AMOSSYS

MFT online

OPEN TRUST

Cible de sécurité CSPN

Logiciel single-tenant MFT online en tant que service (SaaS) version 4.4.1.0 en hébergement On Premise

Référence : CSPN-CDS-MFT online-2.22 Publique

Date : 09/03/2026

Référence interne : EQS006

Siège : Immeuble Le Ouessant • Bâtiment B • 11 rue Maurice Fabre • 35000 Rennes • France • **www.amossys.fr**
SIRET : 493 348 890 00051 • **NAF** : 6202 A • RCS Rennes B 493 348 890 • SAS au capital de 38.000 Euros

FICHE D'EVOLUTIONS

Révision	Date	Description	Rédacteur
1.05	10/07/2020	Cible de sécurité de MFT version 3.4	Amossys
2.00	22/03/2024	Mise à jour de la cible pour MFT online version 4.3	Emilie PRUNIER Gilles POIRET
2.10	28/11/2024	Mise à jour suite aux remarques de l'ANSSI	Philippe GAUTIER
2.11	12/12/2024	Mise à jour de la cible pour MFT online version 4.4	Philippe GAUTIER Gilles POIRET
2.20	01/09/2025	Ajustements de la cible : - ajout de COTS ; - Ajout d'une protection d'un flux	Amossys / Equisign
2.21	15/12/2025	Mise à jour de la plate-forme cible : Redhat Enterprise Linux 9.7 / Rocky Linux	Amossys / Equisign
2.22	09/03/2026	Suppression d'informations confidentielles	Equisign

Ce document a été validé par EQUISIGN après relecture.

SOMMAIRE

1. INTRODUCTION

1.1. OBJET DU DOCUMENT

Ce document est réalisé dans le cadre de l'évaluation, selon le schéma CSPN promu par l'ANSSI, du produit **MFT online**, développé par la société **Equisign**.

Ce document est soumis au contrôle technique et qualité d'**AMOSSYS** ainsi qu'à la validation de **Equisign**. Les mises à jour de ce document sont effectuées par l'équipe projet d'**AMOSSYS**.

1.2. IDENTIFICATION DU PRODUIT

Éditeur	**Equisign** Tour Opus 12 77 Esplanade du général de Gaulle 92081 Paris La Défense Cedex
Lien vers l'organisation	www.mftonline.fr
Nom commercial du produit	MFT online
Numéro de la version évaluée	4.4.1.0
Domaine CSPN	Stockage sécurisé

1.3. REFERENCES

Pour l'établissement de la présente cible de sécurité, les documents suivants ont été consultés par le rédacteur.

Description	Référence
Précédente cible de sécurité	CSPN-CDS-MFT online-2.11
Précédentes Spécifications cryptographiques	CSPN-SC-MFT onLine-2.11
IAR	CSPN-RAI-MFT online v4.4-4.4.1.0-1.10
Procédure CSPN en vigueur	ANSSI-CSPN-CER-P-01_v5.0
Méthodologie d'évaluation CSPN pour les logiciels déployés sur des infrastructures de Cloud Computing	ANSSI-CSPN-NOTE-06_v1.1-1
Managed File Transfer Server Installation and Upgrade Guide	MFT_Server_Installation_and_Upgrade_Guide

Tableau 1 - Références documentaires

1.4. GLOSSAIRE

Acronyme	Description
AC	Autorité de Certification
AD	*Active Directory*
AES	*Advanced Encryption Standard*

Acronyme	Description
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
API	*Application Programming Interface*
CBC	*Cyber Block Chaining*
CESTI	Centre d'Évaluation de la Sécurité des Technologies de l'Information
COTS	*Commercial Off-The-Shelf*
CSPN	Certification de Sécurité de Premier Niveau
ECDSA	*Elliptic Curve Digital Signature Algorithm*
HMAC	*Hash-based Message Authentication Code*
HSM	*Hardware Security Module*
IV	*Initialization Vector*
JDK	*Java Development Kit*
JVM	*Java Virtual Machine*
LDAP	*Lightweight Directory Access Protocol*
MFT	*Managed File Transfer*
SHA	*Secure Hash Algorithm*
SAML	*Security Assertion Markup Language*
TLS	*Transport Layer Security*
TOE	*Target Of Evaluation*

Tableau 2 - Glossaire

2. DESCRIPTION DU PRODUIT

2.1. DESCRIPTION GENERALE

MFT Online (*Managed File Transfer*) est une solution de transfert de fichiers chiffrés en gros volume à destination des entreprises. Le produit se présente comme une alternative à des solutions grand public, comme WeTransfer, Dropbox ou Google Drive.

La solution dispose d'une interface intuitive qui permet à chaque utilisateur de déposer ses fichiers à destination d'une ou plusieurs personnes ou d'un groupe, en indiquant une durée durant laquelle les fichiers seront accessibles aux destinataires. L'utilisateur a ensuite la possibilité de suivre ou de rechercher des messages. Les fichiers transférés sur MFT peuvent l'être avec des utilisateurs inscrits dans MFT, de l'entreprise ou non, ou avec des contacts ponctuels externes. Aucune restriction de taille ne s'applique aux fichiers téléversés sur la plateforme. Des notifications sont également disponibles pour alerter chaque utilisateur de la réception d'un fichier. La solution MFT permet également une traçabilité complète des échanges de fichiers (envoi et réception, hachage des fichiers, horodatage, etc.)

Enfin, les fichiers peuvent être partagés par des utilisateurs physiques (cas classique de l'envoi d'un fichier par Alice à Bob), ou par des systèmes automatisés logiciels (par exemple, partage automatique d'une facture par un applicatif de paiement).

