Experiences applying security standards to cloud hosted services

Brigitte Raumann
Product Manager, Globus
University of Chicago

NSF Cybersecurity Summit
October 15, 2019
Globus lowers barriers to collaborative science and discovery by delivering easy, reliable, and secure research data movement, sharing, and synchronization.
“I need to easily, securely, & reliably move and share my data between systems.”
Globus SaaS / PaaS: Research data lifecycle
Globus SaaS / PaaS: Research data lifecycle

Researcher initiates transfer request; or requested automatically by script, science gateway.
Researcher initiates transfer request; or requested automatically by script, science gateway

Globus transfers files reliably, securely

Instruments

Compute Facility

Transfer

Globus SaaS / PaaS: Research data lifecycle
Researcher initiates transfer request; or requested automatically by script, science gateway.

1. Researcher initiates transfer request; or requested automatically by script, science gateway.

2. Globus transfers files reliably, securely.

3. Researcher selects files to share, selects user or group, and sets access permissions.

4. Globus controls access to shared files on existing storage; no need to move files to cloud storage!
Researcher initiates transfer request; or requested automatically by script, science gateway.

Instrument

Globus transfers files reliably, securely

2

Compute Facility

Globus transfers files reliably, securely

3

Share

Researcher selects files to share, selects user or group, and sets access permissions

Collaborator logs in to Globus and accesses shared files; no local account required; download via Globus

5

Personal Computer

Globus controls access to shared files on existing storage; no need to move files to cloud storage!
Globus SaaS / PaaS: Research data lifecycle

1. Researcher initiates transfer request; or requested automatically by script, science gateway.

2. Globus transfers files reliably, securely.

3. Researcher selects files to share, selects user or group, and sets access permissions.

4. Globus controls access to shared files on existing storage; no need to move files to cloud storage!

5. Collaborator logs in to Globus and accesses shared files; no local account required; download via Globus.

- Use a Web browser or platform services
- Access any storage
- Use an existing identity
Globus SaaS / PaaS: Research data lifecycle

1. Researcher initiates transfer request; or requested automatically by script, science gateway

2. Globus transfers files reliably, securely

3. Researcher selects files to share, selects user or group, and sets access permissions

4. Globus controls access to shared files on existing storage; no need to move files to cloud storage!

5. Collaborator logs in to Globus and accesses shared files; no local account required; download via Globus

6. The Globus Command Line Interface, API sets, and Python SDK provide a platform…

7. ... for building science gateways, portals and publication services.

8. Automating research workflows and ensuring those that need access to the data have it.

• Use a Web browser or platform services
• Access any storage
• Use an existing identity

Instrument

Globus transfers files reliably, securely

Compute Facility

Transfer

Share

Personal Computer

Build

Instrument

Compute Facility

Transfer

Share

Personal Computer

Build
Study drug efficacy in rare disease patient population.

21 sites, each with several patients enrolled

Magnetic Resonance Imaging (MRI) and fluorodeoxyglucose (FDG)-positron emission tomography (FDG-PET)

Mixture of research and clinical sites

KARL G. HELMER
MASSACHUSETTS GENERAL HOSPITAL, HARVARD MEDICAL SCHOOL
Globus Security and Compliance Effort

Goals

1. Operate Globus cloud hosted services in a HIPAA compliant manner.
   → In order for UChicago to be willing to accept the liability of receiving PHI from other institutions, Globus must meet UChicago data security and privacy policies.

2. Provide a product that allows institutions to meet their own security and compliance requirements when managing sensitive data.
Close engagement of internal stakeholders was critical.

- **Office of Legal Counsel**: Bi-weekly meetings
  - Interpretation of regulations
  - Analysis of how HIPAA regulations apply
  - Analysis of liability and risk

- **CISO Office**: Weekly working meetings
  - Interpretation of NIST security controls
  - Scope definition
  - Gap analysis
  - Control implementation review
  - Procedure review
  - Security Plan

- Regular engagement of both offices continues.
Clear scope definition on multiple dimensions was key to gap analysis and control implementation.

Data in scope

Definition of Protected Environment

People, systems, hardware, and controls in scope
Securing Two Types of Access: Network and AWS API

**Network Access**
- Service 1
- Service 2
- Service 3
- Service 4
- Operations

**AWS IAM Access**
- Service 1
- Service 2
- Service 3
- Service 4
- Bastion
- IAM Users

Arrows indicate access via VPC peering
Arrows indicate access via AWS Roles
Access via AWS API

1. Authenticate with access keys
2. Pass MFA info to get temporary security credentials
3. Call AWS APIs using temporary security credentials
Traditional Network Zones Example
Security Groups (Virtual Firewalls)

Generalized Network Architecture

- Internet
- VPN Connection (via VPC Peering)
- VPC Peering
- Public Interfaces
- Private Interfaces
- Load Balancers
- EC2 Instances
- Isolated Subnet
- Databases
- AWS
- VPCs
Security Groups (Virtual Firewalls)

Generalized Network Architecture
Identifying the Protected Environment

Generalized Network Architecture
Quest for Intrusion detection

• **Solution requirements**
  – Host based
  – Linux support
  – Support for elastic resources
  – Managed service

• **Not provided by AWS**

• **Trade offs were PHI disclosure and limit on kernel upgrades.**
**Increased Laptop Security Posture**

- **Solution requirements**
  - Multiple platform support
  - Support geographically distributed team
  - Allow admin access to users
  - Light weight for small team
  - Privacy

- **One option is managed Chromebooks to connect to a secure EC2 instance, which serves as virtual endpoint.**
Audit log collection and management

• Added application audit logs
• Enabled AWS service logs
• Centralized log aggregation to facilitate access
• Instituted log retention and monitoring procedures
• Scoped logs in the Protected Environment
Compliance Tradeoffs of Using IaaS

• Some fully inherited controls (primarily Physical Environment).

• AWS services available for relatively low cost (effort and $).

• Requires disclosure of data to 3rd party.
Shared security responsibilities of Hybrid SaaS

Customer owned and administered storage system with Globus Connect running on it

No data relay or staging via Globus, files move directly between storage locations

User identity mapped to local account

Globus service orchestrates file movement via communication with Globus Connect

Powered by Amazon Web Services
Features to enable customers to secure their own environment

- **Additional authentication assurance**
  - Reauthentication after specified time period
  - Authenticates with the specific identity within session

- **Isolation of applications**
  - Authentication context is per application, per session

- **Enforced encryption of data in transit**

- **Local audit logging**
Estimation of Effort

• 1.5 yr effort
  – 1st half = market analysis, gap analysis (internal and 3rd party)
  – 2nd half = implementation of controls, product development
    o Sustained effort from four team members, significant effort across all staff members

• On-going
  – Effort required from all functions in the organization
  – Some operational costs
Globus Announces Support for Protected Data

SEPTEMBER 11, 2018 | FOR IMMEDIATE RELEASE

Chicago, IL – Sept. 11, 2018 – Globus, the leading research data management service, today announced support for management of protected data, including data regulated by the Health Insurance Portability and Accountability Act (HIPAA) and Controlled Unclassified Information (CUI). With higher assurance levels for protected data, researchers can now easily manage Protected Health Information (PHI), for example, and share it securely with collaborators.
Acknowledgements

University of Chicago

• Tom Barton and the Information Security Office
• Stefan Quick and the Office of Legal Counsel
• Rachana Ananthakrishnan and Stu Martin and the Globus team

This work was supported in part by NIH U24CA209996.
Thank you to our supporters...
...and to our subscribers.