BESTMIX
SOFTWARE feeding the future

BESTMIX® Software designs best-in-class software solutions for nutrition industries that combine industry-specific knowledge with a relentless passion for innovation.

WWW.BESTMIX.COM

Cyber security & privacy policy

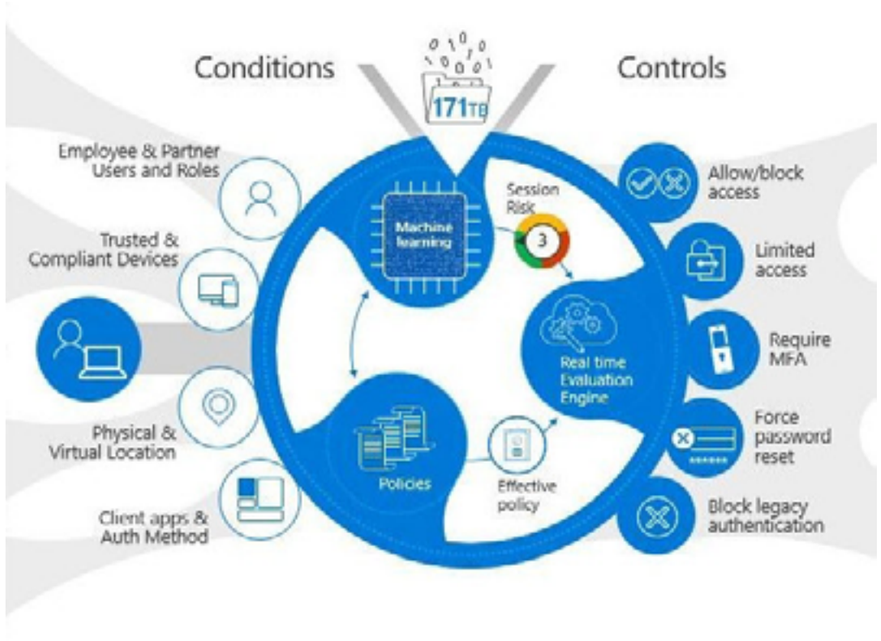
Discover how BESTMIX® Software handles security

Organizational

Security is handled by the system department, a team of system and cloud engineers with the sole responsibility of keeping infrastructures running as predictive and secure as possible. On an organizational level, we achieve this through regular awareness sessions. We apply a strict access policy with a role-based access control structure. As a Belgian company we make sure all data is stored in European datacenters and we sctrictly abide to the GDPR regulations.

General Security

Our internal datacenter is hosted in Maldegem. Physical access to the server room is granted to authorized personnel only. All systems are set up in a redundant manner. The entire server room is connected to an uninteruptable power supply (UPS) and a diesel generator, to safeguard against longer periods without electricity. All devices in the server room are in warranty with an active maintenance contract.



Identity

Every employee has a unique user ID, their user account, an identity on the network. We use Microsoft's best practices when it comes to password policies:

Microsoft Password policy recommendations

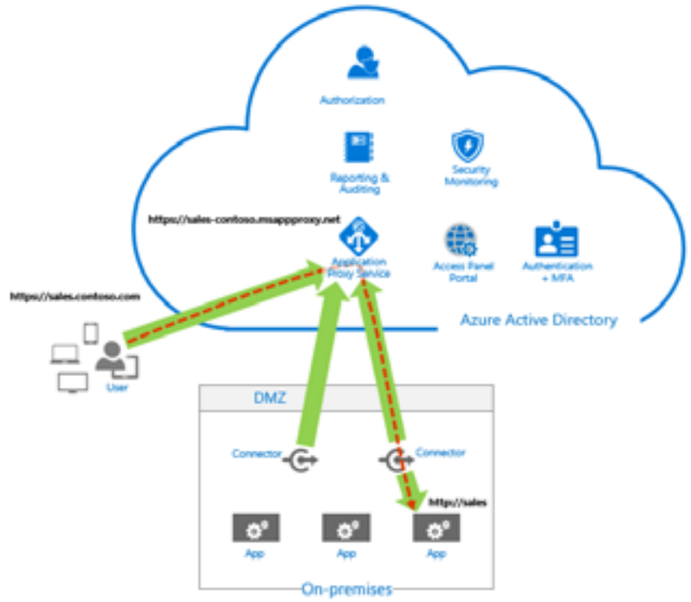
Every user - employee and guest is required to register for multi factor authentication (MFA) during the onboarding process. To protect the credentials, we use Microsoft Identity Protection. Policies are set to prevent risky sign-ins and risky users:

Microsoft Identity Protection

Single Sign On (SSO) is configured for cloud applications. All applications are protected with Azure Conditional Access. This includes access to on premise applications, these are published with Azure Active Directory Proxy. This means that a user has to authenticate with correct credentials and provide an answer to an MFA challenge before access to the application is granted. Every attempt to login is logged in Azure Active Directory. Whenever someone leaves the company, their user account is disabled and removed. The result is that the user cannot access any application anymore.

