NOUMENA CLOUD INFRASTRUCTURE
HIGH-LEVEL SECURITY ARCHITECTURE OVERVIEW

This document presents an overview of the high-level security architecture implemented within NOUMENA Cloud infrastructure. It outlines our security practices across critical domains:

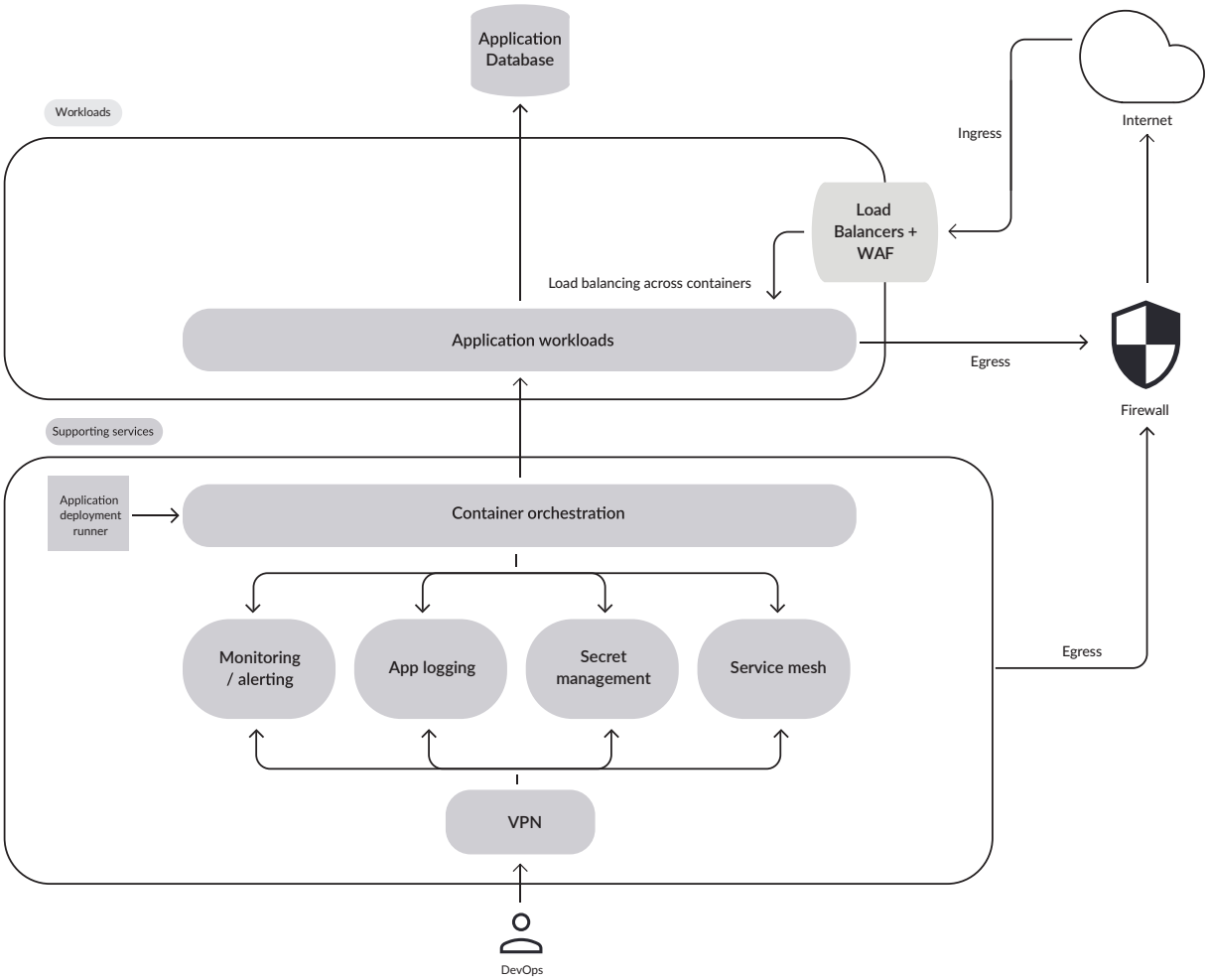
SECURE NETWORK ARCHITECTURE

Our cloud infrastructure employs rigorous network segmentation, with clearly defined subnets such as DMZ, Storage Network, and Workloads. Inter-subnet communication is strictly controlled and limited to only necessary interactions, significantly reducing lateral movement risks within the network.

All outbound network traffic is controlled by a network firewall, adhering strictly to allow-listed destinations only. This effectively prevents unauthorized exfiltration or unintended external communications.

