AMOSSYS

VirtualBrowser

CIBLE DE SECURITE DU LOGICIEL SINGLE-TENANT VIRTUALBROWSER EN TANT QUE SERVICE (SAAS) EN HEBERGEMENT ON-PREMISE

VirtualBrowser

2025-12-08
Version 1.07
Référence : CSPN-CDS-VirtualBrowser-1.07
Code interne : OOD017

Amossys
11 Rue Maurice Fabre
35000 Rennes
SAS au capital de 38 000 €
SIREN 493 348 890
TVA FR 21 493 348 890

www.amossys.fr

FICHE D'EVOLUTION

Révision	Rédacteur	Description	Date
0.10	Emilie Prunier	Version originale	12/02/2024
0.20	Emilie Prunier	Prise en compte des retours du développeur	22/02/2024
0.30	Emilie Prunier	Prise en compte des retours du développeur	18/03/2024
0.40	Emilie Prunier	Prise en compte des retours du développeur	26/03/2024
0.50	Emilie Prunier	Prise en compte des retours du développeur	04/04/2024
0.60	Emilie Prunier	Prise en compte des retours du développeur	26/04/2024
1.00	Emilie Prunier	Version finale, communiquée à l'ANSSI lors du dépôt du dossier	24/05/2024
1.01	Emilie Prunier	Changement de nom du commanditaire	01/10/2024
1.02	Emilie Prunier	Mise à jour suite aux remarques de l'ANSSI	28/10/2024
1.03	Emilie Prunier	Mise à jour au démarrage de l'évaluation	12/02/2025
1.04	Mathieu Lafon	Mise à jour pour une évaluation sur une nouvelle version	10/07/2025
1.05	Mathieu Lafon	Prise en compte des retours de l'ANSSI et mise à jour des COTS	06/08/2025
1.06	Mathieu Lafon	Version publique	24/11/2025
1.07	Mathieu Lafon	Ajout références documentaire	08/12/2025

Ce document a été validé par **VirtualBrowser**.

SOMMAIRE

1. INTRODUCTION **4**

1.1 Objet du document **4**

1.2 Identification du produit **4**

1.3 Références **4**

1.4 Glossaire **5**

2. DESCRIPTION DU PRODUIT **6**

2.1 Description générale **6**

2.2 Principe de fonctionnement **7**

2.2.1 Protection du poste de l'utilisateur lors de la navigation 7

2.2.2 Protection de l'accès aux serveurs métier de l'entreprise 8

2.2.3 Administration du produit 8

2.2.4 Architecture détaillée 8

2.3 Description des dépendances **9**

2.4 Description de l'environnement technique et de fonctionnement **10**

2.4.1 Matériel compatible ou dédié 10

2.4.2 Système d'exploitation retenu 10

2.5 Périmètre de l'évaluation **11**

2.5.1 Périmètre 11

2.5.2 Plateforme d'évaluation 12

3. PROBLEMATIQUE DE SECURITE **13**

3.1 Description des utilisateurs du produit **13**

3.2 Description des biens sensibles **14**

3.3 Description des hypothèses sur l'environnement **15**

3.4 Description des menaces **16**

3.5 Description des fonctions de sécurité **17**

3.5.1 Fonctions métier 17

3.5.2 Fonctions de sécurité 17

3.5.3 Fonctions désactivées 19

3.6 Description de la surface d'attaque **19**

3.7 Matrices de couverture **20**

3.7.1 Menaces et biens sensibles 20

3.7.2 Menaces et fonctions de sécurité 21

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 VirtualBrowser en hébergement *On-Premise*, développé par la société **VirtualBrowser**.

Ce document a été initialement créé par **AMOSSYS** et a, par la suite, été repris et modifié par **VirtualBrowser**.

1.2 Identification du produit

Editeur	**VirtualBrowser** 18 rue de Miromesnil 75008 Paris
Lien vers l'organisation	https://www.virtualbrowser.com
Nom commercial du produit	VirtualBrowser
N° de la version évaluée	4.0.9
Catégorie du produit	Communication sécurisée

1.3 Références

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

Tableau 1 - Références documentaires

Référence	Description
[Doc-Admin]	« Documentation VirtualBrowser 4.0 » • VirtualBrowser 4.0 – Guide d'installation serveur version 2025-08-r1 du 31/07/2025 • VirtualBrowser 4.0 – Guide d'administration version 2025-08-r1 du 01/08/2025 • VirtualBrowser 4.0 – Guide d'utilisation version 2025-08-r1 du 29/07/2025
[Doc-Archi]	VirtualBrowser 4.0: Dossier d'architecture, 2024-02-07
CSPN-CER	« Certification de sécurité de premier niveau des produits des technologies de l'information », ANSSI-CSPN-CER-P-01_v5.0
[NOTE-06]	« Méthodologie d'évaluation CSPN pour les logiciels déployés sur des infrastructures de Cloud Computing », ANSSI-CSPN-NOTE-06, version en vigueur
[NOTE-09]	« Contenu et structure de la cible de sécurité CSPN », ANSSI-CSPN-NOTE-09_v1.0

