GANG SCOPE
Gang Ingelligence Database

REQUIREMENTS

AWS GOVCLOUD

AVAILABLE APPROACHES

Approach #1 - Tunnel - CloudFlare approach (simple):

- View Hosting Diagram
- Recommended for 10 or less licenses. Email-tied, we must provision your emails for portal access.
- GangScope™ Cloud by default uses CloudFlare Access secure tunneling.
- This makes use of a gateway portal which provisions temporary access tokens to registered (whitelisted) email addresses. This grants your web browser access to the application directly.
- Which is why we do not recommend more than 5 user licenses for this approach, as it can become exponentially more costly the higher the user count.
  IPSec - VPN approach (hardware)

Approach #2 - View Hosting Diagram

- This requires you to have a top-level network device capable of establishing IPSec vpn connections.
- This cannot work behind a NAT device unless port-forwarded & routed properly (advanced networking). It generally must be at the top level of your network.
- Minimum capabilities required for hardware(yours) to software (ours):
  - Phase 1 Proposal: sha1-aes256 (non aggressive)
  - Phase 2 Proposal: esp-sha1-aes256 (tunnel mode)
  - Diffie-Hellman group: 5

AWS GOVCLOUD COMPLIANCE INFORMATION

Cloud Services security controls

- AWS ISO/IEC Certification
  - ISO 27001 - 2013 SOA
  - CSA STAR 2
- Approach #1 - certification is listed here: Cloudflare Link
  - Note: this is a layer in addition to the application itself on AWS (see information below in email), and is respective only to data transmission between browser (you) and tunneled application (cloudflare Access/Argo).
  - We can request the reports from CloudFlare if needed, but it may take time as it requires a NDA signature by you and us.

- Approach #2 (VPN) uses FIPS 140-2 (See Here)

Latest SOC report - AWS

- SOC-1-Current.pdf
- SOC-2-Current.pdf
- SOC-3-Current.pdf
- SOC_Continued_Operations_Letter.pdf

Datacenter Locations

- We utilize AWS GovCloud (overview link), which is:
    - US Data Centers only
    - US citizen only physical access
    - GangScope Staff are background checked (fingerprint + fbi scan)

HIPAA compliance, and HITRUST certification

- HITRUST_CSF_Certification_Letter.pdf
  The AWS utilized services are HITRUST certified for HIPAA compliance

Security Incident handling and Response Time

- We maintain active monitoring utilizing the CloudWatch aws service
- We also maintain the product at regular intervals including latest bug fixes and improvements (security or otherwise).
- In accordance with CJIS:
    - We perform weekly security audits, including heuristic analysis of traffic for anomalous activityIn the event of a breach or possibility of breach, we would notify you immediately upon detection & provide you with transparency as to the details of the event accompanying our course or plan of action.

Other Information Regarding compliance:

We do not restrict your ability to add differing types of information (28 CFR, CJI, ITAR, or HIPAA regulated).

We provide our best effort on maintaining security & compliance through:

- System usage patterns (GI initiator for all data & Approval/Review processes, clear labeling and warnings for data viewing & transmission)
- Technology available to us through AWS GovCloud
    - AWS CJIS technology stack example: Click here
    - Our actual structure: (see graphs for approach #1 or #2 at top of email)
    - Compliance Matrices for AWS resources: Click here and here

CJIS compliance:

We enable you to meet the CJIS compliance standards (per Building CJIS Compliant Solutions in AWS) by using encryption for at-rest and in transit.

In addition to security reviews and workflows designed for compliance