M-FILES CORPORATION

M-FILES CLOUD - SERVICE DESCRIPTION

LAST UPDATED 28 APRIL 2025

VERSION 2.2

Contents

1. Introduction

Agility, efficiency, and innovation are not just buzzwords in the ever-evolving landscape of business, but the pillars upon which successful enterprises stand. At M-Files, we want to help you focus on your core business objectives. That's why we provide a comprehensive M-Files Cloud service to take care of the technical complexities, allowing you to concentrate on what truly matters - your business.

This document serves as your guide to the features and benefits that make M-Files Cloud the epitome of a modern, dynamic, and scalable cloud solution. Built side by side with Microsoft experts, we utilize recognized industry standard frameworks, such as Cloud Adoption Framework (CAF) and Well-Architected Framework (WAF).

M-Files Cloud is a secure and scalable cloud-based deployment option for knowledge work automation. With M-Files Cloud, you can manage your documents and information without investing in local server infrastructure and maintenance.

2. Why M-Files Cloud?

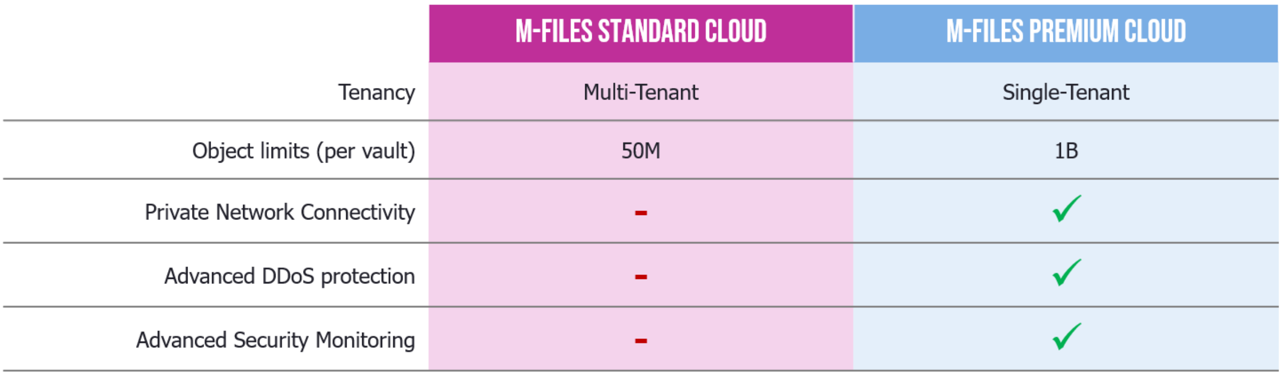
We take care of the technical intricacies to empower your business. This allows you to focus on what truly matters – your core business.

Why M-Files Cloud stands out:

TERM	DEFINITION
Scalability	Easily scale your computing resources up or down based on your business needs.
Accessibility	Break free from the confines of a physical office. Access your data and applications anytime, anywhere. M-Files Cloud fosters collaboration among remote teams and enhances overall productivity.
Automatic Updates	Stay on the cutting edge effortlessly. Enjoy the latest features, security patches, and improvements without the hassle of manual updates.
Cost Efficiency	Eliminate the need for expensive hardware and maintenance costs associated with on-premises solutions. Pay for a subscription model that suits your budget.
Data Security	You can trust in our advanced security measures including data encryption, regular backups, and compliance with industry standards. Your organization's sensitive information is secure in M-Files Cloud.
Collaboration	Bridge the geographical gap. Foster collaboration among team members regardless of their physical location. Real-time document sharing and editing enhance teamwork.
24/7 Support	We've got your back around the clock. To receive continuous support from the SaaS provider, you can select to receive 24/7 support (subject to conditions). With 24/7 support, any issues are quickly resolved and downtime for your business operations is minimized.
Reliability	You can rely on the service's robust infrastructure and high availability. M-Files Cloud reduces the risk of disruptions and ensures consistent service for your business-critical applications.
Quick Implementation	Embrace agility. Rapidly deploy new applications and services without the lengthy installation processes associated with traditional on-premises software.
Customization	Make it yours. Tailor M-Files Cloud to fit your specific business needs with the flexibility to add or remove features as your requirements evolve.

3. M-Files Cloud

3.1 Plans



	M-FILES STANDARD CLOUD	M-FILES PREMIUM CLOUD
Tenancy	Multi-Tenant	Single-Tenant
Object limits (per vault)	50M	1B
Private Network Connectivity	-	✓
Advanced DDoS protection	-	✓
Advanced Security Monitoring	-	✓

M-Files Cloud offers two plans to fulfill all business needs. The M-Files Standard Cloud plan is our world-class cloud service that scales for most use cases. M-Files Premium Cloud is a fully isolated single-tenant environment that provides predictable performance and enhanced compliance. The dedicated capacity enables larger data volumes and an additional layer of security.

