AWS State, Local, and Education Learning Days

Philadelphia

aws Learning Days
State, Local, and Education

Secure Research Environment and Portal

Compliant Research Data Architecture and Data Sharing

Brian McCarthy (he/him)

Solutions Architect
AWS
btmccar@amazon.com

aws **Learning Days**
State, Local, and Education

Why now?

Why now?

Securing research data has never been more important

Hacker Groups

Criminal gangs

Ransomware

Nation states

Internal threats

IP theft

Why now?

Securing research data has never been more important

Research data has value and is an active target

Ransom costs

Remediation costs

Forensic costs

Hacker groups

Criminal gangs

Nation states

Internal threats

Ransomware

IP theft

Reputational damage

Why now?

Responsible stewardship of research data is expected

HIPAA

GDPR

CCPA

Data privacy

Responsible use

NIST / CUI

DFARS

CMMC

Why now?

Responsible stewardship of research data is expected

Compliance defines specific responsibilities for research data

Penalties and fines

data breach

HIPAA

GDPR

CCPA

Data privacy

Funding withheld

non-compliance/data exfiltration

NIST / CUI

DFARS

CMMC

Responsible use

Reputational damage

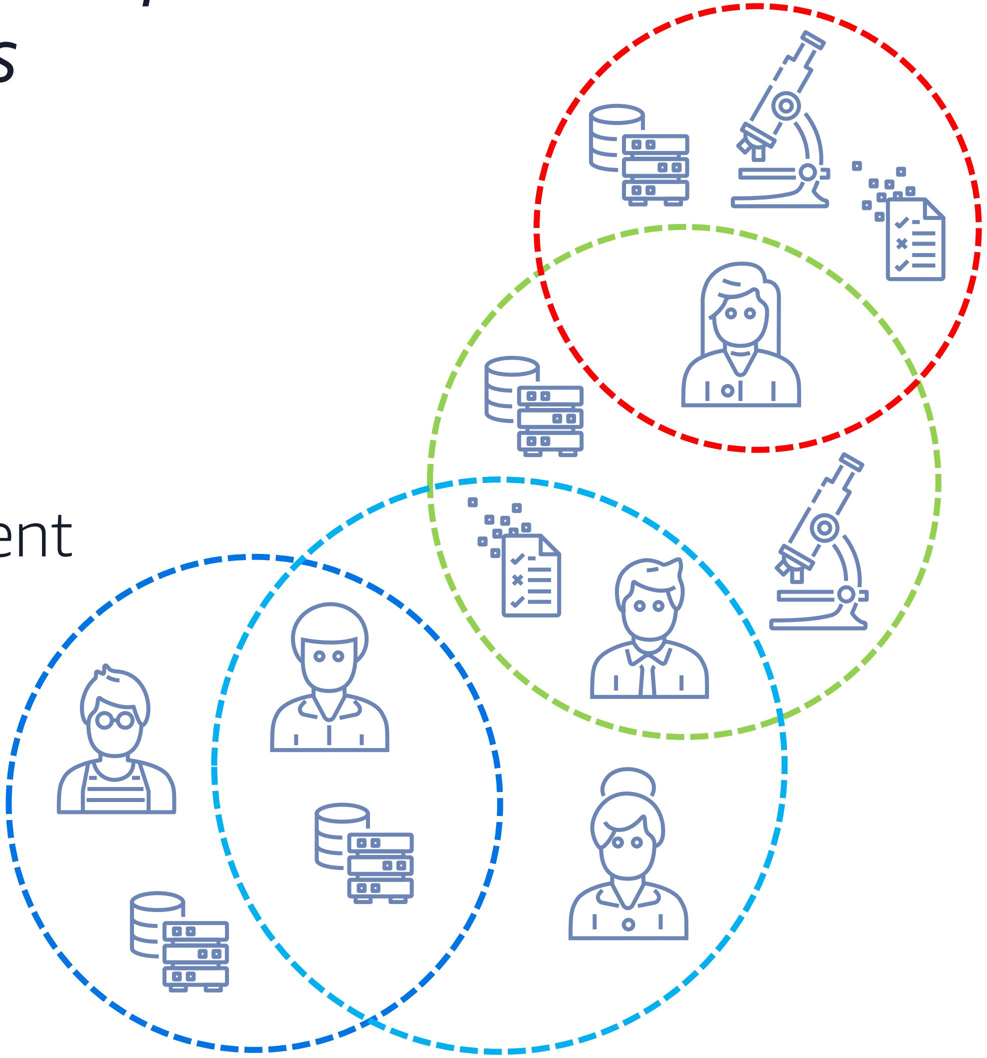
Research is a unique challenge

Research presents a unique challenge

Research is challenging to secure and make compliant because it often operates within and between islands

