Dalet Flex: Security Overview

December 2022 – v1.1

CS Cloud Operations

Flex 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			

Flex 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).
30 days activity logs retention (local log stack)

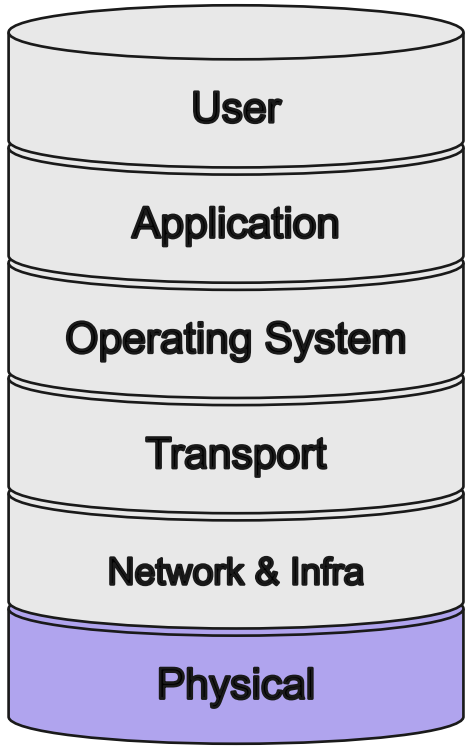
For Administrators

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

Hardened Linux-only infrastructure ecosystem
with no-password policy.

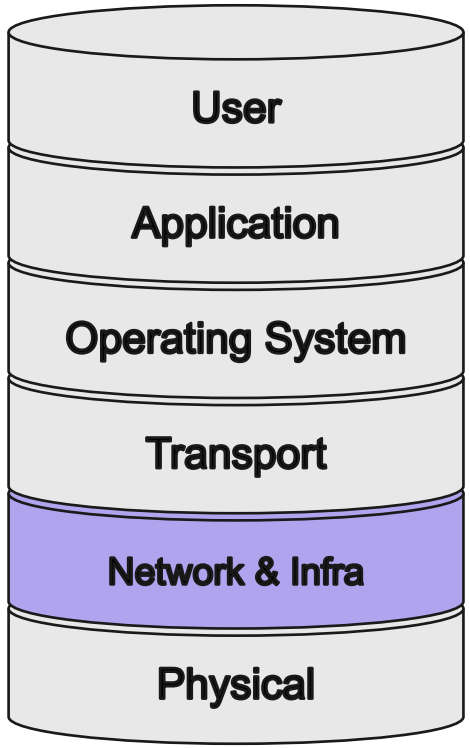
Realtime time-based eventing and monitoring metrics & KPIs.

Flex Physical Layer Security Policy



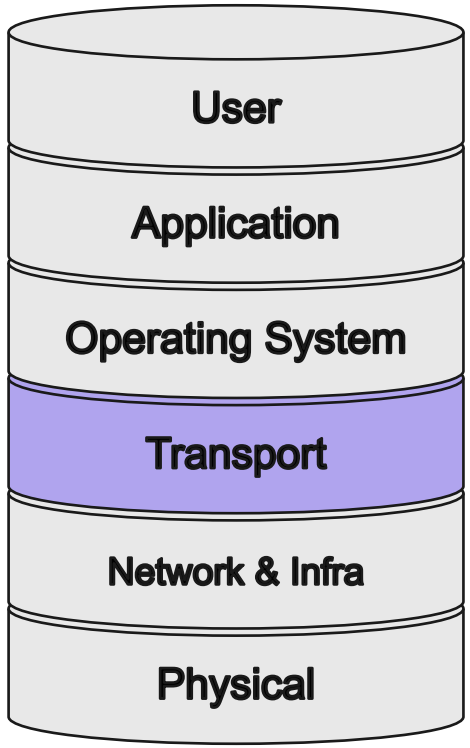
	AWS	GCP	Azure
Access	CCTV, MFA physical access, 24x7 intrusion alarming.	Comprehensive cameras, biometric authentication, 24x7 guard staff.	CCTV, Body scanning, biometrics MFA, 24x7 surveillance.
Autonomy	Regions and Availability Zone (AZ)	Regions and Zones	Regions, Availability Zones and Availability Sets
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		

Flex 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.