1.4 Glossaire

Tableau 2 - Glossaire

Acronyme	Définition
ANSSI	Agence nationale de la sécurité des systèmes d'information
BDD	Base de données
BYOD	*Bring Your Own Device*
CESTI	Centre d'Évaluation de la Sécurité des Technologies de l'Information
DMZ	*Demilitarized Zone*
ICAP	*Internet Content Adaptation Protocol*
LDAP	*Lightweight Directory Access Protocol*
SAML	*Security Assertion Markup Language*
SaaS	*Software as a Service*
SSH	*Secure Socket Shell*
TOE	Target Of Evaluation
COTS	Commercial Off-The-Shelf
TOTP	*Time-based One-Time Password*
HTTPS	*Hypertext Transfert Protocol Secure*
HTTP	*Hypertext Transfert Protocol*
TLS	*Transport Layer Security*

2. DESCRIPTION DU PRODUIT

2.1 Description générale

Le produit VirtualBrowser est une solution de navigation déportée (*Remote Browser Isolation*) visant à protéger de manière proactive le poste de l'utilisateur en isolant physiquement son activité de navigation.

Trois modes de configuration sont possibles :

- **Chaînage au proxy local** : le proxy du client intercepte les connexions et prend la décision de rediriger dans VirtualBrowser tout ou partie du trafic selon les catégories, les utilisateurs ou d'autres critères qu'il aura définis. Cette possibilité dépend des fonctionnalités proposées par le proxy du client ;
- **Proxy des postes** : le serveur VirtualBrowser est proxy du poste. Il intercepte toutes les connexions et les redirige dans VirtualBrowser. Les règles de navigation se paramètrent dans la Management Platform VirtualBrowser ;
- **Mode explicite** : depuis n'importe quel poste de travail, l'utilisateur entre l'URL du serveur VirtualBrowser sur un navigateur supporté et s'authentifie. Il peut ensuite surfer sur n'importe quel site, de manière sécurisée, depuis le serveur distant VirtualBrowser. Cela permet également de sécuriser l'accès aux applications métiers dans le cadre du BYOD et pour les postes non maîtrisés.

Figure 1 – VirtualBrowser, solution de navigation déportée



Quel que soit le mode de configuration, les pages web sont chargées sur un serveur et rendues à l'utilisateur via un streaming vidéo. Chaque session de navigation déclenche l'instanciation d'un container dédié à l'utilisateur, dans lequel seront effectués le rendu des pages et l'exécution des codes actifs. Le produit gère les interactions de l'utilisateur et l'affichage du rendu final afin de rendre l'utilisation la plus transparente possible tout en protégeant le poste et en permettant de limiter certaines interactions lorsque cela est nécessaire.

Des règles de navigation et de gestion des fichiers peuvent être paramétrées pour répondre à certaines menaces.

La solution est disponible sous deux formes :

- ***Cloud*** : la solution est déployée dans le *Cloud*. L'ensemble des composants est hébergé dans l'infrastructure d'un *cloud provider* dont les serveurs sont hébergés en France. Aucune installation n'est requise par le client.
- ***On-Premise*** : l'ensemble de la solution est hébergée par le client, ce qui lui permet de maitriser l'intégralité des éléments de la solution. **VirtualBrowser** fournit alors à ses clients la solution sous forme de *virtual appliance* ou permet l'installation sur certains OS supportés.

Seule la méthode *On-Premise* est évaluée, en utilisant la *virtual appliance* fournie.

2.2 Principe de fonctionnement

Le produit s'utilise depuis n'importe quel navigateur récent, avec deux cas d'usage principaux.

2.2.1 Protection du poste de l'utilisateur lors de la navigation

L'utilisateur dispose d'un navigateur ou d'un poste préalablement configuré avec l'infrastructure VirtualBrowser comme proxy web et comme autorité de confiance. Il pourra continuer à naviguer de manière habituelle, en lançant son navigateur ou en cliquant sur des liens (mail, favoris, pdf, …). Sa navigation sera automatiquement redirigée vers le serveur VirtualBrowser qui l'authentifiera, puis appliquera la politique de sécurité définie.

VirtualBrowser propose plusieurs méthodes d'authentification des utilisateurs :

- Authentification via login/mot de passe. Les utilisateurs sont créés manuellement depuis l'interface d'administration ;
- L'ajout d'un serveur d'authentification LDAP permet aux utilisateurs de s'authentifier à VirtualBrowser avec leurs identifiants LDAP. Il est possible de configurer plusieurs serveurs LDAP ;
- VirtualBrowser propose un service d'authentification unique aux applications web fondé sur SAML V2. Il est possible de créer plusieurs configurations SAML. Le serveur doit être configuré pour signer les assertions SAML avec des algorithmes recommandés par l'ANSSI.

Lorsque cela sera nécessaire, une session de navigation déportée sera alors automatiquement démarrée dans un container vierge, instancié pour l'occasion. À la fin de la navigation, ce dernier sera automatiquement détruit.