Le produit est disponible dans plusieurs offres : Cloud public, Cloud privé, ou *On Premise*.

Seule l'offre *On Premise* est évaluée pour cette CSPN.

2.2. PRINCIPE DE FONCTIONNEMENT

Les utilisateurs ont la possibilité d'uploader leurs fichiers sur MFT au travers d'une interface Web. Dans celle-ci, ils peuvent définir un sujet et un message qui seront échangés par email avec le lien de téléchargement du fichier. Ils doivent également définir la liste des destinataires qui seront autorisés à accéder aux fichiers. Ces destinataires peuvent être internes à l'entité, ou externes. Enfin, l'expéditeur peut définir un mot de passe de chiffrement symétrique utilisé pour chiffrer les fichiers (voir précisions ci-après).

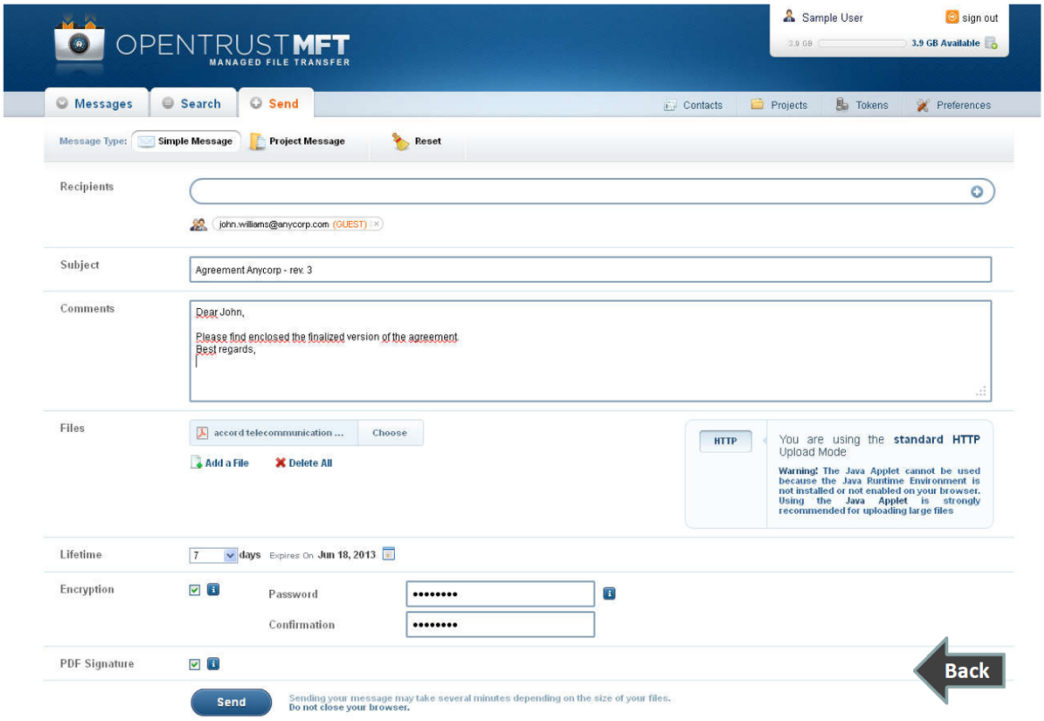

Figure 1 - Envoi d'un fichier par MFT

Les utilisateurs peuvent être des utilisateurs internes ou externes de l'entreprise et qui disposent d'un accès à MFT. Dans ce cas, ils peuvent déposer des fichiers, les partager avec toute personne (disposant ou non d'un compte sur la solution) et les administrateurs peuvent leur appliquer des politiques de sécurité (politique d'envoi (ce qu'il est possible d'envoyer), politique d'échange (à qui il est possible d'envoyer), politique d'authentification (règle d'authentification)), avec une segmentation par Domaine MFT. Par exemple, les utilisateurs d'un domaine A ne pourront envoyer des fichiers PDF qu'aux utilisateurs du domaine B, et pas aux invités. Les utilisateurs peuvent également être des utilisateurs externes à l'entreprise (par exemple, des prestataires). Ceux-ci disposent également d'un compte sur la plateforme, et l'administrateur peut leur appliquer des politiques restrictives (par exemple, possibilité de n'échanger des fichiers qu'avec les utilisateurs membres d'un groupe particulier sur la solution).

Enfin, les utilisateurs de la solution ne disposant pas de compte sont des invités et n'ont pas, par défaut, la possibilité de déposer des fichiers. Ils peuvent simplement accéder aux fichiers qui leurs ont été partagés. Les utilisateurs inscrits sur la plateforme peuvent cependant leur envoyer, au travers de MFT, un « token », qui leur permet ensuite de déposer un fichier pendant un laps de temps donné (par exemple, pour déposer un contrat signé) à destination de l'émetteur du token.

