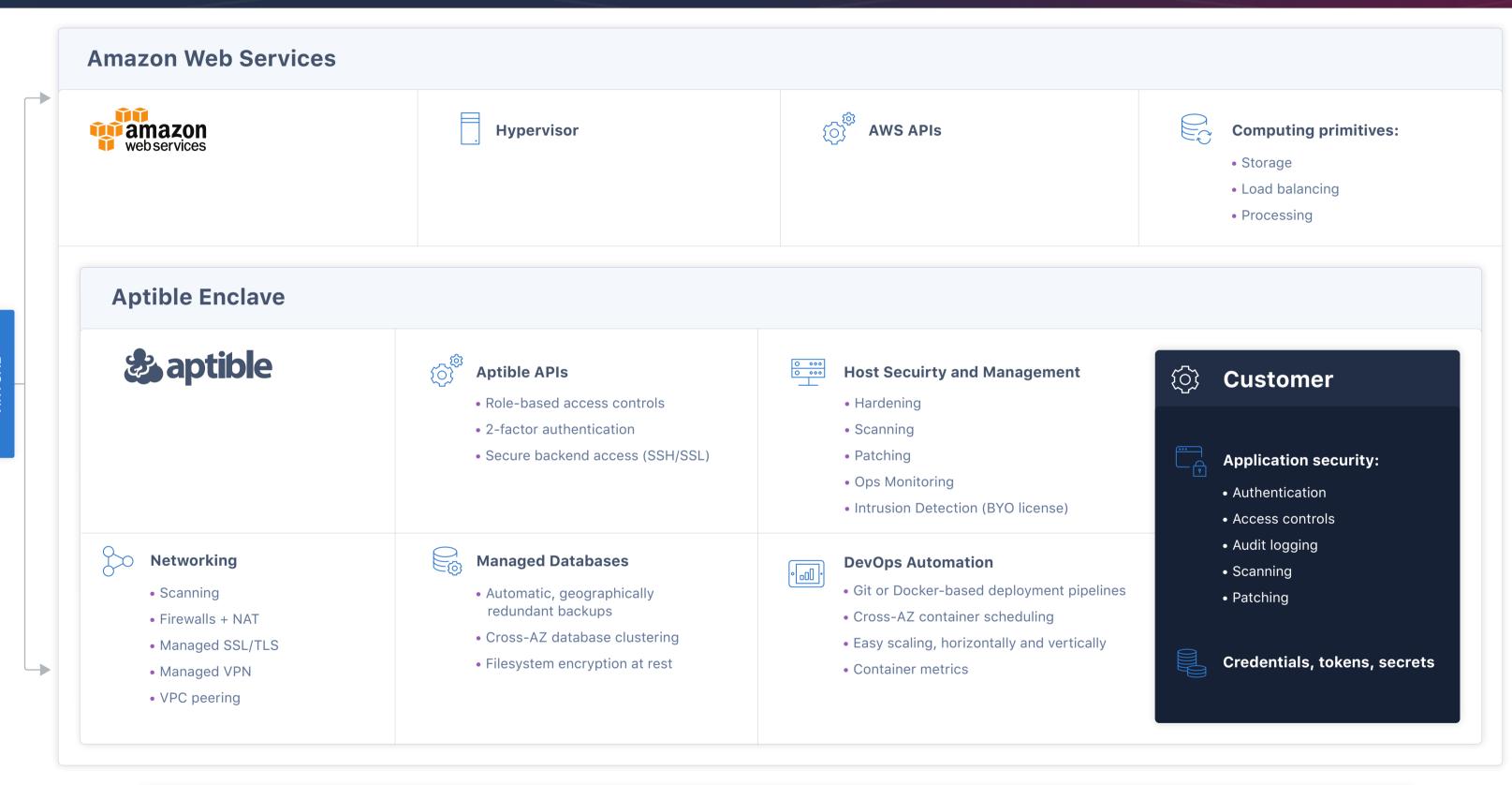# Enclave - Division of Responsibilities

Aptible Enclave helps engineering teams meet strict security and compliance requirements while keeping technical debt low. Engineering teams get more done using Enclave to automate DevOps and security engineering tasks, freeing up time to focus on product. Aptible and AWS (through Aptible) take responsibility for providing secure cloud computing environments. You are responsible for the apps you deploy and securing your Enclave account.

aptible

Amazon Web Services

amazon web services

Hypervisor

AWS APIs

Computing primitives:
- Storage
- Load balancing
- Processing

Aptible Enclave

aptible

Aptible APIs
- Role-based access controls
- 2-factor authentication
- Secure backend access (SSH/SSL)

Host Secuirty and Management
- Hardening
- Scanning
- Patching
- Ops Monitoring
- Intrusion Detection (BYO license)

Customer

Application security:
- Authentication
- Access controls
- Audit logging
- Scanning
- Patching

Credentials, tokens, secrets

Networking
- Scanning
- Firewalls + NAT
- Managed SSL/TLS
- Managed VPN
- VPC peering

Managed Databases
- Automatic, geographically redundant backups
- Cross-AZ database clustering
- Filesystem encryption at rest

DevOps Automation
- Git or Docker-based deployment pipelines
- Cross-AZ container scheduling
- Easy scaling, horizontally and vertically
- Container metrics

VIRTUAL

AWS Data Centers

amazon web services

Physical and environmental security
- Access controls
- Fire detection and suppression systems
- Redundant UPS power systems
- Redundant networking
- Climate and temperature controls

PHYSICAL