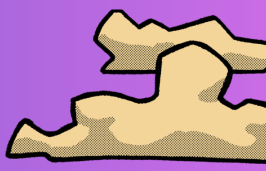
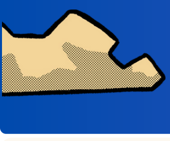


Aptible

Security Division of Responsibilities

Aptible is a HITRUST R2 certified, AWS-based container orchestration platform for deploying highly available, secure apps and databases into isolated cloud environments. Software teams use Aptible to automate DevOps and security engineering best practices and requirements for HIPAA, HITRUST, SOC 2, PCI DSS for Service Providers Level 2, and other security frameworks.



✓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 Aptible 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 Aptible 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 Aptible environment variables to store sensitive information and configuration.

Aptible

✓

HITRUST R2 Validated Assessment

Demonstrate the maturity of our cloud computing stack with Aptible's HITRUST r2 Validated Assessment, the gold standard for information protection assurances due to its comprehensive control requirements and consistent oversight.

✓

HIPAA Compliance

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

✓

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 environments with granular access control.

✓

Enhanced Support

All Aptible accounts include business-level support. Support upgrade options include private Slack channels with the Aptible team and 24x7 Urgent Support.

✓

Aptible API Audit Logs

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

✓

Container Recovery

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

✓

Memory Management

Aptible 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 Aptible workloads.

✓

Endpoint IP Filtering

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

✓✓

Container Log Drains

Route Aptible 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.

✓✓

Host Hardening

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

✓

Fault-Tolerant Container Distribution

Aptible 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.

✓✓

Automatic Host Security Updates

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

✓

App Docker Image Security Scans

Identify vulnerable system packages in your Docker images.

✓✓

Managed TLS Endpoints

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

✓✓

Internal Endpoints

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

✓✓

Managed VPNs

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

✓✓

VPC Peering

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

✓

Database Replication

Easily replicate or cluster databases in high-availability setups.

✓

SSH Session Audit Logs

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

✓✓

Container Scaling

Easily scale your app and database containers 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.

✓

Deploy from Git

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

✓

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 Aptible.

✓✓

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.

✓✓

Network and Host Vulnerability Scanning

Aptible 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.

✓

Managed Host Intrusion Detection

Aptible 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 24/7 to investigate and resolve issues as they arise.

✓✓✓

Automatic Database Backups

Aptible takes automatic daily and monthly backups of your databases and distributes those backups across geographically separate regions. Yearly backups can be additionally configured.

✓

Major OSS Database Support

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

✓

DDoS Avoidance

Aptible VPC-based approach means that most stack components are not accessible from the Internet and cannot be targeted directly by a DDoS attack. Aptible 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.

✓

SSH Access

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

✓✓

Database Disk Encryption at Rest

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

✓✓

Safe Deploy Automatic Rollbacks

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

✓

Web Service Health Checks

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

✓✓

Dedicated Stacks and Environments

Each Aptible 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.

✓

Database Tunneling

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

✓✓

Security Group Firewalls

Public-facing EC2 instances use inbound Security Group rules configured to deny by default. Only necessary ports are opened, and the configuration is checked and enforced regularly.

✓

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.

✓✓✓

Intermediate Backups

Aptible 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

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

✓

Aptible Service Status Page

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

AWS

✓

AWS Shield DDoS Protection

Aptible 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

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

✓✓

Hypervisor Security

Aptible Stacks benefit from the AWS Nitro Hypervisor, which limits guest OS privileges and provides hardware-level security and performance. AWS is responsible for patching and maintaining the Nitro Hypervisor.

✓

Port Scanning Protection

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

Secured by Aptible

Aptible empowers engineering teams to bring products to market faster by implementing and operating all of the rigorous infrastructure security controls required to comply with regulatory frameworks and pass security audits. The table below highlights the full list of security and availability controls provided by Aptible directly or through our infrastructure provider, AWS.

Secured by Aptible

HIPAA Compliant
Secured by Aptible

HITRUST Compliant
Secured by Aptible

PCI DSS for Service Providers Level 2
Secured by Aptible