2.2.2 Protection de l'accès aux serveurs métier de l'entreprise

L'utilisateur en mobilité agissant en qualité d'interne, prestataire, sous-traitant, etc. dispose d'un navigateur et d'un accès à un serveur VirtualBrowser accessible depuis Internet. Il pourra se connecter au serveur VirtualBrowser afin de lancer une session de navigation déportée, lui permettant de naviguer sur des serveurs métier situés sur le réseau interne. Le pare-feu protégeant le serveur VirtualBrowser permet à un utilisateur externe de s'y connecter sur le port 443 TCP. Ainsi, les serveurs métier ne seront pas accédés directement par l'utilisateur et son navigateur (potentiellement non sécurisé, non maîtrisé), mais uniquement par le navigateur instancié dans le container du serveur VirtualBrowser, limitant de ce fait les risques d'attaque et les interactions avec l'application qui pourront être limités afin, par exemple, de réduire la fuite d'information.

2.2.3 Administration du produit

L'administration de VirtualBrowser se fait à partir d'une console d'administration web. Les administrateurs s'authentifient via *login*/mot de passe. Une authentification multifacteurs avec l'utilisation d'un mot de passe à usage unique (OTP) est également implémentée. Après authentification sur la console et selon les droits dont il dispose, l'administrateur accède à l'interface de management de la solution.

Les différentes fonctions d'administration sont :

- Authentification des utilisateurs : création de comptes et groupes locaux, configuration d'une authentification externe (LDAP, SAML) ;
- Configuration : activation et paramétrage des différentes fonctionnalités, catégorisation des URLs, règles de navigation et de téléchargement ;
- Supervision : accès aux logs, à l'état du ou des serveurs, aux informations sur les containers actifs.

Un accès système en SSH permet d'effectuer des tâches de maintenance et de diagnostic.

2.2.4 Architecture détaillée

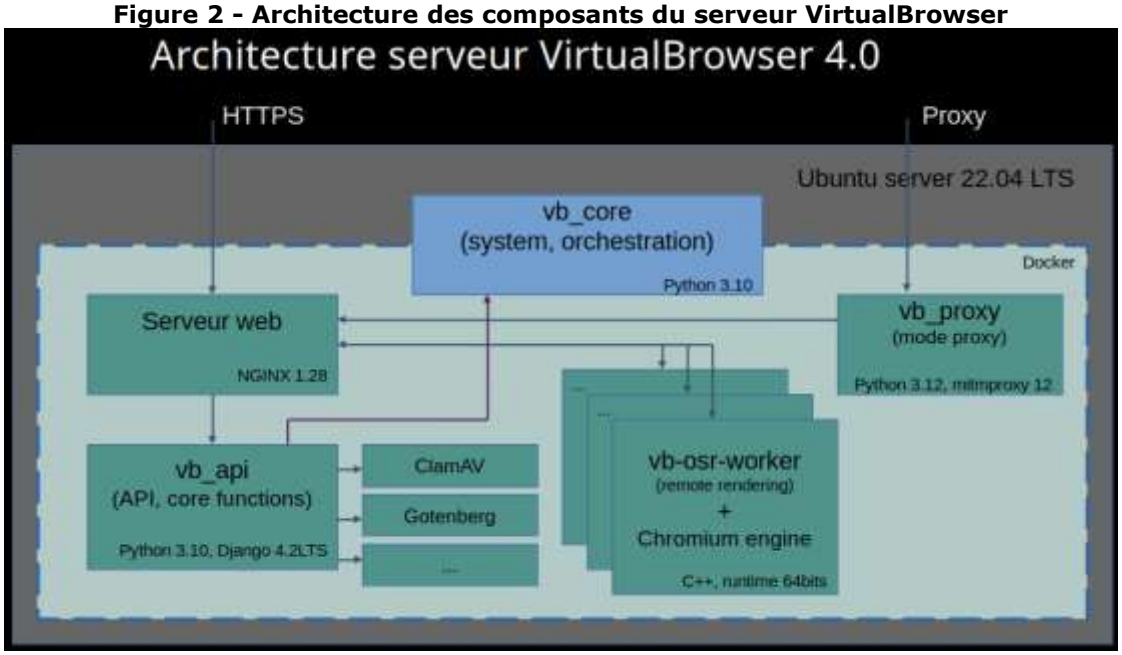
L'architecture détaillée du serveur VirtualBrowser est la suivante :

- Le composant `vb_core` est chargé à la fois des interactions avec le système et de l'orchestration des différents containers ;
- Le serveur web est un container NGINX qui gère l'ensemble des flux HTTP/HTTPS du produit ;
- Le composant `vb_api` gère principalement les différentes requêtes d'API ;
- Le composant `vb_proxy` gère les connexions proxy provenant des utilisateurs. Il est basé sur le composant *opensource* mitmproxy[1] et réalise une interception SSL/TLS de la majorité des connexions HTTPS ;
- Le container `vb-osr-worker` est le composant principal d'une session de navigation VirtualBrowser en permettant l'interaction entre le client VirtualBrowser et le moteur Chrome. Il y a autant de containers vb-osr-worker que de sessions de navigation actives.

Mis à part le composant `vb_core`, les autres composants sont déployés dans des containers docker.

[1] https://github.com/mitmproxy/mitmproxy

Figure 2 - Architecture des composants du serveur VirtualBrowser



La fonctionnalité WebGL sera désactivée dans le cadre de l'évaluation, permettant ainsi de limiter la consommation des ressources sur le serveur VirtualBrowser.

