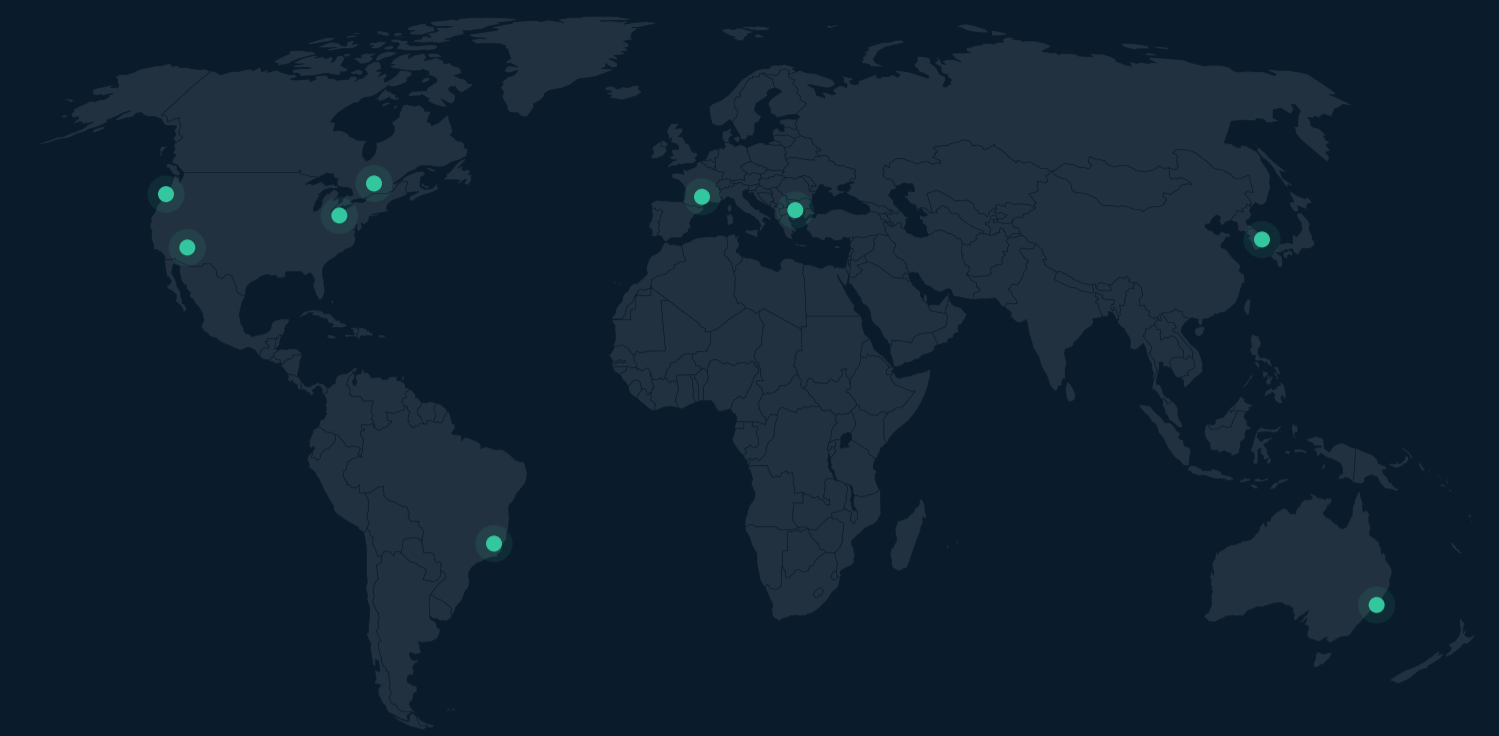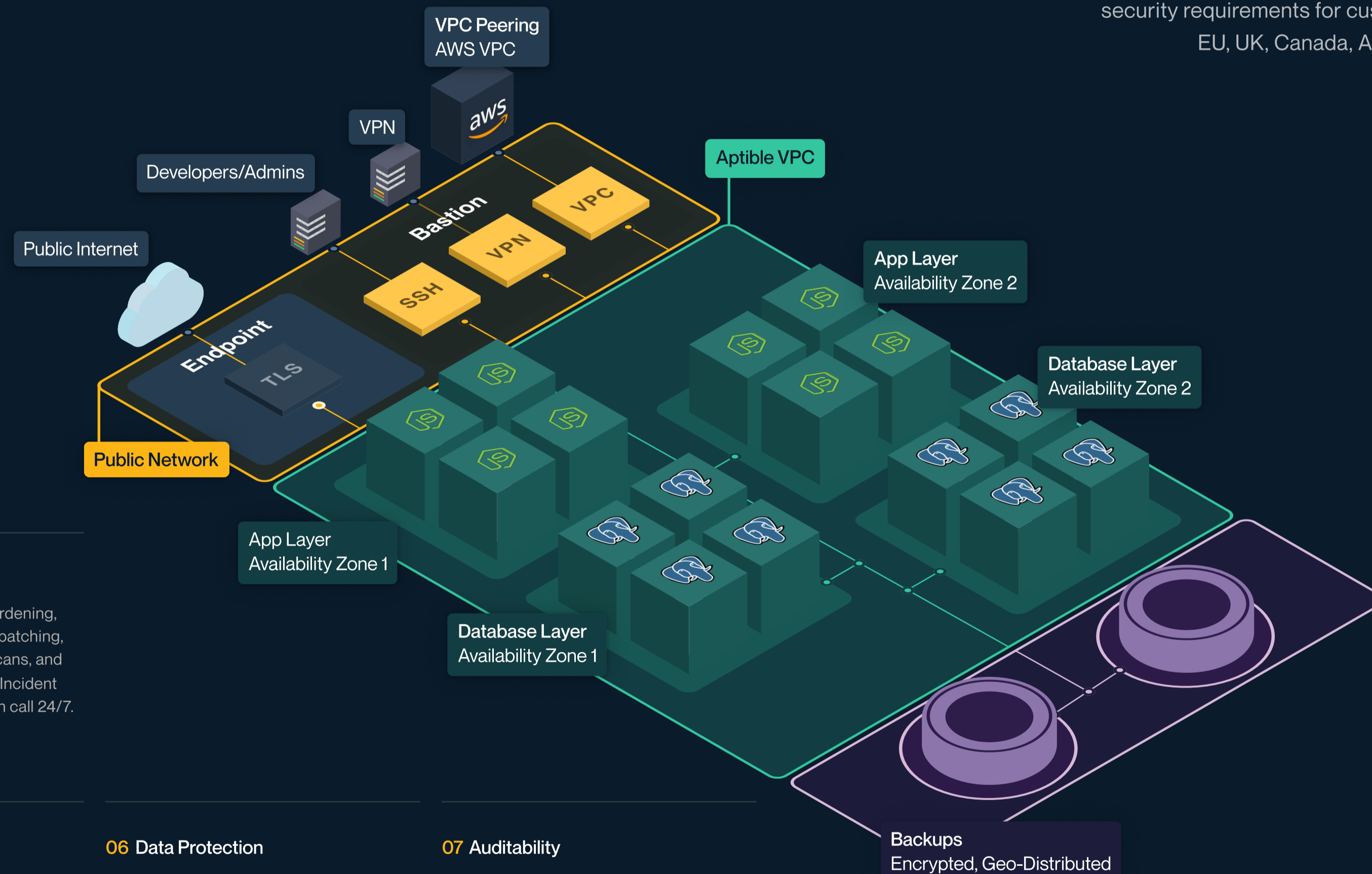# Aptible Reference Architecture