This document applies for both plans, unless otherwise specified. For more information on the additional capabilities of M-Files Premium Cloud, see section 4.

3.2 Scalability

M-Files Cloud offers a flexible and transparent pricing model that scales with your usage. You only pay for the number of user licenses and the amount of storage you need, which enables efficient cost control.

Industry-leading cloud platform technologies provided by Microsoft Azure allow us to automatically scale Azure resources needed to handle your workload. Whether you have a few users or thousands of users, M-Files Cloud provides fast and reliable performance for your document management tasks. You do not have to worry about managing servers, storage, or updates. M-Files Cloud takes care of these tasks for you.

M-Files Cloud scales to support your business growth and expansion. You can easily add new users, departments, or locations to your M-Files Cloud service to collaborate on documents across different teams and regions. M-Files Cloud is currently available in over 20 regions worldwide.

M-Files Cloud offers both vertical and horizontal scaling. This enables us to add more nodes for clients or increase node resources when demand rises.

3.3 Accessibility and Availability

With M-Files Cloud, you are not tied to location or device to perform your critical tasks. M-Files Cloud allows you to access your documents anytime, anywhere. Whether you are using a desktop, laptop, tablet, or smartphone, you can have full access to your M-Files environment. You can use the web browser, the desktop client, or the mobile app to view, edit, and share your documents. You can also sync your documents offline and then work on them without an internet connection.

We ensure that your documents are available and secure. M-Files Cloud uses Microsoft Azure, a leading cloud platform that offers high availability, reliability, and scalability. All communication between your devices and M-Files Cloud is encrypted.

You can access your documents from different sources and systems. We enable integrating M-Files Cloud with your existing applications, such as Microsoft Teams and Outlook, Salesforce, and more. You can also connect M-Files Cloud to other cloud storage services, such as Microsoft OneDrive and SharePoint, Google Drive, and more. This way, you can access all your documents from one place and avoid duplication and confusion.

3.4 Reliability

M-Files Cloud is hosted in Microsoft Azure. The Microsoft Azure data centers are highly secure and designed to automatically survive hardware and infrastructure failures. The redundant infrastructure offers, for example, emergency power support, fire detection and suppression systems, video surveillance, dual internet service providers, and much more.

M-Files Cloud uses Microsoft Azure SQL Database to store the object metadata and other important customer content including vault metadata structures. Microsoft Azure SQL Database stores all the permanent data to redundant storage to mitigate outages that failures of server components (such as hard drives, network interface adapters, or even entire servers) can cause. Additionally, database backups and transaction logs are stored in geo-redundant storage to enable recovery to another data center in case of a major disaster.

Files stored in M-Files Cloud use Microsoft Azure Storage services. Data is automatically geo-replicated, and six copies of your data are always maintained. Your data is replicated three times within the primary region and three times within a secondary region hundreds of miles away from the primary region. Replication provides high-level durability in case of catastrophic failures. In the event of a failure in the primary region, Azure Storage transitions over to the secondary region. Geo-replication ensures that your data is secured in two separate Azure regions.

In the M-Files Cloud infrastructure, each high-availability cluster has at least two M-Files application instances that are both attached to the vault database and file storage at the same time. Azure Load Balancer routes traffic to either one of the application server instances. In case the load balancer detects that one server instance is down, it directs the queries to the other instance while the failing instance is being recovered. There is no need to move the data because permanent data is stored in a separate database and file storage. This includes all vault content together with configuration data and customer data (metadata and files).

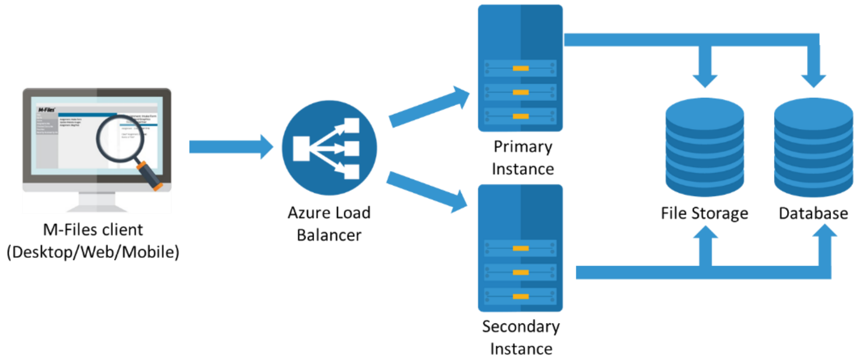


Figure 1: High-availability cluster in M-Files Cloud.

