SHERLOCK CLOUD
A Secure Cloud Solution
San Diego Supercomputer Center @ UC San Diego
“In recognition of the growing number of cyber threats against research universities and health care systems, UC Office of the President has initiated a series of systemwide actions to strengthen the UC system’s ability to prevent, detect, and respond to such attacks.”
Businesses, research and health care organizations need to be knowledgeable and responsible about cybersecurity and meet the regulatory requirements or suffer dire consequences. In many cases, institutions lack resources, budget and expertise to face this challenge.
Sherlock Cloud’s Managed Infrastructure as a Service (IaaS) Cloud was developed to provide secure end-to-end Cyberinfrastructure for data and computing for academic, state and government partners.
Sherlock Cloud is HIPAA, FISMA compliant and developed in accordance with NIST controls governing system access, information security, and management processes.

- Policies, Processes & Procedures
- Annual Audits & Assessments
- Administrative Safeguards
- Lifecycle Documentation
- Regulatory Know-How
- Technical & Security Safeguards
- Physical security
MORE THAN YOUR TYPICAL IAAS PLATFORM

Commodity HW & SW + Compliance (HIPAA, FISMA, CUI, CSF) + Professional Services + Data Center/Colocation + Advanced Technology Solutions = End-to-End Cyberinfrastructure for Safeguarding Sensitive Data
TECHNOLOGY PLATFORM

Best of Class Enterprise & Open Source Products

**Storage**: NetApp, Dell (File, Block, Database)

**Compute**: Commodity Hardware (Dell, IBM, etc.)

**Virtualization**: VMWare

**OS Support**: Windows and Linux

**Shared Services**: **Backups** (CommVault), **Authentication** (RSA, Active Directory), **Configuration Mgmt.** (Windows GP, Puppet), **Vulnerability Management** (Nessus), **Ticketing**, **Managed File Transfer** (GlobalScape), **Secure Access** (HW and SW VPNs), **Anti Virus** (Sophos)

**Security**: **Customized Firewalls** (Juniper, Cisco, Vyatta, Sophos), **IDS/IPS** (Bro, Snort), Auditing and **Log Management** (Splunk)
Sherlock Cloud platform has already helped support a number of critical applications including Medical Fraud, Cancer Research, Enterprise Risk Management, Healthcare Research and more.
WHY SHOULD IT BE YOUR STORY?

Because collaborating with Sherlock Cloud offers you a value-added solution. How?

We’ve already done the work...so you don’t have to - with sizable investments in people and technology.

Plus, you can maximize the benefits of your affiliation with UCSD, including:

- Technical and domain expertise within UCSD.
- Access to top-notch researchers and scientists - experts in high performance computing, big data, and data science.

You’ll be partnering with an outstanding team of technologists & researchers that can help you leverage and pursue grants and contracts.
HOW CAN WE HELP YOU BETTER SAFEGUARD SENSITIVE DATA?

Simply, Through Our Managed Sherlock Cloud Services

- GREAT ECONOMICS OF SCALE
- BREADTH OF DOMAIN KNOWLEDGE
- EXPERT TECHNICAL STAFF
- INDUSTRY KNOWLEDGE
- FORMAL IT AND SECURITY PROCESSES
- COMMON POLICIES AND TEMPLATES
- MSP RESPONSIBLE FOR COMPLIANCE
There are inherent risks of hosting sensitive data without Sherlock on your side.

Sensitive Data (PHI/PII) is a proven hacker target:

According to BitSight Technologies, medical records on the black market sell for more than credit card numbers.

Records are used by criminals to obtain drugs and other treatments.

Many organizations dealing with ‘Ransomware’

Impact to individuals whose records are affected by breach.

Penalties if a breach takes place.

Impact to reputation/notification to media outlets.