La fonctionnalité d'authentification par certificat client, non activée par défaut et nécessitant l'utilisation d'une extension, ne sera pas évaluée.

2.3 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.

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

- Hyperviseur : chaque *appliance* VirtualBrowser est déployée sur un hyperviseur VMWare ESX/ESXi, Proxmox, Hyper-V ;
- Base de données : un serveur de BDD externe MySQL/MariaDB ou PostgreSQL est nécessaire dans une configuration cluster, afin d'héberger la configuration et certaines données internes. La configuration cluster n'est pas évaluée ;
- Serveur *Identity Provider* dans le cadre de l'authentification SAML V2.

À cela s'ajoutent les dépendances issues du système hôte, dont la liste est présentée la suivante :

- Dépôts Ubuntu : dépôts principaux et liés aux mises à jour de sécurité.
- Dépôts et Registry (Docker) VirtualBrowser : permettant l'accès aux mises à jour applicative de la solution
- Serveurs de mise à jour des bases de signatures antivirales ClamAV.

2.4 Description de l'environnement technique et de fonctionnement

2.4.1 Matériel compatible ou dédié

Le serveur VirtualBrowser est livré sous la forme d'une Appliance Virtuelle (OVA) disponible pour les infrastructures VMware, Proxmox, Hyper-V, fondée sur une version serveur d'Ubuntu 22.04 LTS. L'installation sur certains OS supportés (Debian 12, Ubuntu 22.04 LTS, Ubuntu 24.04 LTS, RHEL 8 et RHEL 9) est également possible. **VirtualBrowser** recommande de déployer les serveurs dans une DMZ afin que ces derniers soient limités dans leurs accès sur le réseau interne.

Deux types d'architecture sont disponibles pour le déploiement du serveur :

- L'architecture single : les services VirtualBrowser sont réunis sur un seul et unique serveur virtuel. L'architecture single sera limitée aux configurations ne nécessitant pas plus de 100 sessions simultanées ;
- L'architecture cluster : permet de déployer plusieurs serveurs. Cette architecture est recommandée pour toute configuration nécessitant plus de 100 sessions simultanées.

Dans le cadre de l'évaluation, l'architecture single est retenue. Le tableau ci-dessous détaille la configuration minimale requise pour supporter 100 sessions simultanées sur un serveur :

Figure 3 - Dimensionnement serveur recommandé

CPU (Virtual Core)	16
Mémoire (RAM)	96 GB
GPU (NVENC)	1
Stockage	64 GB

Le poste de l'utilisateur doit avoir un navigateur récent et à jour compatible HTML5 (Edge, Chrome, Firefox, Safari), peu importe l'OS (Windows, macOS, Linux).

Par ailleurs, les fichiers pourront être analysés avant récupération sur le poste de travail ou *upload* sur le serveur VirtualBrowser. L'analyse des fichiers se fait via un serveur ClamAV intégré au produit ou via un serveur externe supportant les protocoles ClamAV ou ICAP. Dans ce cas, le client a la charge de la maintenance de ce serveur.

Dans le cadre de l'évaluation, l'analyse antivirale s'appuiera sur le serveur ClamAV interne à la solution (les communications ne seront pas évaluées).

2.4.2 Système d'exploitation retenu

Dans le cadre de l'évaluation, le serveur VirtualBrowser sera déployé sur une plateforme de virtualisation Proxmox en version 8.x, en utilisant l'image OVA fournie.

Le poste utilisateur sera un Windows 11 avec Microsoft Edge.

Pour finir, un serveur d'authentification SAML sera mis en place.

2.5 Périmètre de l'évaluation

2.5.1 Périmètre

Le périmètre de l'évaluation est composé du serveur VirtualBrowser en mode « Proxy des postes » et avec la configuration single.

L'analyse portera sur les points suivants :

- L'étanchéité des conteneurs ;
- L'autoprotection : le produit ne doit pas pouvoir porter atteinte au système hôte ;
- L'authentification et le contrôle d'accès des utilisateurs :
  - Authentification multifacteurs pour les administrateurs (TOTP) ;
  - Authentification login/mot de passe pour les utilisateurs du service ;
  - Authentification SAML pour les utilisateurs du service (les communications ne seront pas évaluées).
- La robustesse de la console d'administration et de l'interface web ;
- La sécurité des communications entre les composants de la solution (le déchiffrement SSL du produit sera activé lors de l'évaluation) :
  - Entre le serveur VirtualBrowser et les navigateurs Web des utilisateurs ;
  - Entre les composants et containers docker du serveur VirtualBrowser (sans besoin de confidentialité).
- La journalisation des événements de sécurité, ces logs sont distingués selon 3 catégories différentes :
  - logs d'accès au service ou à la console d'administration ;
  - contenu des logs applicatifs ;
  - traçabilité des actions administrateur.
- Protection des données :
  - données métiers du profil utilisateur stockés chiffrés sur le disque (non sauvegardés par défaut) : cookies, localStorage.

