Infrastructure and Security Standards

> **Disclaimer**: The information contained herein reflects the infrastructure and security standards in effect at the time of publication. Such standards are subject to change without prior notice in order to comply with evolving legal, regulatory, and security requirements. Accordingly, this documentation may be modified or updated at any time.

Infrastructure

Cloud Architecture

The Forma Cloud service is delivered through a modern, resilient, and fully managed cloud infrastructure built on Amazon Web Services (AWS). The platform is deployed in AWS data centers located within the European Union (Ireland), with optional database mirroring available in Italy when required.

- Our **application layer** runs on a Kubernetes-based architecture designed for high availability and elastic scalability. Workloads are distributed across multiple nodes that automatically scale up or down in response to real-time demand, ensuring consistent performance even during peak usage. All traffic is routed through AWS Global Accelerator to optimize connectivity and reduce latency for users worldwide.
- The entire environment is secured within an **isolated Virtual Private Cloud (VPC)**, complemented by an AWS Web Application Firewall (WAF) that provides protection from common web threats such as SQL injection, cross-site scripting, and denial-of-service attempts.
- **Load balancing** mechanisms ensure even distribution of application requests across all active nodes. Two static IPs are exposed.
- Persistent data is stored in an **encrypted Aurora MySQL (RDS) cluster** in Multi-AZ configuration that provides automatic failover, multi-node read scalability.
- Application files are maintained in a durable and automatically scalable **Amazon EFS shared file system**, while Redis/Valkey is used as an in-memory datastore for session management and caching.
- The entire infrastructure is provisioned and managed through **Terraform**, following Infrastructure-as-Code (IaC) principles. This ensures repeatable deployments, strict

version control, and a consistent configuration across environments.
- **Continuous monitoring**, automated alerting, backup procedures, and business continuity measures support the reliability of the service and help maintain guaranteed availability levels.

Physical Security

The Forma Cloud Services relies on AWS who is responsible, in accordance with the AWS Shared Responsibility Model (available at https://aws.amazon.com/compliance/shared-responsibility-model), for implementing controls for the physical security of data center facilities, backup media, and other physical systems, providing comprehensive and state-of-the-art security capabilities (available at https://aws.amazon.com/compliance/data-center/controls).

Information Protection and Security Standards

Backup

Infrastructure

- **Hosting**: Amazon Web Services (AWS) - Region eu-west-1 (Ireland, EU)
- **Database**: Amazon Aurora MySQL in Multi-AZ cluster configuration
- **Backup Management**: AWS Backup (AWS managed service)

Backup Policies

- **Daily Backup** (DailyBackups)
  - Automatically runs at 5:00 AM UTC
  - Retention: 7 days (1 week)
  - Managed by AWS Backup plan
- **Weekly Backup** (WeeklyBackups)
  - Automatically runs on Saturdays at 5:00 AM UTC
  - Retention: 4 months (120 days)
  - Managed by AWS Backup Long-term plan
- **Monthly Backup** (MonthlyBackups)
  - Automatically runs on the first Saturday of the month at 5:00 AM UTC
  - Retention: 12 months (365 days)
  - Managed by AWS Backup Long-term plan
- **EFS Automatic Backup**

    - Automatically runs daily at 5:00 AM UTC
    - Retention: 2 weeks (14 days)
    - Managed via aws/efs/automatic-backup-rule
    - Cross-region copy to a dedicated backup vault in AWS eu-central-1 (Frankfurt, Germany), retention 14 days

Backup Status

- Last 30 daily backups: all completed successfully
- Active monitoring system with automatic failure notifications
- 58 Aurora snapshots available for the database cluster
- 180+ total recovery points available on AWS Backup (database)
- 30+ recovery points available on AWS Backup (EFS file system)

Access Control

- Backup access limited via specific IAM roles
- MFA required for critical operations
- Service Role: AWSBackupDefaultServiceRole with minimal permissions
- Full audit trail on AWS CloudTrail

Data Storage, Localization and Segregation

Geographic Location

- Primary Location: AWS eu-west-1 (Dublin, Ireland)
- Secondary backup location (disaster recovery): AWS eu-central-1 (Frankfurt, Germany)
- All data and backups remain within the European Union (GDPR compliant)
- No data transfer outside the EU

Redundancy

- Multi-AZ Architecture (3 independent Availability Zones)
- Backups are automatically replicated across multiple AZs
- Storage: AWS EFS and Amazon Aurora with synchronous replication

Backup Vault

- Dedicated vault with automated lifecycle management
- AWS default vault for Aurora snapshots
- Access controlled via IAM roles with the least privilege principle

- Immutable backups: backup vaults are protected by AWS Backup Vault Lock (WORM) in compliance mode. Recovery points cannot be modified or deleted before the end of their retention period, not even by privileged accounts, mitigating the risk of ransomware attacks and malicious or accidental deletion

Data Segregation

Forma Cloud implements logical tenant isolation across application, storage, and database layers.