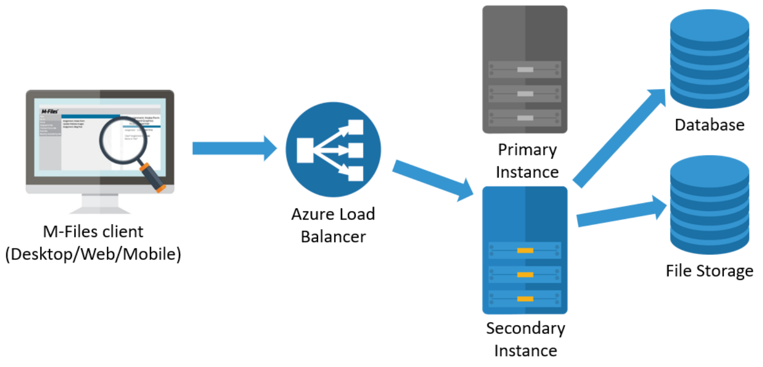


Figure 2: If an application instance fails over in M-Files Cloud, data remains accessible without any interruptions.

3.4.1 Data Availability

M-Files saves each modification to content and metadata as new versions. This allows users to roll back to any previous version using the client software.

Deletion and permissions

Customer administrators can specify the rights to delete data (including documents) from M-Files. Deletion can be restricted to administrators or allowed for all M-Files users.

When an object is deleted in M-Files, it is hidden from the user interface but not permanently destroyed. This acts as a soft-delete mechanism for easy recovery of data.

Customer administrators can restore or permanently destroy deleted objects through the M-Files user interface without the need for backups. These actions are available to users with extended access, such as customer administrators.

Data retention

In M-Files Standard Cloud, destroyed data is retained for up to seven days before it is permanently deleted. There is an option to extend this period to 35 days by upgrading to the extended backup plan.

The M-Files Cloud backup system can store data for longer periods, enabling recovery in the event of extortion attacks or other unintentional data loss.

3.4.2 Outage Communication

If there is a service outage that cannot be resolved in 30 minutes, M-Files sends an email to the impacted customers. M-Files also sends additional progress updates on an hourly basis.

We measure service availability for every M-Files Cloud vault once per minute.

3.5 Service Updates

M-Files Cloud is updated monthly during scheduled maintenance breaks. The service is updated to the latest M-Files Server version right after a new version has been released. Customers can benefit from new features, security updates, and other software updates as soon as they become available. All M-Files software updates go through rigorous testing procedures to ensure high-quality standards.

M-Files normally carries out maintenance for servers on the third Sunday of the month, between 8 AM and 2 PM UTC on services outside Europe and between 10 AM and 4 PM UTC in Europe.

M-Files may schedule additional maintenance breaks. If an additional maintenance break that might influence the availability of the service is planned, M-Files will inform M-Files Cloud customers no later than two (2) days before starting the maintenance tasks. M-Files shall further have the right to suspend the provision of the software service for a reasonable period as an emergency action to recover from issues. For example, a data security issue that M-Files has become aware of or a data network outage issue outside of M-Files' control.

3.6 Security

With M-Files Cloud, your data is stored safely. M-Files Cloud uses data encryption to protect your information from unauthorized access. Your data is secure both when it is stored in the cloud and when it is transferred over the internet (data at rest and data in transit).

The M-Files Cloud service includes regular backups of your data to ensure that your information can be recovered in case of failures. M-Files backs up your data daily. Backups are hosted in a different storage than your production data to ensure business continuity. Data is automatically geo-replicated, and six copies of your data are maintained.

M-Files Cloud supports various identity providers (IdPs), such as Microsoft Entra ID, Google, and Okta. You can integrate M-Files Cloud with any IdP that supports the OAuth 2.0 protocol. This way, you can simplify your login process, manage your users and permissions centrally, and enable features, such as multi-factor authentication.

M-Files offers ways to securely integrate your systems with M-Files. M-Files Application Accounts can be tied to existing Azure service principals which are under your control. You can refer to Microsoft documentation for further guidance on Applications and service principals.

We utilize Azure Key Vaults to make sure that your secrets and encryption keys stay safe. M-Files Cloud supports HYOK and provides an option to host file encryption keys in your own Azure Key Vault.

One of the ways that M-Files Cloud enhances its security is the implementation of Azure DDoS Protection. Azure DDoS Protection is a service that provides enhanced distributed denial of service (DDoS) mitigation features to defend against DDoS attacks. For more information, refer to What is Azure DDoS Protection? in Microsoft documentation.

M-Files has available additional services to enhance your cloud security even further (see section **Error! Reference source not found.**).