Les éléments considérés comme hors TOE sont les suivants :

- Le ou les hyperviseurs sur lesquels sont déployés les *appliances* Virtualbrowser ;
- Serveur local ClamAV et ses communications ;
- Renvoi des logs en Syslog ;
- Serveur d'authentification SAML et ses communications.

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

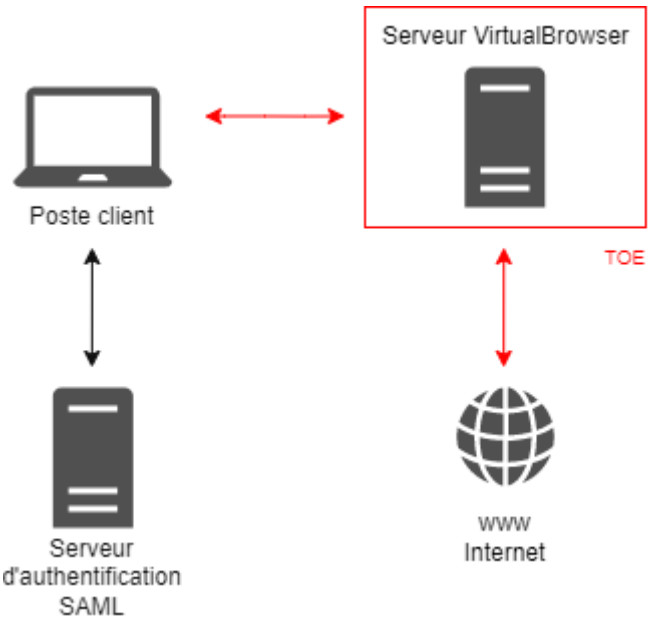
Tableau 3 - Configuration du produit évalué

Composant du système global		Inclus dans la cible d'évaluation (TOE)	Non évalué (environnement de la TOE)	
			Supposé de confiance[2]	Est un attaquant potentiel
Serveur VirtualBrowser	Proxmox v8.1.4		√	
	`vb_core`	√		
	`vb-osr-worker`	√		
	`vb_proxy`	√		
	`vb_api`	√		
	`web-server`	√		
	ClamAV			√
Serveur d'authentification	SAML		√	

2.5.2 Plateforme d'évaluation

La figure suivante représente la plateforme d'évaluation.

Figure 4 - Plateforme d'évaluation



[2] La bonne configuration des composants de confiance est susceptible d'être vérifiée durant l'évaluation.

3. PROBLEMATIQUE DE SECURITE

3.1 Description des utilisateurs du produit

Par définition, les utilisateurs concernent les personnes et les services applicatifs qui interagissent avec le produit évalué. Les rôles suivants sont à considérer dans le cadre de l'évaluation de sécurité :

- **Utilisateur interne** : utilisateur final du produit disposant d'un identifiant lui permettant l'accès au service VirtualBrowser afin de lancer une session de navigation ;
- **Utilisateur externe** : Utilisateur externe, agissant en qualité de prestataire, sous-traitant, client, etc. et disposant d'un identifiant permettant l'accès au service VirtualBrowser depuis Internet ;
- **Administrateur métier** : administrateur disposant d'un accès à la console d'administration web du produit. Il est chargé de la configuration et de la supervision de la solution. Ses droits peuvent être limités par la définition de rôles : par exemple accès en lecture seule, accès restreints à certains éléments ;
- **Administrateur système** : personne en charge d'administrer le système support sur lequel est installée la solution VirtualBrowser. L'administrateur dispose de droits importants sur une *appliance* VirtualBrowser. Il peut se connecter au système et obtenir les droits du super-utilisateur s'il dispose du mot de passe correspondant. Il peut effectuer des tâches de diagnostic et a un accès possible aux containers en cours d'exécution et aux fichiers présents sur le serveur.

La répartition des rôles pour le déploiement *On-Premise* est présentée dans le tableau suivant.

Tableau 4 - Répartition des rôles

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

Biens sensibles de l'utilisateur final de la TOE :

- **B1.Données d'authentification des utilisateurs**
  Les données relatives à la connexion des utilisateurs permettant l'accès à la TOE, incluant le nom des comptes.
  Besoin de sécurité : confidentialité et intégrité.
- **B2.Données métier et données utilisateurs**
  Ce bien concerne les données métiers du profil utilisateur : *cookie* et *localstorage* (non sauvegardés par défaut), etc. Elles ne sont accessibles qu'aux personnes habilitées et après authentification.
  Besoin de sécurité : intégrité et confidentialité.

Biens sensibles de la TOE :

- **B3.Système Hôte**
  La TOE n'induit pas de menaces sur le système hôte.
  Besoin de sécurité : disponibilité, intégrité, confidentialité et authenticité
- **B4.Configuration**
  Les données utiles pour assurer le fonctionnement de la TOE.
  Besoin de sécurité : intégrité et confidentialité
- **B5.Flux réseau**
  Les flux réseau entre les différents conteneurs, entre la TOE et les divers autres composants. Les flux internes au sein de la TOE, et en particulier les flux entre les différents conteneurs ne sont pas chiffrés et donc non protégés en confidentialité.
  Besoin de sécurité : confidentialité (hors flux internes), intégrité et disponibilité.
- **B6.Journaux**
  Les évènements générés lors des processus d'authentification et d'identification des utilisateurs sont journalisés. Ces données ne sont accessibles que par les administrateurs après s'être authentifiés.
  Besoin de sécurité : intégrité et confidentialité.
- **B7.Matériel cryptographique**
  Le matériel cryptographique utilisé par le produit.
  Besoin de sécurité : confidentialité et intégrité.