CRITICAL DOMAINS

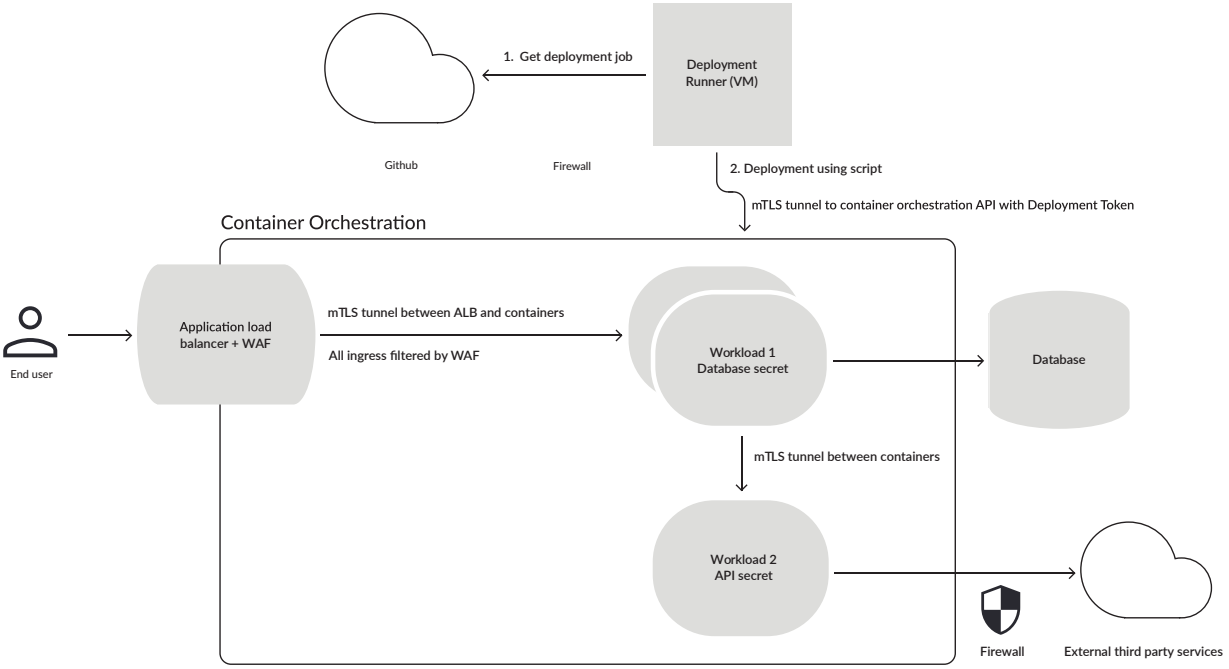
- Secure network architecture
- Authentication and authorization
- Secure application deployment
- Reliability and redundancy measures
- Logging, monitoring, and alerting
- Proactive vulnerability management
- Governance processes



AUTHENTICATION AND AUTHORIZATION

At NOUMENA we have robust authentication and authorization practices. All cloud infrastructure access requires Multi-Factor Authentication (MFA). Our point-to-site VPN, which is used for system administration, also requires MFA. Authentication procedures for infrastructure are completely isolated from the customer authentication system, creating a distinct security boundary.

Authorization follows the principle of least privilege.
Access rights are explicitly limited to essential personnel only. Administrative access to the underlying infrastructure is tightly restricted, and VPN and secrets access are separately managed, granted solely on an as-needed basis.
Apart from the network load balancer connecting to public HTTP interfaces, our infrastructure is inaccessible directly from the internet. All other remote connections require VPN



APPLICATION DEPLOYMENT AND SECURITY

Our application deployment process is streamlined, fully automated, and inherently secure. We employ self-hosted runners in our Continuous Integration/Continuous Deployment (CI/CD) pipelines, leveraging mutual TLS (mTLS) combined with secure token-based authentication for runner communication with our container clusters. This ensures secure, authenticated, and encrypted communication pathways.

To mitigate potential vulnerabilities within our CI/CD pipelines, we minimize reliance on pre-made GitHub actions. This reduces the risk of incorporating malicious scripts into our deployment routines. All application secrets are securely managed and retrieved via dedicated secret management tools, further minimizing exposure.

