CLARISYNC

SECURITY OVERVIEW

Security at Clarisync

Protecting the Technology Behind Your Operations

OVERVIEW

Security at Clarisync

Protecting the Technology Behind Your Operations

Security is built into how Clarisync designs, develops and operates its technology. From application architecture and cloud infrastructure to software releases and day-to-day operations, security considerations are integrated into the way our platform is managed.

Our approach focuses on protecting customer environments, maintaining controlled access, identifying potential threats and ensuring that security remains an ongoing part of our engineering and operational practices.

01

Security by Design

Security is considered throughout the platform lifecycle, not treated as a separate layer added after development.

Secure Architecture	Our platform is designed with controlled service access, isolated environments and defined communication paths between application components.
Infrastructure Protection	Cloud resources are deployed within controlled network environments, with security configurations governing access to applications, databases and supporting services.
Application Security	Security considerations are incorporated into application design, development, testing and deployment.
Environment Separation	Development, staging, user acceptance testing and production environments are maintained separately to control changes and protect live operations.

02

Cloud & Infrastructure Security

Clarisync operates its platform on Amazon Web Services (AWS), using cloud infrastructure and security capabilities to support controlled, reliable and secure service delivery.

Our infrastructure security practices include:

Network Security	Network segmentation, controlled inbound and outbound traffic, firewall policies and restricted administrative connectivity.
Perimeter Protection	Web Application Firewall (WAF) capabilities help protect application endpoints against common web-based threats.
Infrastructure Hardening	Cloud resources are configured and reviewed to reduce unnecessary exposure and limit potential attack surfaces.
Administrative Access	Access to infrastructure management services is restricted to authorized personnel through controlled authentication and permissions.
Security Configuration Monitoring	Infrastructure configurations and security findings are monitored to identify potential weaknesses and deviations.

03

Application & Platform Security

Our engineering practices focus on maintaining the integrity, reliability and security of the Clarisync application.

API Security	Application interfaces use authenticated access and controlled authorization to protect services and data exchanges.
Input Validation	Application requests and submitted data are validated to reduce the risk of unauthorized or unintended operations.
Session Management	Authentication and session controls help protect access to application functionality.
Activity Logging	Relevant application activities are recorded to support operational visibility, traceability and investigation.
Controlled Integrations	External system integrations use defined interfaces and authorized communication mechanisms.

04

Secure Engineering & Deployment

Security is incorporated into our software engineering and release processes to ensure that application changes are developed, reviewed and deployed in a controlled manner.

Version Control	Source code and development changes are maintained through controlled repositories.
Peer Code Review	Code changes undergo review before being approved for integration.
Automated Build & Deployment	CI/CD workflows support controlled builds, testing and deployment activities.
Release Validation	Changes are validated in non-production environments before being promoted to production.
Controlled Configuration	Application configurations, credentials and deployment settings are managed through controlled mechanisms.

05

Continuous Security Visibility

Maintaining visibility across our technology environment is essential to identifying potential security concerns.

Clarisync uses infrastructure and monitoring capabilities to provide visibility into system activity, security findings and operational events.

Our monitoring practices cover:

- Cloud infrastructure security findings and configuration risks.
- Application, server and network performance indicators.
- System and API activity logs.
- Unusual activity and potential security events.
- Infrastructure health and service availability indicators.

Security findings and alerts are reviewed to support timely investigation and appropriate action.

06

Managing Security Events

Clarisync follows an established approach to handling security-related events and potential threats.

Our operational response focuses on:

01 Identifying and assessing potential security events.

02 Determining the affected systems and potential impact.

03 Applying appropriate containment and corrective actions.

04 Investigating relevant logs and activity records.

05 Restoring affected services where required.

06 Reviewing findings and identifying opportunities for improvement.

This approach helps ensure that security events are handled systematically, with appropriate technical and operational involvement.

07

Security as an Ongoing Commitment

Technology and security threats continue to evolve. We therefore treat security as an ongoing responsibility across our engineering, infrastructure and operational teams.

Through continuous monitoring, controlled engineering practices, infrastructure reviews and improvements to our security capabilities, we work to maintain the protection and integrity of the Clarisync platform.

Talk to Our Security Team

For technical security enquiries, platform architecture discussions or questions about our security practices, please contact our team.