And even if not audited, if a breach takes place, scrutiny will follow after the fact.
The Managed IaaS Solution Offered by Sherlock Cloud

<table>
<thead>
<tr>
<th>The Good News?</th>
<th>Goes beyond IaaS as compliance involves the entire architecture and management processes</th>
<th>Maintains security and oversight aspects of a traditional managed services model</th>
<th>FISMA, HIPAA, CUI, CSF compliant</th>
<th>Managed using NIST 800-53 Physical, Technical and Administrative Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scalable, Multi-tenant Cloud</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Meets federal “Cloud First” requirements and flexibility goals</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Economies of scale and a shared knowledge base</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
THE BETTER NEWS?
We Manage Your Entire Stack

Policies, Assessments & Audits

Yearly Security Training, Employee Background Checks

Access Control and Authentication

Vulnerability Scanning and Monitoring

OS Management, Log Management, Configuration Management

Data at Rest Encryption, Data in Transit Encryption

Physical Security, Segmented Architecture, Backup Archiving

The better news? We manage your entire stack.
Choosing us as your partner has many benefits...

- Minimizes financial burden while maximizing security posture
- Eliminates risk of hosting data on systems that are ill-equipped to protect sensitive data
- Incentivizes pursuing research grants that require heightened security
- Provides competitive advantage in proposals
- Understands research needs differ from those of the users of commercial cloud platforms
- Benefit from economics of scale based on shared infrastructure, processes, and documentation
- Broadening societal impact while protecting intellectual assets

AND THERE’S MORE
PUBLIC CLOUD APPROACH TO COMPLIANCE

Customer Data

Platform, Applications, Identity, and Access Management

Customer

Operating Systems, Network, and Firewall Configuration

Responsible for security “in” the Cloud

Client Authentication & Authorization

Server-Side Encryption File System and/or Data)

Network Traffic Protection
(Encryption /Integrity/Identity)

Compute

Storage

Database

Networking

AWS

Responsible for security “of” the Cloud

AWS Global Infrastructure

Regions

Availability Zones

Edge Locations

Source: https://aws.amazon.com/compliance/shared-responsibility-model/
### SHERLOCK’S APPROACH TO COMPLIANCE

**Custom Solutions**
- Platform, Applications, Identity, and Access Management
- Operating Systems, Network, and Firewall Configuration
  - Client Authentication & Authorization
  - Server-Side Encryption (File System and/or Data)
  - Network Traffic Protection (Encryption, Integrity, Identity)

**SHERLOCK Cloud Infrastructure**
- Compute
- Storage
- Database
- Networking

**Regions**
- Availability Zones
- Edge Locations

**Customer Data**

- Responsible for security “in” and “of” the Cloud
# Our Current Collaborations

## UC System, Federal and State

<table>
<thead>
<tr>
<th>UCOP Enterprise Risk Management (ERM)</th>
<th>UC Med Centers</th>
<th>Calit2 Center for Wireless and Population Health Systems (CWPHS)</th>
<th>Centers for Medicare and Medicaid Services</th>
<th>NCI and City of Hope</th>
<th>Clemson University</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERM platform to help manage risk, reduce loss, create financial stability and protect UC resources</td>
<td>Disaster Recovery and Business Continuity for Tier 2/3 clinical applications</td>
<td>GeoDB: Develop and validate novel GIS-based total daily environmental exposure measures</td>
<td>Investigating Medicaid fraud, waste and abuse. FISMA-certified platform for data and analytics</td>
<td>Data Management platform for California Teachers Study</td>
<td>CORPA: Disaster Recovery for Clemson University Campus IT Operations</td>
</tr>
<tr>
<td>HIPAA-Compliant Hadoop platform for managing UC Healthcare Liability Program</td>
<td>UC Clinical Data Warehouse</td>
<td>Be There: Clinical study focused on helping reduce heart attacks in San Diego</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

**SDSC**

**UNIVERSITY OF CALIFORNIA**

**SAN DIEGO SUPERCOMPUTER CENTER**
ISN’T IT TIME THAT YOU JOINED THE SHERLOCK CLOUD TEAM?

Built and operated at SDSC to support the UC System, Academia, and State and Federal Government Agencies

Sherlock Cloud is an SDSC “Center of Excellence”

Unique UC-wide Resource, Recognized by the Sautter Award Program

Expertise in operations and maintenance of a managed, secure, compliant infrastructure and services platform
TEAM SHERLOCK

Sandeep Chandra  
Director

Winston Armstrong  
Chief Information Security Officer

Leslie Morsek  
Program Manager
To learn more about how we can put the Sherlock Cloud to work for you, visit our website at:

**sherlock.sdsc.edu**

Or

Email us at:

**sherlock@sdsc.edu**