Diasorin

Diasorin Cloud for LIAISON NES®

Cybersecurity

Secure by design

Cybersecurity

Approach

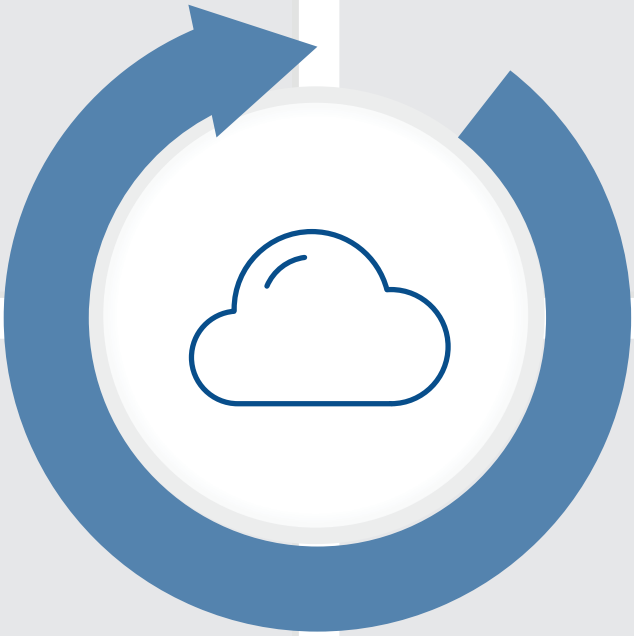
Diasorin approaches cybersecurity as a continuous, proactive discipline. The Diasorin Cloud integrates security into every phase of development, from initial concept through planning, development, testing, deployment, and maintenance.

PLANNING

Diasorin maintains a comprehensive Risk Management Plan that guides security oversight throughout the development lifecycle. This includes threat modeling to proactively identify and address potential risks through secure product design.

DEVELOPMENT

Development activities occur in an environment that is separated from customer data to prevent any impact on live systems.



DEPLOYMENT

Released software is monitored continuously for vulnerabilities and threats using Microsoft Defender, with timely updates applied as new risks emerge.

TESTING

Prior to each release, thorough Vulnerability Assessments and Penetration Testing are conducted to identify and evaluate potential security risks. Any findings are addressed before deployment to help ensure the integrity and security of the solution.

Securely Connected Ecosystem

LIAISON NES® Security

Access Controls
- Login credentials with Username, Password, and configurable timeouts

User Authentication
- Different permissions for administrators vs. operators

Data Storage Protections
- Data encrypted on devices at rest

Security Oversight
- External vulnerability assessments as part of development.
- Risk Assessments are performed prior to each release

Diasorin Cloud Security

Access Controls
- Multi-factor authentication with role-based permissions and automatic timeouts

