mx mendix

Security for Cloud and On-Premises Deployment

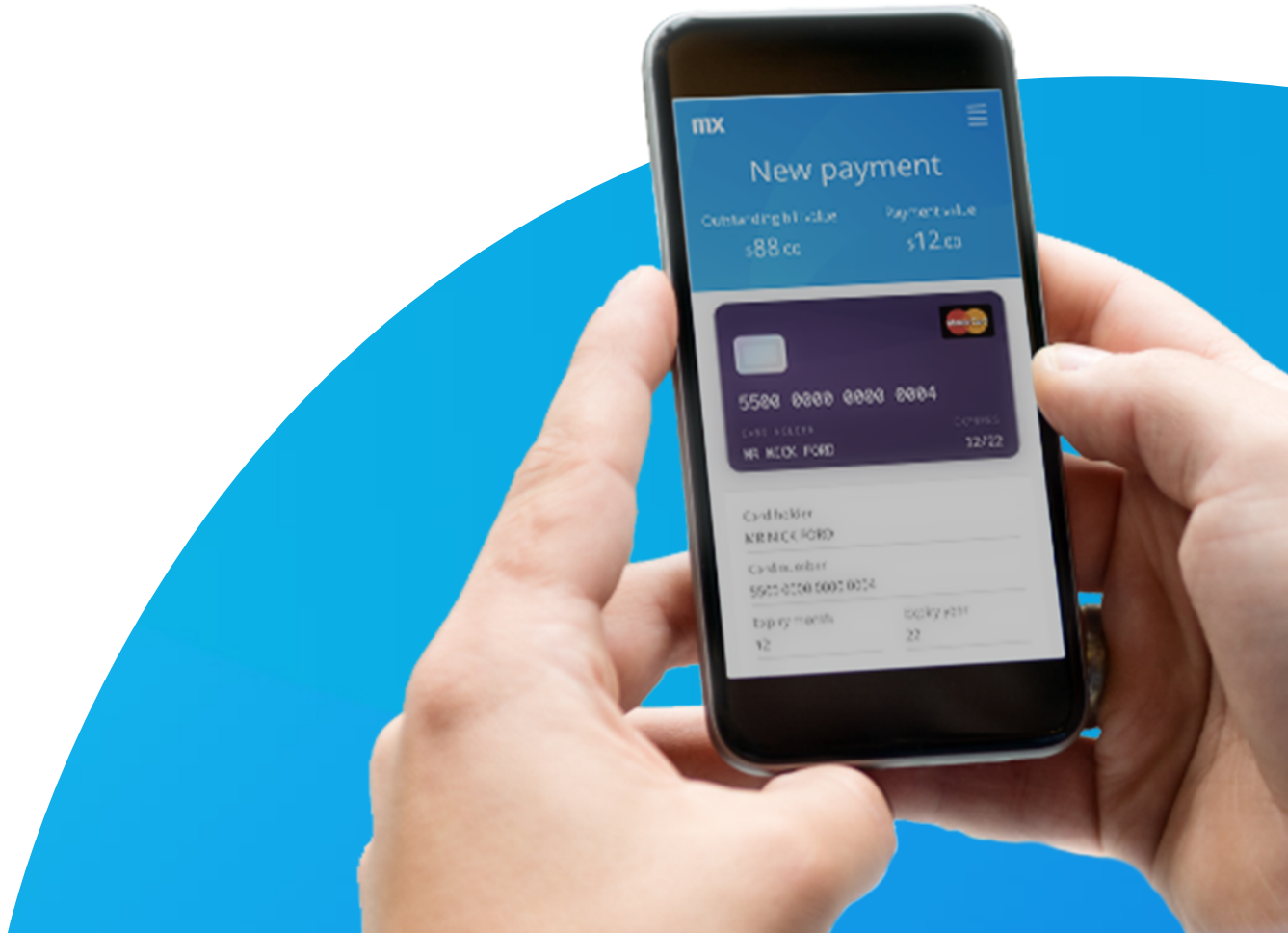

Table of Contents

Executive Summary

Mendix offers an industry-leading high-productivity application Platform-as-a-Service

for organizations to build web and mobile applications. Being a platform provider, it is of utmost importance to ensure that the platform itself, the applications built on the platform and the cloud operations to run the platform meet the highest security standards. The Mendix Platform contains a runtime environment including the Mendix Runtime, and a set of components to design, develop, deploy and manage apps. In addition, the platform offers governance services like Mendix ID for identity & access management and services to manage the environments on which the apps run.

Security ensured for cloud and on-premises deployment

Mendix offers the platform as a service in the cloud, but also supports on-premises deployments with the same product. Security measures in the Mendix Platform and for development of apps are equal. The difference is that for on-premises deployments, the customer is responsible for implementing the recommended deployment architecture and security-related platform and application administration activities.

Enterprise-ready security

The Mendix Platform meets enterprise-level requirements for security and addresses security measures on multiple levels of granularity, including multi-tenancy aspects:

- The Mendix Runtime handles known security threats
- The Mendix Modeler supports application security settings to define roles and authorizations
- Mendix ID supports identity & access management. Mendix can also integrate with third-party identity management solutions.
- The Mendix Cloud Portal supports app management, deployment and monitoring.
- Mendix complies to SAP security and compliance requirements as Mendix is an SAP Solution Extension partner.

Application lifecycle logging

The Mendix Platform logs relevant activities during the app delivery cycle, from requirements management, to development, deployment and application monitoring to ensure compliance with customers' requirements for auditability.

Mendix cloud deployment and containment of environments

The Mendix Platform deployment architecture is based on Cloud Foundry. Cloud Foundry is the industry-standard cloud application platform which is used by SAP, IBM, Pivotal, and GE, among others. Cloud Foundry logically separates Mendix applications using containers, that includes an (optional) Test, Acceptance and Production environment, each running in their own App Environment. This App Environment also includes firewall-, web server- and database services. The purpose of an App Environment is to contain the behavior and consumption of an environment, shielding other environments (and apps) from each other.

Backup and disaster recovery

All data (model, database and file storage) is automatically backed up, on a daily basis as a minimum. For enterprise applications, data replication and real-time backups are in place. Backups are stored in secure, geographically dispersed locations. Mendix offers disaster recovery services that include high availability across multiple availability zones, horizontal scaling of App Environments and auto recovery in the event of an unexpected outage. Additionally, a fallback environment can be made available which delivers data replication and real-time backups allowing companies to resume operations from a different physical location.

