MaintMaster® Security White Paper

Welcome to MaintMaster! MaintMaster is a leading tool for return on operational reliability for discrete manufacturing. This white paper gives a bird's eye perspective of the security aspects of the MaintMaster system, it's deployment and to some extent how it is developed.

Security Overview

MaintMaster services are delivered as Software as a Service, SaaS and is implemented as a standard three tier content management system (client, server, database). The server and the database (Azure db) are deployed to the cloud service Microsoft Azure and the client is installed at local devices, typically at the customer site but it can be used anywhere when you have an internet connection.

MaintMaster is deployed side by side with a service portal called Wide which handles authentication, upgrades, monitoring and similar services.

The customer's data only leaves Microsoft Azure when it is requested by an authenticated user using a MaintMaster client. Any information persisted by the application on the local device for caching purposes is encrypted. This can safely be deleted when desired by an extra security conscious user.

MaintMaster is highly configurable, and it is frequently the customer's own application administrators who do this configuration. From a security point of view, MaintMaster does not handle configuration differently than other content. All is considered confidential information, owned by the customer.

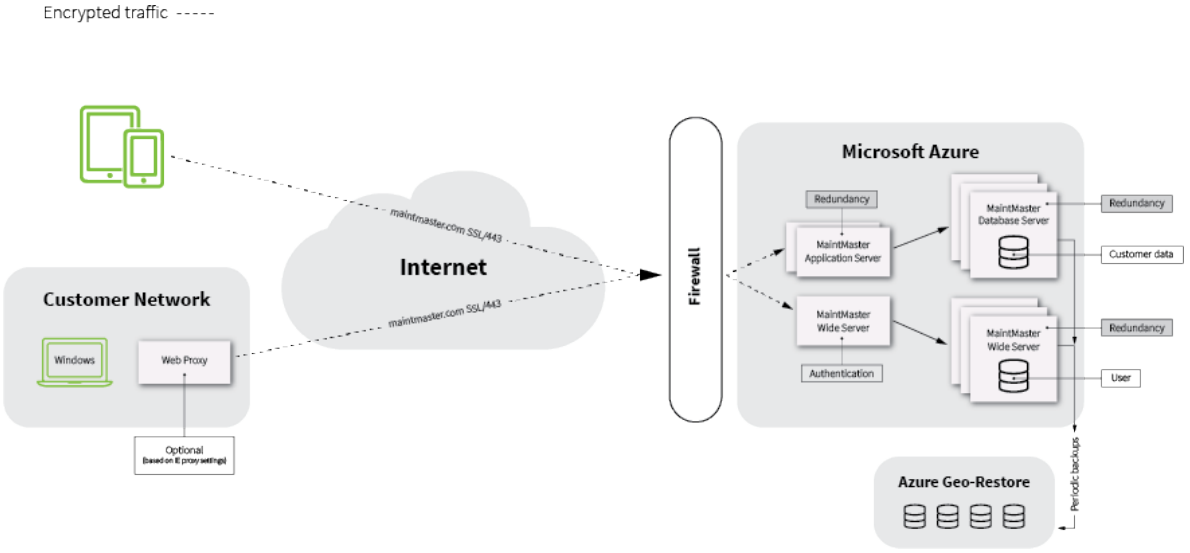

Fig 1. MaintMaster network diagram

Securing the MaintMaster Application

The MaintMaster application is developed by the MaintMaster company in accordance with industry standards for secure software development. This means that we have measures such as manual and

automated testing, peer reviewing of code, continuous integration and continuous static code analysis including rules for secure development from CWE and OWASP among others. This means that our code is continuously audited, manually, and automatically, for vulnerabilities and security hotspots and a live report on this is always available internally.

The source code (C#.NET and React) is kept in Microsoft Azure DevOps and the source code management system (Git) keeps a complete audit trail of all changes to the system, who did them, when and for what purpose.

Deployment of MaintMaster

A deployment of MaintMaster is done 100% in Microsoft Azure with Azure's tools for the purpose. Once a release is built and relevant parts are cryptographically signed, it is uploaded to our service portal where installations and upgrades of production, test or sandbox system can be ordered by MaintMaster or our customers. The service portal then monitors the health of the installed application and alerts our support function if there is any problem.