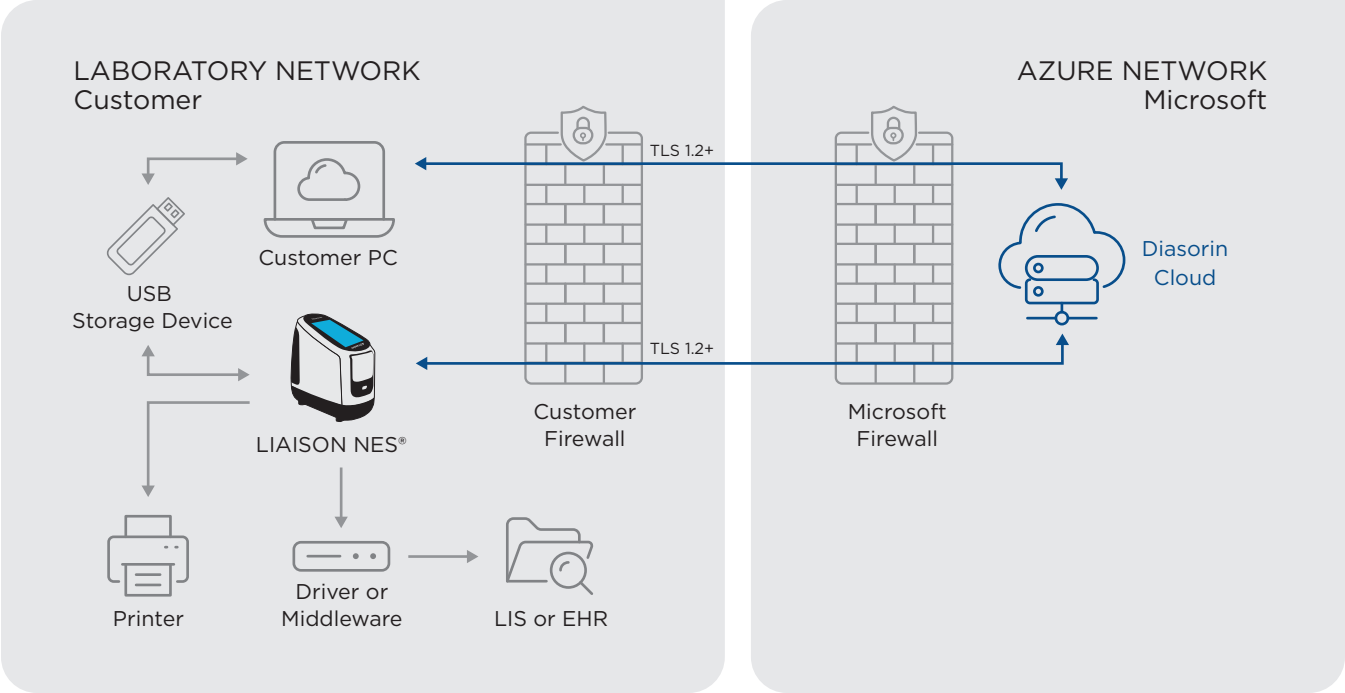
Data Storage Protections
- Data encrypted on Azure servers at rest

Connectivity Controls
- Ability to remotely manage device connectivity and user access

Security Oversight
- External vulnerability assessments as part of development.
- Risk Assessments are performed prior to each release
- Continuous threat monitoring of cloud resources provided by Microsoft Defender

Secure Data Transfer

Data transmitted between Diasorin Cloud servers and LIAISON NES® devices is protected using Transport Layer Security (TLS) version 1.2 or higher to help ensure secure and encrypted communication.



Diasorin Cloud Cybersecurity Feature Details

	Feature
Microsoft Access Controls & User Authentication	Multi-factor authentication via Azure AD B2C
	Role-based access control with defined permission levels determined by laboratory
	Automatic session timeout after inactivity
	User oversight and management with automatic disablement of inactive users
Data Transfer Protections	Data is encrypted in transit from instrument to servers and from servers to the user interface using Transport Layer Security (TLS) of 1.2 or higher
	Administrative oversight to enable or disable device communication to prevent data transfer
	Device software updates delivered via controlled deployment with MD5 checksum verification and status tracking
Data Storage Protections & Architecture Resilience	Data is encrypted at rest on Azure servers managed with unique database encryption keys
	System follows Azure's geo-redundant backup and disaster recovery policies
Security Oversight	Logging of actions managed via Azure Log Analytics and Microsoft Defender
	Vulnerability assessments and penetration testing are integrated into the development process and performed by external companies
	Risk assessments are performed prior to each release
Legal Oversight & Compliance Alignment	Legal and privacy acknowledgements provided to users at initial login
	Compliant with HIPAA and GDPR privacy frameworks
	ISO 27001 Certified Information Security Management System

Privacy Commitment

The Diasorin Cloud uses a secure-by-design approach to receive and process only anonymized diagnostic system data generated by instruments operated in accordance with their respective User Manuals. This approach ensures the Diasorin Cloud does not access, transmit, or store patient-identifiable or protected health information. Diasorin Cloud ensures compliance with applicable privacy regulations, including US HIPAA and EU GDPR requirements.

We are committed to protecting the confidentiality of all personal data relating to customers, partners, employees, and stakeholders. Diasorin maintains ISO 27001 certification at the company level, providing independent assurance that our information security management system is structured, risk-based, and aligned with internationally recognized standards.

Diasorin

Cypress, CA

p: 800 838 4548
w: diasorin.com
e: ts.cloud@diasorin.com

diasorin.com/liaison-nes

BR1156250.US.0326