3.7 Product Support

M-Files Cloud customers are eligible to receive M-Files Product Support that includes updates and other basic support elements, such as issue solving and troubleshooting. Product Support covers only technical issues. It is not provided for user help, guidance, training, consulting, implementation, or other similar purposes. These are available for a separate fee as agreed between M-Files and the customer and specified under an applicable Statement of Work (SoW).

Product Support covers only the standard version of the service and software. It does not cover third-party software or services, or any customized software applications developed for the customer. Support for customizations and customer-specific software requires procuring additional support services. The content of these services is specified under Statement of Work.

Learn more about the M-Files Product Support at https://www.m-files.com/product-support-policy/.

3.8 Performance and Availability Monitoring

M-Files monitors the performance and availability of M-Files Cloud constantly to ensure a high quality of service. This includes corrective actions to detect irregularities in the service regardless of the time of the day. We utilize Azure-based monitoring automation, which triggers alerts if customer vaults exceed the alert threshold that we monitor. This applies to both availability and performance. M-Files monitors the quality of the service 24/7. Our monitoring and alert automation considers both the current and historical performance of the vault.

Continuous vault availability monitoring is provided for each M-Files Cloud vault to ensure accessibility of the service. M-Files aims for at least 99.5% monthly availability. M-Files leverages an external monitoring service Pingdom for monitoring the availability of each vault every minute. If any issues are detected, our automation will look to resolve them. If automation cannot resolve an availability issue, our experts are alerted to investigate further. For outages lasting over an hour, we notify affected M-Files customers by email and provide regular updates on the progress toward a solution. In these cases, we contact trusted person of each affected vault. You can define the trusted person for each vault.

Our monitoring also covers performance, tracking multiple performance indicators in real-time for each M-Files vault. Based on monitoring data, the M-Files platform can automatically scale up resources when necessary. Our standard service includes performance scaling to support your workloads. The number of concurrent users, activities, and vault-specific configurations have an effect on vault performance. For any availability or performance issues you may experience, you can contact us through our support portal.

3.9 Subscription Management

You can use M-Files Manage to control your M-Files subscription. It is a web-based self-service portal that is tailored for administrators to help their organizations to get the most out of their M-Files. With constantly improving self-service capabilities, the time to value is minimized.

With M-Files Manage, M-Files administrators can set up M-Files users, user access, and user license management based on Microsoft Entra ID user groups. M-Files Manage also has an online shop where you can purchase user licenses. * Other self-service capabilities include creating new M-Files cloud vaults and monitoring the vault usage through M-Files Cloud analytics.

*Available only for direct customers

3.10 Disaster Recovery

M-Files informs the customer of a disaster event at the primary data center if there is a chance that data has been permanently lost or if the disaster event causes a system outage. Frequent updates on disaster recovery efforts will be provided via email or phone to the designated customer personnel. Please make sure that the contact information in M-Files Manage is up to date. Disaster recovery actions are managed as priority 1 issues defined in the service-level agreement (SLA).

3.10.1 RPO and RTO

Recovery Point Objective (RPO) and Recovery Time Objective (RTO) are not currently defined in SLA. Target RPO for M-Files Cloud is one hour. Data is geo-replicated asynchronously by the Azure services to another data center in the same geographical area except for Brazil South. The regional pairs are managed by Microsoft. You can read more about the region pairs at https://docs.microsoft.com/en-us/azure/best-practices-availability-paired-regions.

Service levels and fix times are defined in the M-Files Online Agreement where priority 1 level incident is defined as "The Service is down and cannot be accessed". By default, M-Files recovers the service in the primary data center. If it is not possible, the service is restored in the secondary data center.

3.10.2 Recovering the Vault Database

If the vault database is destroyed or corrupted due to an error in the M-Files Cloud service, it can be necessary to restore the database from a backup to recover the vault database. For example, if significant unwanted changes have been introduced to the database structure and there is not another way to roll back, the vault database must be recovered.

In this case, M-Files notifies the customer's contact person about the issue and possible data loss. M-Files verifies whether the database is permanently lost and restoration from a backup is necessary. The point-in-time-restore functionality in Azure SQL Database is then used to restore the database. After the database is restored, it is attached to the original high-availability cluster. When everything works as before, M-Files communicates the online status of the vault and the restoration timestamp to the customer. Any possible modifications made after the restoration time may have been destroyed.

3.10.3 Recovery from the Loss of a Microsoft Azure Region

Microsoft Azure is divided physically and logically into units called regions. A region consists of one or more data centers in proximity. Microsoft Azure has tens of regions around the world. Regions are designed to minimize the possibility that a failure in one region could affect other regions.

Database backups are geo-replicated by Microsoft Azure. If a primary data center goes down, it is possible to restore the database to another data center with point-in-time-restore.