Factors:

- Researcher-procured and managed equipment
- Researcher population is
  - Collaborative, distributed, mobile, and transient
  - Bring your own device (BYOD)



Research presents a unique challenge

On-prem solutions for secure and compliant research have limits

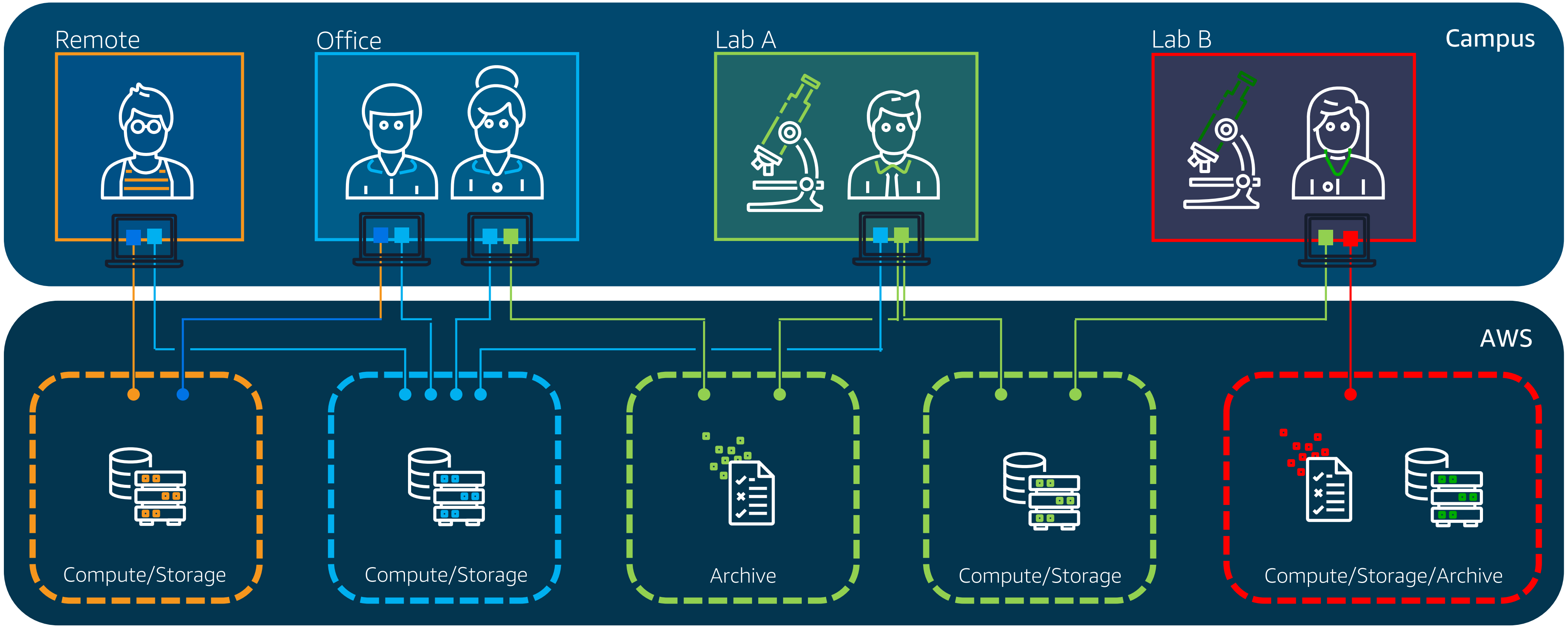
Factors:

- Based on point-in-time technology and are either overly generic or tailored to an initial research project’s needs
- Adapting to evolving research and compliance requirements is complex and expensive
- Researchers often resist using a solution that doesn’t meet their specific needs

Why AWS?