Organization-level security measures

Mendix, as an organization, embeds security in company processes by adopting a representative subset of Annex A controls from the ISO/IEC 27001:2013 Information Security Management System standard. Mendix has achieved ISAE 3402 Type II and SOC 1 Type II assurance reports, and is ISO/IEC 27001:2013 certified with 113 Annex A controls in scope. In addition, a CSA star self-assessment is available for customers. An independent auditing firm periodically performs security audits. Furthermore, a leading IT security firm performs penetration tests on the Mendix Platform on a monthly basis. Penetration tests are based on OWASP and the ISSAF (Information Systems Security Assessment Framework) and OSSTMM (Open Source Security Testing Methodology Manual).

Introduction

This paper addresses the security aspects of Mendix Platform deployments for Mendix Cloud, private cloud and on-premises environments. The scope is restricted to security aspects of the deployment architecture rather than security aspects related to Service Organization Control, and ISO certification audits.

The Mendix Platform

The Mendix Platform is a completely integrated platform to manage the entire software development lifecycle of designing, building, deploying and managing apps. The Mendix Platform contains a runtime environment, the Mendix Business Server and a set of components to design, develop, deploy and manage apps. In addition, the platform offers governance services like Mendix ID for identity & access management and services to manage the environments that the apps are running on.

These components are integrated and connected through the Platform Portal:

- **Projects** – A collaborative environment to manage app development projects
- **Desktop Modeler and Web Modeler** – The modeling environments to build apps using visual models
- **Team Server** – The central repository to manage and version app models
- **App Store** – A marketplace for Apps, AppServices, Widgets and Libraries
- **Cloud Portal** – A portal to deploy, manage and monitor Apps on the Mendix Cloud.

The Projects module, the App Store and the Cloud Portal are built with the Mendix platform itself, so that the security measures of the core platform, implemented in the Mendix Runtime, automatically apply to these components as well. The Team Server is built on top of Subversion (SVN), a proven, secure and widely adopted solution for software versioning and revision control. The Team Server is automatically configured through the Projects module.

The Mendix Runtime is developed in Java and is responsible for the interpretation and execution of models at runtime.

The Mendix Platform, as a whole, is audited for organizational and technical security periodically. In this whitepaper, we will specifically zoom into the following platform components: the Mendix Runtime, Mendix ID, the Desktop Modeler and the Cloud Portal, as these components are most relevant in the context of platform- and application-level security.

Mendix Security at a High Level

Mendix applications are implemented by a large variety of companies to support numerous and varied business processes. All these different Mendix users share the critical need for their applications to be secure and accessible.

Mendix is used by large enterprises and public sector organizations that deal with highly confidential information. For example, justice departments, healthcare organizations, banks and insurance companies rely on Mendix to manage online transactions, store medical, insurance or legal data, enable international financial traffic and regulate other mission-critical processes and information flows.

Mendix Cloud versus Private Cloud versus On-Premises Deployment

Flexible Deployment Options, Depending on Your IT Strategy

Apps developed on the Mendix Platform can be deployed to users in various ways. Whether your company decides to run applications and store data in the Mendix Cloud, private cloud, or to use your own infrastructure depends on your company's strategy, decisions and policies regarding cloud computing. Your choice may be influenced by the nature of the application(s) to be built. In some sectors and countries, it also depends on laws and regulations.

Your choice for the Mendix Cloud, private cloud or on-premises deployment will define who is primarily responsible for the security measures to be put in place. To provide an overview of the security measures that Mendix offers – as an integral part of the platform as well as within the cloud infrastructure – both deployment options are described below.

Mendix Cloud

Mendix Cloud is the infrastructure provided and operated by Mendix to run the Mendix Platform and the applications deployed to the Mendix Cloud. The configuration is standardized, optimized and fully automated. Mendix Cloud facilitates administrators with fast one-click deployment of applications and tools to manage and monitor apps in a very user-friendly way. Besides the standard security measures applied, we offer the possibility to extend the security measures with additional pre-defined services to meet specific customer requirements.

Private cloud

As Mendix uses Cloud Foundry as a deployment platform and is also compatible with Kubernetes, any private cloud like SAP Cloud Platform, IBM Cloud, Microsoft Azure or Pivotal Cloud Foundry can be used to deploy Mendix applications. The security of a private cloud deployment depends on the security measures that are in place within the selected private cloud and your organizational measures.

Mendix On-Premises

Mendix on premises is a local installation of the Mendix Runtime within your own company's infrastructure. The security of on-premises installation depends on the security measures and controls that are in place within your organization's private infrastructure. Mendix has achieved excellent results in realizing optimally secure infrastructure for Mendix applications in cooperation with in-house IT specialists.

Security Measures for Mendix Runtime

This section describes specific security measures that are implemented in the core Mendix Runtime. These measures apply to both deployment in the Mendix Cloud, private cloud and on-premises, as the same runtime architecture is used.

The architecture of the Mendix Runtime consists of three layers:

- UI layer
- Logic layer
- Data layer

The UI layer is implemented in the Mendix Client as JavaScript libraries running in the browser. For hybrid mobile applications, the UI layer runs in a native Cordova container. The Logic and Data layers are implemented in the Mendix Runtime (the Mendix Runtime itself is developed in Java and runs on a JVM). The Mendix Runtime can be deployed either in the Mendix Cloud or on-premises. Figure 1 depicts the Mendix Runtime architecture.

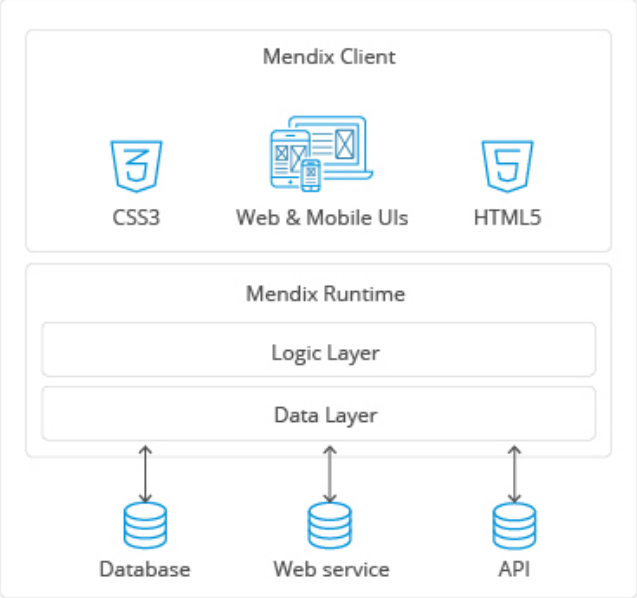

Figure 1. Mendix Runtime Architecture

Within the Mendix Client, measures against JavaScript based security threats such as Cross Site Scripting are implemented. This prevents other websites / web applications running in the same browser from obtaining sensitive information (e.g. cookies). The Mendix Runtime addresses server-side security threats, such as SQL Injection and Code Execution. By default, a request originating from any client (including the Mendix Client) is perceived as untrusted.