File data is geo-replicated by Microsoft Azure. If a failover is necessary, these actions are taken:

- Microsoft determines whether the data can be recovered in the primary location and whether a failover is necessary.
- Microsoft changes the primary DNS entries to point to the secondary location to do the failover of the storage account.

In case of Azure region level failover, the M-Files Cloud service must also be restored to the new region. The cloud service is built through our automation layer that sets up M-Files Cloud in the new region and connects it to the existing storage.

3.11 M-Files Cloud Architecture

Here is an overview of the M-Files Cloud architecture that is based on Azure Kubernetes Services (AKS) architecture. As part of our standard update cycle, we are updating all workloads to use AKS-based architecture.

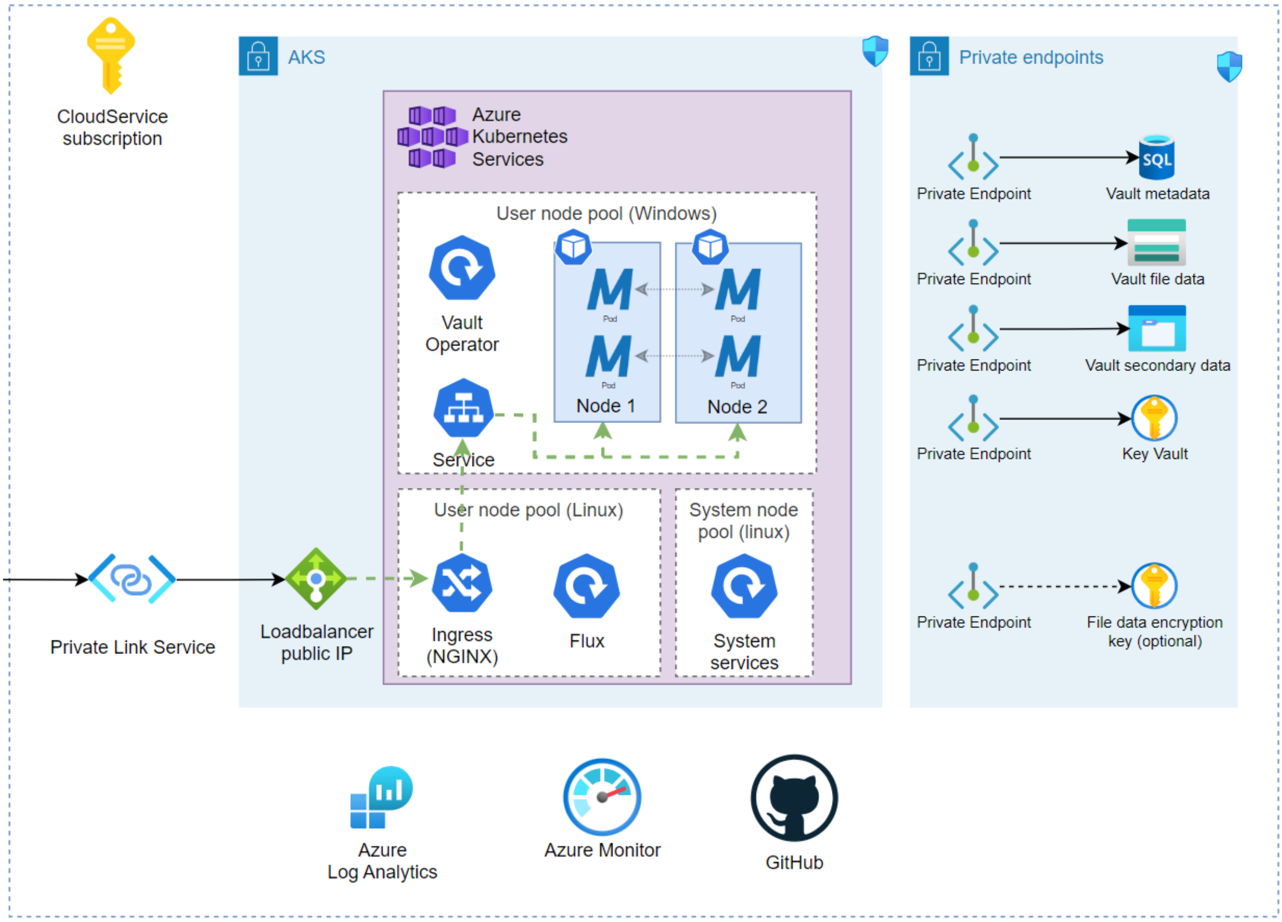


Figure 3: M-Files Cloud service architecture.

A single M-Files Cloud service, as shown in the image above, is a standard unit for delivering the service. In the standard service, customers use a shared cloud service and are hosted on the same nodes. In M-Files Premium Cloud, each customer has their own dedicated cloud service.

