Novorender AS
Vestre Svanholmen 12
4313 sandnes
info@novorender.com

Microsoft Partner

Novorender is a proud Microsoft Certified Partner (MCP), meaning that we have passed a number of rigorous tests and proven our skills within the Microsoft Domain. Microsoft have considered us to be an official MCP as we work effectively and help customers within specific products and services.

Contents

Security

Novorender uses the Azure cloud platform, where security is integrated into every aspect of the services provided. We chose Azure because Microsoft invests more than USD 1 billion on cybersecurity research and development every year, with more than 3,500 security experts dedicated to data security and privacy. Furthermore, Azure has more certifications than any other cloud provider.

Through Azure, the Novorender portfolio is able to offer you unique security advantages derived from global security intelligence, sophisticated customer-facing controls, and a secure hardened infrastructure. This powerful combination helps protect your applications and data, support your compliance efforts, and provide cost-effective security. As Novorender relies on the Microsoft Azures platform, this document will highlight some of the key aspects below. For more information and the latest updates, please refer to Azure Security Documentation and the Windows Azure - Security Privacy Compliance white paper.

High Availability

As Novorender is delivered as a cloud related service, a key aspect of our resilient foundation is availability. At Novorender, we consider High Availability as maintaining acceptable continuous performance despite temporary failures in services, hardware, or data centers, or fluctuations in load. Highly available systems are consistently operational over long periods of time.

Geo-redundant Storage

Azure Storage always stores multiple copies of your data so that it is protected from planned and unplanned events, including transient hardware failures, network or power outages, and massive natural disasters. Redundancy ensures that your storage account meets its availability and durability targets even in the face of failures. At Novorender, we always provide Geo-redundant storage (GRS) copies of your data, which synchronously copies everything three times within a single physical location in the primary region using LRS. It then copies your data asynchronously to a single physical location in the secondary region. Azure guarantees that at least 99.9% (99% for Cool Access Tier) of the time, they will successfully

process requests to read data from Redundant Storage (GRS) Accounts. For more information, please refer to Azure Storage Redundancy and SLA for Storage Accounts.

Encryption at rest

At Novorender, we offer Encryption at rest, providing data protection for stored data (at rest). Attacks against data at-rest include attempts to obtain physical access to the hardware on which the data is stored, and then compromise the contained data. Encryption at rest is designed to prevent the attacker from accessing the unencrypted data by ensuring the data is encrypted when on disk. If an attacker obtains a hard drive with encrypted data but not the encryption keys, the attacker must get past the encryption to read the data. This attack is much more complex and resource consuming than accessing unencrypted data on a hard drive. For this reason, encryption at rest is highly recommended and is a high priority requirement for many organizations.

For more information, please refer to Azure Data Encryption at rest.

Encryption in transit

For more information, please refer to Azure data security and encryption best practices.

Login

Active Directory

Novorender allows you to use Active Directory to give employees, partners, customers, or anyone else access based on their access rights within your organization. Azure Active Directory is a comprehensive identity and access management solution in the cloud. It combines core directory services, advanced identity governance, security, and application access management. Azure AD makes it easy for your developers to build policy-based identity management into the Novorender applications.

Active Directory MFA

Enhance the security and convenience of your data by requiring an additional layer of security when accessing Novorender. In Novorender it is possible to enable Microsoft Azure Multi-Factor Authentication which reduces organizational risk and helps enable regulatory

compliance by providing an extra layer of authentication, in addition to a user's account credentials, to secure employee, customer, and partner access. You can choose from call, text, or mobile app during registration. End users can change their method anytime.

Sharing

Active Directory

See chapter “Login - Active Directory” above

Generate Viewer Scene

A model can be shared by using the “Generate Viewer Scene” option. It can be distributed either by requiring the viewer to authenticate with a user login, or simply by allowing access based on URL availability.

Microsoft Teams

A model can be shared directly in Microsoft Teams. Give access to anyone who is a member of your team where the model is located.