Dalet Pyramid: Security Overview

December 2022 – v1.1

CS Cloud Operations

Pyramid Security Responsibility Matrix

R&D	Cloud Ops	Sys Admins	IT Admin	User
Product Development	Customer Environment Setup	Physical Infrastructure Reliance	Manage Users	Follows company compliance policy
Infrastructure Automation	Infrastructure Automation	Network Resilience	Configure ACLs	
Work exclusively on sandbox environments	OS Maintenance	Storage Resilience	Manage Workflows	
On-Demand access to anonymized data and dashboards for debug	Application Rollout	Raw Resources Availability		
App Security Awareness	Infra Security Awareness	Offer Added-Value Infrastructure Services		
	Production Systems Access			

Pyramid Global Security Policy

For Users

Ephemeral JWT token-based authentication

Support for MFA when provided by customer's IdP.

TLS 1.2+ (RSA/SHA-256) secured connections
through HTTPS protocol only.
AES-256 encrypted data at rest for object storage.

Persistent replicated data storage (99.99+% SLA).
90 days activity logs retention (Control Tower).

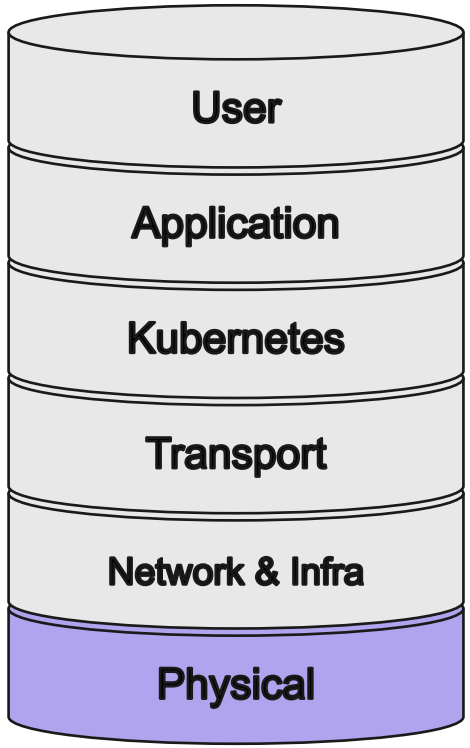
For Administrators

Nominative MFA authentication for Ops VPN access.
Nominative MFA authentication for Ops IaaS services access.
Nominative personal certificates for resources access.

Hardened Kubernetes

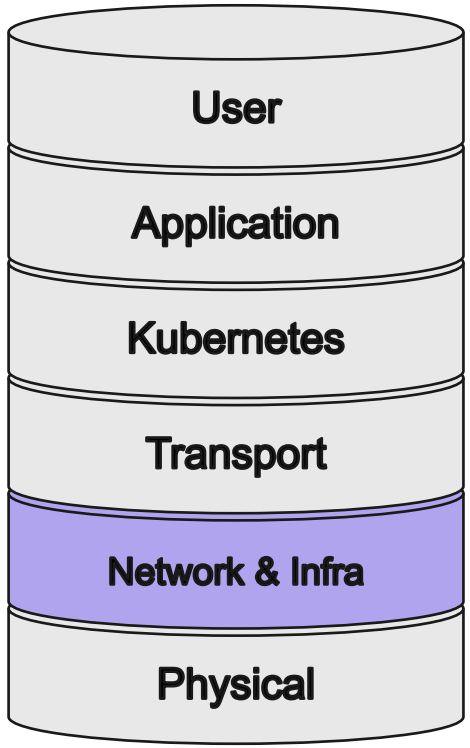
Realtime time-based eventing and monitoring metrics & KPIs.