Biens sensibles de l'administrateur métier :

- **B8.Données d'authentification de l'administrateur**
  Les données relatives à la connexion des administrateurs.
  Besoin de sécurité : confidentialité et intégrité.

Le tableau suivant présente les besoins de sécurité sur les biens sensibles.

Tableau 5 - Besoins de sécurité des biens sensibles

Biens sensibles	Confidentialité	Intégrité	Disponibilité	Authenticité
B1.Données d'authentification des utilisateurs	√	√		
B2.Données métier et données utilisateurs	√	√		
B3.Système Hôte	√	√	√	√
B4.Configuration	√	√		
B5.Flux réseau	√	√	√	
B6.Journaux	√	√		
B7.Matériel cryptographique	√	√		
B8.Données d'authentification de l'administrateur	√	√		

Dans le cas du déploiement *On-Premise*, les biens sensibles sont stockés dans l'infrastructure du bénéficiaire (client).

3.3 Description des hypothèses sur l'environnement

Par définition, les hypothèses sont des déclarations portant sur le contexte d'emploi de la TOE ou de son environnement. Les hypothèses sur l'environnement de la TOE à considérer sont les suivantes :

- **H1.Système hôte sain**
  Le système d'exploitation de la TOE met en œuvre les mécanismes de protection adéquats : paramétrés et configurés selon les bonnes pratiques. De plus, le système d'exploitation est à jour des correctifs en vigueur au moment de l'installation, sain et exempt de virus.
- **H2.Installation intègre**
  Tous les outils nécessaires à l'installation et à la configuration du produit sont intègres.
- **H3.Administrateurs**
  Les administrateurs, métier et système, de la TOE sont considérés comme de confiance. Ils ont également été formés aux bonnes pratiques de sécurité et à l'usage de la TOE.
- **H4.Environnement serveur sécurisé**
  Les serveurs VirtualBrowser sont correctement administrés, configurés et sont déployés dans une DMZ. Ils sont également régulièrement mis à jour, en particulier s'il existe des correctifs de sécurité. Les machines serveur hébergeant la TOE se trouvent dans une zone sécurisée réputée de confiance. En particulier, l'accès physique à ces derniers est strictement réglementé et n'est accessible qu'au seul personnel autorisé.
- **H5.Filtrage réseau**
  Les connexions réseau de chaque *appliance* VirtualBrowser sont filtrées par des règles de Firewall afin de limiter l'impact d'une session de navigation exécutant du code hostile. La configuration des flux nécessaires au bon fonctionnement de la solution est indiquée dans la documentation d'administration.

3.4 Description des menaces

Par définition, une menace est une action ou un événement susceptible de porter préjudice à la sécurité de la TOE. Les agents menaçants à considérer pour l'évaluation de sécurité sont les suivants :

- un attaquant présent sur le réseau. Il peut :
  - tenter d'intercepter les communications réseau (attaquant **hors-bénéficiaire**) ;
  - accéder aux interfaces web, mais ne dispose pas d'un compte utilisateur (attaquant **hors-bénéficiaire**).
- un attaquant disposant d'un compte utilisateur non privilégié sur la TOE. Il pourrait tenter de porter atteinte aux biens sensibles sur la TOE (attaquant **intra-bénéficiaire**) ;
- un attaquant ayant compromis un conteneur (attaquant tout type de bénéficiaire) ;
- un attaquant disposant d'un compte utilisateur pourrait tenter de porter atteinte aux biens sensibles d'un autre utilisateur (attaquant **inter-bénéficiaire**).

Les administrateurs ne sont pas considérés comme des attaquants.

Les menaces portant sur les biens sensibles de la TOE sont les suivantes :

- **M1.Vol des données d'authentification**
  Un attaquant parvient à récupérer les données d'authentification d'un utilisateur ou d'un administrateur muni d'un compte VirtualBrowser.
- **M2.Altération des données de journalisation**
  Un attaquant parvient à accéder, modifier, ajouter ou supprimer les données de journalisation afin de masquer des actions, injecter de fausses informations.
- **M3.Compromission du système hôte**
  Un attaquant parvient à corrompre le système hôte en exploitant la TOE.
- **M4.Contournement du contrôle d'accès**
  Un attaquant parvient à contourner le mécanisme d'authentification.
- **M5.Corruption des communications**
  Un attaquant parvient à capturer et à modifier les données échangées avec la TOE.
- **M6.Compromission des données métiers et utilisateurs**
  Un attaquant parvient à modifier/lire des données métiers et les données utilisateurs manipulés par la TOE.
- **M7.Altération des données de configuration**
  Un attaquant parvient à modifier les données de configuration dans le but d'abaisser le niveau de sécurité de la TOE ou d'exfiltrer des données sensibles.
- **M8.Déni de service**
  Un attaquant parvient à provoquer un déni de service sur un bien sensible avec un besoin en disponibilité.
- **M9.Compromission du matériel cryptographique**
  Un attaquant parvient à accéder, modifier ou supprimer le matériel cryptographique utilisé par la TOE.