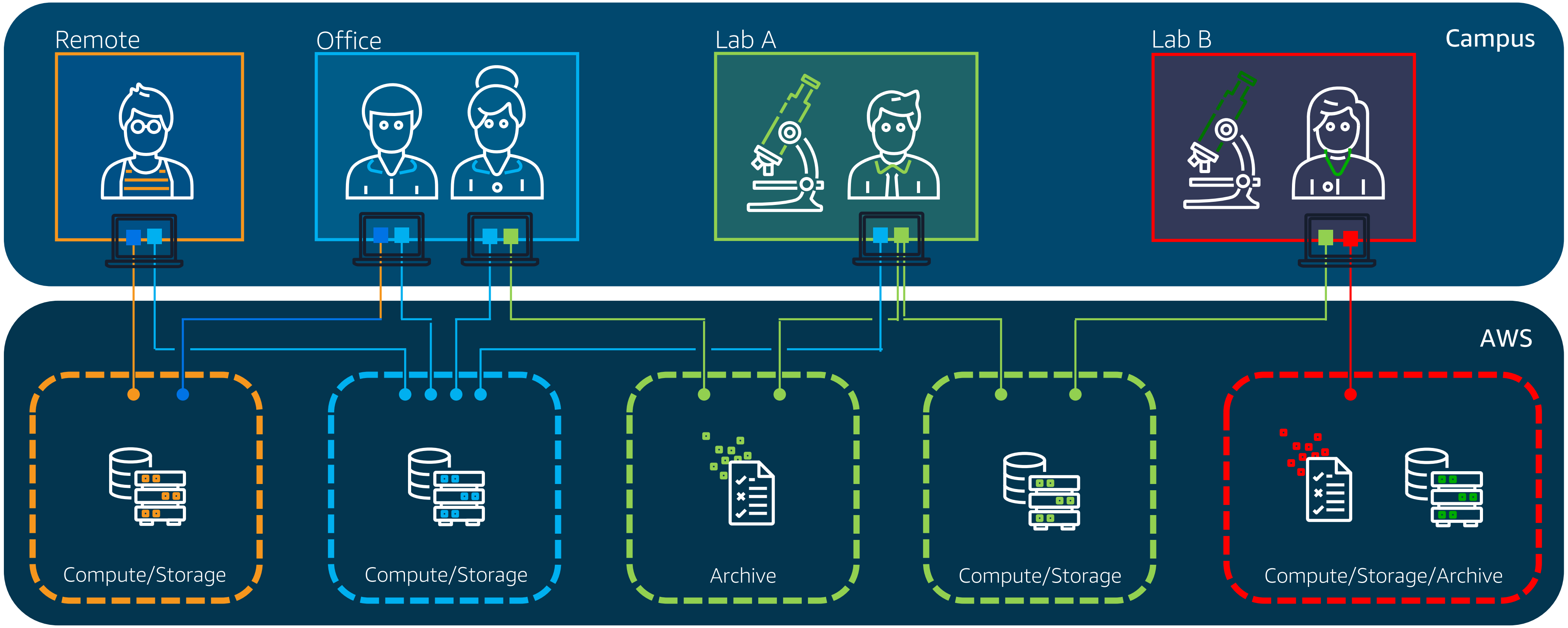
Why AWS?

Enables deployment of repeatable research environments that help institutions achieve their security and compliance goals



Why AWS?

Offers a wide range of flexible, on-demand infrastructure that enables and evolves with researcher demand



Why AWS?

Provides a wide range of services enabling institutions to create solutions to meet their security and compliance requirements

Identity & access management

- IAM
- IAM Identity Center
- Organizations
- Directory Service
- Amazon Cognito
- AWS RAM

Detection

- Security Hub
- GuardDuty
- Amazon Inspector
- CloudWatch
- AWS Config
- CloudTrail
- VPC Flow Logs

Infrastructure protection

- Firewall Manager
- Shield
- AWS WAF
- Amazon VPC
- AWS PrivateLink
- Systems Manager

Data protection

- Macie
- AWS KMS
- CloudHSM
- ACM
- Secrets Manager
- AWS VPN
- Server-Side Encryption

Incident response

- Detective
- CloudEndure DR
- AWS Config Rules
- Lambda

Why AWS?

Elevates your institution’s research capabilities along with its security and compliance posture

Inherit global security and compliance controls

Scale with superior visibility and control

Highest standards for privacy and data security

Automate and reduce risk with deeply integrated services

Largest community of security partners and solutions

How?

You need a landing zone

- A secure, scalable, multi-account AWS environment based on AWS best practices
- A starting point for net new development and experimentation
- A starting point for migrating applications
- An environment that allows for iteration and extension over time

Landing zone elements

Secure and compliant

Meets the organization’s security and auditing requirements

Scalable and resilient

Ready to support highly available and scalable workloads

Adaptable and flexible

Configurable to support evolving mission requirements

The **Landing Zone Accelerator on AWS** is an open-source software solution that accelerates the implementation of a customer’s technical security controls and infrastructure foundation on AWS

Landing Zone Accelerator benefits

Customer resources focus on learning to ‘operate’ in the cloud

Accelerate environment setups in days, not weeks

Leverages AWS expertise

Innovate through open source model

Flexibility to integrate with other management tools

Establish a compliant and improved security posture

Enables customers on day 1, day 10, and day N, supporting them throughout their AWS journey