- Each customer deployment is hosted as a dedicated project within the Kubernetes cluster.
- Each deployment is connected to customer-specific storage paths used to segregate application files.
- Customer data is stored using separate databases, database users, and credentials for each customer project.
- Application-level authorization controls and tenant-aware configuration prevent unauthorized cross-tenant access.
- Administrative access to production data is restricted to authorized personnel and subject to logging and monitoring.

Data Deletion and Disposal

Customer data is deleted or rendered inaccessible through controlled procedures aligned with AWS storage lifecycle and secure deletion mechanisms. Backup data is retained according to the applicable backup retention schedule and subsequently managed according to AWS service policies.

Post-contract retention and final deletion timelines are governed by the applicable contractual documentation and legal requirements.

Data Encryption

Encryption at Rest

- Algorithm: AES-256 via AWS Key Management Service (KMS)
- Encryption enabled by default on all Aurora databases
- Snapshots automatically encrypted with the same key as the source database
- Key rotation: encryption keys are managed in AWS KMS and automatically rotated every 365 days
- Key scope: a single platform-level encryption key is used for each service (database, file storage); encryption keys are not segregated per customer. Customer data segregation is enforced at the database, credential and storage-path level (see Data Segregation)
- Backup data encrypted at rest using AWS-native encryption controls

Encryption in Transit

- TLS 1.2+ for all application connections
- Database connections forced over SSL/TLS
- Backup transfer managed internally by AWS over an encrypted private network

TLS Certificates Management

To ensure secure communications, TLS certificates are fully provisioned, deployed, and managed through **AWS Certificate Manager (ACM)**. This integration eliminates manual handling and human error during certificate generation and renewal.

- **Supported Algorithms:** ACM-managed public certificates comply with strict security requirements, supporting robust cryptographic standards including **RSA (2048-bit or higher)** and **ECDSA (P-256 or P-384)**.
- **Automated Lifecycle Management:** Public certificates issued directly by ACM have a standard validity period of **198 days**. ACM monitors and automatically initiates the renewal process well before the expiration date. This automated lifecycle guarantees that the 2-year maximum lifecycle limit for asymmetric certificates is consistently met without service interruption.
- **Imported Certificates:** Any third-party or custom certificates imported into ACM do not benefit from automated AWS renewal. These specific assets follow a dedicated, documented operational workflow for manual renewal and re-importation prior to their expiration.
- **Symmetric Secrets and Application Credentials:** Symmetric encryption keys, application-level credentials, and environment secrets are out of scope for ACM. They are managed and documented separately under explicit access control and rotation policies.

Monitoring & Uptime

The infrastructure is equipped with the following service monitoring procedures and mechanisms:

- **Server log**: All accesses and errors are logged on individual server machines (frontend and database) and the load balancer (aggregated across all machines connected to the service).
- **Email pre-alerts** when peak thresholds are exceeded (CPU usage, number of DB connections).
- **Uptime Robot**: Domain monitoring. If the site is unresponsive, the team is notified via email and internal communication channels (Slack).
- **Automatic application error notification**: Any errors generated by application functionality on the server are notified to the support team.
- **Monitoring and multi-channel alert system**: The difference between available and utilized resources (CPU and RAM) is continuously monitored. When preset thresholds are exceeded, the system triggers autoscaling and communicates the event via various channels to technical staff.

- **AWS CloudWatch**: AWS-native monitoring and logging services are used for managed infrastructure components where applicable.
- **Log retention**: Retention periods and storage destinations are defined according to the configuration applied to each service component and may vary depending on operational and compliance requirements.