Pyramid Physical Layer Security Policy



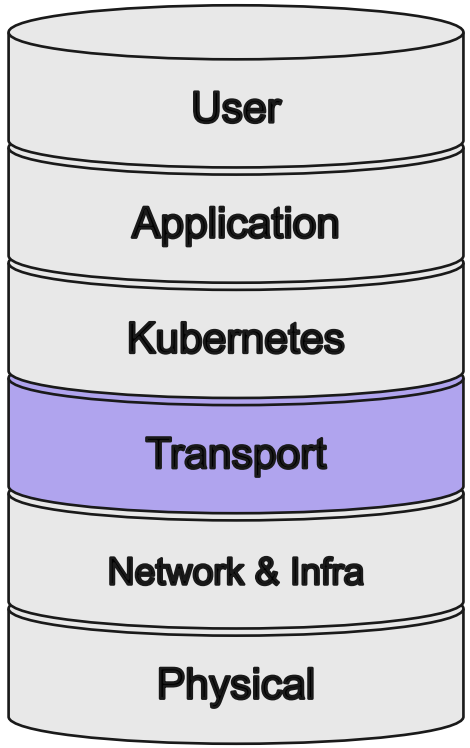
	AWS (Dalet Hosted)
Access	CCTV, MFA physical access, 24x7 intrusion alarming.
Autonomy	Regions and Availability Zone (AZ)
Power Supply	Primary and alternate equal power source. Diesel backup generators.
Fire	Heat, fire and smoke detectors. Fire detection and suppression equipments.
Cooling	Evaporative Cooling Outside Air Water Cooling
Compliance & Certifications	ISO 9001, ISO 27001, ISO 27017, ISO 27018, SOC 1/2/3, CSA, C5, FERPA, PCI-DSS, MPAA

Pyramid Network & Infrastructure Layers Security Policy



- **Instances are isolated** to their respective VPC only:
  - No public IP address.
  - No inbound Internet connectivity.
  - Except for network edge / load-balancers
- **Firewall** is configured:
  - At IaaS VPC or instance level, depending on partner.
  - With a deny-all policy, except for HTTPS (443) protocol on network edges.
- **Load-Balancer**:
  - Is redundant and distributed.
  - Works at Layer 7 and performs application routing.
  - Enforces secure traffic (unsecure HTTP redirection).
  - Exposes traffic over HTTP/2 (H2) and HTTP 1.1 protocols.
  - Terminates SSL.
  - Is the only Internet-exposed part of the infrastructure.

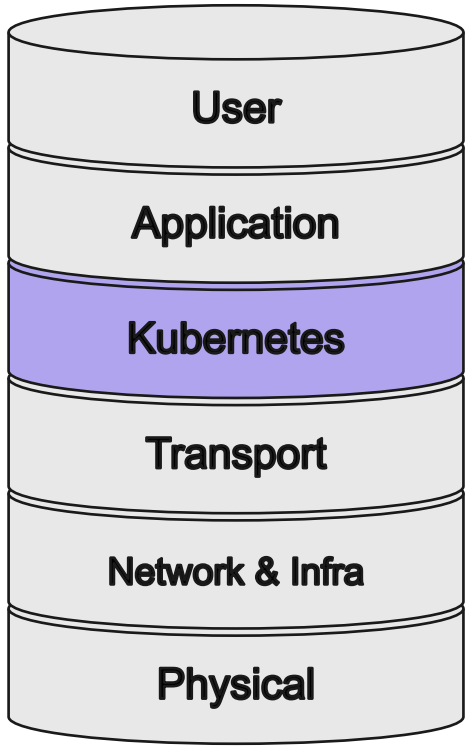
Pyramid Transport Layer Security Policy



- **HTTPS** traffic is:
  - Enforced through HTTP Strict Transport Security (**HSTS**)
  - Supports TLS Server Name Indication (**SNI**)
  - Offered through **RSA 2048 bits wildcard certificate** signed over **SHA256**.
  - Deprecates weak SSL v2/v3 and TLS 1.0/1.1 in favor of **TLS 1.2+**.
  - Offers **ECDHE RSA** with **AES 256/128 GCM** and **CHACHA20** ciphers only.

- Exposed protocol:
  - Robust to DROWN, BEAST, POODLE variants, Heartbleed, Ticketbleed, ROBOT vulnerabilities and currently known OpenSSL attack vectors.
  - Support Downgrade Attack Prevention
  - Provides Perfect Forward Secrecy support.
  - Does not use common Diffie-Hellman (DH) prime numbers.
  - Mangles backend servers name and version numbers against scan attacks.
  - Ranked **A+** on Qualys Labs SSL Report