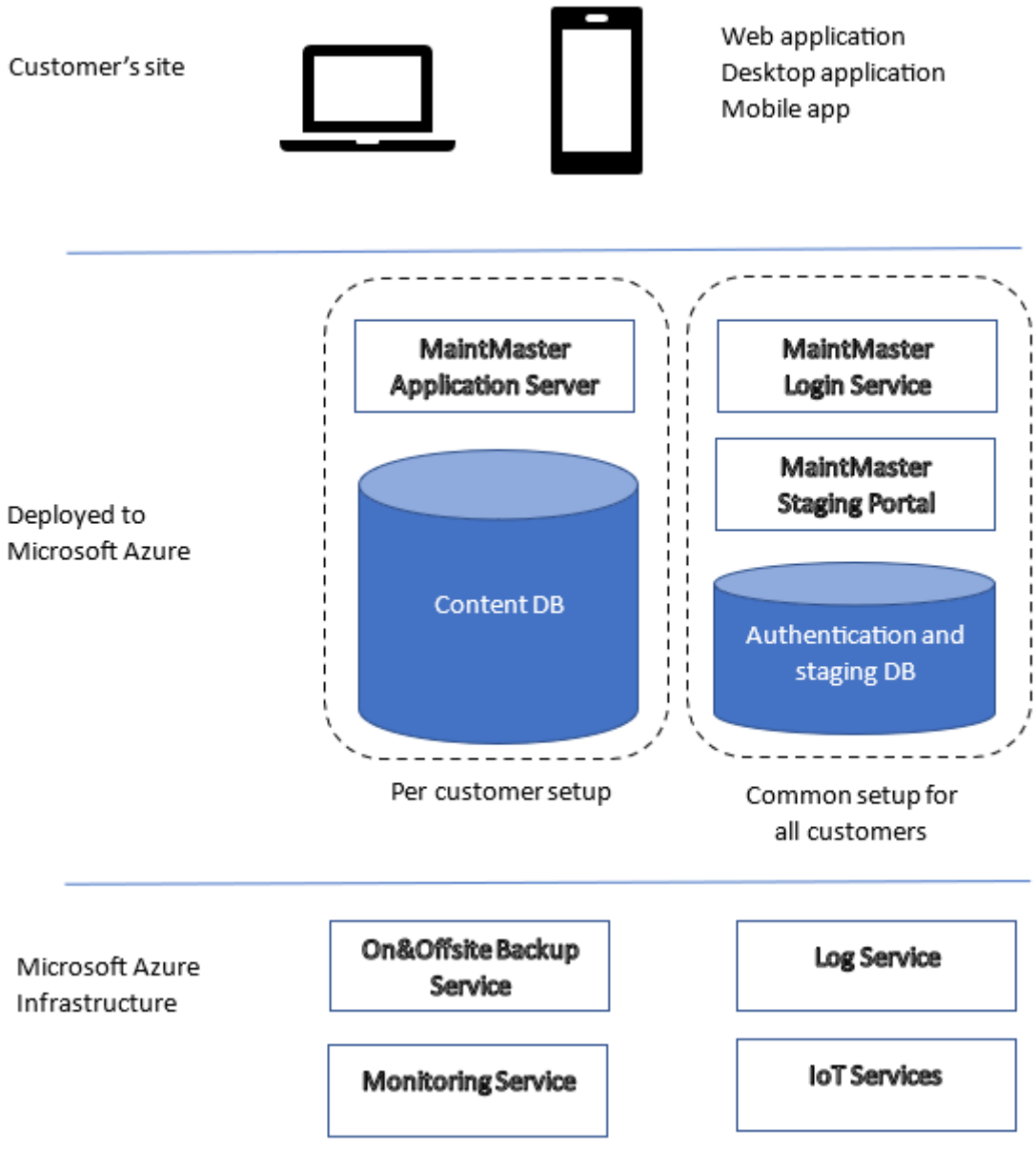

Fig 2. MaintMaster deployment diagram

Azure security

MaintMaster understands that to realize the benefits of the cloud, you must be able to trust the cloud. So do our hosting partner, Microsoft. Microsoft Azure offers the most secure and trusted platform for cloud services. Microsoft has been leading the industry in establishing clear security and privacy requirements and then consistently meeting these requirements. Azure meets a broad set of international and industry-specific compliance standards, such as ISO 27001, HIPAA, FedRAMP, SOC 1 and SOC 2. MaintMaster utilizes many of the features offered by Azure to operate, secure and monitor our services.

Azure is available in most regions of the world. MaintMaster can therefore be hosted in a region near you and your data is always kept in that region. By default, our systems are hosted in Azure Region West Europe (Netherlands) with Azure North Europe (Ireland) as fallback.

MaintMaster uses hosting partners who support and administer our production system in Azure 24/7/365. They work under the same restrictions as Microsoft's technicians. This means that neither Microsoft nor our hosting partner can view your data. Our hosting partners are physically located and working in the same jurisdiction as the hosted system. We commit to informing our customers at least 30 days before any significant changes to our hosting organization or model is enacted.

All Azure data, including our databases are encrypted at rest. For more information, see https://learn.microsoft.com/en-us/azure/security/fundamentals/encryption-atrest.

For more information on Microsoft Azure Security, see https://azure.microsoft.com/en-us/explore/security/.

Security of your data is one of our top priorities

- Microsoft Azure – More certifications than any other cloud provider.
- Network security – All data is encrypted (TLS) before sent over multiple secured network connections.
- Privacy security – All passwords are kept in an irreversible state, not even our technicians or developers can reverse them. For more information, see the *MaintMaster Privacy Policy*.
- Backup – Point in time restore and additional long-term backups available. See the Backup section of this document.
- Disaster recovery plan – Everything needed to recreate the entire hosting environment is available off site, including backups of your data, still never leaving your region.