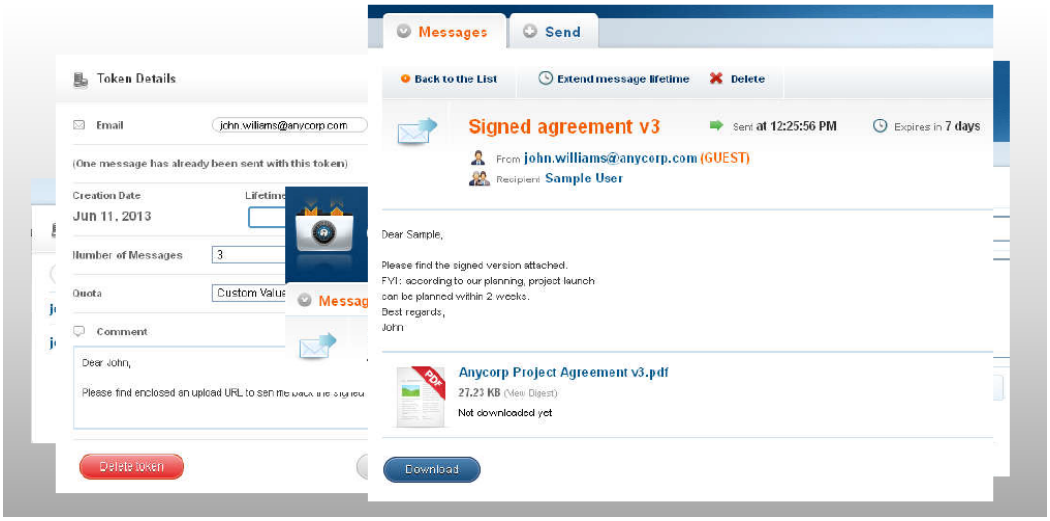

Figure 2 - Partage de fichier par « token »

Plusieurs modes de protection sont disponibles sur le serveur MFT. Ces modes peuvent être activés par configuration d'un administrateur sur le serveur :

- Niveau 0 (par défaut) : les fichiers sont anonymisés avant d'être stockés sur le serveur (le nom du fichier sur le disque est remplacé par un identifiant unique, stocké dans la base de données) ;
- Niveau 1 : les fichiers sont chiffrés en AES-256 avant d'être stockés sur le serveur. La clé de chiffrement est propre à chaque fichier, et est générée aléatoirement pour l'occasion.
- Niveau 2 : les fichiers sont chiffrés en AES-256 en utilisant une clé aléatoire et unique. Cette clé est stockée en base de données après chiffrement par une clé AES-256 stockée dans le HSM (*Hardware Security Module*) du serveur.

Un mode de chiffrement supplémentaire est disponible à la discrétion de l'utilisateur qui uploade les fichiers. Ceux-ci sont alors encapsulés dans une archive chiffrée en AES-256. Dans ce cas, l'utilisateur définit le mot de passe utilisé dans l'interface Web du serveur, au moment où il dépose les fichiers. Celui-ci doit également être renseigné par les destinataires lors de l'accès aux fichiers. Le chiffrement est réalisé par le serveur lors de l'envoi des fichiers, et la clé n'est pas conservée sur le serveur.

La plateforme complète est composée de plusieurs serveurs (physiques ou virtualisés) :

- Un ou plusieurs serveurs servant uniquement de Reverse-Proxy « External/Internal MFT Web », peuvent être placés en DMZ ou en zone serveur interne ; Un ou plusieurs serveurs applicatifs, supports d'un serveur Tomcat, sur lesquels les utilisateurs se connectent via le reverse-proxy, pour déposer ou accéder à des fichiers ;
- Un serveur « MFT-Admin », qui peut être installé sur un des serveurs applicatifs, sur lequel sont démarrés :
    - L'applicatif principal de MFT, en charge du contrôle d'accès et de la gestion des fichiers ;
    - Le module de journalisation ;
- Un serveur de base de données, qui stocke les données de la TOE ;
- Un relais SMTP pour l'envoi des emails de notification ;
- Un système de stockage des fichiers ;
- Une fédération d'identités pour la gestion des droits d'accès ;

- MFT pourra également être connecté à un annuaire Active Directory ou LDAP, pour la gestion des utilisateurs internes (provisioning, mots de passe, etc.). Les utilisateurs externes sont nécessairement gérés par l'application depuis l'interface administrateur.