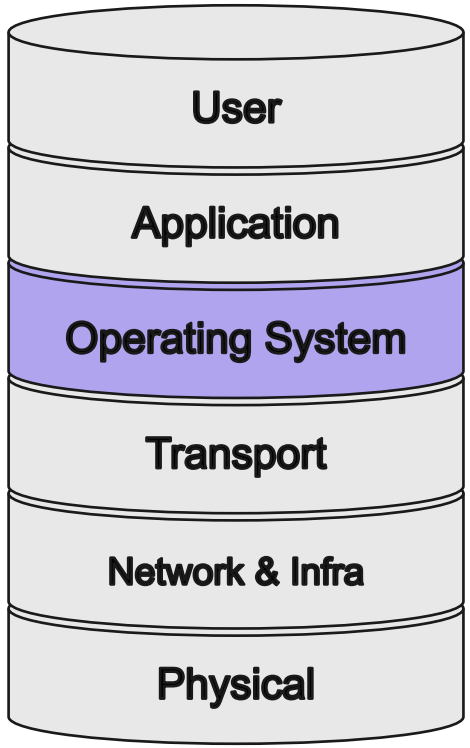
Flex Transport Layer Security Policy



- **HTTPS** traffic is:
  - Enforced through HTTP Strict Transport Security (**HSTS**)
  - 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/CBC 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.
  - Is ranked **A+** on Qualys Labs SSL Report

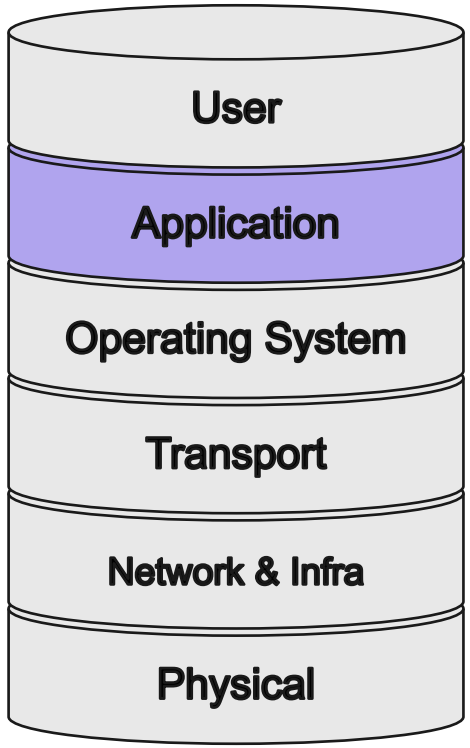
Flex Operating System Layer Security Policy



- **Operating System**:
  - All instances run on GNU/Linux **Ubuntu 20.04 / 22.04 LTS**
  - All instances are installed using server-edition, minimalistic templates. No X11/GUI or any non-relevant packages are installed as to minimize attack surface.
  - Is fully managed by **Terraform** and **Ansible** Infrastructure-as-Code tools: no manual human handover.
  - Provides applications and services resource isolation through **containerization** and **namespace isolation**.
  - External third-party agents/probes can be added to comply with customer's IDS/IPS systems in place.

- **Ops Remote Access**:
  - Is only offered through **SSH over VPC Peering or IPSec**-based tunnel from Dalet Ops management network.
  - Prevents root access.
  - Uses a **no-password SSH policy** (PKI with private/public key exchange only, prevents from brute-force attacks).
  - Features **nominative Ops users access only**, each administrator account being added/revoked through Ansible.

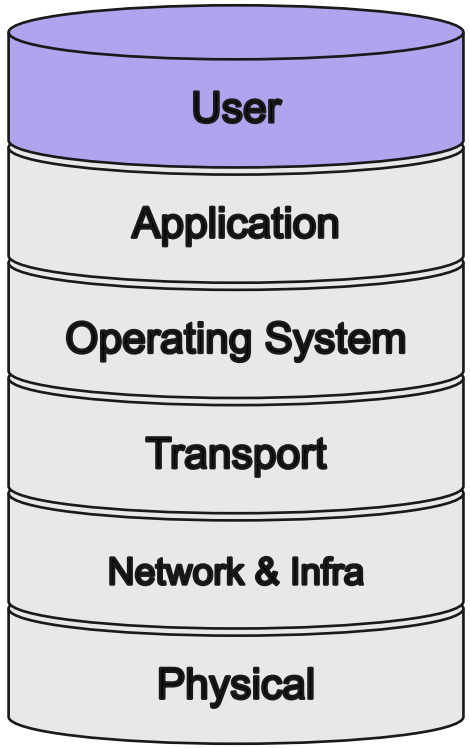
Flex Application Layer Security Policy



- **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.
  - User passwords are bcrypt hashed and salted in databases and so, can't be recovered.
  - No encrypted password is being stored when authentication is deferred to customer's IdP.

