

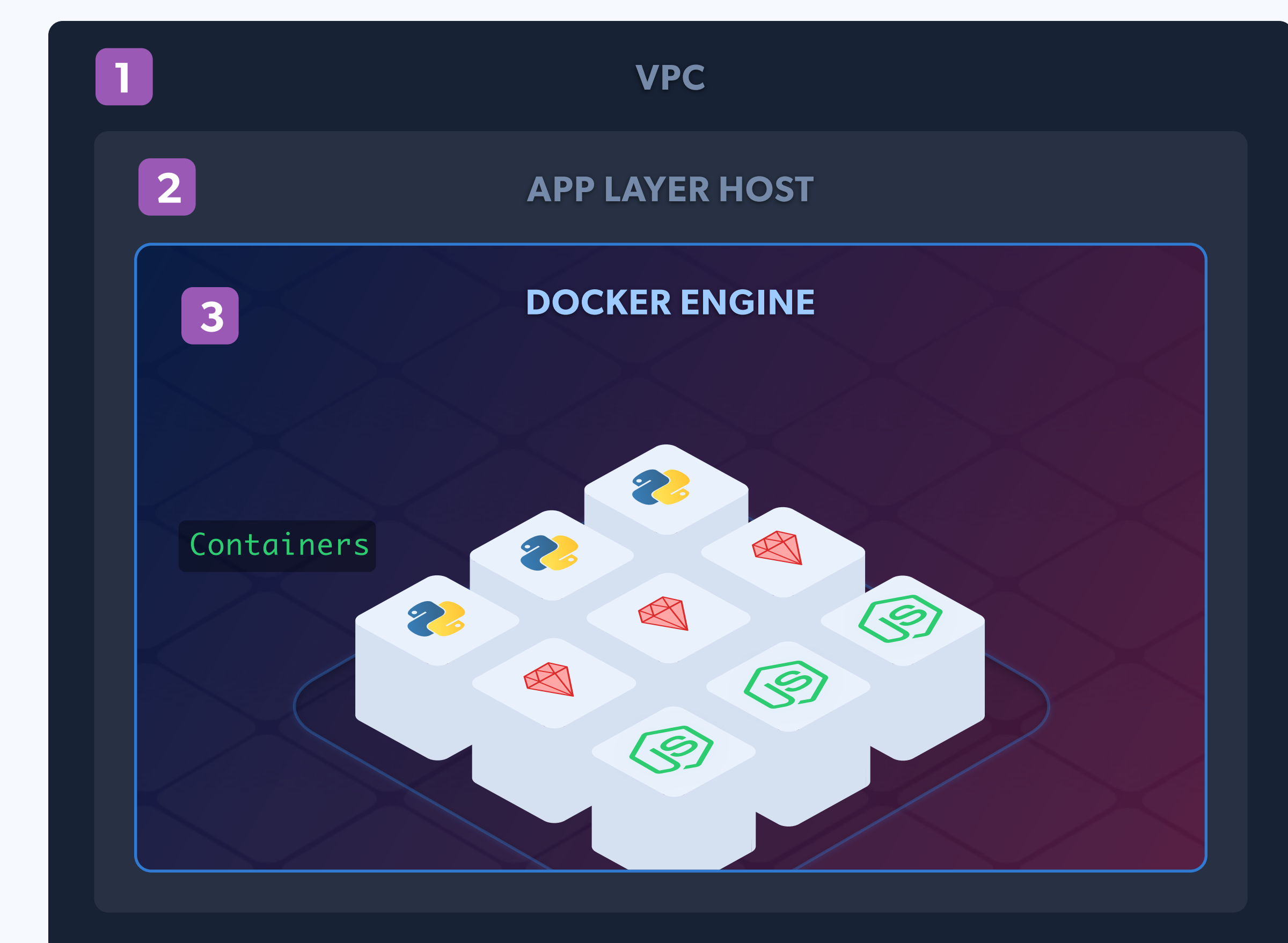
# Enclave Reference Architecture

Aptible Enclave® is an ISO 27001 certified, AWS-based container orchestration platform for deploying highly available, secure apps and databses 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.

- 1 Each Enclave VPC ("stack") gets its own isolated network, permitting Enclave Managed VPN and VPC peering connections.
- 2 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.
- 3 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.
- 4 Enclave 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.
- 5 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.
- 6 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.
- 7 Container, database, SSH session, and Enclave API logs provide high auditability.



Enclave® 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.



- 1 Enclave® secures the VPC networks and hosts with managed scanning, patching, and automatic security updates.
- 2 Enclave® App Security Scans integrate with AppCanary to identify vulnerable system packages in Docker images.
- 3 Customers are responsible for container image and application security.