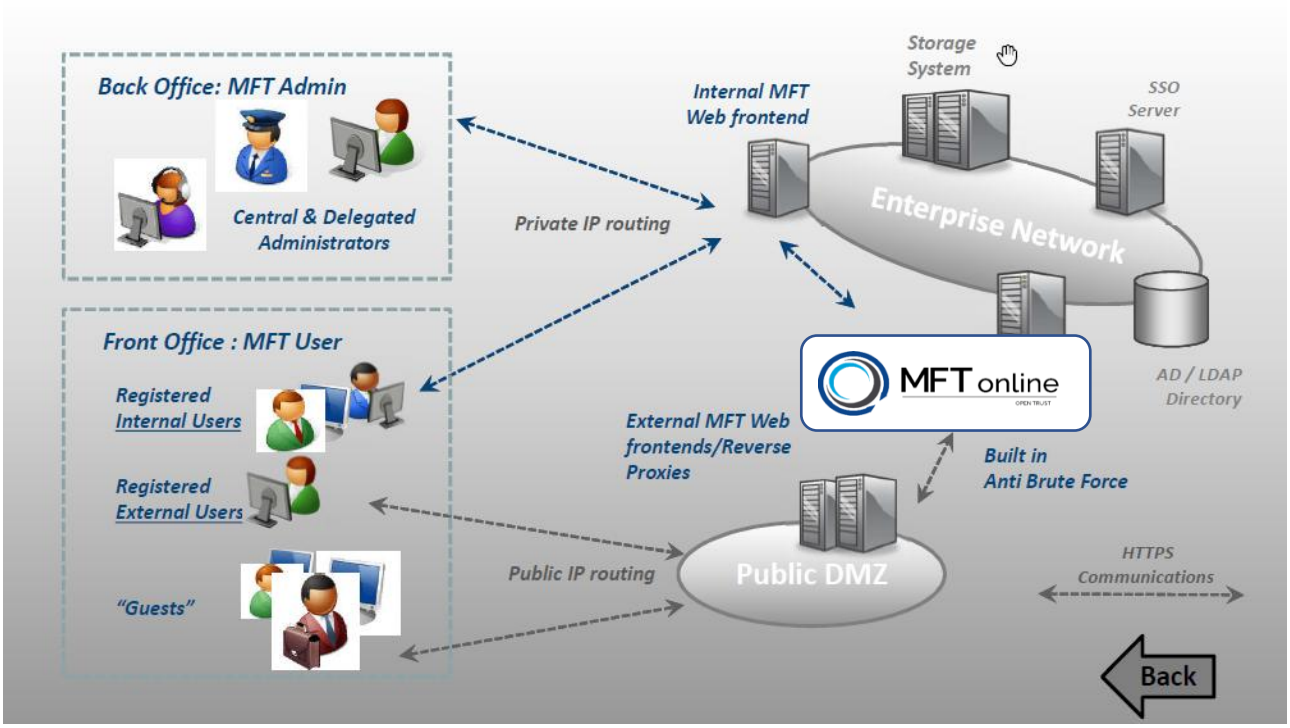

Figure 3 - Schéma d'architecture de la plateforme MFT

2.3. DESCRIPTION DE L'ENVIRONNEMENT TECHNIQUE DE FONCTIONNEMENT

2.3.1. Description des dépendances

Une dépendance est un composant nécessaire à la TOE pour fonctionner, mais non fourni directement par la TOE. Le maintien en condition de sécurité de cet élément doit être assuré par l'administrateur de la plateforme. Ces dépendances peuvent être liées ou non au système hôte.

Cette section liste ces deux types de dépendances, suivant qu'elles soient ou non embarquées dans la distribution du système d'exploitation.

Les dépendances non embarquées dans le système et requises sont les suivantes :

- le composant Apache Tomcat (version 9.0.112) ;
- OpenJDK en version 21 LTS

À cela s'ajoutent les dépendances issues du système hôte, dont la liste est présentée dans le tableau ci-dessous.

Dépendances	Rôle	Version utilisée
Clamd	Antivirus	1.4.3-3.el9
OpenSSL	Librairie Crypto	3.5.1-4.el9

Tableau 3 - Liste des dépendances issues du système hôte

2.3.2. Matériel compatible ou dédié

La plateforme nécessite 5 serveurs pour faire fonctionner les différentes briques de la solution :

- Le serveur *Frontend* ;
- Le serveur *Backend* (applicatif MFT) ;
- Un serveur de base de données ;
- Un système de stockage des fichiers (serveur NAS de type NFS ou SMB) ;
- Un serveur SMTP pour l'envoi des emails de notification.

Un HSM est nécessaire pour utiliser le niveau 2 de chiffrement des fichiers.

Les serveurs nécessitent le système d'exploitation RedHat 9 ou assimilé.

2.3.3. Système d'exploitation retenu

Les systèmes d'exploitation suivants ont été retenus pour l'évaluation :

- Serveurs : Rocky Linux 9.7 ;
- Poste client : Windows 11.

2.4. PERIMETRE DE L'EVALUATION

2.4.1. Périmètre

L'évaluation porte sur la plateforme MFT Online dans son déploiement **On Premises uniquement**, installé en mode de protection « Niveau 2 », dans lequel tous les fichiers sont chiffrés avec un HSM tiers (bien que le choix du HSM soit laissé libre, l'éditeur recommande Trustway Proteccio NetHSM[1]). L'analyse portera sur les points suivants :

- La sécurité des communications dans l'environnement d'intégration (VLAN, …) de la TOE :
  - entre les composants des serveurs MFT ;
  - entre les serveurs MFT et les navigateurs Web des utilisateurs.
- L'authentification locale et l'identification des utilisateurs ;
- La journalisation des évènements de sécurité ;
- Le stockage sécurisé des données utilisateurs ;
- La protection du matériel cryptographique.

Seuls les 3 serveurs spécifiques à MFT sont considérés dans le périmètre de l'évaluation.

Les éléments considérés comme hors TOE sont les suivants :

- Le serveur de mail et le HSM (ainsi que les communications associées)
- le navigateur Web client ;

La configuration du produit évalué est présentée dans le tableau suivant.

Composant du système global		Non évalué

[1] https://atos.net/fr/produits/cybersecurite/chiffrement-donnees/hsm-trustway-proteccio-nethsm

		Inclus dans la cible d'évaluation (TOE)	(environnement de la TOE)	
			Supposé de confiance[2]	Est un attaquant potentiel
Serveur *Frontend*	Système d'exploitation compatible Red Hat Entreprise 9.x		√	
	Reverse proxy	√		
Serveur *Backend*	Système d'exploitation compatible Red Hat Entreprise 9.x		√	
	Logiciel MFT	√		
	Serveur Applicatif Apache Tomcat		√	
HSM	HSM		√	
Serveur de base de données		√		
NAS	Serveur de fichiers NFS		√	
Mail	Serveur de messagerie		√	
Antivirus	Clamav ou tout autre		√	

Tableau 4 - Configuration du produit évalué

2.4.2. Plateforme d'évaluation

La plateforme d'évaluation sera composée de 3 serveurs métier composant la TOE, ainsi qu'un NAS, et un serveur de messagerie :

- MFT-FRONT_WEB1, pour héberger le serveur frontal utilisateur en *frontend* ;
- MFT-ADMIN_USER1, pour héberger les rôles suivants en *backend*:
  - Serveur d'Application administrateurs ;
  - Serveur d'Application Utilisateurs ;
  - Module de journaux d'audit
- MFT-BDD, pour héberger les données de la TOE ;
- Serveur NAS, pour le stockage des fichiers ;
- un serveur de messagerie

Les utilisateurs se connecteront à la plateforme depuis des navigateurs Mozilla Firefox (en dernière version), sur des postes Windows 11. Les utilisateurs internes et externes sont gérés directement par le serveur MFT *backend*. Les invités utilisent le mode « jeton ».