Mendix app developers do not need to take these technical security aspects into consideration when building Mendix apps, as the platform handles this as a service. Obviously, this does not mean that developers do not have to consider security at all. Application-level authorization and access rights need to be configured in the application model by the app developer.

Each operation within the Mendix Runtime is called an "action". The Mendix Runtime provides many pre-defined actions, such as triggering and executing workflows, evaluating business rules, etc. To prevent any bypasses of the technical security mechanisms, these actions are implemented on the lowest levels of the Mendix Runtime and can not be changed by app developers.

The core interface of the Runtime - responsible for the execution of any action - has a security matrix that contains all executable actions and data access rules per user role. The data access rules are applied at runtime when a query is sent to the database. This ensures that only data within the boundary of the access rule constraint will be retrieved.

Application Security defined in the Mendix Modeler

Out of the box, the Mendix Platform provides role-based user access to applications built with Mendix. Applications in Mendix consist of one or more modules. A module typically has a functional scope (e.g. items, customers, orders, etc.) and is self-contained so that modules can be re-used in multiple applications. Due to the distinction between applications and modules, security aspects are defined on both levels. Application-level security settings apply to all the modules within the application. Module-level settings are specific to each module.

Application-level security & application model consistency

The Mendix Platform supports configurable integrity checks for security on all relevant aspects of applications deployed on the platform. Mendix checks the consistency of the security settings as well. For example, a person who is allowed to see a certain UI element that lists data from a table must also be authorized to view the data associated with that UI element.

Depending on the stage of development, application and integrity checks can be applied more or less stringently. This is advantageous in development and prototype contexts to avoid unnecessary activities regarding consistency and security in the preproduction stage. Security levels 'Off' and 'Prototype / demo' are only allowed for apps deployed to a development and/or local test environment, not for deployments in production environments. Deployment to the Mendix Cloud (except for Sandboxes) requires the 'Production' security level and complete configuration of all security settings.

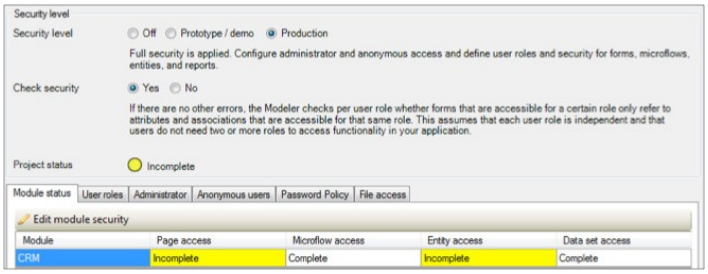

Figure 2. Application project security overview and consistency check

User Roles

An end user of the application is assigned one or more user roles by an administrator or provisioned automatically from a (3rd party) identity & access management solution that can be integrated with an app. The user then gets all access rights that these user roles represent. Within the user role, it is possible to assign user management rights for this particular role as well, so that users assigned to this user role can then manage access rights for other users with selected role(s). This feature is relevant to support a delegated administration concept. Every user role has one or more module roles. Module roles define a role on a module level e.g. "order entry" or "approver". This means that users with that user role have all the access rights that are defined for those module roles. End users of your application only see the user roles and not the module roles. So only user roles can be assigned to an end user, while module roles are assigned to user roles. A user role aggregates multiple access rights on data, pages and microflows (the graphical designer to model logic) from the module roles.

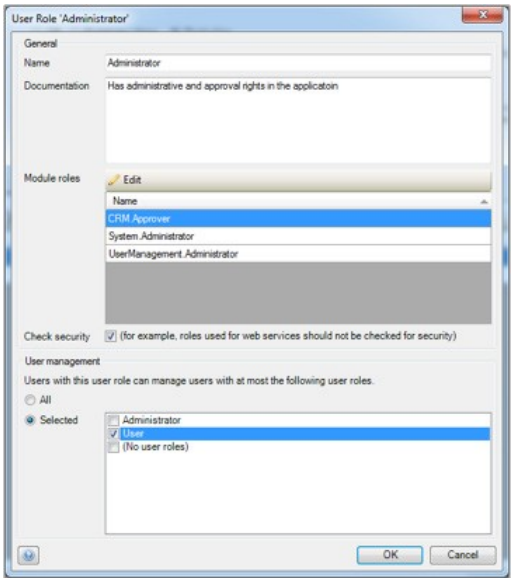

Figure 3. User roles

Anonymous users

Mendix supports log in to applications by anonymous users through configuration of a specific role for this purpose.

Password policy

Password policies can be defined flexibly e.g. configuring password strength, characters sets allowed / prescribed and password expiry policies. A password policy can also be defined by the organization when implementing SSO authentication using for example SAML or OpenID. Additionally, two factor authentication can be enabled within the Mendix Cloud for sensitive activities. Two factor authentication can also be added anywhere within a Mendix application to further secure access to the app or parts of the app.

File access

Access rights for file storage and use of images in Mendix applications are fully configurable.

Module-level security

Because the application modules are self-contained, the security model for pages, microflows (that execute actions), entities and data sets is defined in the module itself.

Module roles

Mendix distinguishes module roles in addition to user roles so that the module, including its roles, can be reused in different applications and/or published to the App Store.

Module-level security settings

At the module level, the security logic is separated from the application logic, which allows for easy accessibility, maintenance and validation of security settings even for less technical users. All security settings are managed from the Mendix Modeler to define access rights for:

Pages/UI

Page access defines for each module role which application pages users with this module role can access. The navigation items (menu bars/buttons) are optimized so that it only shows items directing to pages to which the user has access.
Page access takes the shape of a matrix showing pages and module roles. For each combination, the developer can indicate whether or not the module role has access tothe page. This information can also be edited within a page using the property 'Visible for'.

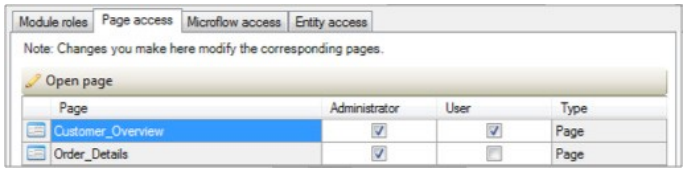

Figure 4. *Modular security settings for UI*

Microflows/Logic

Microflows are used to visually define business and process logic. Microflow Access defines which microflows can be executed by users with a certain module role. The navigation items (menu bars/buttons) are optimized so that it only shows microflows that the user has access to.