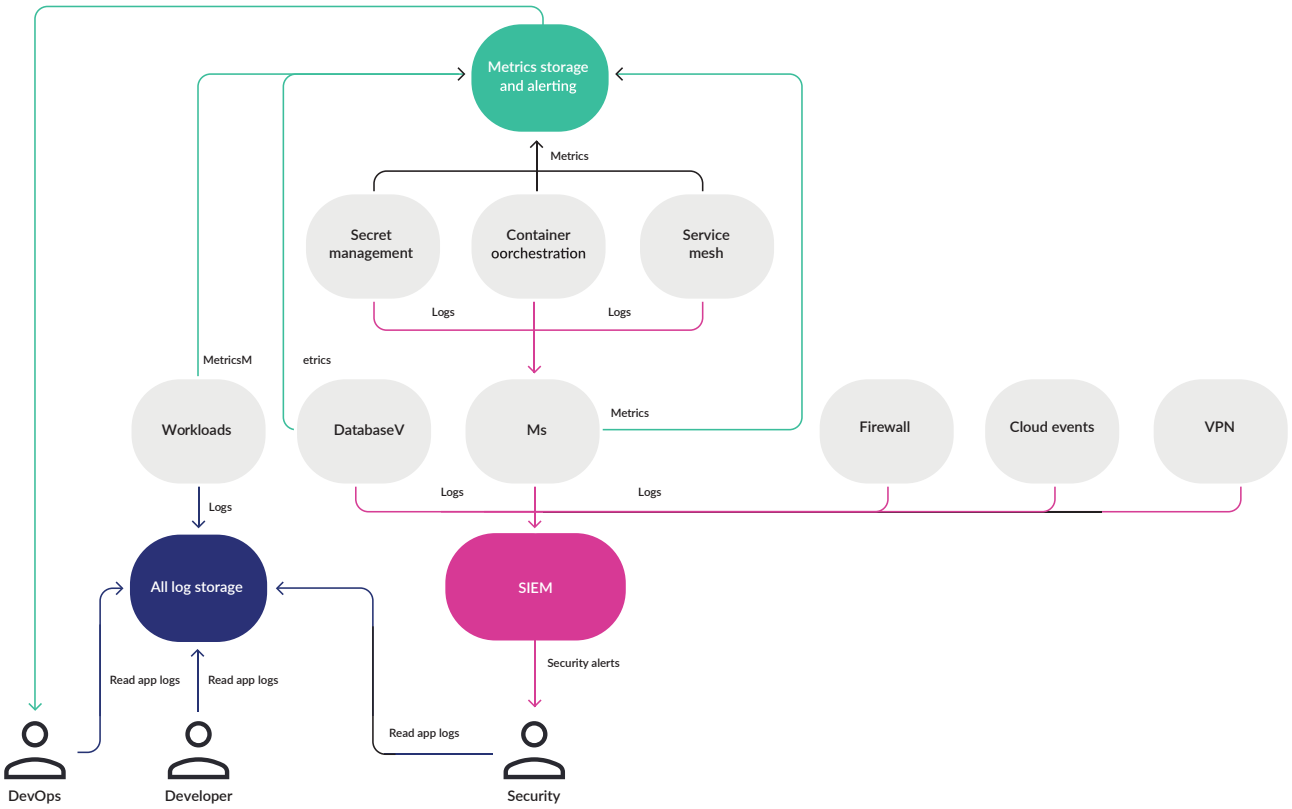
Internal container communication utilizes mTLS proxies, providing strong encryption and mutual verification of container identities.

External HTTP traffic goes through Web Application Firewall (WAF) filtering, protecting applications from common web-based threats.

RELIABILITY AND REDUNDANCY

Noumena's infrastructure is engineered for resilience and high availability. Incoming HTTPS and MQTT traffic is distributed across multiple Application Load Balancers (ALBs), ensuring service continuity even if an individual ALB fails. These ALBs further distribute traffic across multiple container instances, preventing downtime from single-container failures.

Containers are distributed across multiple Virtual Machines (VMs). Thus, the failure of a single VM will not interrupt service availability. Critical services — such as secret management, container orchestration, and the service mesh — operate within robust clusters of three or more nodes, eliminating single points of failure and maintaining high availability.



CLUSTER SECURITY

Underlying container infrastructure services — including secret management, orchestration, and service mesh — authenticate and authorize interactions using both mTLS and token-based mechanisms. This layered approach guarantees secure inter-service communication and precise access control.

BACKUP AND DISASTER RECOVERY

We perform systematic backup and disaster recovery procedures. Daily full snapshots of essential resources like databases provide full restoration capabilities. Additionally, databases maintain detailed transaction logs for point-in-time recovery to minimize data loss.

INFRASTRUCTURE DEVELOPMENT, DEPLOYMENT, AND VULNERABILITY MANAGEMENT

Infrastructure as Code (IaC) approach guides all Noumena's infrastructure development. IaC configurations are managed through Git repositories, ensuring full traceability, accountability, and collaborative review by multiple engineers. Automated daily tests verify infrastructure stability and functionality by rebuilding a test environment.

Vulnerability management practices are comprehensive, including regular scanning of IaC for known vulnerabilities. We actively monitor CVE databases for threats and conduct frequent penetration tests to identify and remediate vulnerabilities proactively.

SECURITY PROCESSES AND GOVERNANCE

We maintain robust governance through well-defined processes, including:

- **Environment promotion process (dev -> test -> pre-prod -> prod),**
- **Incident response strategy, and**
- **Risk management practices.**

These ensure controlled changes, rapid incident mitigation, and proactive risk assessments, strengthening our security framework.