Network

The internal network is connected to the Internet over multiple internet connections with a backup over 4G, protected by a firewall. The firewall can use the connections simultaneously for outbound connections. Together with Azure AD Proxy, the internal applications are still accessible even if we lose an internet connection. Access to the internal network from the Internet is only possible with a virtual private network (VPN) connection. No application is accessible through the firewall. To access an application, users authenticate against Azure Active Directory first. To access the wireless network users need to authenticate against a Radius server.



Systems

Server

Our internal server infrastructure is equipped with host based firewalls and up to date antivirus software. Operating system security updates and patches are installed on a weekly basis. We automate this with Azure Updatex[2] Management

We make a full backup of all systems during the weekend. During the week we make differential backups. Backups are stored on a backup server on premises, on a removable NAS and in the cloud.

Endpoints

All endpoints are equipped with a Windows 11 Enterprise license and are managed by Microsoft Intune. Endpoints need to be marked as compliant before access to applications is granted. A compliant device is a device with an active firewall and an active and up to date antivirus. Windows update rings are also managed by Intune. The endpoints for members of the system department are set on "Windows Insider - Slow", all other devices are set on "Semi-Annual Channel - SAC".

All drives are encrypted with Bitlocker. Whenever a device is retired, stolen, lost, ... the devices is wiped remotely.

Customer Applications

Customer cloud applications are hosted in the Microsoft cloud - Azure.

Microsoft has datacenters in regions all over the world. Every region is paired with another region. Adifo hosts services in the Europe North region. This region is paired with Europe West. An Azure region is a set of datacenters, deployed within a latency-defined perimeter and connected through a dedicated regional low-latency network. In the case that we need access to the user workstation/laptop we use ISLight. This is an on demand desktop control tool such as Team Viewer.

The user and customer service support both can see and (optionally) interact with the screen.

BESTMIX® Recipe Management

BESTMIX® Recipe Management is hosted as a Platform as A Service application. We use Azure components to compose the backend of the application. The frontend is a C# application running on the client computer. The backend is a collection of web applications and a database server. Each customer has a separate database. Communication between the frontend and backend is secured by a TLS 1.2 connection. The web applications run on Azure Web App Plans, the databases run on an Elastic Pool. Azure Web Apps are a platform offered by Microsoft and act as a cluster of web servers with a load balancer in front of it. This provides out of the box redundancy:

App Service Overview

Elastic Pool is a platform offered by Microsoft to host databases. It acts as a database cluster for performance and redundancy. On this platform we have a backup of 7 days in time with a granularity of a few minutes.

Elastic Pool Overview

Access to the user acceptance and the production environment is limited. Only an handful of people have access. There are separate environments for development and testing.

BESTMIX® ERP Suite

BESTMIX® ERP Suite is an extension on Microsoft Dynamics 365 and is as such a Software As A Service application. All security, governance and availability of Dynamics 365 apply to MILAS. In effect the customer is in control of security and backup of the Dynamics 365 instance.

How to create a backup and restore dynamics 365 online database

BESTMIX® Software has no access to customer data. Only when a customer delegates access through a user account, access is granted. Microsoft provides a status page. To visit the health status page, click here.

BESTMIX® SpecTrack & Customer Care Portal

BESTMIX® Spectrack and the BESTMIX® Customer Care Portal are cloud applications hosted on the Microsoft Azure platform. They are web-based applications, accessible through any modern web browser. Only regular web traffic for the protocols http and https, need to be allowed to the Internet. There are no requirements to open any port on the firewall.

To access the applications, users must be authenticated first. Our customer applications use Azure AD B2C as an identity provider. Azure AD B2C is a customer identity access management (CIAM) solution that enables you to login with local identities or with enterprise identities. When one chooses to use enterprise identities, the customer is in control of the identities, including password strength, password location, password security and whether to use multifactor authentication. BESTMIX® ERP uses the customers AD to authenticate users.

BESTMIX
SOFTWARE feeding the future

BESTMIX® Software NV • Industrielaan 11b, 9990 Maldegem, BELGIUM • +32 50 303 211 • info@bestmix.com

www.bestmix.com