Microflow access is managed within a matrix of microflows and modules roles. For each combination developers can indicate whether or not the module role has access to the microflow.

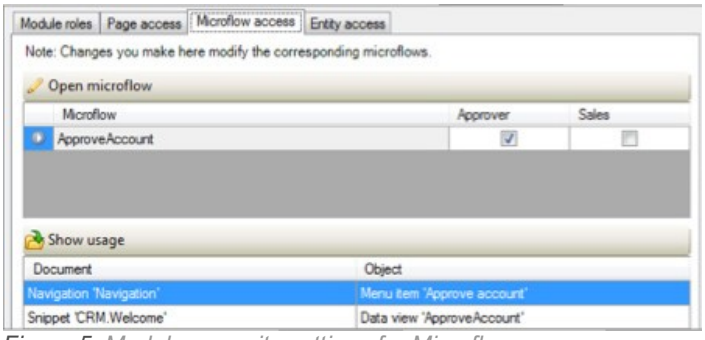

Figure 5. *Modular security settings for Microflows*

This information can also be edited within a microflow using the property 'Allowed roles'.

Entity Access & Access Rules

Entity access defines for each module role whether users with this role are authorized to Create, Read, Update and/or Delete objects of the entity. Entity access is configured with access rules that apply to entities. Each access rule in turn applies to a (set of) module role(s). The access rules of an entity define what a user is allowed to do with objects of the entity. Users can be allowed to create and/or delete objects, and to view and/or edit member values. A member is an attribute or an association of an entity.

Furthermore, the data sets of objects available for viewing, editing and removing can be limited by means of an XPath constraint. Every access rule is applicable to one or more module roles. An access rule grants certain access rights to those roles. Rules are additive, which means that if multiple access rules apply to the same module role, all access rights of those rules are combined for that module role. This feature is applied for example when applications are configured for multi-tenant usage.

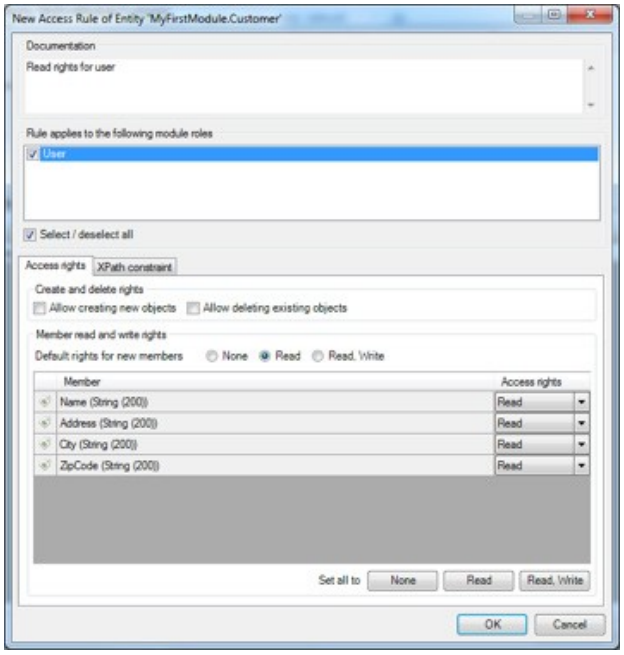

Figure 6. *Object security rule*

Logging throughout the Application Lifecycle

Mendix applies extensive logging of the whole application lifecycle. Not only logging for actions performed by the Mendix Runtime, but also the activities during design, development and deployment are logged, so there's a full audit trail of all relevant activities, who has executed them and when these activities were executed.

Requirements management logging

The Projects module in the Mendix platform supports the definition of requirements in the form of user stories. Mendix logs actions related to the user stories so that it's traceable who defined which requirements.

Design time logging

The integrity of the application being developed is monitored by the Team Server, which allows you to link all change commits within Mendix apps to specific user stories and users. This enables you to trace who has developed which part of your application, and for what reason.

Deployment logging

The Cloud Portal is the component that, amongst other functions, handles the deployment of application packages (called deployment archives in Mendix). Activities pertaining to deployment in the Cloud Portal include deployment and staging of apps across environments. In addition, backup and restore actions are logged, so there's full traceability of the administrative tasks performed.

Runtime application logging

The Mendix Runtime offers the option to log user behavior and object manipulations, enabling audit trails to the lowest level. Aside from the standard log details (such as active users, etc.), the Mendix Modeler allows you to add custom logging, and even to add active alerts based on bespoke integrity triggers. Logs are persistently stored in log files. Mendix offers an API to subscribe to log events. Mendix also integrates with 3rd party tools like RSA for encrypted storage of log files in environments where secure logging and auditing is required.

Identity & Access Management

User Management and Provisioning

Mendix offers MxID, a user management and provisioning service as part of Mendix Cloud. MxID is built on the Mendix Platform and hence inherits all security measures from the platform. MxID provides an administration portal for the management of user access and authentication.

Companies, that are tenants on the Mendix Cloud

Apart from the company profile and settings, Mendix supports the definition of Company Admins who can assign permissions to users following a delegated administration concept. One or more administrators can be identified per tenant who, in turn, can perform certain administrative tasks in the tenant according to the permissions granted.

App User Management

Based on policy rules, users are assigned a user role within an application. MxID automatically reads the user roles from the application.

3rd Party Identity Management Solutions

The built-in security role and authentication mechanisms in the Mendix Runtime, as described in the previous paragraph, support integration with other 3rd party identity managers such as Microsoft Active Directory and SAP IDM using protocols like LDAP (Lightweight Directory Access Protocol) or Kerberos.

Authentication

Authentication of users and services to access Mendix apps is handled through MxID by default. MxID applies the OpenID standard.

Note: For on-premises deployments, the MxID cloud service is not available. In this case, user names and passwords can be defined within the application. This option is typically used for “single app” deployment. For deployments of multiple apps, Mendix supports integration with local active directory (AD) and federation services or other Identity & Access Management solutions.

Single Sign-On

The Mendix Runtime also supports Single Sign-On (SSO) standards like SAML 2.0 and OpenID and provides APIs to other authentication mechanisms that might be implemented by customers, such as implementing two-factor authentication (e.g. via text message codes or tokens).

Like user management and provisioning, authentication can also be integrated with 3rd party Identity & Access Management solutions.

