reviewing and approving data ingress requests
- Reviewing and approving data egress requests
- Maintaining complete audit trails
- Enforcing institutional data handling policies

This governance model ensured researchers could collaborate efficiently while preventing unauthorized movement of sensitive information.

Customized Research Catalog

The standard Research Gateway catalog was customized to align with the institution's research requirements.

Customized offerings included:

- Windows secure research desktops
- Red Hat Enterprise Linux secure desktops
- SAS-enabled research environments
- Standardized research software stacks
- Institution-approved compute configurations

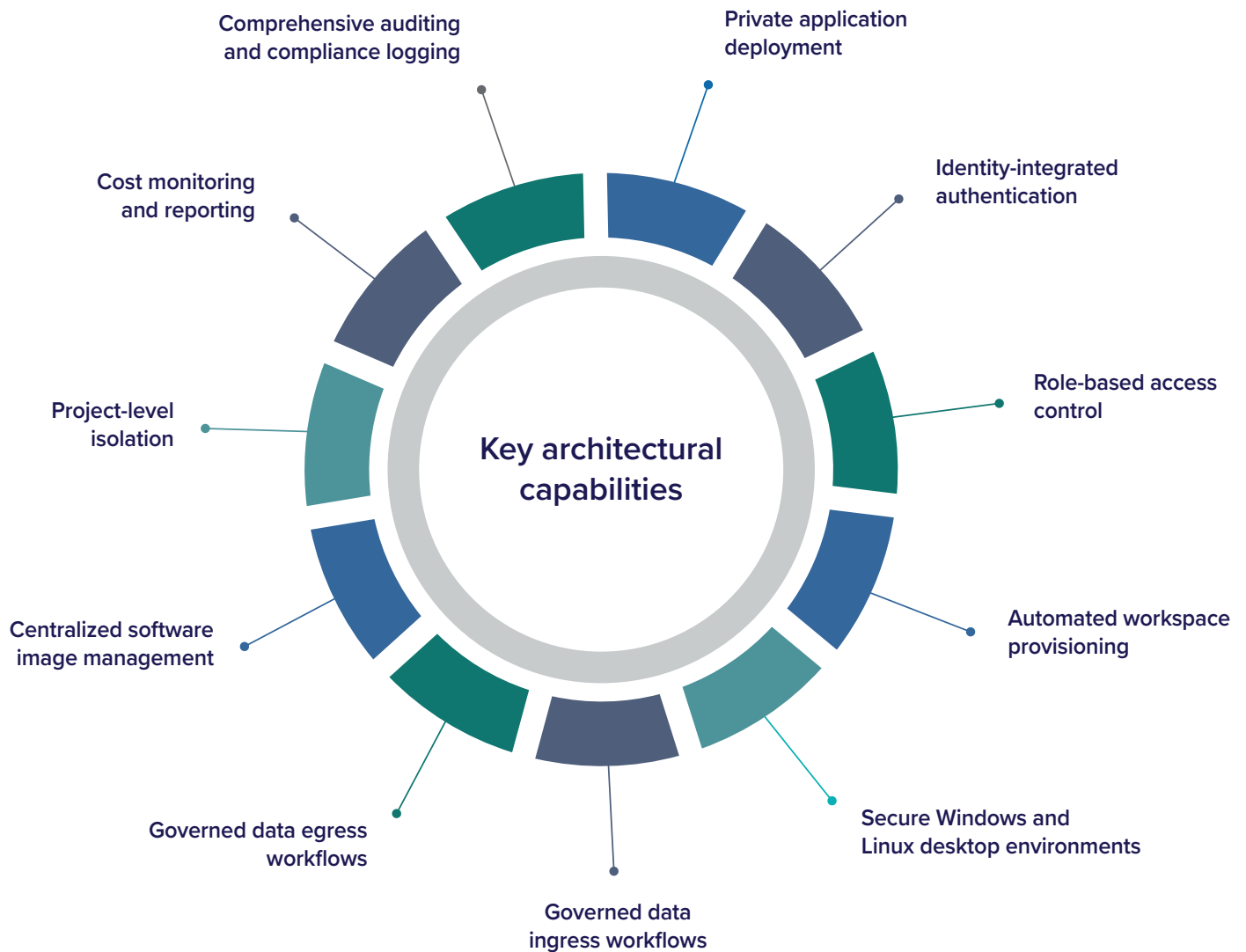
Researchers could provision approved environments without requiring Research IT to manually build individual systems.

Architecture Highlights

Secure Research Platform with Centralized Governance

Researchers access Research Gateway through the institution's internal network, where authenticated users provision secure research workspaces using institution-approved catalog offerings.

Research Gateway orchestrates AWS infrastructure while enforcing governance policies, approval workflows, and role-based access controls



Business Outcomes

Deployment of Research Gateway enabled the institution to securely expand cloud adoption across its research community while reducing operational complexity for Research IT.

Researcher Productivity

Researchers gained rapid access to secure, institution-approved computing environments without waiting for manual infrastructure provisioning.

Benefits included:

- Faster onboarding of new research projects
- Self-service provisioning of approved workspaces
- Consistent research environments across departments
- Immediate access to licensed research software
- Reduced dependency on Research IT for routine requests

Governance and Compliance

Institutional governance became embedded within the research platform rather than relying on manual processes.

Improvements included:

- Controlled data ingress and egress approvals
- Complete auditability of data movement
- Centralized management of sensitive datasets
- Standardized security controls across all projects
- Reduced risk of unauthorized data exfiltration

Operational Efficiency

Research Gateway centralized administrative functions while allowing researchers to operate independently within approved governance boundaries.

Administrative improvements included:

- Simplified onboarding of AWS accounts and business units
- Standardized project creation
- Centralized software management
- Reduced manual provisioning effort
- Consistent policy enforcement across research programs

Financial Visibility

Research administrators gained improved visibility into cloud consumption through project-level cost monitoring and reporting.

This enabled departments to:

- Monitor research spending
- Allocate cloud costs by project
- Improve budget planning
- Optimize cloud utilization

Key Outcomes

- ✓ Secure Trusted Research Environment for sensitive biomedical research
- ✓ Private cloud platform accessible only from the institution's network
- ✓ Governed data ingress and egress approval workflows
- ✓ Standardized Windows and Red Hat Enterprise Linux research workspaces
- ✓ Licensed research software delivered through a customized catalog
- ✓ New Data Administrator role supporting institutional data governance
- ✓ Self-service research platform with centralized administration
- ✓ Improved compliance, governance, and cloud cost visibility



Customer Perspective

“

Research Gateway provided our institution with a secure and scalable Trusted Research Environment that enables our researchers to focus on scientific discovery rather than infrastructure management. By combining standardized research workspaces with governed data workflows and centralized administration, we have significantly improved security, operational efficiency, and researcher productivity while maintaining the compliance standards required for sensitive biomedical research.

— Research IT Leadership, Leading US Academic Medical Center

Accelerate Research with Research Gateway

Secure by Design. Governed by Policy. Built for Research Innovation.

Relevance Lab's Research Gateway enables healthcare organizations, academic medical centers, universities, and research institutions to build secure, governed Trusted Research Environments (TREs) on AWS.

Empower researchers with self-service cloud access while maintaining enterprise security, compliance, and operational control.

[Learn More About Research Gateway](#)

Recognized as a
trusted AWS partner