3.5 Description des fonctions de sécurité

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.Stratégies de navigation et de gestion des fichiers**
  Des règles de navigation et de gestion des fichiers peuvent être paramétrées par l'administrateur afin d'adapter les règles de sécurité en fonction des utilisateurs et des sites visités. Dans le cas où aucune règle n'est définie, la règle par défaut, automatiquement créée par le serveur VirtualBrowser est appliquée. La règle par défaut est personnalisable par l'administrateur du service.
- **FM2.Analyse antivirale**
  Les fichiers peuvent être analysés avant récupération sur le poste de travail ou *upload* sur le serveur VirtualBrowser. L'analyse des fichiers se fait via un serveur supportant les protocoles ClamAV ou ICAP.

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**
  Quel que soit le type de configuration (mode proxy ou explicite), l'accès aux services VirtualBrowser fait l'objet d'une authentification. Une authentification SAML V2 est également supportée. L'administrateur quant à lui s'authentifie via *login*/mot de passe et par authentification multifacteurs (TOTP). Les méthodes login/mot de passe classique, d'authentification multifacteurs et SAML V2 sont considérées dans le périmètre de l'évaluation.
  L'identification est réalisée via des *tokens* de session, ils sont stockés dans le *localstorage* du navigateur. Dans le cas où le proxy authentifie l'utilisateur, le *token* transite sous la forme de cookie.
  Les mots de passe des utilisateurs et des administrateurs de la TOE sont stockés de manière dérivée en base de données. La politique de mot de passe impose une longueur minimale de 12 caractères avec utilisation des 4 jeux de caractères suivant : minuscules, majuscules, chiffres et caractères spéciaux.
- **FS2.Contrôle d'accès et gestion des droits/privilèges entre utilisateurs appartenant au bénéficiaire**
  L'accès aux services VirtualBrowser fait l'objet d'un contrôle d'accès. Il permet d'assurer un cloisonnement des utilisateurs afin de protéger leurs données et leurs sessions de navigations. Ce contrôle d'accès empêche les utilisateurs de se faire passer pour l'administrateur pour porter atteinte à la TOE.
- **FS3.Communications sécurisées**
  Le flux entre les navigateurs Web des clients, le serveur VirtualBrowser et le serveur web final sont protégés en intégrité et confidentialité. Les communications HTTP effectuées lors de la navigation sur un site non sécurisé, ou lors de l'accès initial au serveur VirtualBrowser (avant redirection HTTPS), ne sont pas protégées en confidentialité.

Les communications avec le service `vb_core` se font via socket unix. De plus, le composant `vb-osr-worker` communique avec le client VirtualBrowser à travers des connexions WebSocket. Les communications internes à la TOE ne sont pas protégées en confidentialité.

- **FS4.Protection des données incluant l'effacement sécurisé**

  À la fin de la session de navigation, le conteneur est détruit et toutes les données sont supprimées du serveur. La TOE protège sa configuration afin que cette dernière ne puisse pas être modifiée par un utilisateur non autorisé. Dans le cadre de la fonctionnalité de conservation des profils utilisateur, l'archive contenant les profils est chiffrée sur le disque.

- **FS5.Journalisation**

  Les opérations d'authentification des utilisateurs sont journalisées. Les logs sont distingués selon 3 catégories différentes :

  - Logs d'accès au service ou à la console d'administration :
    - Identifiant de l'utilisateur ;
    - Date et heure de connexion ;
    - Résultat de l'authentification ;
    - Adresse IP de connexion.
  - Contenu des logs applicatifs :
    - Date et heure de connexion ;
    - Identifiant de l'utilisateur (pour les ouvertures de session et les journaux générés depuis une session de navigation) ;
    - Adresse IP de connexion (pour les ouvertures de session et les journaux générés par le proxy) ;
    - Ressource accédée ;
    - Type d'accès réalisé (*Navigate* / *Download* / *Upload* / GET / POST / RESSOURCE etc.).
  - Traçabilité des actions administrateur :
    - Identifiant de l'administrateur ;
    - Date et heure de connexion ;
    - Adresse IP de connexion ;
    - État initial de la valeur modifiée et sa nouvelle valeur modifiée.

  Les journaux de la TOE ne sont accessibles qu'aux administrateurs et sont consultables directement depuis l'interface d'administration. Ils peuvent si besoin, être renvoyés vers un point de collecte en syslog. Le renvoi des logs en syslog ne sera pas activé dans le cadre de l'évaluation. Les journaux sont stockés en base de données ou sur le serveur et l'accès est protégé par le compte de service. Par défaut, les logs de navigation sont fournis par VirtualBrowser.

- **FS6.Innocuité**

  VirtualBrowser isole les sessions de navigations des utilisateurs en exécutant le navigateur dans un environnement virtualisé, assurant ainsi que les codes actifs ne sont pas exécutés sur l'appareil local de l'utilisateur. Dans ce contexte, la TOE protège son fonctionnement, notamment en assurant l'étanchéité des conteneurs.