How AWS delivers

Example: secure and compliant landing zone

UCSD Health Secure Research Cloud (HSRC) for HIPAA compliance

Drivers

- Prevent removal of research data assets and inappropriate third-party data transfers
  (IRB vs. policy and legal compliance)
- Prevent proliferation of unmanaged cloud accounts
  (and gain visibility to monitor activity, data types, workloads, and potential risks)
- Prevent ransomware and research data on mobile devices as a breach source
  (unmanaged, unprotected, or misconfigured devices)

Partnered with AWS, UCSD Health IS security, institutes, and research groups early

- Compliance is more than technical controls: BAA, governance, and policy

How AWS delivers

Example: secure and compliant landing zone

UCSD Health Secure Research Cloud (HSRC) for HIPAA compliance

Solution goals

1. Access controls – technical policies and procedures allowing only authorized persons to access electronic protected health information (ePHI)
2. Audit controls – hardware, software, and/or procedural mechanisms to record and examine access and other activity
3. Integrity controls – policies, procedures, and measures to ensure and confirm ePHI is not improperly altered or destroyed
4. Transmission security – technical security measures guarding against unauthorized access to ePHI transmitted over a network

How AWS delivers

Example: deployment of a research workload

UCSD Health Virtual Research Desktop (VRD) – within UCSD HSRC (saw earlier)

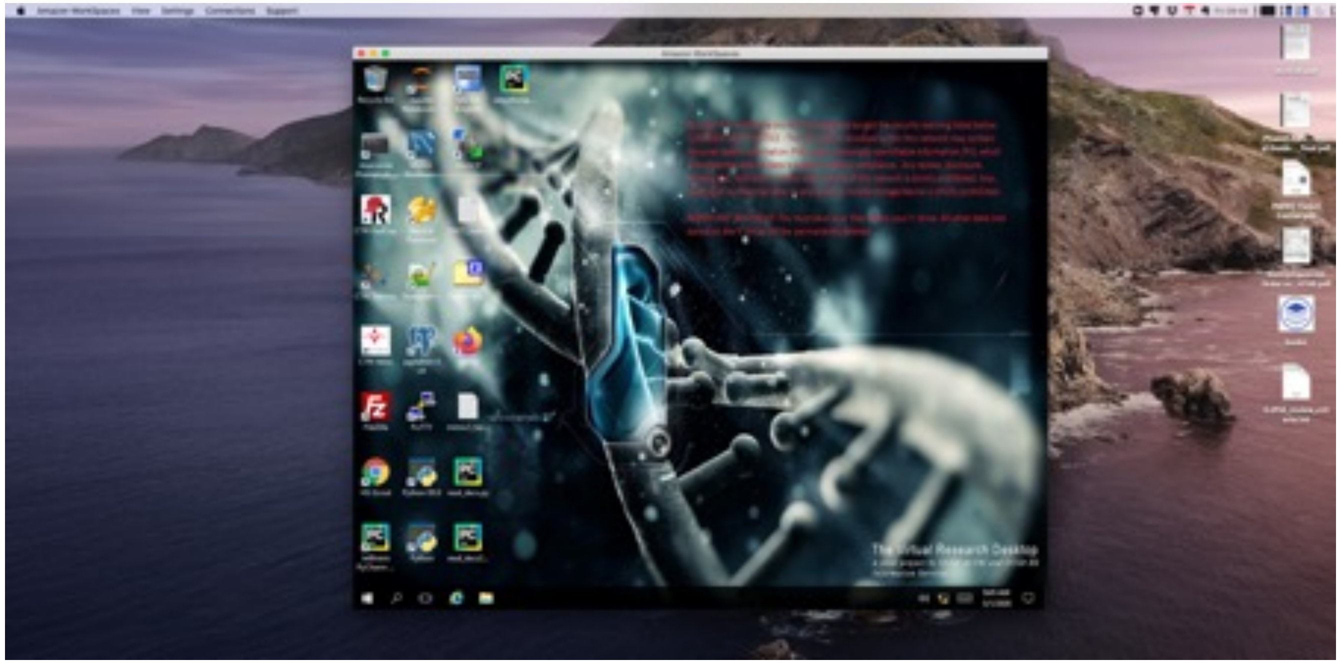
Researcher enablement

- A solution that balances security and privacy while still providing a quality user experience
- Access to ePHI via UCSD Data Extraction Concierge Service (DECS) and VRDs
  (data extracted from clinical data warehouse by DECS and placed into investigator's VRD "secure" folder)
- Hardened Amazon WorkSpaces Windows 10 virtual machines
  - Runs within UCSD HSRC and approved by UCSD Health CISO for ePHI
  - Provisioned with: SPSS, R/RStudio, Python/PyCharm, Java 8, and others
  - With approval, access to internal databases