[2] La bonne configuration des composants de confiance est susceptible d'être vérifiée durant l'évaluation, notamment la partie authentification et sécurisation des flux.

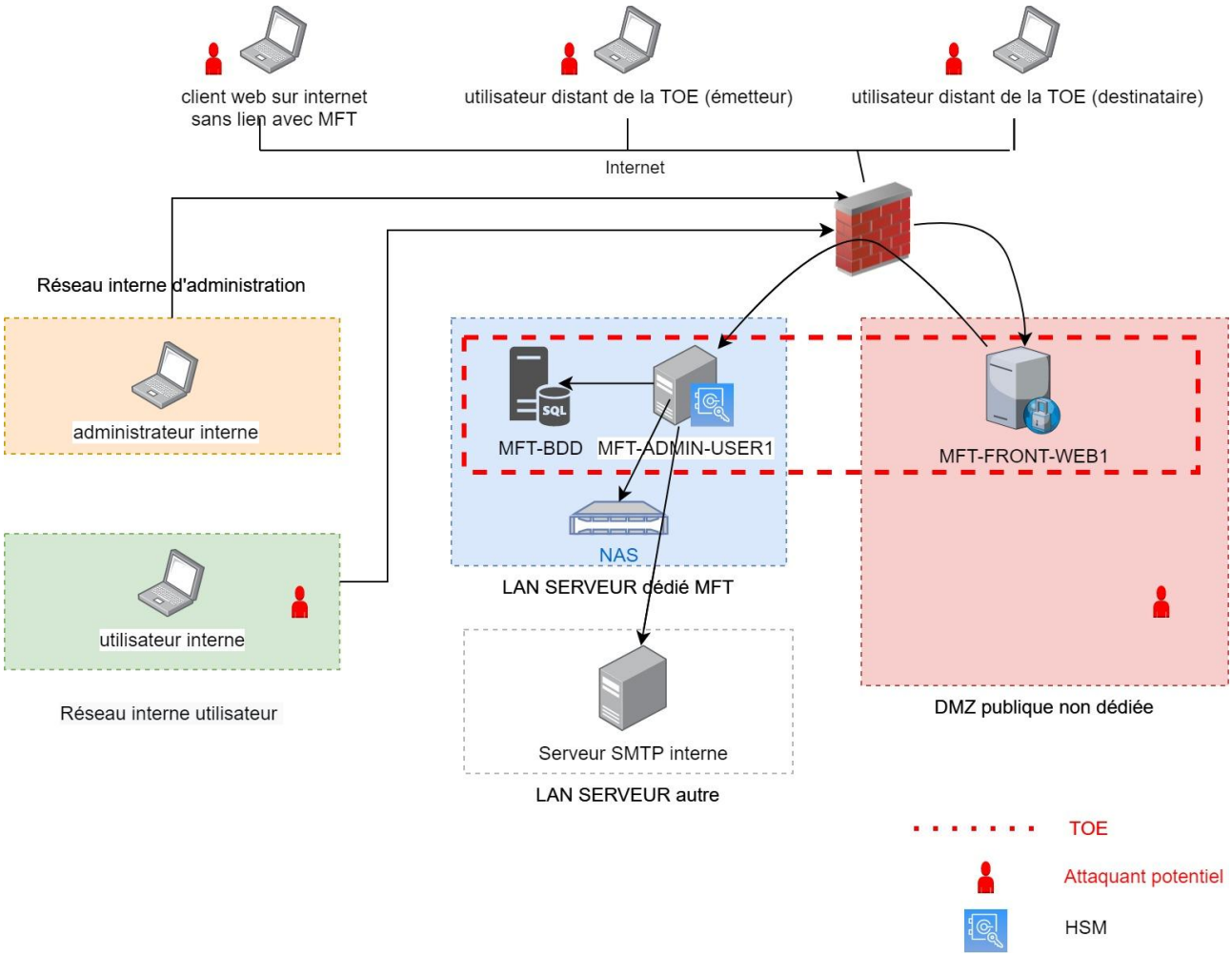

Figure 4 - Schéma de l'architecture utilisée pour l'évaluation et positionnement des attaquants

3. PROBLEMATIQUE DE SECURITE

3.1. DESCRIPTION DES UTILISATEURS DU PRODUIT

Par définition, les utilisateurs concernent les personnes et services applicatifs qui interagissent avec le produit évalué.

Les rôles suivants doivent être pris en considération dans le cadre de l'évaluation de sécurité :

- ***Utilisateur interne :*** utilisateur de la solution, disposant d'un compte utilisateur, et disposant des droits suffisants pour échanger des fichiers avec tout utilisateur (avec ou sans compte) ;
- ***Utilisateur externe :*** utilisateur de la solution, disposant d'un compte utilisateur, et disposant de droits restreints ne lui permettant d'échanger des fichiers qu'avec les utilisateurs internes ;
- ***Invité :*** utilisateur de la solution ne disposant pas de compte utilisateur. Il peut accéder aux fichiers qui lui ont été partagés par des utilisateurs internes, et déposer des fichiers s'il dispose d'un *token* ;
- ***Administrateur :*** utilisateur de la solution, disposant d'un compte utilisateur, et disposant de droits privilégiés lui permettant d'administrer la solution ;
- ***Auditeur :*** utilisateur de la solution, disposant d'un compte utilisateur, et disposant de droits privilégiés lui permettant d'accéder aux journaux de la solution. Il ne dispose pas de droits pour administrer la solution ;
- ***Administrateur système :*** personne en charge d'administrer le système support sur lequel est installée la solution MFT.
- ***Officier de sécurité :*** Personne en charge de la sécurité physique, du réseau et du stockage

Pour la répartition des rôles, le type d'hébergement étant *On Premise*, c'est le bénéficiaire qui a la charge de chaque rôle. C'est donc aussi au bénéficiaire de s'assurer que les hypothèses sont satisfaites.