User Name & Passwords

Passwords in Mendix can only be stored in a hashed format. Mendix supports multiple hashing algorithms. If a user fails to login with right password three times, the user account is blocked automatically for a minimum of 10 minutes.
An administrator can manually override such blockage by resetting the password.

Web Services, REST Services & APIs

Just like for users, system or service interfaces must be authenticated in the context of the attached role as well. The default option is through a username and password. Other options like tokens are also possible. Authorization for APIs is derived from authorizations defined in the application model. For authentication, Mendix supports the following technical implementations:

- HTTP authentication
- Web Service Security standards
- Custom defined authentication mechanism including Java

These options make it possible to apply identity propagation.

Multi-Tenancy

Mendix offers out-of-the-box support for developing multitenant applications. Multitenant apps in Mendix share the same database, application logic and user interface. Application logic can be extended with tenant-specific logic.
Also, the user interface can be styled per tenant. Tenants are defined by identifying companies in the Mendix Identity Management module MxID. The company / tenant ID is used to:

- Define a tenant-aware object model for the application. Tenant-level access to domain objects is configured using XPath definitions. This restricts access to those application object instances for the company that the user belongs to.
- Define tenant-specific Microflows and configure access rights to implement tenant-level application- and process logic.
- Apply tenant-specific styling of the user interface by making the cascading style sheets (CSS) dependent on companies defined in MxID.

Tenants can be custom defined in the application as well by using identifiers like division, country, site, etc.

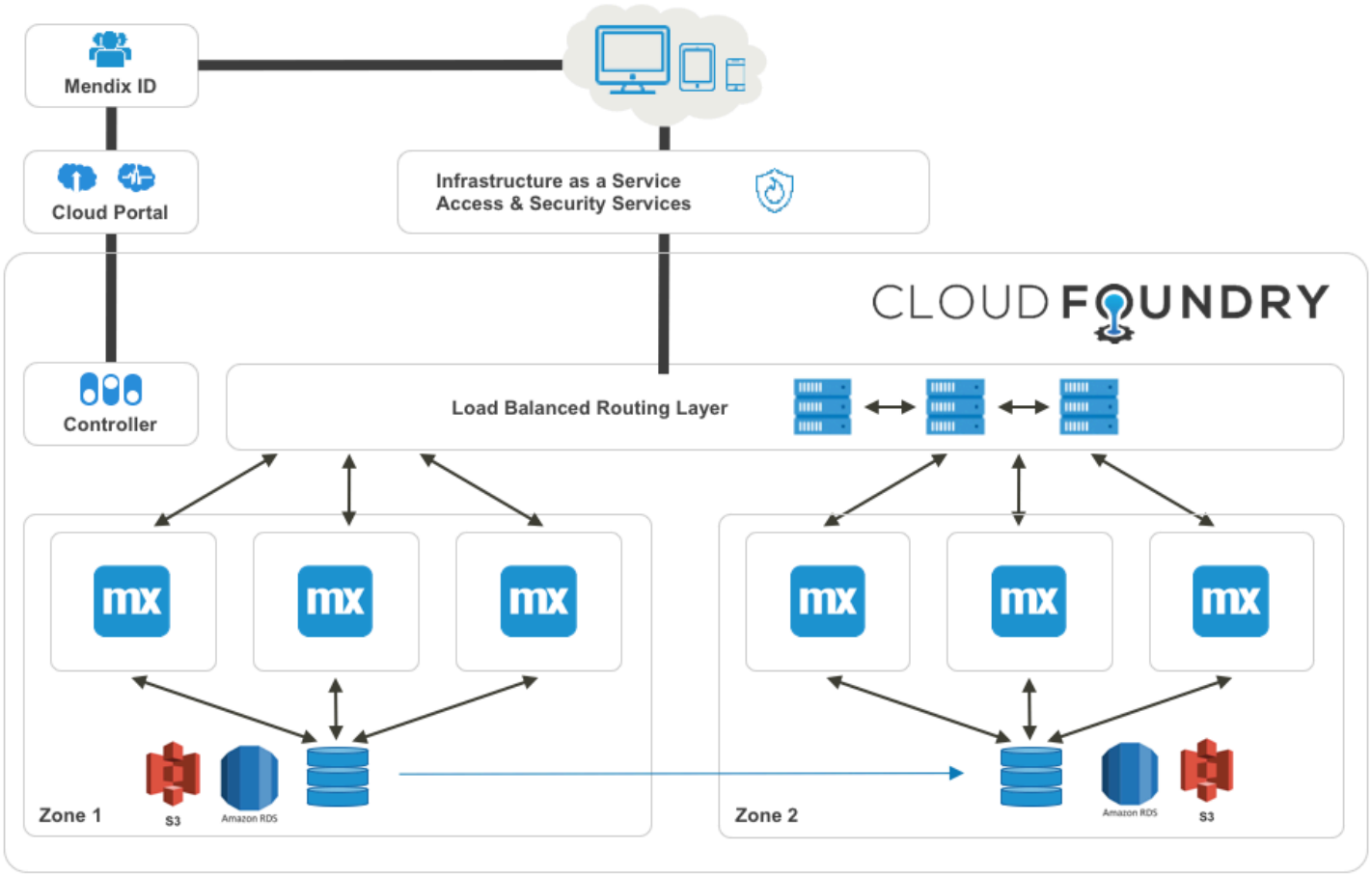

Figure 7. Multi-tenancy

Security for cloud deployment through Mendix Cloud

Mendix Cloud is the infrastructure provided and operated by Mendix to run the Mendix platform and applications built on the platform. Mendix Cloud also offers MxID as well as a Cloud Portal to manage users and for deploying, monitoring and managing apps across environments.

High-Level Deployment Architecture

Deploying your application on the Mendix Cloud takes place on a Mendix Cloud Node that Mendix provisions for your company in a cloud datacenter from one of the Infrastructure-as-a-Service (IaaS) providers that Mendix works with (see paragraph on IaaS Providers below).

Containment

A Cloud Node is a grouping of virtual and autonomous instances of the Mendix runtime, dedicated to your company that includes an (optional) Test, Acceptance and Production environment, each running in their own App Environment. This App Environment also includes firewall, web server, and database services. Mendix Cloud Nodes run on Cloud Foundry containers. The purpose of an App container is to contain the behavior and consumption of an environment and shield other environments (and apps) from each other.

As each App Environment has its own dedicated web server and firewall services, Mendix supports customization on an App Environment level through the Cloud Portal without affecting other App Environments. For example, the customization of request handlers for a specific App Environment is not compromised by the demands and desires of other Mendix customers.