Communication in the MaintMaster system

All communication in the MaintMaster system is encrypted. Client to server communication is done over the standard Internet protocol using port 443. Any client needs to be able to reach all servers in MaintMaster.com (both MaintMaster.com and *.MaintMaster.com). All other application communication is inside Azure but is still always encrypted using either TLS (highest possible version with regards to end users operating system compatibility) or similar built-in encryption in for example database communication tools.

MaintMaster reads the current user's Windows Proxy Settings. This process includes the IE options to automatically detect proxy settings, use an automatic configuration script, manual proxy server settings, and advanced manual proxy server settings.

Extensions and Integrations

MaintMaster can be extended by certain out of the box or customized addons and integrations. These are usually, but not always developed and supported by MaintMaster. When we do this, all of MaintMaster's security practices, policies and restrictions still apply, except that for some integrations, the customer's information may be permitted to leave the MaintMaster system and Azure if that is the purpose of the integration.

Ownership of- and access to data

The customer always owns, and is responsible for, the data they put into their system. MaintMaster and our hosting partners may not view or edit the customer's information unless MaintMaster's policy for handling of customer's data permits it. Briefly put, accessing customer's data is only permitted if any of these conditions are fulfilled:

Approved reasons for accessing customer data	Explanation
1. **Training, project, configuration etc.**	When we perform training, projects, or configuration in the customer's production system (or a copy of it) with their data rather than demo data. This is only done at the customer's request or with their explicit permission.
2. **Ongoing support issue**	When the customer has logged a support case with MaintMaster where we may need to see the customer's data or configuration in order to help the customer resolve the problem, MaintMaster may view relevant the data in the customer's system. (In this case, the customer is considered to have invited relevant MaintMaster personnel to do so.).
3. **Volunteered information**	When the customer's unbidden volunteers their information to us in some other way (presentation, meeting, email, screen sharing) outside of the aforementioned reasons.
4. **Emergency**	MaintMaster's Chief Information Security Officer (CISO) or MaintMaster's CEO may approve exception if it is deemed that that accessing of data is warranted in order to prevent even worse damage to the customer's data, or the security thereof. In this case, we must let the affected customers know of this exception as soon as possible.

General restrictions apply for all these cases (scope limitation, relevance, full discretion etc.).

Logging

MaintMaster by default logs certain events in the system for security, performance, and monitoring purposes. Logs never contain any personal information save for the username, and never contain any customer data. We do not log all events in the system as this would quickly become quite expensive in terms of log size. Security events in MaintMaster are however always logged. These logs are generally not accessible to anyone other than MaintMaster personnel.

Test and Sandbox Environments

For customers having integrations or extensions, a test environment is usually required. For security purposes, MaintMaster treats test and sandbox environments exactly like production systems since they may still contain the customer's sensitive data. They do not have the same backup schemas however, as data in these environments are not considered important other than for preventing unauthorized access.

MaintMaster User Account

A user with adequate permissions, often the administrator, invites new users to take part of a MaintMaster system. When inviting, the administrator sets permissions and roles, it's all done in the normal MaintMaster desktop client. The invite is sent via e-mail and the new user create a MaintMaster account if not already a MaintMaster user.

Azure Active Directory and SSO

When the new user confirms the account there's an option to get authentication from an Azure AD. This requires that the customer has an Azure AD (or has an Azure AD in sync with a local AD) and that this AD (domain) has MaintMaster authentication privileges set. Existing users can logon to the MaintMaster Portal and change the authentication to Azure AD. If requested, MaintMaster Support can set a whitelist for your domain to make sure that all your accounts are authenticated from your AD.

Backups

We use Microsoft Azure SQL as our backbone for database management, compatible with Microsoft SQL Server 2022. Azure offers Point-in-time-restore. In addition, we offer weekly distributed backup files in bacpac format to our Enterprise Edition customers. If you ever need to read a backup file from your system you need to have Microsoft SQL Server 2022.

From the admin client you can always export all data to Excel readable format.

How long backups are retained varies by edition and backup type:

	Sandbox/Test	Team Edition	Standard	Enterprise
Point in time restore	7 days	14 days	14 days	35 days
Weekly backup	-	5 weeks	5 weeks	5 weeks
Monthly backup	-	12 months	12 months	12 months

When a customer leaves MaintMaster, all databases and backups are deleted at most 14 days after their contract with us ends, or sooner if the customer asks.

Incident Routine

MaintMaster has an incident management policy aimed at proactively identifying and fixing potential security or availability problems. We classify incidents by type and severity, and document and act accordingly both during and after an incident occurs (real or exercise). Incident retrospectives are always held as well as regular risk assessments, mitigations, and management.

MaintMaster aims to be as transparent as possible when it comes to incident management. For this reason, the first responder (or the Chief Information Security Officer if available) is tasked with informing the customer if we suspect that their system or their data might have been at risk.

We also have a policy of sacrificing availability rather than risking unauthorized access to data, which means that if we have a serious ongoing security incident, we may shut down a customer's system to prevent data from leaking to unauthorized parties.