Enclave Security Division of Responsibilities

Aptible Enclave® is an ISO 27001 certified, AWS-based container orchestration platform for deploying highly available, secure apps and databases into isolated cloud environments. Software teams use Enclave® to automate DevOps and security engineering best practices and requirements for HIPAA, ISO 27001, SOC 2, and other security frameworks.

Categories

- Security
- Audit-Ready
- Flexible + Scalable
- DevOps: Reliability
- DevOps: Convenience

Customer

Application-level Controls

You are responsible for implementing security controls in your app business logic, such as authentication, app-level access controls, and audit logging.

Web App Vulnerability Scanning

You are responsible for detecting and mitigating vulnerabilities in your Enclave apps.

Web App Dependency Management

You are responsible for managing your apps' dependencies (e.g. package.json, Gemfiles, etc.) and patching vulnerabilities. You may use Enclave App Security Scans to detect potential issues with system packages installed in your Docker images.

Protection of Credentials, Tokens, Secrets

You are responsible for managing your passwords, API keys, and other secrets. You may use Enclave environment variables to store sensitive information and configuration.

aptible

ISO 27001 Compliance

Use Aptible's ISO 27001 certification to show your customers that your cloud computing stack meets the international gold standard for security.

HIPAA Compliance

Run healthcare workloads that process, store, and transmit HIPAA protected health information with Aptible. BAAs are available for Enclave dedicated stacks and Gridiron.

2-Factor Authentication

Use both token-based 2FA and FIDO U2F security keys to protect your Aptible accounts.

Role-based Access Controls

Securely control access to your Aptible services.

Enhanced Support

All Aptible accounts include Business-level support. Support upgrade options include private Slack channels with the Aptible team and 15-minute critical response times.

Aptible API Audit Logs

Weekly Activity Reports aggregate Aptible API operations from each of your environments for review.

Container Recovery

Enclave containers that exit unexpectedly are restarted in pristine condition, ensuring uptime even if your app crashes.

Memory Management

Enclave containers that exceed their memory allocation are allowed to gracefully exit before being restarted. This helps avoid contention on the underlying EC2 instances and increases overall stability of your Enclave workloads.

Fault-Tolerant Container Distribution

Enclave automatically deploys horizontally-scaled app and database containers across separate AWS Availability Zones, to ensure high availability.

SRE Team Monitoring and Response

The Aptible SRE Team monitors your infrastructure 24/7 and responds to host and network incidents on your behalf.

Host Hardening

Enclave host operating systems are hardened to disable unnecessary services and limit surface area for attacks.

Managed TLS Endpoints

Enclave automatically procures and renews free TLS certificates via Let's Encrypt on your behalf.

Endpoint IP Filtering

Restrict access to Enclave apps and databases to a set of whitelisted IP addresses or networks, and block other incoming incoming traffic.

Container Log Drains

Route Enclave container logs to logging destinations for review, alerting, and archiving. Stream logs to your console in real time with the Aptible Toolbelt.

Container Metrics

Easily view container memory and CPU load, database IOPS, and disk usage in the Aptible dashboard.

Automatic Host Security Updates

The Aptible Security Team patches kernel vulnerabilities and other host- and network-level issues on your behalf.

Managed VPNs

Integrate with partners or connect privately to your Enclave dedicated stacks using Managed IPsec VPNs.

Internal Endpoints

Restrict access to apps and databases to other services in the same dedicated stack.

aptible Enclave

VPC Peering

Securely connect your Enclave dedicated stack to other AWS VPCs in the same region.

Database Replication

Easily replicate (PostgreSQL, MySQL, Redis) or cluster (MongoDB) databases in high-availability setups.

App Docker Image Security Scans

Identify vulnerable system packages in your Docker images. Optionally integrate with Appcanary to be notified when new vulnerabilities are discovered.

SSH Session Audit Logs

Capture output from ephemeral `aptible ssh` sessions and route to log drains for auditing, analysis, and compliance.

Direct Deploy from Docker Image

Build your Docker image locally or in a CI platform, push the image to a Docker registry, and deploy straight to Enclave.