The Mendix Runtime is connected to a dedicated database for the App Environment. The database is only accessible by this specific Mendix Runtime instance.

The App Environment setup allows test, acceptance and production instances of the same application to operate identically but independently. Because the App Environments are fully standardized, Mendix has been able to optimize the combination of OS, integration software, virtualization software, etc. and to implement the highest possible degree of security and performance. Furthermore, Mendix offers encryption for data-at-rest out of the box for App Environments.

Routing & network encryption (TLS)

The Mendix Runtime running in a container is accessed via a load-balanced routing layer of clustered Nginx web servers that routes the traffic to the relevant App Environment whereby the web server is responsible for the TLS connections. Additionally, all common access and security services from the IaaS provider are used for the traffic that goes to their infrastructure. The TLS connection starting from the browser terminates at the web server service on the load-balanced routing layer. This ensures that data is encrypted end to end so that other App Environments cannot intercept any data from the target App Environment.

Cloud Portal

The Mendix Cloud Portal enables you to manage users and environments, deploy apps to the cloud with a single click and manage and monitor their performance. The Cloud Portal itself is built with Mendix and hence inherits all security measures from the platform.

User Management

The Cloud Portal allows administrators to manage users (defined in MxID) and configure role-based access for users to environments to deploy and manage apps. The Cloud Portal security interface is integrated into the project dashboard, so you have a 360° view of all access rights for a specific person within the context of an app. Mendix enforces the segregation of duties between (at least) the developer and application administrator, whose roles are both safeguarded using personal accounts. Mendix will not allow you to configure a general management account, to ensure that all actions are traceable to a person.

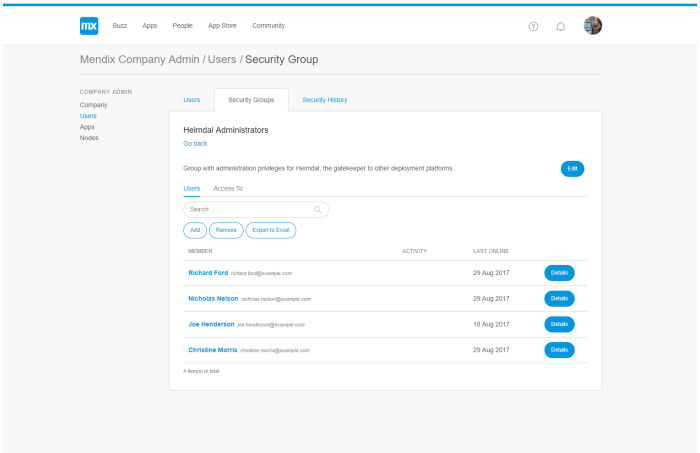

Figure 8. User Management Dashboard

Configuration Management

Technical contacts (administrators) can configure the environments assigned to them from the Cloud Portal. Mendix provides the full runtime environment, App Environments, needed to run an app. Network access, hardware, operating system, database and all other necessary infrastructure components are automatically provisioned so configuration management is done on a more functional level, such as URL, log behavior, application & environment specific parameters (defined in the model), etc.

Deployment Management

The Single-Click Deployment concept in Mendix makes it easy to deploy apps from the Cloud Portal to one or more environments, the App Environments.

Mendix supports a staging procedure for Development (on the Mendix developer's local machine) – Acceptance – Production (DAP) environments, possibly extended with an additional Test environment to DTAP. Every step in the procedure is controlled by those who have been specifically authorized to do so. Every stage-change of the application is logged extensively. Because each App Environment is fully identical to the others, there are no additional risks with regards to the non-synchronicity of test, acceptance and production environments. The chronology within your D(T)AP procedure, which includes not only the required chronology of activities but also the specific access roles for deployment, ensures that you will never be faced with surprises once you release an application version in your production environment. By assigning specific access rules for deployment environments (i.e. administrator A may update the acceptance environment only, while administrator B is allowed to update both acceptance and production environments), you will always have optimal control over your DTAP procedure. In addition, critical actions within the cloud, such as deployments and restoring backups, are authenticated using two-factor authentication.

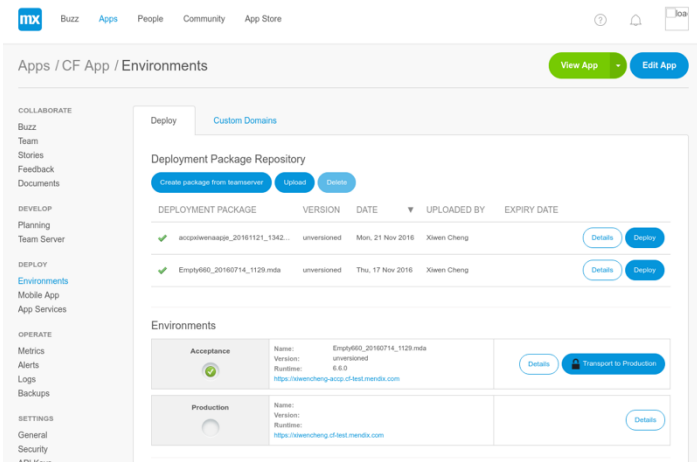

Figure 9. Deployment Package Overview

Monitoring & Alerting

Administrators have a comprehensive, real-time view of application performance metrics through a dashboard within the Mendix platform. This includes details on CPU and memory usage, App Environment and database usage, database requests and user logins, as well as preconfigured alerts.

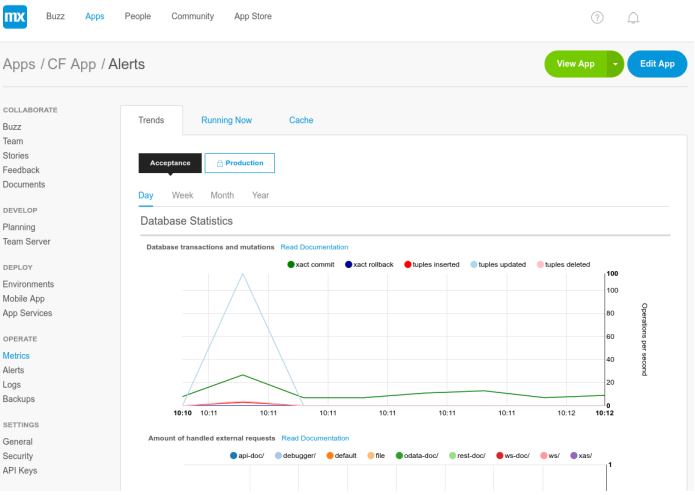

Figure 10. Monitoring Dashboard

Auditability

All relevant actions – both within your Mendix apps and cloud environment – are logged. The logs can be viewed and downloaded from the Cloud Portal.