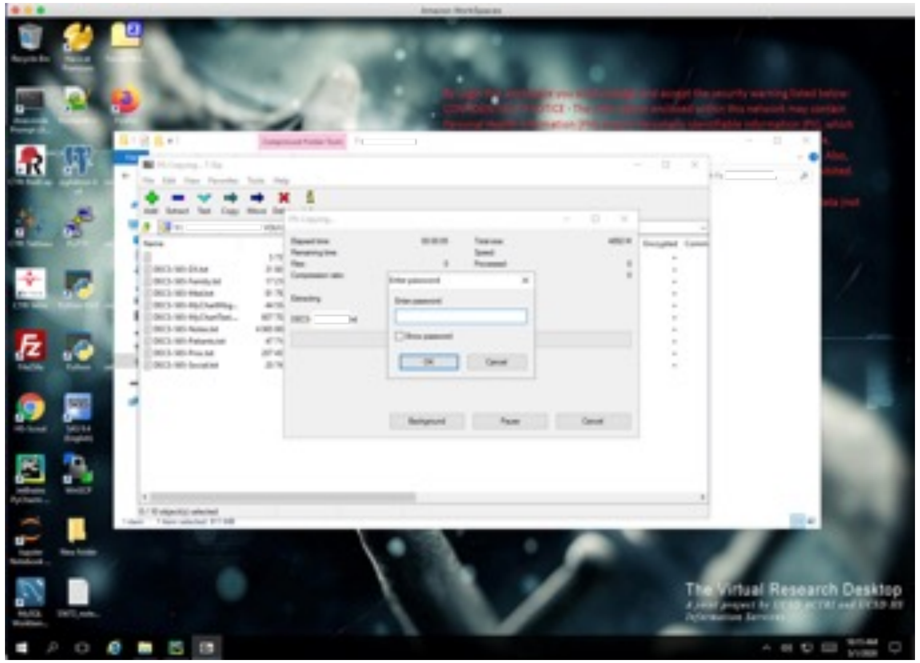
How AWS delivers

Example: deployment of a research workload

UCSD Health Virtual Research Desktop (VRD) – within UCSD HSRC (saw earlier)



View of remote desktop from investigator's computer



VRD desktop with application running

How AWS delivers

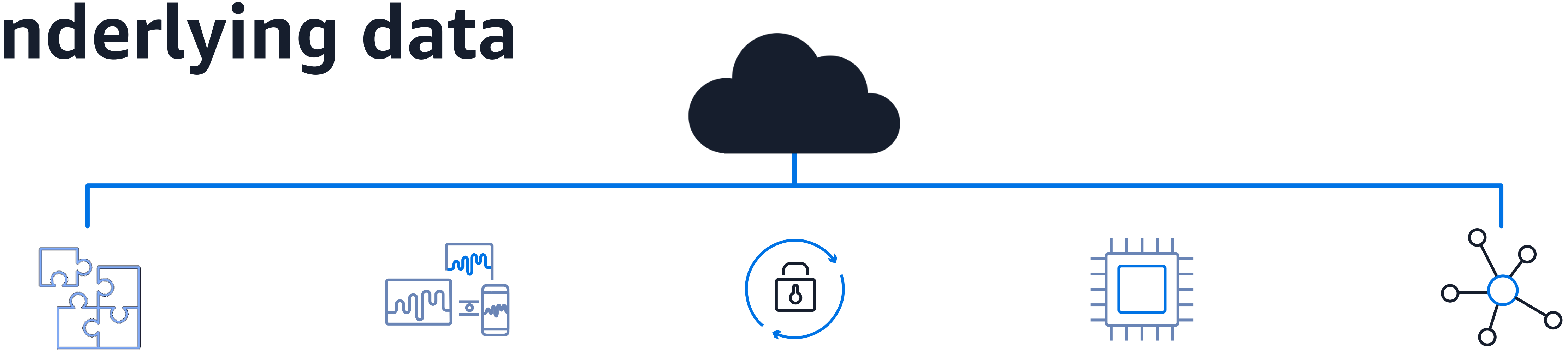
Outcomes

UCSD HSRC and VRD

- A flexible environment that supports security, compliance, and researcher workflow
- Structured, limited, and controlled access to ePHI data for research using defined process
- Automated security controls and configuration monitoring limits configuration drift
- Consistent logging makes audits and re-assessments less challenging
- Ability to flexibly add additional research tools and data environments as needed
- Security, compliance, and administrative support (early involvement key)
- Faculty and researcher project/environment support (early involvement key)

What about data?