Tableau 5 - Répartition des rôles

Rôle	Socle	Tenue du rôle
Utilisateur final (Utilisateur interne, externe et invité)	Utilisation métier	Bénéficiaire
Administrateur métier (Administrateur & Auditeur)	Paramétrage métier	Bénéficiaire
Administrateur système	Logiciel et données	Bénéficiaire
	Intergiciels et autres logiciels de base	Bénéficiaire
	Système d'exploitation	Bénéficiaire
	Ressources virtualisées	Bénéficiaire
	Couche de virtualisation	Bénéficiaire

Rôle	Socle	Tenue du rôle
Administrateur de l'infrastructure technique (Administrateur système)	Machines physiques, réseau et stockage	Bénéficiaire
Officier de sécurité	Sécurité des locaux et du personnel	Bénéficiaire

3.2. DESCRIPTION DES BIENS SENSIBLES

Par définition, un bien sensible est une donnée (ou fonction) jugée comme ayant de la valeur par la TOE. Sa valeur est estimée selon des critères de sécurité (aussi appelés besoins de sécurité) : disponibilité, intégrité, confidentialité et authenticité. Les biens à protéger sont les suivants :

- **B1.Système Hôte**

  La TOE n'induit pas de menaces sur le système hôte.

  Besoin de sécurité : disponibilité, intégrité.

- **B2.Fichiers échangés**

  MFT doit protéger les fichiers échangés par ses utilisateurs.

  Besoin de sécurité : intégrité et confidentialité.

- **B3.Matériel cryptographique**

  Les clés de chiffrement utilisées pour chiffrer les fichiers partagés, et les communications réseau.

  Besoin de sécurité : intégrité et confidentialité.

- **B4.Journaux**

  Les évènements générés lors des processus d'authentification, de partage de fichiers, d'accès à un partage, ou de déchiffrement, sont journalisés. Ces données ne sont accessibles que par les auditeurs ou les administrateurs après s'être authentifiés.

  Besoin de sécurité : intégrité et confidentialité.

- **B5.Configuration**

  Les données utiles pour assurer le fonctionnement de la TOE (fichiers de configuration des serveurs Web, de fichiers et SQL du serveur *MFT*).

  Besoin de sécurité : intégrité et confidentialité.

- **B6.Flux réseau**

  Les flux réseau de la TOE entre

  - les postes clients et le serveur frontal.
  - le serveur frontal et le serveur applicatif métier ;
  - Le serveur applicatif métier et le serveur de base de données ;

Le flux réseau vers le NAS est exclu, les fichiers transitant chiffrés.

Besoin de sécurité : intégrité, authenticité et confidentialité.

- **B7. Données d'authentification utilisateur**

  Les données relatives à la connexion des utilisateurs (administrateurs métier inclus) permettant l'accès à un compte MFT.

  Besoin de sécurité : intégrité et confidentialité.

Les besoins de sécurité de chacun des biens à protéger sont synthétisés dans le tableau suivant.

Biens sensibles	Disponibilité	Intégrité	Authenticité	Confidentialité
B1.Système Hôte	√	√		
B2.Fichiers échangés		√		√
B3.Matériel cryptographique		√		√
B4.Journaux		√		√
B5.Configuration		√		√
B6.Flux réseau		√	√	√
B7.Données d'authentification		√		√

Tableau 6 - Besoins de sécurité des biens sensibles

Le tableau ci-dessous permet d'identifier à qui appartiennent les biens sensibles :

Biens sensibles	Utilisateur final	Administrateur métier	TOE
B1.Système Hôte			√
B2.Fichiers échangés	√		
B3.Matériel cryptographique			√
B4.Journaux		√	√
B5.Configuration			√
B6.Flux réseau			√
B7.Données d'authentification	√	√	

3.3. DESCRIPTION DES HYPOTHESES SUR L'ENVIRONNEMENT

Par définition, les hypothèses sont des déclarations portant sur le contexte d'emploi de la TOE ou de son environnement.

- **H1.Administrateurs**

  Les administrateurs système sont considérés de confiance et formés à l'utilisation ainsi qu'à l'administration du système support sur lequel est installé la TOE et des systèmes supports des serveurs participant à la mise en œuvre de la solution.

  Les administrateurs métier de la TOE et les auditeurs sont considérés de confiance et formés à l'utilisation et à l'administration de la TOE.

  L'ensemble des tâches à effectuer pour mettre le produit en condition de sécurité est détaillé dans le guide Managed File Transfer Server Installation and Upgrade Guide, notamment la section « Chapter 3. Securing the Managed File Transfer installation ».

  L'accès à l'interface web d'administration est filtré (conformément à la documentation) au niveau réseau pour n'autoriser que les administrateurs métier et les auditeurs, depuis un réseau dédié, à s'y connecter.

