

# Secure Remote Browser Isolation

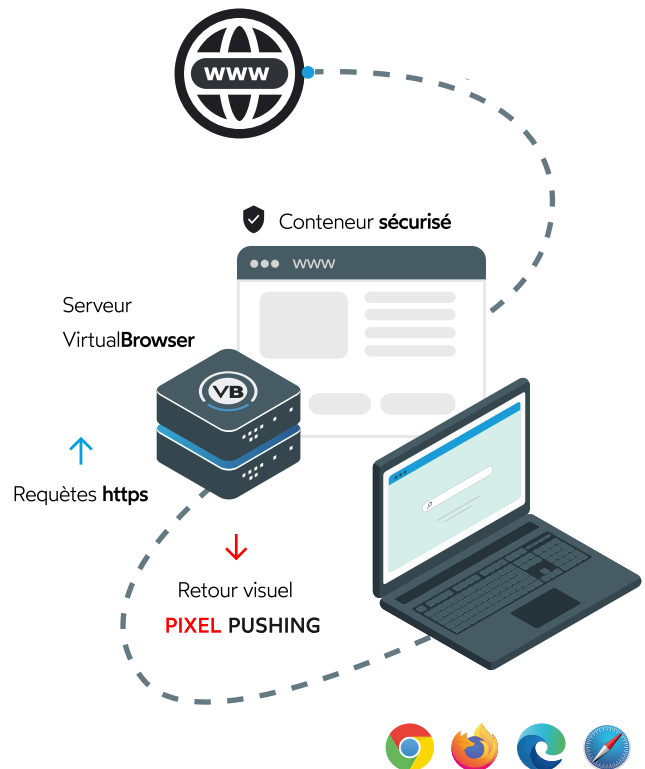


Le navigateur web constitue une cible privilégiée pour les attaquants, responsable de 60% des attaques en ligne<sup>1</sup>. Dans ce contexte, la technologie Remote Browser Isolation (RBI) se présente comme une solution de cybersécurité indispensable pour contrer les menaces web, sans compromettre l'expérience utilisateur.

La navigation web déportée est un modèle de cybersécurité qui vise à isoler physiquement l'activité de navigation d'un utilisateur de son propre poste. Tout le contenu est exécuté à distance, à l'écart du réseau local, puis transmis à l'utilisateur via un flux de pixel sécurisé. À la fin de chaque session de navigation, toute l'activité est intégralement détruite sur le serveur.

Lorsqu'elle est utilisée pour protéger contre les contenus non fiables, l'isolation du navigateur à distance réduit considérablement la surface d'attaque d'une organisation, étant donné qu'un grand nombre d'attaques visent les utilisateurs et terminaux. **De cette façon, VirtualBrowser sécurise de manière proactive la navigation Internet des cyberattaques.**

La solution RBI permet également de réduire les risques en protégeant les données et applications sensibles de l'entreprise accédées depuis des appareils non maîtrisés.



## Sécurité Renforcée

Les solutions de sécurité existantes (SWG, CASB, ZTNA ...) bien que bénéfiques ne sont pas infaillibles face aux cyberattaques. Ainsi, elles peuvent potentiellement laisser passer du contenu malveillant s'exécutant sur le terminal de l'utilisateur.

L'isolation du navigateur à distance permet de contrer efficacement ces menaces.

En complément, l'utilisation de VirtualBrowser permet également :

- Améliorer l'expérience utilisateur en ne bloquant plus l'accès vers les sites non-catégorisés,
- Réduire le risque d'attaques de phishing en isolant les URLs reçus par email,
- Sécuriser le télétravail en ajoutant un point de contrôle pour les appareils non gérés,
- Remplacer une solution de VDI plus coûteuse et compliquée à utiliser.

## Défense Multi-Couches

Le simple fait d'isoler le navigateur du poste de travail de l'utilisateur final améliore considérablement la posture de sécurité de l'entreprise contre les menaces suivantes :

Malwares

Phishing

Trackers malveillants

Attaques par injection

Zero-Day

Fingerprinting

Drive-by Downloads

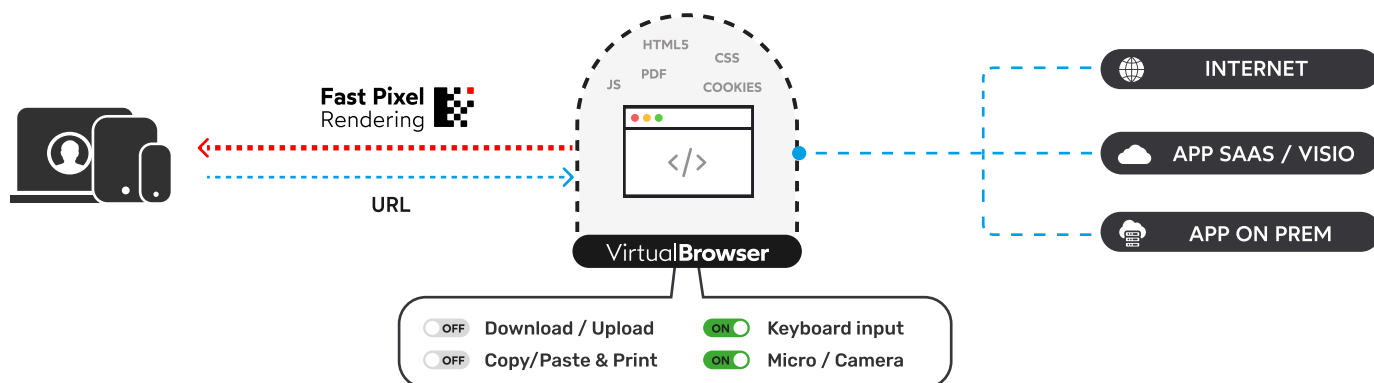
Man-in-the-Middle (MitM)