3.12 Implementation Examples

Here are some example implementations of M-Files Cloud to illustrate the volumes that our customers have.

METRIC	DESCRIPTION
Power users	10 000
Repository size	150 million documents (70 TB)

METRIC	DESCRIPTION
Power users	50
Read-only users	Tens of thousands
Throughput	Peak of 93,000 new documents per day / 10,000 per hour
Repository size	10 million documents (4 TB)

4. M-Files Premium Cloud

M-Files Premium Cloud is the go-to option for organizations that require scaled experiences. This section tells you the differences between M-Files Premium Cloud and Standard Cloud.

M-Files Premium Cloud is our most secure and scalable cloud-based deployment option for knowledge work automation. With M-Files Premium Cloud, you have the option to deploy additional services for your use.

4.1 Why M-Files Premium Cloud?

Compared to M-Files Standard Cloud, M-Files Premium Cloud provides various additional capabilities, such as:

- Private Azure Subscription
- Private infrastructure and computing resources
- Capability to install unsigned custom applications

The M-Files Premium Cloud also offers a range of additional services, such as:

- Advanced Security Monitoring - included
- Advanced DDoS Protection - included
- Anti-Malware Scan - included
- Private Compute for Databases - included
- Private Network Connectivity - available as additional service

4.2 Additional Capabilities

4.2.1 Private Azure Subscription

An Azure Subscription is a logical container used to provide resources in Microsoft Azure. With M-Files Premium Cloud, all Azure resources for the service are hosted within an Azure Subscription that is dedicated for the customer.

Benefits of private Azure subscription:

- More control: Dedicated resources and predictable performance.
- More flexibility: Additional security and performance services.
- More scalability: Enhanced vertical scaling based on solution requirements.
- Security and compliance: Added transparency and enhanced auditability.

4.2.2 Private Infrastructure and Computing Resources

Private Azure infrastructure and computing resources ensure more predictable performance as there is no load coming from other users. It is easier to scale the infrastructure to precisely match the solution needs. Private infrastructure also enables the activation of advanced security features of Azure.

4.2.3 Capability to Install Unsigned Custom Applications

It is possible to enable the owner of the M-Files Premium Cloud service to install customer-created code (vault applications and scripts) without code validation by M-Files.

4.2.4 Advanced Security Monitoring

Enhanced security monitoring implements advanced incident monitoring for your M-Files Cloud with Microsoft Defender for Cloud and Microsoft Sentinel.

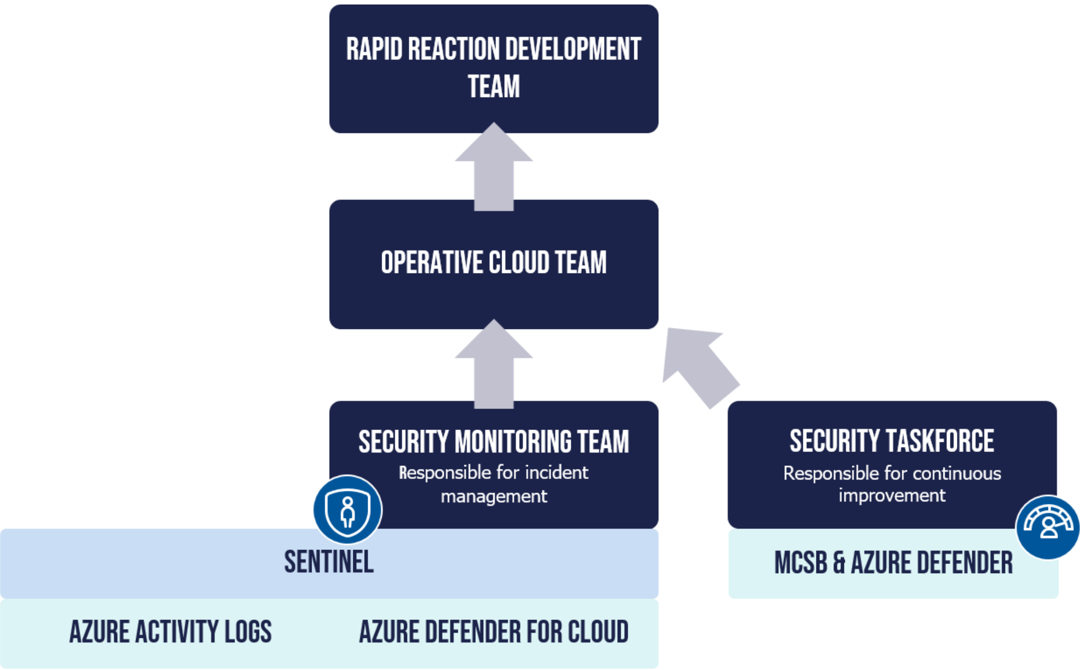


Figure 4: M-Files Cloud security model with advanced security monitoring.