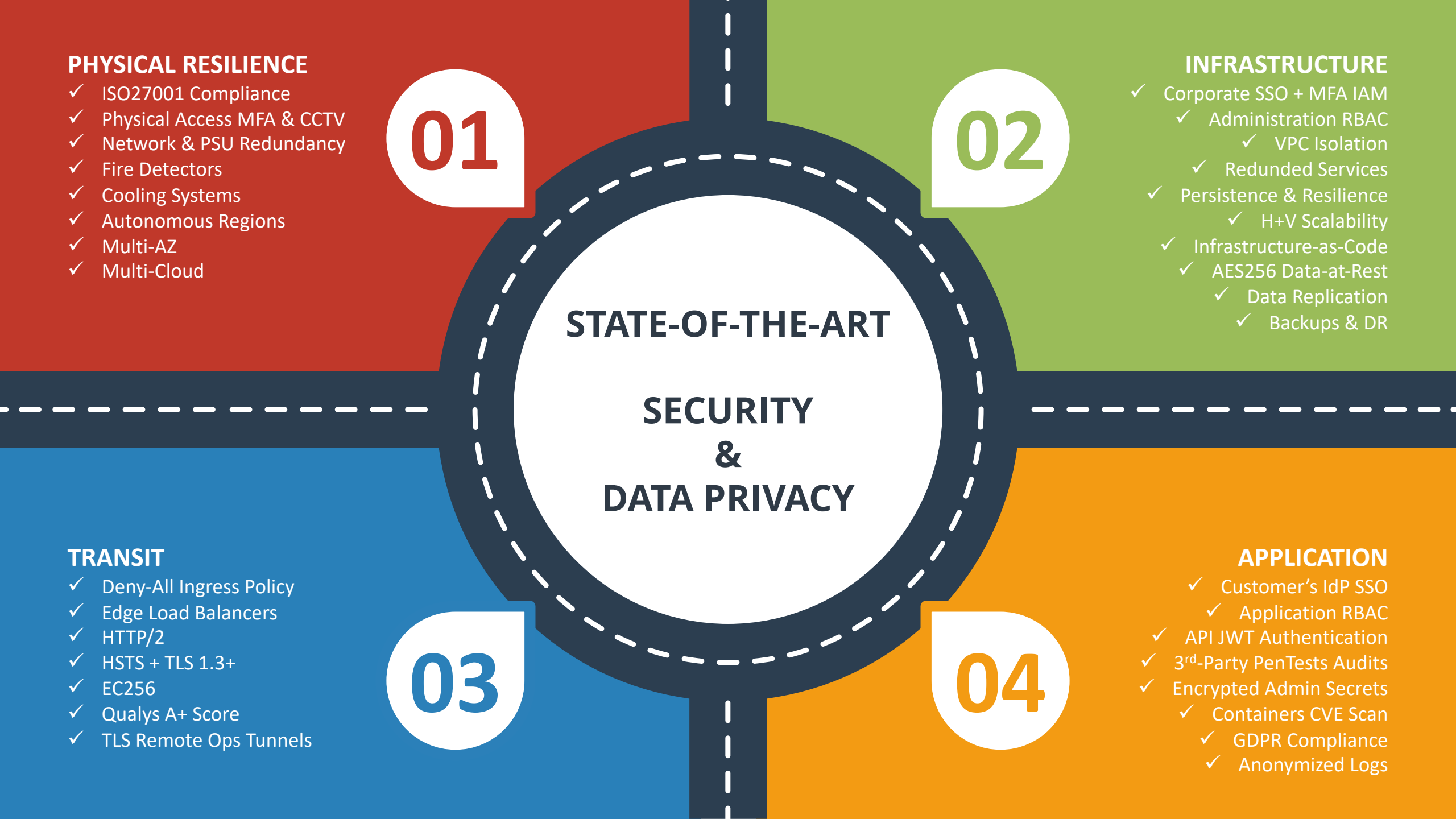
- **Application**:
  - Logs are anonymized and no user password or sensitive data can be extracted from there.
  - ClamAV anti-virus scanning of small files and attachment.

Flex 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:
    Guest, 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
✓ Multi-Cloud
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

Flex Future Security Improvements

- **Network & Infrastructure Layer**
  - Provide out-of-the-box Web Application firewall (WAF)
  - Provide out-of-the-box Intrusion Detection & Prevention Systems (IDS / IPS).
  - Provide continuous runtime vulnerability scanning systems.
- **Transport Layer**
  - Support for TLS 1.3
  - Update SSL certificates to use EC256 instead of RSA2048.
- **Operating System Layer**
  - Introduce inter-VPC firewalling and instance-local Linux firewall.
  - Database encryption at rest.
- **Application Layer**
  - Static Application Security Testing (SAST) at CI/CD stage.
  - Provide out-of-the-box two-factors-authentication (2FA).
  - oAuth service-to-service authentication.
  - Service-to-service TLS encryption.
  - Provide “service” users.

dalet

Thank you.