- **H2.Environnement sécurisé**

  Le serveur MFT ainsi que les serveurs participant à la mise en œuvre de la solution sont installés sur des systèmes d'exploitation sains et correctement mis à jour. Les services et partages inutiles sont désactivés. Les serveurs MFT sont dédiés à cet usage.

  Les serveurs *frontend* de la solution MFT sont installés au sein d'une DMZ. En particulier, des moyens techniques sont mis en place en entrée de la DMZ (pare-feu, anti-DDOS, etc.).

  Les serveurs *backend* : serveur applicatif et serveur de base de données, ainsi que le NAS ont un VLAN dédié et, le cas échéant, le HSM physique, dont l'accès est contrôlé au niveau réseau.

  Les serveurs de la solution MFT sont déployés dans un local dont les accès sont nominativement contrôlés.

- **H3.Environnement clients**

  Les postes client sont dotés d'un système d'exploitation et d'un navigateur Web sains et correctement mis à jour, en particulier concernant les correctifs liés à la sécurité.

3.4. DESCRIPTION DES MENACES

Par définition, une menace est une action ou un évènement susceptible de porter préjudice à la sécurité de la cible évaluée.

Les agents menaçants à considérer pour l'évaluation de sécurité doivent être les suivants :

- un attaquant humain ou entité qui interagit avec la TOE mais ne disposant pas d'accès légitime à celle-ci (attaquant hors bénéficiaire) ;
- un utilisateur légitime (muni d'un compte MFT, ou non (invité)) qui souhaite contourner certaines restrictions d'accès (attaquant intra-bénéficiaire).

Cet attaquant peut se trouver sur le réseau internet, le réseau local de l'utilisateur ou en DMZ.

Les administrateurs ne sont pas considérés comme des attaquants (H1).

La présente cible étant en hébergement On Premise et en architecture single-tenant, elle ne dispose donc pas de menace inter-bénéficiaire.

Les menaces portant sur les biens sensibles de la TOE sont les suivantes (tous les agents de menace sont considérés donc chaque menace peut correspondre à un attaquant hors bénéficiaire et intra-bénéficiaire) :

- **M1.Vol des données d'authentification**

  Un attaquant arrive à récupérer les données d'identification et/ou d'authentification d'un utilisateur muni d'un compte MFT.

- **M2.Accès illégitime aux clairs des fichiers**

  Un attaquant parvient à accéder aux fichiers chiffrés d'un utilisateur, stockés sur le serveur MFT ou envoyés à un destinataire, et arrive à les déchiffrer.

- **M3.Altération des données utilisateurs**

  Un attaquant parvient à modifier les données utilisateurs à l'insu de l'utilisateur légitime.

- **M4.Altération des données de journalisation**

  Un attaquant parvient à modifier les données de journalisation afin de masquer des actions illégitimes.

- **M5.Altération des éléments secrets**

  Un attaquant parvient à modifier les clés cryptographiques utilisées pour le chiffrement des fichiers.

- **M6.Altération des données de configuration**

  Un attaquant parvient à modifier les données de configuration du produit dans le but d'abaisser le niveau de sécurité du serveur MFT ou d'exfiltrer des données sensibles.

- **M7.Compromission du système hôte**

  Un attaquant parvient à corrompre le système hôte en exploitant la TOE.

3.5. DESCRIPTION DES FONCTIONS

3.5.1. Fonctions métier

Les fonctions métier sont l'ensemble des fonctions actives et mises en œuvre par la TOE pour assurer son fonctionnement et répondre au besoin pour lequel elle a été développée. Ces fonctions métier ne seront pas évaluées en conformité, mais seront prises en compte en tant que vecteurs d'attaque potentiels sur la TOE. Les fonctions métier de la TOE sont les suivantes :

- **FM1.Dépôt de fichiers**

  La TOE permet aux utilisateurs de déposer leurs fichiers sur MFT au travers d'une interface Web.

- **FM2.Récupération de fichiers**

  La TOE permet aux utilisateurs d'accéder aux fichiers qui leur ont été partagés.

- **FM3.Transfert de fichiers à des tiers interne ou externe**

  La TOE permet aux utilisateurs de partager leurs fichiers avec toute personne disposant ou non d'un compte sur la solution. Ces fichiers transférés sont scannés par un antivirus dont la maintenance est laissée à un administrateur local.

3.5.2. Fonctions de sécurité

Les fonctions de sécurité sont l'ensemble des mesures techniques et des mécanismes mis en œuvre par la TOE pour protéger de façon proportionnée ses biens sensibles contre les menaces identifiées. Les fonctions de sécurité de la TOE à considérer sont les suivantes :

- **FS1. Identification et authentification du bénéficiaire**

  L'accès aux fonctionnalités du produit (compte MFT) est protégé par un système d'authentification. Les utilisateurs internes sont gérés par un serveur d'authentification interne à la TOE, et les utilisateurs externes sont authentifiés via un jeton unique.

  FS2. Contrôle d'accès et gestion des droits/privilèges entre utilisateurs appartenant au bénéficiaire La TOE permet de cloisonner les utilisateurs internes entre différents royaumes et de contrôler les échanges (exemple : les utilisateurs d'un domaine A ne pourront pas accéder aux fichiers utilisateurs du domaine B).

- **FS3.Protection de données**

  Le produit protège en confidentialité et en intégrité les fichiers de l'utilisateur de plusieurs façons :

  - Par défaut, dans le mode de protection de niveau 2, par un mécanisme de chiffrement robuste et non prédictible
  - Si l'expéditeur choisit l'encapsulation des fichiers échangés, ceux-ci sont chiffrés en AES-256, avec un mot de passe défini par l'utilisateur ;

  Dans les tous les cas, les noms de fichiers sont également chiffrés. Le chiffrement est réalisé par le serveur MFT. Les fichiers temporaires téléchargés sont supprimés systématiquement à la fin du processus de chiffrement. Aucun contrôle d'intégrité n'est effectué. Les empreintes SHA-256 des fichiers sont stockées et affichées lors de la réception.