These cloud-native solutions provide the following services:

- Security information and event management (SIEM)
- Security orchestration, automation, and response (SOAR)
- Intelligent security analytics

- Threat intelligence

M-Files uses advanced security monitoring to analyze security incidents and to ensure integrity and security of your data. For more information, refer to Service Description - Advanced Security Monitoring.pptx in the M-Files knowledge base.

4.2.5 Advanced DDoS Protection

M-Files Cloud has Azure Infrastructure protection enabled by default to all customers. To further reduce the risk of service unavailability due to Distributed Denial of Service (DDoS) attacks, we provide Advanced DDoS Protection.

	Standard DDoS Protection	Advanced DDoS Protection
Active traffic monitoring & always on detection	X	X
Automatic attack mitigation	X	X
Availability guarantee		X
DDoS Rapid response support from Microsoft		X

Third-level support from Microsoft's Rapid team is available during an active attack and for post-attack analysis.

For more information, refer to Service Description - Advanced DDoS protection.pptx in the M-Files knowledge base.

4.2.6 Private Network Connectivity

M-Files Private Network Connectivity is an additional service for M-Files Premium Cloud customers. It enables secure one-way connections from office networks to M-Files Cloud services.

When Private Network Connectivity is enabled, users can access M-Files Cloud only from the customer's office network. This way, M-Files Cloud is accessible only from a private network, which improves security.

M-Files Private Network Connectivity uses Azure Private Link Service. It is a managed service that links the customer's private network to the virtual network of the M-Files Cloud service.

5. Add-Ons

The add-ons given in this section are additional services that can be included in your M-Files Cloud subscription.

5.1 Backup Services

M-Files Cloud offers the standard backup service as part of every M-Files subscription. The table below lists the additional services to extend your backup capabilities. You can select to use both extended backup and backup delivery to expand your services backup capabilities. These services are not included in the standard backup capabilities.

M-Files has extensive in-client data recovery capabilities, which reduces the need for regular backups. For more information, see section 3.4.1.

5.1.1 Extended Backup

STANDARD BACKUP	EXTENDED BACKUP	BACKUP DELIVERY
	ALL STANDARD BACKUP FEATURES	*ALL STANDARD BACKUP FEATURES*
Daily document vault backups	One recovery point per day for the last 35 days	Storing quarterly backups for a year
One recovery point per day for the last 7 days		Quarterly backup available for download

Extended backup increases daily restore points from 7 to 35 days. This covers cases where the requirement to return the system to an earlier state exceeds the 7 days that standard backup offers. Extended backup is purchased separately for each vault.

5.1.2 Backup Delivery

For customers who want to have regular copies of their data available as separate backups, we offer the backup delivery service. This service lets customers download copies of their data from M-Files Cloud to an off-site location.

Backup delivery is purchased separately for each vault. Backup deliveries are also available as a one-time service.

5.2 Isolated Container

By default, customer data in M-Files Cloud is isolated on multiple levels. However, some M-Files use cases require an even higher level of isolation. For that purpose, we offer isolated containers. An isolated container means that a dedicated, containerized environment is reserved for the customer's M-Files subscription.

