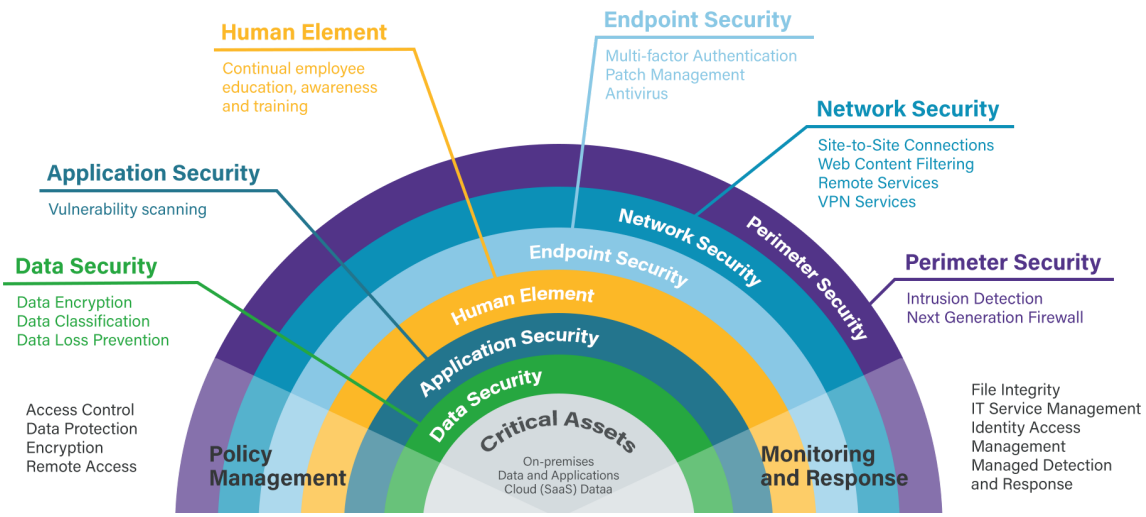
Overview of AutoCRM Security Features

An overview of the security features that AutoCRM is equipped with:



Authentication

Ability to set up two-factor authentication (including forcing 2FA settings on users)

Ability to set the length of validity of the login token

Ability to limit the number of logins to a maximum of one active session.

Setting password rules (length, special characters, etc.)

LDAP support.

Authorization

AutoCRM accounts can be administrator or regular. Regular accounts are subject to permission control via an ACL (Access Control List).
Users or teams can be assigned an unlimited number of roles whose permissions are permissively merged. Users can belong to any number of teams.
An administrator can define detailed access to individual CRUD operations in different areas (scopes) of the application for each role.
Individual operations can be set to own, team, or all records.
This system allows the flexibility to set almost any access restriction, but we are capable of writing custom access control rules for special requirements.

Password storage

Passwords are hashed and salted using standard secure methods.
Passwords that the application requires to know in plaintext format (e.g. SMTP passwords) are encrypted using the AES algorithm and thus stored securely in the database.

Server Security

AutoCRM instance and data is backed up once a day.
The server is regularly updated to ensure maximum security.