Aptible is an 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, ISO 27001, SOC 2, and other security frameworks.

Aptible stacks can run in most AWS Regions. Aptible supports data security requirements for customers all over the world, including the EU, UK, Canada, Australia, Singapore, and more.

VPC Peering AWS VPC

VPN

aws

Developers/Admins

Aptible VPC

Bastion

VPC

VPN

SSH

Public Internet

App Layer Availability Zone 2

Database Layer Availability Zone 2

Endpoint

TLS

Public Network

App Layer Availability Zone 1

Database Layer Availability Zone 1

Backups Encrypted, Geo-Distributed

01 VPC

02 App Layer Host

03 Containers

01 Isolated Network

Each Aptible Deploy VPC ("stack") gets its own isolated network, permitting Aptible-Managed VPN and VPC peering connections.

02 Encrypted Endpoints

Access to each stack is controlled by encrypted endpoints. TLS Endpoints support IP filtering. Backend access via SSH to a bastion layer is managed with granular, role-based API permissions and 2-factor authentication with FIDO U2F security key support.

03 Private Subnets

App and database Docker containers run in private subnets, protected from being targeted directly from the Internet. Internal Endpoints provide private networking inside the stack.

04 Host Hardening

Aptible Deploy manages host hardening, automatic security updates and patching, network and host vulnerability scans, and host intrusion detection. Aptible Incident Response and SRE Teams are on call 24/7.

05 High Availability

Fast, self-serve app and database scaling, safe deploys with automatic health checks and rollbacks, automatic Container Recovery, safe Memory Management, and automatic cross-AZ container scheduling increase resiliency and reliability

06 Data Protection

Database disks are encrypted at rest and backed up automatically. Encrypted backups are distributed across geographic regions for redundancy. Databases are easily replicated or clustered.

07 Auditability

Database disks are encrypted at rest and Container, database, SSH session, and Aptible Deploy API logs provide high auditability.

01 VPC

Aptible secures the VPC networks and hosts with managed scanning, patching, and automatic security updates.

02 App Layer Host

Aptible App Security Scans integrate with CoreOS Clair to identify vulnerable system packages in Docker images.

03 Containers

Customers are responsible for container image and application security.