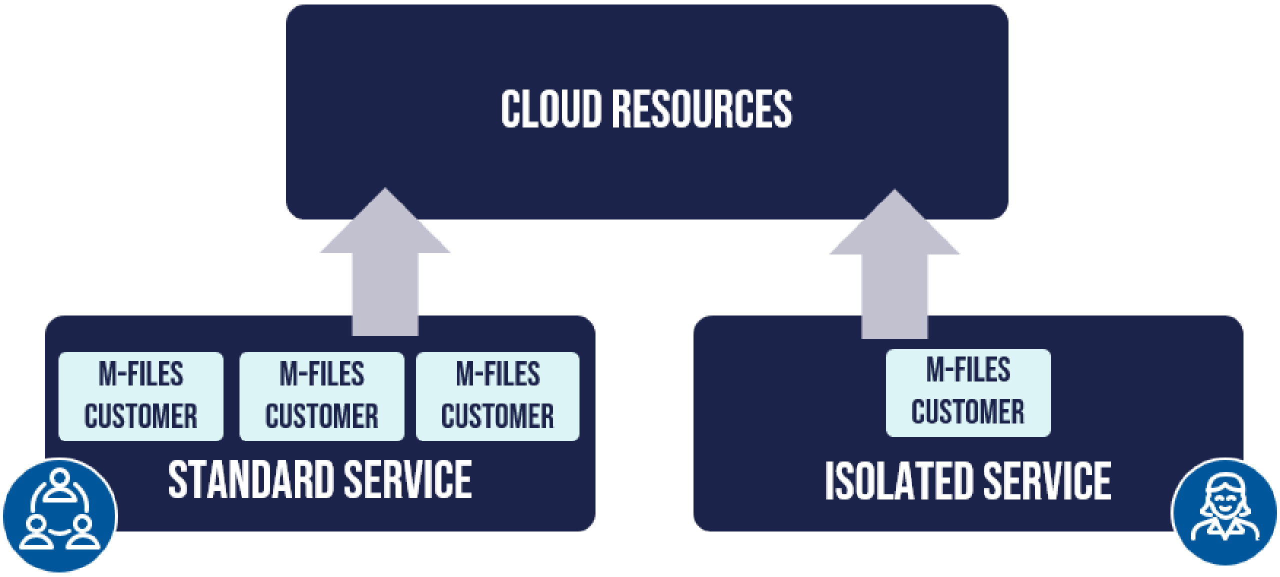


Figure 5: M-Files Cloud isolated container

The standard service implements a base layer of isolation with each hosted service in its own virtual container. The isolated container adds another layer of isolation, where a single container is owned by a single customer.

You can purchase multiple isolated services, for example, to isolate your quality control and production environments from each other.

Isolated containers are specific to cloud regions, which is an important factor to consider when designing your M-Files architecture:

- I want M-Files to host vaults in the UK and US regions.
  → Two isolated containers needed.
- I want to control the upgrade schedule of production and QA environments within the same region separately.
  → Two isolated containers needed.

If you want to control the upgrade schedule of the production environment, but the development environment can be upgraded with the standard upgrade cycle, isolated container is needed only for the production environment.

5.3 Custom Upgrade Schedule

Custom Upgrade Schedule (CUS) allows you to control M-Files product update cycle outside the usual monthly release. We offer specific stable M-Files versions for long-term support (LTS) to minimize changes to your M-Files Cloud environment. You will still receive critical security updates, but any functional updates for the M-Files product are scheduled separately.

LTS version of M-Files is released twice a year. Each version is supported for 15 months from the release with service releases. You can select when to update to a new version. Upgrades are separately scheduled with M-Files.

6. What is Expected from the Customer?

In M-Files Cloud, you as M-Files Customer are responsible for:

- Managing M-Files users with M-Files Manage
- Using supported software versions and devices to access the M-Files Cloud vaults
- Maintaining vault trusted person information in M-Files Manage
- Clearly communicating any special system or technical requirements, if applicable, to your M-Files contact
- Communicating swiftly to M-Files Customer Support, or M-Files Key Account Manager if there are any technical or service issues in the manner agreed in the contractual documents.

7. Compliance and Certifications

M-Files operates an ISO and SOC certified Quality and Information Security Management System to provide you with a secure and high-quality service and takes a legal and ethical approach to its business practices.

Our cloud operations have been certified for the ISO 27001:2013 standard and our quality system adheres to the ISO 9001:2015 standard. Additionally, M-Files has been certified for SOC2. You can find full list of M-Files Certifications from https://www.m-files.com/m-files-compliance/.

8. M-Files and Microsoft Azure Consumption Commitment (MACC)

M-Files Cloud is eligible for Microsoft Azure consumption commitments (MACC/CtC). When you buy the M-Files Cloud service through the Azure Marketplace, the capacity costs of the service are taken into account in your MACC contract.

Learn more about Azure consumption commitment benefit at https://learn.microsoft.com/en-us/marketplace/azure-consumption-commitment-benefit.

9. Changes to Service Description and Delivery

We reserve the right to modify the service, the service description, and the methods of service delivery at any time. We continuously improve our cloud platform which might influence the way we deliver the M-Files Cloud service.

10. Change History

The table describes the changes by document version.

VERSION	DATE	ESSENTIAL CHANGES
1.0	2023/11/28	Initial version.
1.1	2024/01/05	Section 9 added.
1.2	2024/01/22	Added information about outage communication. Other minor changes throughout the document.
1.3	2024/02/20	Added an illustration of standard and isolated service deployment to section 5.2.
1.4	2024/04/14	Added sections about disaster recovery and data availability.
1.5	2024/04/18	Added section on Advanced DDoS Protection, modified disaster recovery details.
1.6	2024/06/12	Section 4.2.6 about Private Network Connectivity added.
1.7	2024/08/28	Added more details about security, isolation, example cases, architecture image, and scalability.
1.8	2025/01/02	Added details about architecture and monitoring. Added backup service model.
1.9	2025/01/02	Updated terminology and removed duplicate paragraph in section 3.5.
2.0	2025/01/13	Expanded availability and performance descriptions.
2.1	2025/01/23	Added details for backup and availability mechanisms.
2.2	2025/04/17	Added Cloud plans and Premium Cloud description.