AWS Clean Rooms helps organizations collaborate on datasets without sharing underlying data



Multi-party collaborations

Collaborate with up to five parties in a single collaboration; extract insights from multiple companies

No AWS data movement

Use Amazon S3 data with direct permissioning and no AWS data movement

Query controls and enforcement

Configure analysis rules to restrict the type of analysis allowed on your data

Cryptographic computing

Pre-encrypt data so that it is encrypted at all times, including during query execution

Programmatic access

Automate and integrate functionality into existing workflows and products; create white-labeled clean room offering

Amazon DataZone

UNLOCK THE POWER OF ALL DATA FOR ALL USERS WITH TRUSTED AUTONOMY

Data producers

Teams who want to share data

Amazon DataZone

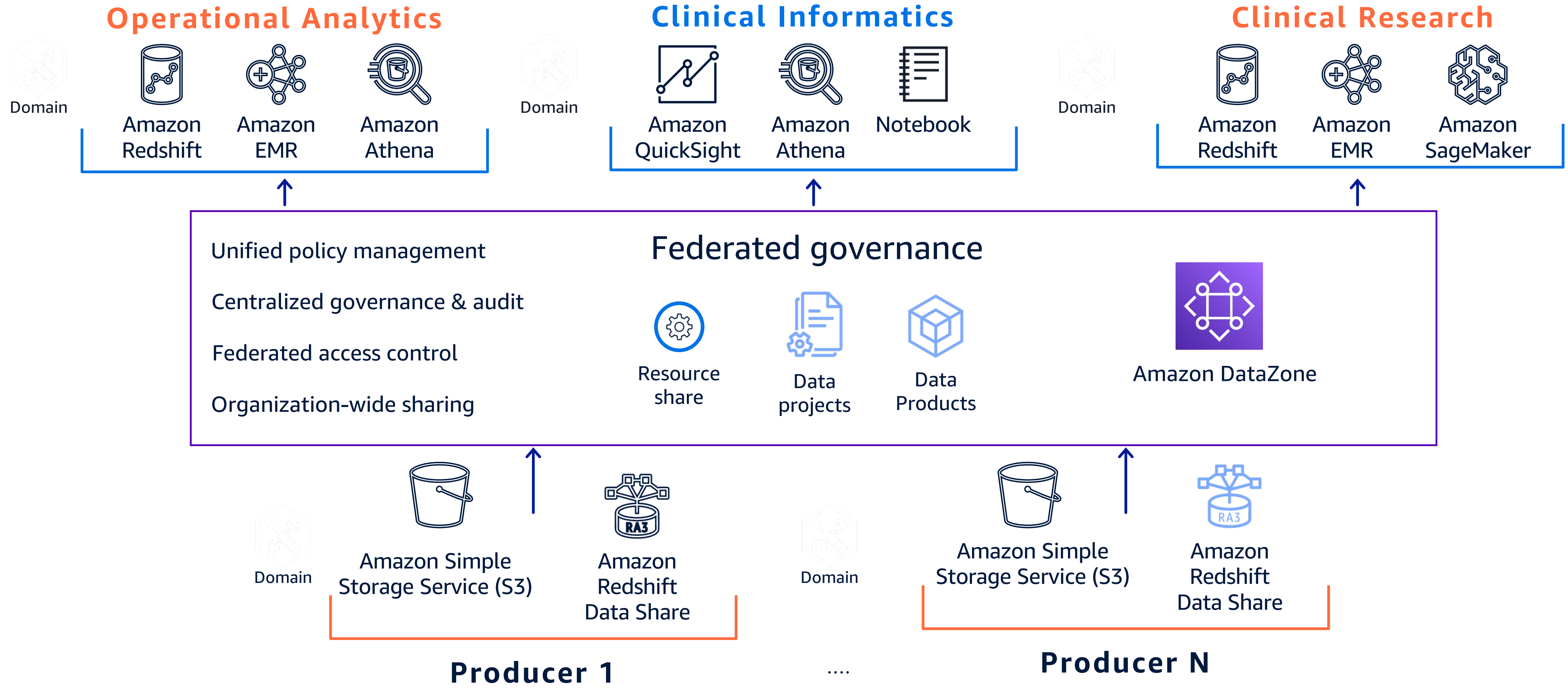
Team who runs the data marketplace

Data consumers

Teams who want to use data

Modern Health Data Mesh Architecture

Decentralized, lightweight federated governance across domain-oriented data systems to drive governed sharing



CHOP Accelerates Pediatric Research using AWS-Powered Data Resource

Children's Hospital of Philadelphia

Challenge

As medical researchers generate more and more clinical data, they're faced with the challenge of storing and organizing that data so that researchers can access, study, and cross-reference it to facilitate medical breakthroughs.

Benefits

CHOP provided the research community with access to genomic and associated clinical data and increased KFDRC's collaborative potential.

CHOP stored 26 billion occurrences of 215 million unique genomic variants from 5,000 participants, while meeting the FHIR industry standard.