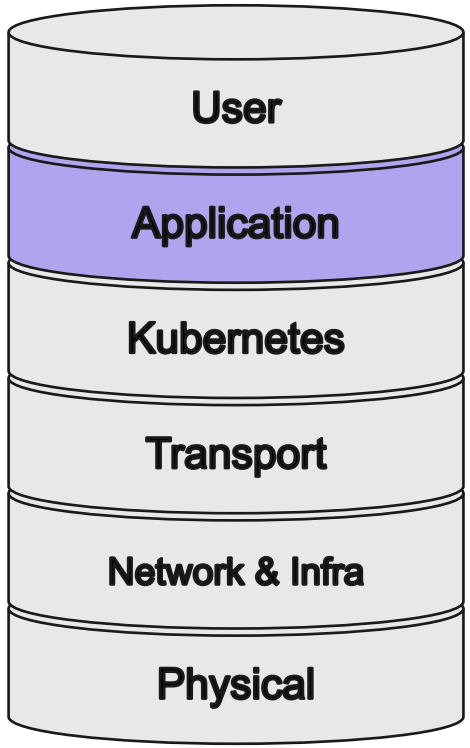
Pyramid Kubernetes Layer Security Policy



- **Kubernetes Hardening:**
  - **Cluster Control Plane:**
    - Complete RBAC on administration APIs
    - No control over ETCD nor exposure.
    - Regular kube-bench CIS conformance checks.
  - **Cluster Data Plane**:
    - Fixed quotas and limits on pods resources.
    - Remote logs remanence and integrity for trailing and auditing.
  - **Container / Pod**:
    - Lightweight containers to minimize attack surface.
    - Services resource isolation through namespace isolation.
    - Non-root containers to prevent host privilege escalation
    - Read-only filesystem to preserve integrity
    - Container CVE vulnerability scans at build and release stages.
    - No public pod exposure.

- **Ops Remote Access & Administration**:
  - Nominative AWS IAM RBAC with corporate IdP + MFA authentication and authorization.
  - Is only offered over VPC Peering or IPSec-based tunnel from Dalet Ops management network.
  - Fully managed by **Terraform** & **Ansible** IaC tools: no manual human handover.
  - Perform 3rd-party conducted external penetration tests.

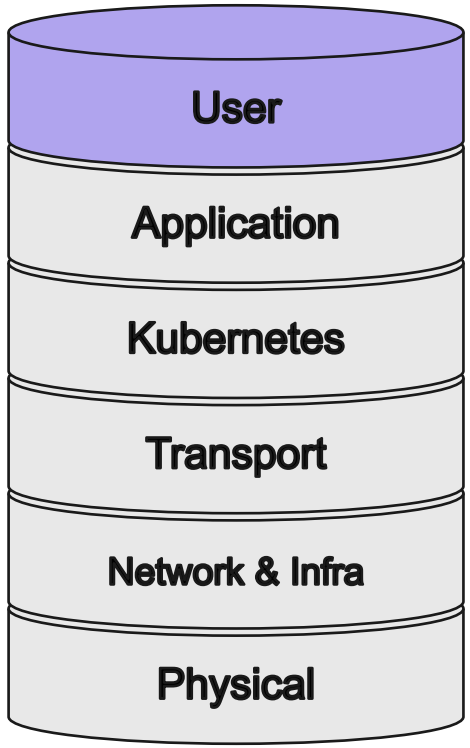
Pyramid Application Layer Security Policy



- **Passwords**:
  - Application accounts credentials and secure information are stored under vault mechanisms at source control layer prior to being deployed.
  - User authentication relies on ephemeral JWT token to be provided on each API call.
  - No user password is ever being stored (authentication being deferred to customer's IdP).