  Le produit assure la protection en confidentialité et intégrité d'une clé nécessaire au chiffrement du niveau 2 en utilisant un HSM pour la stocker. De même, les éléments permettant l'accès aux serveurs tiers (base de données, NAS, …) sont protégés en confidentialité et intégrité.

- **FS4.Communication sécurisée**

  Les flux entre les navigateurs Web des clients et le serveur frontal web MFT sont protégés en intégrité et confidentialité (TLS 1.3). C'est également le cas pour les flux entre le serveur frontal en DMZ et le serveur applicatif interne, et ceux entre le serveur applicatif et la base de données.

- **FS5.Journalisation**

  Le produit assure la protection en intégrité des journaux en les protégeant par un mécanisme de signature et chaînage. Seuls les utilisateurs autorisés peuvent accéder à ces journaux.

3.5.3. Fonctions désactivées

Les fonctions désactivées sont des fonctions considérées comme étant en dehors du périmètre de l'évaluation (hors-TOE). Ces fonctions ne seront pas évaluées, mais seront prises en compte en tant que vecteurs d'attaque potentiels sur la TOE (protection vis-à-vis d'une activation par un attaquant). Les fonctions désactivées de la TOE sont les suivantes :

- **FD1.Contrôle d'intégrité des fichiers**
- **FD2.Gestion de file d'attente dans le traitement des fichiers**
- **FD3.Reprise de téléchargement**
- **FD4.Interface de classification**
- **FD5.Suppression automatique après le premier téléchargement**
- **FD6.Authentification SAML**
- **FD7.Chiffrement au repos activable par domaine**

3.6. MATRICES DE COUVERTURES

3.6.1. Menaces et biens sensibles

La matrice suivante présente la couverture des menaces par rapport aux biens sensibles (les lettres « D », « I », « C » et « A » représentent respectivement les besoins en Disponibilité, Intégrité, Confidentialité et Authenticité).

	B1.Système Hôte	B2.Fichiers échangés	B3.Matériel cryptographique	B4.Journaux	B5.Configuration	B6.Flux réseau	B7.Données d' authentification
M1.Vol des données d'authentification		C		C			**C**
M2.Accès illégitime aux fichiers		**C**					
M3.Altération des données utilisateurs		**I**					
M4.Altération des données de journalisation				**I**			
M5.Altération des éléments secrets		**D**	**IC**			**IC**	
M6.Altération des données de configuration					**IC**		
M7.Compromission du système hôte	**DICA**	**DICA**	**DICA**	**DICA**	**DICA**	**DICA**	**DICA**

Tableau 7 – Couverture des biens sensibles par rapport aux menaces

3.6.2. Menaces et fonctions de sécurité

La matrice suivante présente la couverture des menaces par rapport aux fonctions de sécurité.

	FS1. Identification et authentification du bénéficiaire	FS2. Contrôle d' accès et gestion des droits/privilèges entre utilisateurs appartenant au bénéficiaire	FS3.Protection de données	FS4.Communication sécurisée	FS5.Journalisation
M1.Vol des données d'authentification	√				
M2.Accès illégitime aux fichiers		√	√	√	
M3.Altération des données utilisateurs		√	√	√	
M4.Altération des données de journalisation				√	√
M5.Altération des éléments secrets			√		
M6.Altération des données de configuration		√			
M7.Compromission du système hôte		√			

Tableau 8 – Couverture des menaces par rapport aux fonctions de sécurité

3.7. SURFACE D'ATTAQUE

Note : cette section devrait être retirée de la cible qui sera publiée avec le rapport de certification.

Cette section décrit l'ensemble des moyens par lesquels il est possible d'interagir avec le produit (interfaces physiques, logiques, locales ou distantes).

Compte tenu du type de produit (*systèmes et applicatifs*), **seules les surfaces d'attaque logiques** (et non physiques) sont prises en compte dans le tableau ci-après.

En bleu sont indiqués les flux associés aux administrateurs, en orange les utilisateurs des utilisateurs.

Serveur de la TOE	Interfaces (accessibles ou non accessibles)	Fonction concernée (évaluée ou non)	Acteurs ayant accès aux interfaces
MFT-FRONT-WEB1	0.0.0.0:443 (https) URL : /mft	FS4	Administrateur venant du réseau d'administration
	0.0.0.0:443 (https) URL : *autres que /mft*	FS4	Tout utilisateur venant des réseaux interne et externe (Internet)
MFT-ADMIN-USER1	0.0.0.0:8443 (https) URL : /mft	FS1, FS2, FS4	Administrateur venant depuis le réseau d'administration, accès via MFT-FRONT-WEB1 exclusivement
	0.0.0.0:8443 (https) URL : /zephyr	FS1, FS2, FS3, FS4, FM1,FM2, FM3	Tout utilisateur venant des réseaux interne et externe (Internet), accès via MFT-FRONT-WEB1 exclusivement
	0.0.0.0:9443 (https) URL : /mft/logs	FS1, FS2, FS5	Administrateur connecté depuis le réseau d'administration, accès via MFT-FRONT-WEB1 exclusivement
MFT-BDD	0.0.0.0:5432	FM1, FM2	Compte de service, accès via MFT-ADMIN-USER1 exclusivement.

Tableau 9 – Surface d'attaque

Fin du document