Uptime SLA

Metric	Value	Note
Granted Uptime	99,9%	Excluding scheduled maintenance events

Disaster Recovery

Data RPO (Recovery Point Objective): 5 minutes

- Database: Aurora maintains continuous incremental backups every 5 minutes for point-in-time recovery
- Maximum database data loss is limited to the last 5 minutes of operation
- Point-in-time restore available with second-level granularity

Filesystem RPO (Recovery Point Objective): 24 hours

- File System: 24 hours (automatic daily backups via AWS Backup)
- Maximum filesystem data loss is limited to the last 24 hours of operation

Data RTO (Recovery Time Objective): 72 hours

- Contractually guaranteed time for complete recovery in a full disaster recovery scenario
- Includes: database restore, instance startup, application integrity check

Disaster Recovery Assessment

Disaster recovery procedures are tested on an annual basis to ensure business continuity and validate the reliability of restoration procedures. These tests include restoring database snapshots to a temporary test environment, validating successful system recovery, and verifying data integrity.

The recovery assessment includes a full database restore, startup of a temporary Aurora test cluster, application connectivity checks, execution of queries on critical tables, and data consistency validation. These controls confirm that systems can be effectively recovered in the event of a failure and that the declared RTO/RPO objectives are supported by operational recovery procedures.

Last test performed

- Date: October 10, 2025
- Procedure: Aurora snapshot restore on a temporary test cluster
- Outcome: Positive - database restored successfully, data integrity verified

Verification steps performed

- Full database restore from snapshot
- Aurora test cluster startup
- Application connectivity verification
- Query testing on critical tables
- Data consistency check

Remote Administrative Access

Remote administrative access to systems processing customer data is restricted to authorized personnel only, protected by multi-factor authentication and conducted over encrypted channels.

- Database administrative access is performed through protected connectivity.
- Access to file storage resources is performed through controlled administrative channels.
- Administrative activities are logged and subject to monitoring and access review.

Secure SDLC and Change Management

FormaFarm applies a controlled software delivery lifecycle designed to govern software development, configuration, maintenance, and production changes.

- Development, test, staging, and production environments are separated.
- Code changes are subject to review before release.
- Testing is required before deployment to production.
- Secure coding practices are applied in line with recognized web application security principles.
- Significant production changes are documented and include rollback considerations.

Incident Management

FormaFarm maintains procedures for the identification, escalation, containment, resolution, and post-event analysis of incidents affecting service continuity, confidentiality, integrity, or availability of customer data.

Confirmed security breaches are notified without undue delay in accordance with applicable contractual commitments and legal requirements.

Vulnerability Assessment and Penetration Testing (VAPT)

Forma Cloud is subject to periodic Vulnerability Assessment and Penetration Testing (VAPT) activities conducted by qualified third-party security firms. These assessments are carried out in accordance with industry-standard methodologies (e.g., OWASP Testing Guide, PTES) and cover both the application layer and the underlying infrastructure.

VAPT Management Process

- **Periodic assessments**: VAPT activities are performed on a regular basis and upon significant platform changes (major releases, architectural modifications, or new integrations).
- **Scope**: Assessments cover the full attack surface, including web application interfaces, APIs, authentication flows, session management, and infrastructure-level exposure.
- **Findings management**: All identified vulnerabilities are classified by severity (Critical, High, Medium, Low, Informational) and tracked through a structured remediation workflow. Critical and High severity findings are prioritized for immediate remediation; Medium and Low findings are scheduled within subsequent release cycles.
- **Retesting**: After remediation, affected areas are retested to verify that fixes effectively resolve the identified vulnerabilities without introducing regressions.

Application Security Controls

Multiple layers of security controls are implemented at both infrastructure and application level to proactively mitigate common web vulnerabilities and address findings from VAPT assessments.

Web Application Firewall (WAF)

All incoming traffic passes through an AWS Web Application Firewall (WAF) that provides protection against common attack vectors, including:

- SQL injection (SQLi)
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)
- Denial-of-Service (DoS) attempts
- Malicious bot traffic and request rate abuse

WAF rules are regularly reviewed and updated in response to newly identified threats and VAPT findings.

Where appropriate based on the service profile and operational needs, additional AWS-native security services such as Amazon Inspector, AWS Security Hub, and Amazon GuardDuty may be evaluated or adopted to strengthen vulnerability management, posture monitoring, and threat detection capabilities.