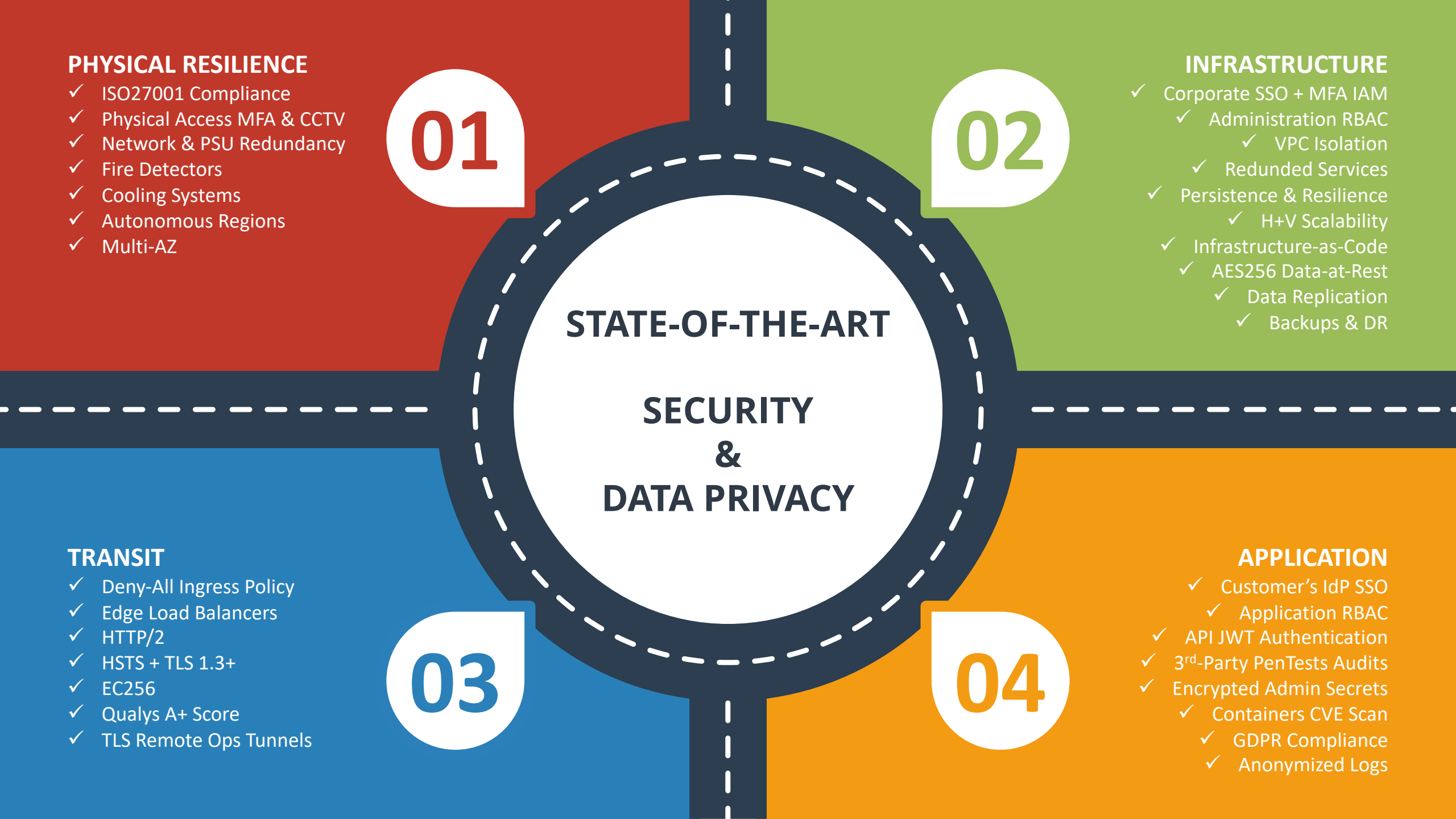
- **Application**:
  - Logs are anonymized and no user password or sensitive data can be extracted from there.

Pyramid User Layer Security Policy



- **Password Policy**:
  - User passwords policy and complexity is configured by customer.
  - Use of external Identity Provider (IdP) allows for MFA support.

- **Access Control:**
  - Access control to services is based on role assigned to user:
    User, Company Admin, Support, Service Admin, …
    Roles are defined by the customer.


PHYSICAL RESILIENCE
✓ ISO27001 Compliance
✓ Physical Access MFA & CCTV
✓ Network & PSU Redundancy
✓ Fire Detectors
✓ Cooling Systems
✓ Autonomous Regions
✓ Multi-AZ
01
INFRASTRUCTURE
✓ Corporate SSO + MFA IAM
✓ Administration RBAC
✓ VPC Isolation
✓ Redunded Services
✓ Persistence & Resilience
✓ H+V Scalability
✓ Infrastructure-as-Code
✓ AES256 Data-at-Rest
✓ Data Replication
✓ Backups & DR
02
STATE-OF-THE-ART
SECURITY
&
DATA PRIVACY
TRANSIT
✓ Deny-All Ingress Policy
✓ Edge Load Balancers
✓ HTTP/2
✓ HSTS + TLS 1.3+
✓ EC256
✓ Qualys A+ Score
✓ TLS Remote Ops Tunnels
03
APPLICATION
✓ Customer's IdP SSO
✓ Application RBAC
✓ API JWT Authentication
✓ 3rd-Party PenTests Audits
✓ Encrypted Admin Secrets
✓ Containers CVE Scan
✓ GDPR Compliance
✓ Anonymized Logs
04

dalet

Thank you.