Solution

CHOP built the Gabriella Miller Kids First Data Resource Center (KFDRC), a data source that brings genomics, clinical and imaging data as an open resource for researchers to focus on discoveries in pediatric cancer and structural birth defects.

All of our system is currently built on AWS. . . . We went from zero to managing a few petabytes of genomic data within a year using this setup."

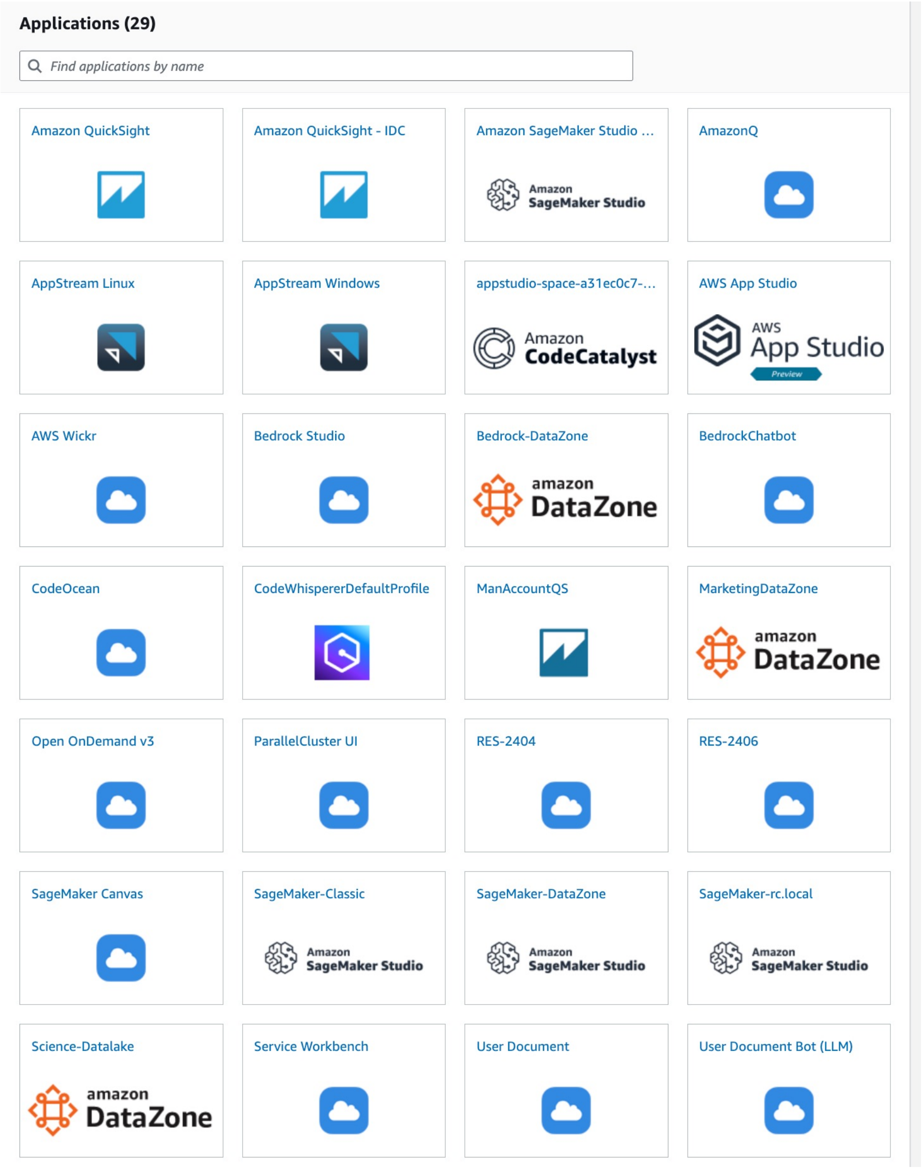
Allison Heath
Director of Data Technology and Innovation, Center for Data-Driven Discovery in Biomedicine

What about access?

Portal for Secure Research Environment

The Secure Research Portal (SRP) is a landing page that:

