shibumi

2020 Update

Security, Risk and Compliance

Our customers trust Shibumi with their most sensitive and strategic data, and justifying their trust is a mission-critical priority. Shibumi's platform and processes have been designed from the ground up to meet the requirements of global enterprises. We invest in the highest quality security technology, and regularly update our policies and processes based on evolving industry best practices.

Information Security

Shibumi encrypts and protects sensitive information across the full strategy execution process.

- **Mobile Access** (through browser): TLS encryption for all data exchanged between browser and server, with no data stored on user devices
- **Data at Rest**: AES-256 block cipher encryption
- **Data in Transit**: TLS 1.2 using global step-up certificates from Verisign
- **Network Security**: Cloud-based intrusion detection system monitors for real-time threats, with all traffic passing through a web application firewall

Access Management and Authentication

Shibumi's platform provides enterprises full control of access to all hosted information, as well as transparency to user activities

- **Single Sign-On**: Supported through standard protocols, including SAML 2.0
- **Account Authentication**: User invite and account creation required for any platform access
- **Strong Password Policies**: Required strength factors (minimum characters, required numbers and special characters, common passwords rejected), salted and hashed password storage, and password resets
- **Granular Access Control**: Role-based access, visibility and user action rights, with object-level permissions
- **User Communications**: Ability to create private and limited access collaboration channels
- **Audit Log**: Detailed tracking and audit log of all activities related to hosted objects, with flexible filtering to simplify administrator access to audit data

- SOC 2, Type 2 certification
- AES-256 encryption for all data at rest
- TLS 1.2 for data in transit
- Strong password policies
- Granular access control and audit
- Software development and delivery best practices
- Americas, Europe and Asia/Pac infrastructure instances

shibumi

Security, Risk and Compliance

Software Development Practices

Security is fully integrated into Shibumi's software development process. All developers receive appropriate security training (e.g. OWASP top 10) and all code changes are reviewed.

- Shibumi clients (web, desktop, mobile, and API) are designed with security that meets OWASP standards (at minimum)
- Software Development Lifecycle approach
  - Separation between Production, Development and Test
  - No customer or confidential data on development and test systems
  - Segregation of duties among Operations, Developer, Release Manager and Tester
  - Secured release assets
  - Required reviews of any new code by individuals who a) were not an author of the original code; and b) are educated in the execution of code review techniques and secure coding practices
  - Code changes logged in a central location
  - Restricted access to code repository
- Other SDLC security practices include:
  - Requirements review (security, privacy, process, functional)
  - Design review (threat modeling and analysis, security design review),
  - Development controls (static analysis, manual peer code review)
  - Testing (dynamic analysis, automated testing)
  - Deployment controls (security, confidentiality, integrity, and availability code reviews)

Infrastructure Security

Shibumi leverages Amazon's AWS infrastructure (see architecture diagram), including AWS's best practice security methodology and processes. Shibumi can make available all standard AWS certifications and accreditations for Infrastructure, Physical Security and Secured Services.

Company Policies and Procedures

Shibumi Security, Risk and Compliance processes were developed based on industry best practices and are continuously updated.

- **Security Policies and Training**: Required employee training certification, with formal (audited) policies that include:
  - Employee Background Checks
  - Corporate Facility Access
  - Acceptable Use
  - Corporate Passwords and Production Passwords
  - Access Privileges
  - Incident Response Procedures
  - Security Training
  - Patch Management
  - System Configuration
  - Change Management
- **Platform Network Security**: Continuous security activities, including:
  - Network and host intrusion detection
  - System, network and application log reporting, analysis, archiving and retention
  - Network device baseline standards
  - Continuous internal monitoring
  - Regular vulnerability scanning
- **Incident Response Team** handling any significant security or service event by defined policies
- **Regular Third-Party Security Testing** focused on potential vulnerabilities

shibumi

Security, Risk and Compliance

Standards and Certifications

Shibumi is committed to maintaining compliance with key global information security and regulatory standards, including:

- **Service Organization Control (SOC) 2, Type 2** certification
- **CSA Cloud Controls Matrix** standards compliance
- **EU and Swiss Privacy Shield** certification
- **EU Model Clauses** supported

Shibumi and third-party certification and verification reports are available for limited distribution and shared under confidentiality agreement.

Data Retention

Shibumi retains customer information for as long as the account is active, or as long as needed to provide a customer or sponsoring organization with specific requested services. Customers wishing to cancel an account or notify Shibumi to cease use of customer information to deliver services should contact Shibumi at support@shibumi.com.

Shibumi will retain and use customer information as necessary to comply with legal obligations, resolve disputes, and enforce agreements. Anonymized usage data may be collected to help improve the performance of Shibumi's platform and service offerings (see Shibumi Data Privacy Policy).

Data Breach

If, despite all other protections in place, company or personal employee data is accessed without authorization, we will notify you. Notification of any personal data breach will be made in accordance with applicable law.

Backup, Replication and Data Recovery

Shibumi provides multiple layers of protection for customer data, fully leveraging the capabilities of the AWS Relational Database Service.