Network Integration

HTTPS

In the Mendix Cloud, firewalls prevent all incoming traffic from accessing the Mendix environments on all ports other than port 80 (web) and 443 (https), whereby communication received on port 80 will be redirected to port 443. Mendix does not allow unencrypted communication.

Optionally, IP filtering and client certificates can be easily setup in the Cloud Portal.

Certificate-based authentication

This is a security feature whereby the customer or a third party provides certificates that are needed to access an external application not hosted in the Mendix Cloud. This certificate can be easily installed via the Cloud Portal. As an additional service, Mendix offers support for Mendix-side Certificate-based authentication. This is a security feature whereby the customer or a third party provides a certificate that has to be used to access an application in the Mendix Cloud.

Backup

A backup of all data (model, database and file storage) is made on a daily basis for the Acceptance, Test, and Production environments. Backups are stored in secured locations that are geographically dispersed.

Backups are available for restore as follows:

- Nightly Backups: maximum 2 weeks' history (counting from yesterday)
- Sunday Backups: maximum 3 months' history (counting from yesterday)
- Monthly Backups (1st Sunday of each month): maximum 1 year history (counting from yesterday)

Both production data and backup data utilize cloud storage and are subject to the storage limit associated with the Mendix platform subscription purchased. Companies are advised to set up an internal protocol for the usage and testing of back-ups. Administrators can download backups from the Cloud Portal or develop automated downloads of backups using the Mendix App Platform REST API. Mendix offers the option to use live data replication in order to enable a fallback environment.

Disaster Recovery

The Mendix Cloud has multiple mitigations for disasters, including high availability with deployment to multiple availability zones, scaling and auto recovery. As disasters can happen, disaster recovery tests are performed quarterly on the Mendix platform and are reported in our ISAE 3402 Type II report, SOC 1 Type II report, and our ISO/IEC 27001:2013 certification.

High availability & Scaling & Auto recovery

The Mendix Cloud offers high availability for all App Environments, ensuring zero downtime in case of a Mendix runtime outage. Customers are able to scale Mendix App Environments using the Cloud Portal.

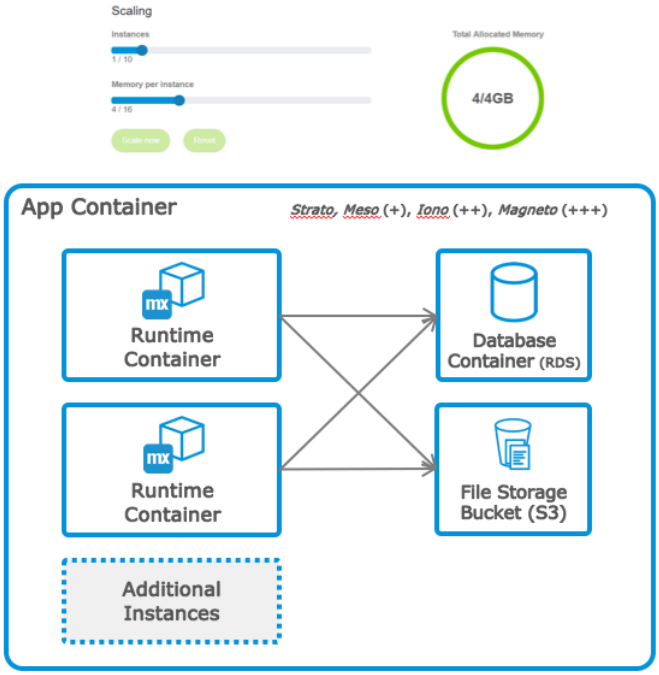

Figure 11. Mendix app scaling

Mendix Cloud architecture automatically distributes Mendix apps via a multi availability zone approach. Cloud Foundry equally distributes runtime containers across availability zones. Database containers and file storage buckets are automatically replicated across multiple availability zones. All backups are copied to other datacenters but the data will not leave the region should your company require this.

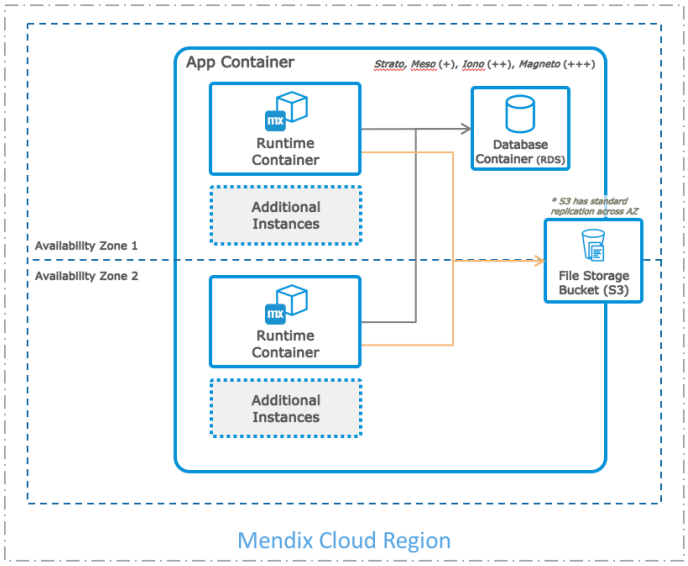

Figure 12. Multi AZ deployment in Mendix Cloud

The Mendix Cloud enables auto recovery and failover within the same availability zone and user load is balanced over two runtime containers. In the rare occurrence a single runtime container crashes, the other runtime container automatically takes over all user requests while the Cloud Foundry Health Manager automatically replaces the crashed runtime container with a new runtime container. Due to the stateless architecture of Mendix, end users won't be impacted.