- **FS7.Autoprotection**

  La TOE ne doit pas pouvoir être utilisée pour porter atteinte à la sécurité du système hôte. Des mesures de durcissement sont mises en place pour protéger la TOE contre des menaces potentielles : utilisation de profils AppArmor spécifiques sur chaque container et isolation de l'espace de noms utilisateur de docker vis à vis de l'hôte.

3.5.3 Fonctions désactivées

Les fonctions désactivées sont les fonctions considérées comme étant en dehors du périmètre de l'évaluation (hors-TOE) et non accessibles à un attaquant. Ces fonctions ne seront donc pas considérées lors de l'évaluation. Les fonctions désactivées de la TOE sont les suivantes :

- **FD1.Mise à jour**
  La mise à jour VirtualBrowser est faite par l'administrateur IT, au rythme de son choix. Cette opération permet la mise à jour du serveur et du moteur de rendu Chromium utilisé dans la solution VirtualBrowser pour la navigation sécurisée.
- **FD2.Catégorisation des URLS**
  Cette fonctionnalité permet de mettre en place des politiques de sécurité autour de la navigation et de la gestion des fichiers (téléchargement et téléversement).
- **FD3.Authentification par certificat client**
  Cette fonctionnalité permet d'utiliser un certificat local au poste afin de s'authentifier sur un serveur web au travers d'une session de navigation VirtualBrowser. L'installation d'une extension et d'un composant natif sur les postes est nécessaire pour l'utilisation de cette fonctionnalité, elle est désactivée par défaut.

3.6 Description de la surface d'attaque

La surface d'attaque représente l'ensemble des moyens par lesquels on peut interagir avec le produit, indépendamment de leur rôle dans une fonction évaluée ou non évaluée. La surface d'attaque de la TOE est indiquée dans le tableau suivant, il s'agit uniquement d'interfaces logiques :

Tableau 6 – Interfaces logiques de la TOE

Interfaces (accessibles ou non accessibles)	Fonction concernée (évaluée ou non évaluée)	Acteurs ayant accès aux interfaces
Interface vers le réseau : HTTP (port TCP/80)	Redirection automatique vers une communication HTTPS	Tout utilisateur réseau
Interface vers le réseau : HTTPS (port TCP/443)	Session de navigation ou administration de la solution	Utilisateurs et Administrateurs métier
Interface vers le réseau : PROXY (port TCP/3128)	Interception de la navigation des utilisateurs	Tout utilisateur réseau
Interface vers le réseau : SSH (port TCP/22)	Administration système de la solution	Administrateurs système
Interface vers l'OS : Socket Unix	Communication avec l'orchestrateur de vb_core	OS (container vb_api et commande vb-cli)
Interface vers le réseau interne Docker (port TCP/80)	Communication avec l'API, via le container nginx	OS (containers)
Interface vers le réseau interne Docker (port TCP/8080)	Communication avec le container vb_api	OS (containers)
Interface vers le réseau interne Docker (port TCP/4500)	Communication avec un container vb_osr (session nav)	OS (containers)
Interface vers le réseau interne Docker (port TCP/3310)	Communication avec le container clamav	OS (containers)

Interface vers le réseau interne Docker (port TCP/3000)	Communication avec le container gotenberg (previsualisation)	OS (containers)

3.7 Matrices de couverture

3.7.1 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).

Tableau 7 - Couverture des biens sensibles par rapport aux menaces

	B1.Données d'authentification des utilisateurs	B2.Données métier et données utilisateurs	B3.Système Hôte	B4.Configuration	B5.Flux réseau	B6.Journaux	B7.Matériel cryptographique	B8.Données d'authentification de l'administrateur
M1.Vol des données d'authentification	**CI**							**CI**
M2.Altération des données de journalisation						**IC**		
M3.Compromission du système hôte			**DICA**	**CI**				
M4.Contournement du contrôle d'accès	**CI**							
M5.Corruption des communications					**CI**			
M6.Compromission des données métiers et utilisateurs		**CI**		**CI**				
M7.Altéraion des données de configuration				**CI**		**i**		
M8.Déni de service					**D**			
M9.Compromission du matériel cryptographique							**CID**	

3.7.2 Menaces et fonctions de sécurité

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

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

	FS1. Identification et	FS2.Contrôle d'accès et gestion des	FS3.Communications sécurisées	FS4.Protection des données incluant	FS5.Journalisation	FS6.Innocuité	FS7.Autoprotection
M1.Vol des données d'authentification	√		√				
M2.Altération des données de journalisation					√		
M3.Compromission du système hôte						√	√
M4.Contournement du contrôle d'accès		√					
M5.Corruption des communications			√				
M6.Compromission des données métiers et utilisateurs			√	√		√	√
M7.Altération des données de configuration				√			
M8.Déni de service						√	√
M9.Compromission du matériel cryptographique			√	√			

AMOSSYS

PARIS_
STRASBOURG_
NANTES_
RENNES_
LYON_
GENÈVE_

À BIENTÔT