Content Security Policy (CSP)

A comprehensive Content Security Policy is enforced via HTTP response headers at the Nginx reverse proxy level. The CSP configuration is dynamically generated at container startup based on environment variables managed through the deployment infrastructure (factory), enabling per-tenant customization without code changes.

- **Directives enforced**: `default-src`, `script-src`, `style-src`, `img-src`, `font-src`, `frame-src`, and `frame-ancestors` are all explicitly configured to restrict resource loading to authorized origins.
- **Domain whitelisting**: Allowed origins include the tenant's own domain (via wildcard), explicitly configured external domains (identity providers, CDN services, embedded content providers such as YouTube and Vimeo), and a curated set of common third-party service domains.
- **Frame embedding control**: The `frame-ancestors` directive restricts which domains may embed the application in iframes, preventing clickjacking attacks. Additional domains can be allowed on a per-tenant basis through dedicated configuration variables.
- **Extensibility**: Tenant-specific CSP requirements (e.g., additional trusted domains for SSO integrations or embedded content) are supported through environment-level configuration, applied without redeployment.
- **Header size management**: An automated optimization pipeline deduplicates, consolidates, and groups CSP domains to ensure compliance with the Nginx maximum header size limit (8 KB). When the combined policy exceeds the limit, directives are automatically split across multiple header entries.

HTTP Security Headers

In addition to CSP, the following security headers are enforced on all responses:

Header	Value	Purpose
`Strict-Transport-Security`	`max-age=31536000`	Enforces HTTPS connections for one year (HSTS)
`X-Content-Type-Options`	`nosniff`	Prevents MIME-type sniffing attacks
`Referrer-Policy`	`strict-origin-when-cross-origin`	Limits referrer information leakage
`Permissions-Policy`	Restrictive policy disabling geolocation, camera, microphone, payment, etc.	Reduces the browser API attack surface

Server Fingerprint Mitigation

Server identification headers are actively suppressed to reduce the information available during reconnaissance:

- Nginx version disclosure is disabled (`server_tokens off`)
- The `Server` and `X-Powered-By` response headers are removed
- PHP version exposure is disabled (`expose_php = Off`)

Sensitive File Protection

The web server is configured to deny access to files and paths that should never be publicly accessible, including:

- Hidden files and directories (e.g., `.git`, `.env`)
- Dependency management files (`composer.json`, `composer.lock`, `package.json`)
- Development and build configuration files (`Makefile`, `phpunit.xml`, `phpcs.xml`)
- Backup and log files (`.bak`, `.backup`, `.sql`, `.log`)
- Server-side scripting files (CGI, Perl)

These rules are enforced at the Nginx level, ensuring that even in case of misconfigurations or accidental file placement, sensitive content is not served to external clients.

Session Security

Session management is hardened through multiple mechanisms:

- **Secure cookies**: Session cookies are marked as `HttpOnly` and `Secure` (when served over HTTPS), preventing client-side script access and transmission over unencrypted channels. In HTTPS environments, cookies use the `__Secure-` prefix for additional browser-enforced protection.
- **SameSite cookie policy**: The `SameSite` attribute is configurable on a per-domain basis, supporting `Strict`, `Lax`, and `None` values. This enables fine-grained control over cross-origin cookie behavior, which is essential for SSO integrations (SAML, OAuth) and iframe embedding scenarios.
- **Distributed session storage**: Sessions are stored in Redis/Valkey for high-availability clusters, ensuring consistent session state across all application nodes with configurable prefix isolation per tenant.
- **Configurable session lifetime**: Session TTL is configurable (default: 2 hours), with automatic expiration and garbage collection.

Brute-Force Protection

The platform includes application-level protection against brute-force login attacks:

- **Configurable attempt threshold**: Administrators can set the maximum number of allowed login failures before triggering a temporary account lockout.

- **Timed lockout**: After exceeding the threshold, further login attempts are temporarily blocked. The lockout duration is configurable and the remaining wait time is communicated to the user.
- **Audit logging**: Failed login attempts are logged with configurable granularity (all failures, only after threshold, or disabled), capturing username, timestamp, attempt count, and source IP address for forensic analysis and compliance reporting.

Revision #33
Created 2025-06-28 06:06:42 UTC by Alberto Pastorelli
Updated 2026-10-28 16:58:39 UTC by Alessandro Affronto