" We estimate that organizations that isolate internet web browsing will experience a 70% reduction in attacks that compromise end-user systems. "

Innovation Insight for Remote Browser Isolation

**Gartner**

# Modèle de cybersécurité proactif de protection de la navigation Internet



## Des Fonctionnalités de Protections Avancées

### Sécurisation Pro-active de la Navigation

VirtualBrowser déporte la navigation Internet de vos utilisateurs sur une bulle virtuelle distante, offrant une isolation physique entre leur poste et les ressources accédées.

### Contrôle d'Accès Granulaire

VirtualBrowser vous permet de définir finement des politiques d'accès et, selon vos critères, de contrôler les interactions de vos utilisateurs : **Saisie Clavier, Copier / Coller, Download / Upload, Impression...**

### Gestion des Périphériques (Caméra, Micro)

Utilisation simplifiée des solutions de vidéoconférence en ligne (Teams, Zoom, Gmeet, Webex ...) tout en éliminant les contraintes techniques liées à la mise à disposition de ces services (ouvertures de flux).

### Technologie de Rendu Unique

Contrairement à la plupart des solutions de RBI traditionnelles qui reposent sur la reconstruction du Document Object Model (DOM) au sein du navigateur local, avec un risque résiduel d'exécution de code malveillant, VirtualBrowser propose une approche plus sécuritaire, le **"Pixel Pushing"**.

L'ensemble du code – qu'il s'agisse de HTML, CSS, JavaScript, Cookies ou même de la visualisation de documents – est exécuté dans un environnement distant, isolé du réseau local de l'utilisateur. **Le rendu final est ensuite transmis sous forme de flux vidéo.**

Fort de plus de 10 ans d'expertise, VirtualBrowser a développé une technologie de rendu innovante **"Fast Pixel Rendering"** (FPR) offrant une expérience de navigation transparente et optimisée.

### 🔧 Catégorisation des URLs

Personnalisez vos catégories d'URLs à appliquer dans vos règles de navigation.

### 🔧 Authentification Utilisateurs

Permettez à vos utilisateurs de s'authentifier facilement avec leur identifiant (SAML/LDAP).

### 🔧 Navigation Anonyme

Protégez vous des trackers malveillants et du fingerprinting.

## Partout, Pour tous, Sans limites



### Compatibilité

Fonctionne en mode natif sur n'importe quelle page web, dans n'importe quel navigateur.



### Transparence

Déploiement sans agent, ni plugin à installer et zéro conduite de changement. Utilisation transparente pour l'utilisateur final.

# Spécifications techniques

## ✦ Fonctionnement

L'utilisateur, par le biais de son navigateur local, fait une demande de navigation. Selon les règles de redirection des flux mises en place par votre entreprise, les étapes seront les suivantes :

1. Interception de la demande de navigation par le serveur VirtualBrowser
2. Authentification explicite ou transparente de l'utilisateur et lancement de VirtualBrowser
3. Création d'un container pour l'utilisateur sur le serveur VirtualBrowser
4. Actions de navigation par l'utilisateur
5. Interception des actions par le container et navigation sur le site demandé
6. Rendu de la page à l'utilisateur via un streaming audio et vidéo
7. Fermeture de la session
8. Destruction du container

## ✦ 3 modes de configurations

### 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 votre proxy.

### 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 terminal, l'utilisateur entre l'URL du serveur VirtualBrowser sur un navigateur 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 à vos applications métiers dans le cadre du BYOD et pour les postes non maîtrisés.

## ✦ Hébergement



### On Premise

- VirtualAppliance - Déploiement < 10min
- Architecture en stand alone ou en mode cluster
- Accès sécurisé depuis l'extérieur à vos applications métiers sensibles



### SaaS

- 100% Opérée par Oodrive
- Hébergement en France
- Authentification SAML
- Serveur mutualisé ou dédié
- Accélération matériel par GPU



### Déploiement simple

Configuration intuitive et intégration rapide avec votre infrastructure.



### Expérience utilisateur transparente

La navigation est fluide, sans compromis entre sécurité et performance.



### Support & mises à jour

Mise à jour régulière pour répondre aux nouveaux défis en matière de sécurité.



### Réduction des coûts

Minimise les dépenses liées à la gestion des équipements de sécurité.