Dockerfile Deploy

Let Enclave build your container images using a Dockerfile you specify, initiated with push to an Enclave git endpoint.

Network and Host Vulnerability Scanning

Enclave scans both the Internet-facing network and private network of a master reference stack each month. The Aptible Security Team remediates adverse findings without customer intervention. You may request a scan of your dedicated stack and its hosts as needed for your own security assessments and audits.

DDoS Avoidance

Enclave's VPC-based approach means that most stack components are not accessible from the Internet, and cannot be targeted directly by a DDoS attack. Enclave SSL/TLS endpoints include an AWS Elastic Load Balancer, which only supports valid TCP requests, meaning DDoS attacks such as UDP and SYN floods will not reach your app layer.

Container Scaling

Easily scale your app and database containers, both horizontally (more containers per service) and vertically (bigger containers). Database disks can be resized from the Aptible dashboard or with the CLI with minimal downtime.

Managed Host Intrusion Detection

Enclave monitors the underlying EC2 instances in your stacks for potential intrusions, such as unauthorized SSH access, rootkits, file integrity issues, and privilege escalation. The Aptible Security Team responds on your behalf 24/7 to investigate and resolve issues as they arise.

Automatic Database Backups

Enclave takes automatic daily backups of your databases, and distributes those backups across geographically separate regions.

Major OSS Database Support

Run Elasticsearch, MongoDB, MySQL, PostgreSQL, RabbitMQ, Redis, or SFTP containers on Enclave.

End-to-End Encryption in Transit

Traffic is encrypted all the way from your endpoints to your app and database containers using strong TLS ciphers.

Database Disk Encryption at Rest

Database volumes are encrypted at rest using AES-256 with Aptible-managed keys.

SSH Access

Easily spin up auditable ephemeral app containers to run management consoles, run ad-hoc jobs, and administer your architecture.

Database Tunneling

Use the Aptible CLI to securely connect to your Enclave databases and audit each access.

Dedicated Stacks and Environments

Each Enclave dedicated Stack runs in its own private VPC, making it easy to provision and manage multiple VPCs to support customers with stringent requirements for isolation and security.

Security Group Firewalls

Public-facing EC2 instances use inbound Security Group rules configured in deny-all mode. Only necessary ports are opened, and configuration is checked and enforced on a regular basis.

Enclave Service Status Page

Access real-time information about the status of the Aptible services at status.aptible.com.

Web Service Health Checks

Enclave performs both release and runtime health checks to ensure your web services are performant and responsive.

Safe Deploy Rollbacks

When encountering a failure during a deployment operation (e.g. one of your stack's underlying EC2 instances fails, AWS S3 has an outage, etc.), Enclave automatically restores your architecture to the last known good state.

Intermediate Backups

Enclave automatically enables data integrity controls for database types that support it (e.g. PostgreSQL write-ahead logs; MySQL binary logging; Redis RDB backups; MongoDB journaling, etc).

Zero-Downtime Deployments

Enclave automatically performs zero-downtime rolling deployments when you release your app.

Maintenance Pages

Configure your apps to serve custom maintenance pages when requests time out, your app is down, or when you scale your app to zero containers.

aws

AWS Shield DDoS Protection

Enclave Stacks benefit from AWS Shield Standard, a managed Distributed Denial of Service (DDoS) protection service that defends against most common, frequently occurring network and transport layer DDoS attacks that target your web site or applications.

Spoofing & Sniffing Protection

The AWS hypervisor only delivers traffic to EC2 instances that the traffic is addressed to, preventing sniffing. AWS's host-based firewalls do not permit instances to send traffic with a source IP or MAC address other than their own.

Physical and Environmental Controls

Enclave runs on AWS, which provides robust, ISO 27001-certified physical and environmental security for data centers.

Hypervisor Security

AWS uses a custom version of the Xen hypervisor that limits guest OS privileges. AWS is responsible for patching and maintenance of the hypervisor.

Port Scanning Protection

AWS monitors for unauthorized port scanning activity and blocks it when detected.

HIPAA ISO SOC amazon web services | Partner Network ADVANCED TECHNOLOGY PARTNER HEALTHCARE COMPETENCY aptible