- **Automated Backup**: Nightly backups of databases and audit logs, with 30-day retention
- **Data Replication**: Customer data updating and replication across multiple infrastructure instances (each in a distinct AWS zone)
- **Data Locations**: Platform instances hosted in AWS datacenters in the European Union, United States and Australia

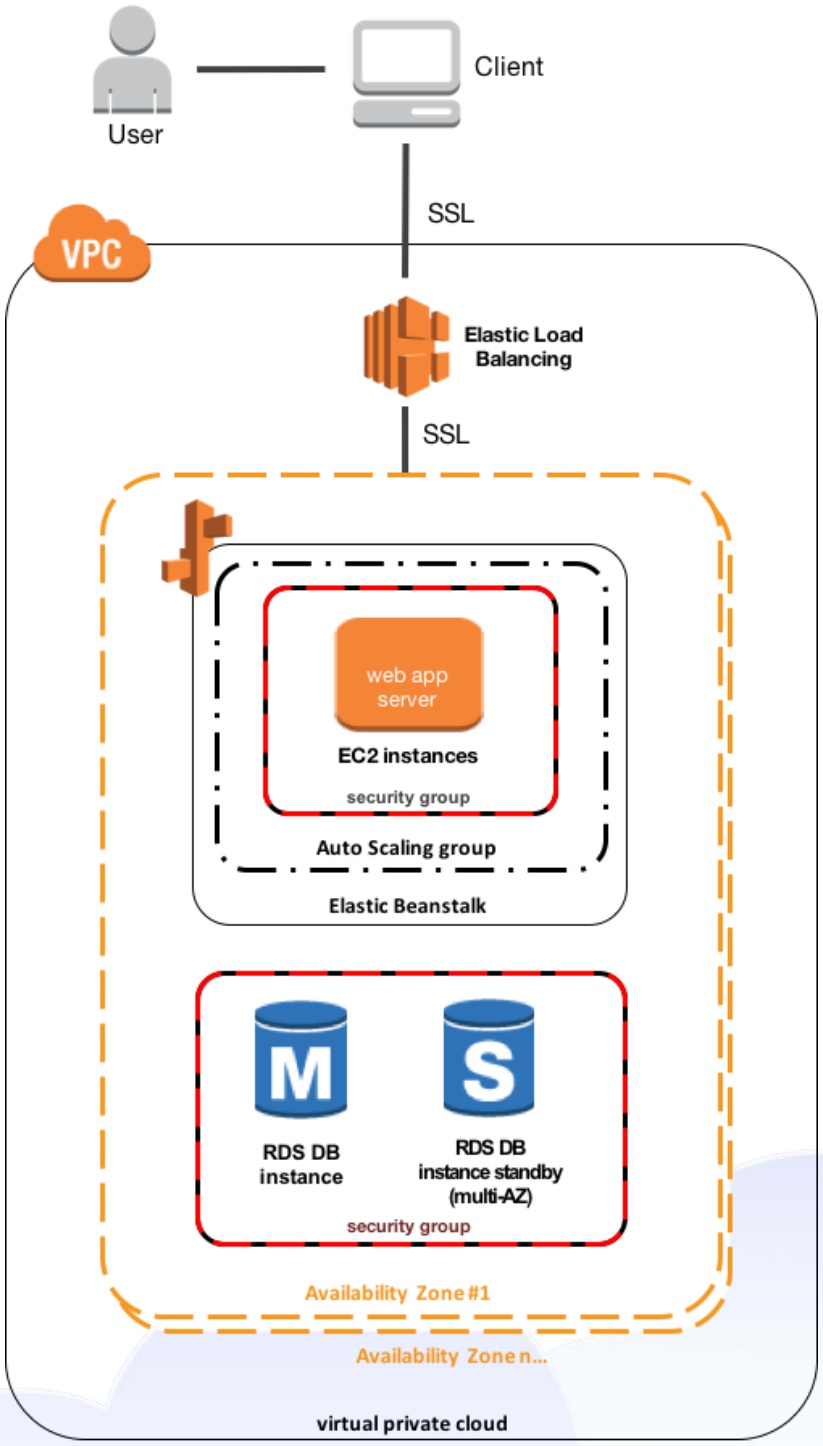
Data Access

Shibumi Service or Engineering teams may occasionally need access to targeted customer data to provide support and address technical issues. Shibumi will only access customer information in one of two ways:

- Invitation through the platform to a specific Shibumi employee for defined and limited access by an entitled customer user (e.g. for customer support). Any access through the platform is tracked and customer-auditable.
- Temporary direct access to data with the written approval of the customer administrator of Shibumi's deployment. Any such direct access request is reviewed and tracked by Shibumi's security team, and requires explicit approval of Shibumi's General Counsel

Shibumi professional services and customer support are located in Australia, European Union, United Kingdom, and United States

Shibumi Platform Architecture Overview



To Learn More

CSA Security Standards
https://cloudsecurityalliance.org/starregistrant/shibumi/

AWS Overview of Security Processes
https://aws.amazon.com/whitepapers/overview-of-security-processes/

AWS Risk and Compliance
https://aws.amazon.com/whitepapers/overview-of-risk-and-compliance/

Shibumi Data Privacy Policy
http://shibumi.com/privacy-policy/

For further information on Shibumi technology, architecture and processes, please contact your client partner or Shibumi's Security, Risk and Compliance team directly at security@shibumi.com