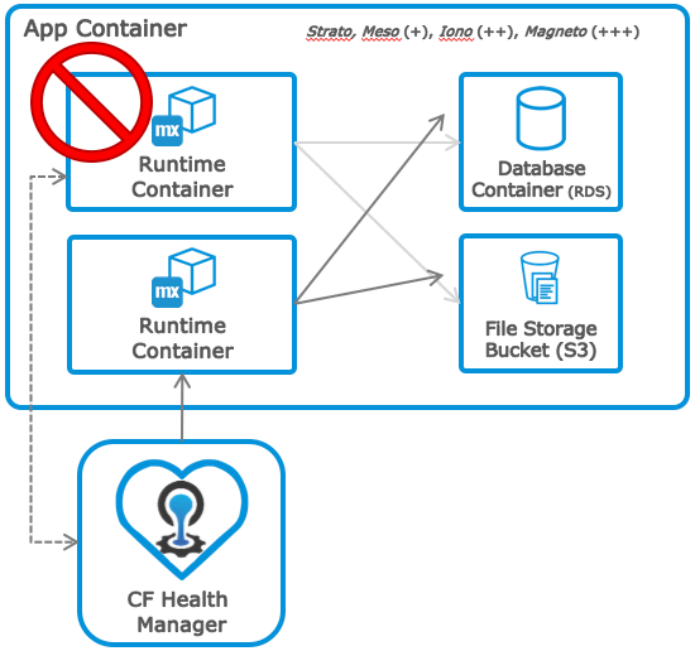

Figure 13. Auto recovery in Mendix Cloud

Upgrades & Patches

All underlying software that allows deployment in the cloud is regularly updated according to the Mendix Information Security Policy in case of security updates or patches. This includes virtualization software, OS, web server, firewall, Java, etc.
The majority of the updates performed to the Mendix platform have no impact on the availability or application settings. If, however, Mendix suspects a potential impact to your apps, we'll follow the SLA guidelines to inform you of the maintenance window.

Data Ownership

The data that underlies the applications running on the Mendix Cloud is, and will remain, the exclusive property of your company. Mendix will never lay claim to your data.

Infrastructure-as-a-Service (IaaS) Providers

Mendix utilizes the services provided by a number of IaaS providers. The Mendix IaaS providers are all providing a secure datacenter infrastructure with underlying Information Security certifications. As a rule of thumb, all apps hosted in the Mendix Cloud are hosted in a certified (SSAE 16, ISAE 3402, etc.) datacenter. Evidence of such certifications can be directly obtained from the respective vendors' website.

The Mendix Cloud can provide hosting facilities in the US, APAC and the EU and guarantee that the data will not leave the region should your company require this.

Compliance

Compliance plays a key role in the success and trust of our customers. Mendix is committed to abide by the law and regulations that apply to Mendix as Mendix conducts business around the world. All Mendix employees are subjected to criminal background checks.

ISO/IEC 27001:2013

Mendix is ISO/IEC 27001:2013 certified. ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system and also includes requirements for the assessment and treatment of information security risk tailored to the needs of Mendix and our customers.

ISAE 3402 attestation:

Mendix obtained the **ISAE 3402 Type II and the SOC 1 Type II** assertion. These independent attestation reports are available for (prospective) customers upon request under NDA.

Periodic Security Audits and Penetration Test

The Mendix platform and cloud hosting infrastructure undergoes monthly penetration tests performed by a leading IT Security firm. Mendix issues these at least once per month or with every major release to ensure it meets the highest security standards. Mendix has a vulnerability management program in place for continuous monitoring of the security posture of the Mendix platform. The penetration test and vulnerability management program is part of the Mendix ISAE 3402 Type II and SOC 1 Type II assurance audits, which is performed by an independent auditor. Penetration tests are based on OWASP and the ISSAF (Information Systems Security Assessment Framework) and OSSTMM (Open Source Security Testing Methodology Manual).

Recommended Mendix On-Premises Deployment Architecture

The safety of an on-premises installation depends on the security measures that are in place within your network. Mendix has achieved excellent results in realizing optimally secure infrastructure for Mendix applications in cooperation with the in-house IT specialists concerned.

An on-premises deployment of the Mendix platform means installing the Mendix Runtime. Mendix recommends the following deployment architecture, which is quite similar to the cloud deployment architecture.

The Mendix Runtime is accessed via a web server (such as IIS, Nginx, Apache) that routes the traffic to the relevant environment whereby the web server is responsible for the TLS connections. We also recommend implementing a firewall in front of the web server in case the application(s) built in Mendix are exposed to external users.

The Mendix Runtime is typically deployed with dedicated environments for Test, Acceptance and Production. The Mendix Runtime runs on (virtual) machines / server, and is normally connected to a dedicated database for the environment.

Non-production environments could share a single instance of the database. We recommend configuring the database for dedicated use by Mendix. For supported versions of web servers, operating systems and databases, see the system requirements for the latest Mendix release as described in the release Reference Guide.

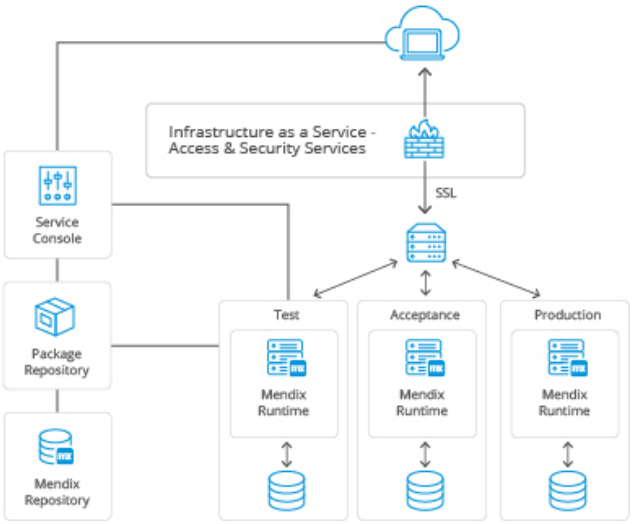

Figure 14. Mendix On-Premises Deployment Architecture

Database security

Mendix supports and has proven to work smoothly when data is encrypted either on a storage or database level.
Through Java extensions, Mendix supports encryption of specific files or tables in the database.

Backup & Restore

Mendix leverages backup and restore functionality supported in the database underneath the Mendix platform (for supported databases, see the above mentioned reference guide). The customer is responsible for the configuration.

Network & Operating Systems security

In the on-premises deployment scenario, the customer is responsible for network and operating system security.

Disaster recovery and data loss prevention

In the on-premises deployment scenario, the customer is responsible for implementing disaster recovery and data loss prevention by use of common tools such as for database and file storage replication.

Training and Documentation

The Mendix Academy courses (Mendix Introduction Course, Mendix Advanced Course and Mendix Cloud Administration Course) address the relevant security aspects of application development and deployment. See: https://academy.mendix.com/

In addition, the online introduction course that is accessible free of charge from the Mendix platform pays attention to security aspects of building apps in Mendix.

Actual documentation can be found at https://docs.mendix.com/ in the release specific “How To” and “Reference Guides”.

Further Information

For further information, please contact us via your local Mendix Account Executive or Customer Success Manager.