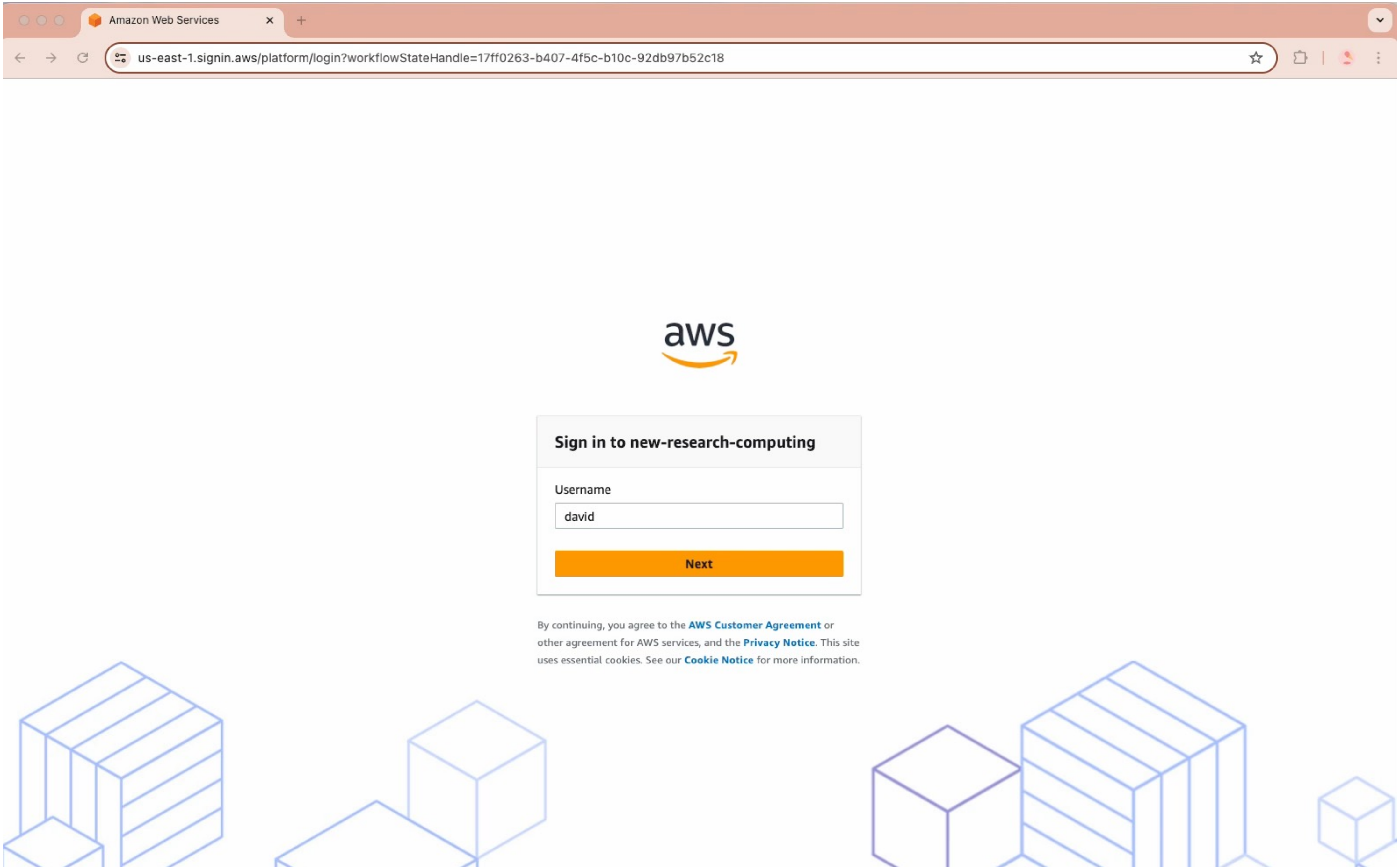
- Simplifies AWS service access for researchers and departments, bypassing the complexity of the AWS console
- Offers a user-friendly interface ensuring federal compliance and enabling all disciplines that require cluster and end-user computing and storage



Applications (29)

Find applications by name

Amazon QuickSight	Amazon QuickSight - IDC	Amazon SageMaker Studio …	AmazonQ
AppStream Linux	AppStream Windows	appstudio-space-a31ec0c7-…	AWS App Studio
AWS Wickr	Bedrock Studio	Bedrock-DataZone	BedrockChatbot
CodeOcean	CodeWhispererDefaultProfile	ManAccountQS	MarketingDataZone
Open OnDemand v3	ParallelCluster UI	RES-2404	RES-2406
SageMaker Canvas	SageMaker-Classic	SageMaker-DataZone	SageMaker-rc.local
Science-Datalake	Service Workbench	User Document	User Document Bot (LLM)



Amazon Web Services
us-east-1.signin.aws/platform/login?workflowStateHandle=17ff0263-b407-4f5c-b10c-92db97b52c18

Sign in to new-research-computing

Username

david

Next

By continuing, you agree to the AWS Customer Agreement or other agreement for AWS services, and the Privacy Notice. This site uses essential cookies. See our Cookie Notice for more information.

Q & A

Thank you!

Brian McCarthy (he/him)
Solutions Architect
AWS
btmccar@amazon.com

Data and Analytics

Secure Research Environment and Portal