



Cloud Security

O V E R V I E W



Data Management

REDUNDANCY

NewStore is architected to have multiple layers of redundancy using best industry practices. Multiple database and application servers with automatic auto-scaling and failover capabilities provide a high-level of redundancy.

- Usage of Amazon Web Services as PaaS.
- Application of “[well-architected principles](#)” recommended by Amazon Web Services.
- Usage of auto-scaling technology, which allows to spin up automatically servers in case of failure.

DISASTER RECOVERY

Data is backed up and automatically replicated to a separate AWS account, which is used only for emergency or disaster recovery. In the very rare event that the main AWS instances fail and fail-safe controls are not available due to underlying hardware or other extreme circumstances, NewStore is able to use the separate backup account and recreate an entire environment following the internal Disaster Recovery Plan (DRP).

Our Recovery Point Objective (RPO) is less than 5 minutes. Our Recovery Time Objective (RTO), depending on the specific scenario, is between less than 1 minute and up to 12 hours for major disasters involving entire AWS zones or accounts not available.

NewStore geographically distributed operations also guarantee that there is suitable personnel available in two countries, which allow us to continue operations in the case of force majeure events.

- Documented practices in disaster recovery.
- Formal risk assessments for different disaster scenarios using the risk assessment defined by ISO 27001:2013.
- Combination of snapshots and continuous recording which brings RPO to less than 5 minutes and in some cases close to zero.

SCALABILITY

NewStore uses the maximum availability provided by Amazon Web Services, the leader of public cloud solutions around the world. Our systems are architected to be scalable from the design phase with multiple automatic systems that spin up new instances as required by loads. AWS Elastic Load Balancer (ELB) also distribute server loads automatically across different instances.

- Auto-scaling technology for spinning-up new servers as required.
- Mandatory and comprehensive load testings before deploying into production.

Application Security

ENCRYPTION

Access to NewStore APIs and applications is only through encrypted TLS communications. Data at rest containing Personally Identifiable Information (PII) or other sensitive information is automatically encrypted with industry-standard protocols.

- Secure AES256 symmetric encryption with managed KMS provided by AWS.
- Encryption of data volumes where sensitive information is stored.
- Data encryption at the disk level.
- Data in transit is only accessible via TLS with a strong 2048-bit key. Our APIs are ranked “A” in the [Qualys SSL Labs test](#).
- Implementation of Forward Secrecy in TLS connections.
- Application passwords securely hashed and salted using Bcrypt algorithm managed by Auth0. NewStore has no access to clear-text passwords.

SECURE LOGIN

NewStore applications and APIs are secured via secure open protocols based in secure tokens, which minimises the impact of credentials being intercepted. Our secure application authentication provider, Auth0, is certified with SOC2, ISO27001, among others industry certifications.

- Mandatory 2FA for accessing AWS.
- Mandatory 2FA in all third-parties where is available.
- Secure OAuth2 authentication system available for our APIs (token-based authentication).

ROBUST PASSWORD POLICIES

Password policies for applications are configured to the highest level of entropy available by our third party. There are automatic anomaly detection and anti-brute force capabilities in place.

- Strong password policies in applications via Auth0 using OWASP recommendations.
- Strong password policies in our AWS platform as recommended by AWS Best Practices.

SECURE DEVELOPMENT

NewStore implements Secure Development Lifecycles (SDLC) which provides a more secure platform from the engineering phase. Developers are required to apply industry-standard best practices when planning, developing, testing and deploying code.

- Usage of [BlackDuck software](#) to scan all our codebase for security issues.
- Mandatory peer review of any code produced.
- Stage separation of development environments (development, sandbox, production, etcetera).
- Established processes to deploy code.

Operational Security

CONTINUOUS MONITORING

NewStore Cloud uses a number of third-party systems for continuous security monitoring with automatic alerting capabilities. Our Intrusion Detection System (IDS) alerts of any suspicious activity.

- Continuous monitoring of suspicious activities in the platform.
- Daily vulnerability assessment on the platform.
- Weekly vulnerability assessment on web applications.
- Daily evaluation of AWS secure configuration to ensure there is a minimum of 90% compliance with AWS Best Practices.
- Real-time alerting of any production issues in the platform.

SEPARATION OF DUTIES AND RBAC

Access to the cloud infrastructure is done on the basis of separation of duties and need-to-know. Using robust access policies NewStore has implemented a Role-Based Access Control (RBAC) system, which limits employee access to production environments. In addition, 2FA is mandatory for all development and production stages.

- RBAC in all AWS stages, including development stages.
- Minimum access of NewStore personnel to the platform.
- Recent implementation of a zero-trust access to the platform through [Lumin8.io](https://lumin8.io) implementing a very granular and fully traceable access control.
- Monitored emergency access to the platform through OpenVPN as a backup.

DEDICATED SECURITY TEAM

NewStore employs dedicated personnel to look after security in coordination with cloud infrastructure specialists and with AWS support.

- Company-wide security and privacy policies.
- Allocation of a training budget to keep personnel up to date.
- Internal security awareness initiatives.
- External Data Protection Officer, specialized in legal and technical aspects of GDPR.

Performance

SCALABLE ARCHITECTURE

The microservices architecture, upon which NewStore is built, allows for a high-performing cloud application with multiple caching and performance optimization techniques.

- Complete implementation of a microservices architecture for performance and threat containing.
- Advanced caching and load balancing techniques minimizing latency even in the event of server failure.
- Usage of containers

PERFORMANCE MONITORING

Hardware and software performance are monitored 24/7 using automatic tools with immediate alerts to our Infrastructure Team. NewStore also has continuous on-duty agents who can respond within the hour to any performance issues.

- Automatic alerts of performance issues with defined escalation paths.
- On-duty agents around the clock to respond immediately to performance incidents.
- Comprehensive logging of all events around the infrastructure.

Availability

SERVICE LEVEL COMMITMENT

NewStore is built on top of AWS world-class infrastructure, which provides an extremely high availability across services.

HIGH AVAILABILITY ARCHITECTURE

Architecture patterns that include multiple application and infrastructure layers provide NewStore with a highly available architecture, which can overcome most common infrastructure issues. The API is also behind load balances and AWS application firewalls that filter out most DDoS attacks.

- Automatic throttling, blocking and unblocking on our APIs to counteract application-level Denial-of-Service attacks.
- Usage of [AWS Shield](#) to deflect low-level Distributed Denial-of-Service attacks.

HIGH-AVAILABILITY PHYSICAL INFRASTRUCTURE

The underlying physical infrastructure provided by AWS is managed by Amazon and provides a high level of data durability and availability in general by providing multiple redundancies and physical failovers, including backup generators and alternative data centers locations within the region.

- AWS guarantee of physical performance of infrastructure.
- High data durability.