VirtualBrowser

DATENBLATT

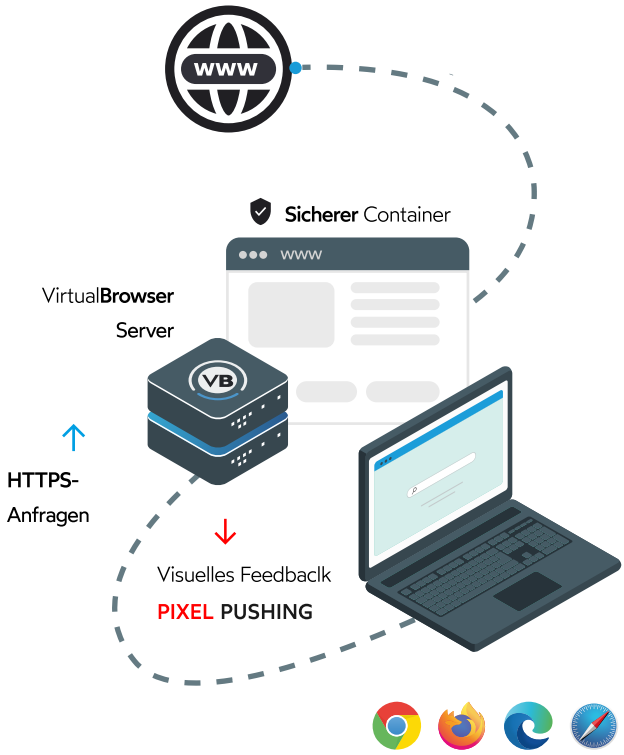
Secure Remote Browser Isolation

Der Webbrowser ist eines der bevorzugten Angriffsziele und für rund 60 % aller[1] Online-Attacken verantwortlich. Remote Browser Isolation (RBI) ist eine zentrale Cybersicherheits-technologie, um Webbedrohungen wirksam abzuwehren – ohne das Nutzererlebnis zu beeinträchtigen.

RBI trennt die gesamte Browseraktivität eines Nutzers vollständig vom Endgerät. Alle Webinhalte werden in einer isolierten Remote-Umgebung ausgeführt und anschließend als sicherer Pixelstream an den Anwender übertragen. Am Ende jeder Sitzung wird die komplette Aktivität auf dem Server gelöscht.

Durch den Einsatz von RBI sinkt die Angriffsfläche einer Organisation erheblich – insbesondere, da Angriffe zunehmend über Nutzer und Endgeräte erfolgen. **VirtualBrowser schützt das Internet-Browsing vor Cyberangriffen und verhindert, dass nicht vertrauenswürdige Inhalte das Unternehmensnetzwerk erreichen.**

Darüber hinaus schützt RBI sensible Daten und Anwendungen, wenn auf diese von unsicheren oder nicht korrekt verwalteten Geräten zugegriffen wird.



Erhöhte Sicherheit

Lösungen wie SWG, CASB oder ZTNA erhöhen zwar das Sicherheitsniveau, bieten jedoch keinen vollständigen Schutz vor modernen Webbedrohungen. Trotz dieser Maßnahmen kann schädlicher Code in bestimmten Fällen weiterhin auf Endgeräten ausgeführt werden.

Remote Browser Isolation schließt genau diese Sicherheitslücke, indem potenziell gefährliche Inhalte gar nicht erst auf das Gerät gelangen und Risiken wirksam ausgeschlossen werden.

VirtualBrowser bietet zusätzlich folgende Vorteile:

- **Verbesserte Nutzererfahrung, da der Zugang zu nicht kategorisierten Webseiten nicht mehr blockiert werden muss.**
- **Reduziertes Phishing-Risiko durch isoliertes Öffnen von URLs aus E-Mails.**
- **Mehr Sicherheit beim Remote-Arbeiten dank eines zusätzlichen Kontrollpunkts für unverwaltete Geräte.**
- **Ersatz von komplexen und kostenintensiven VDI-Lösungen.**

Mehrschichtige Verteidigung

Durch die vollständige Trennung des Browsers vom Endgerät erhöht VirtualBrowser die Sicherheitsresilienz gegenüber:

Malware | **Phishing** | **Malicious trackers**
Injection attacks | **Zero-Day** | **Fingerprinting**
Drive-by Downloads | **Man-in-the-Middle (MitM)**

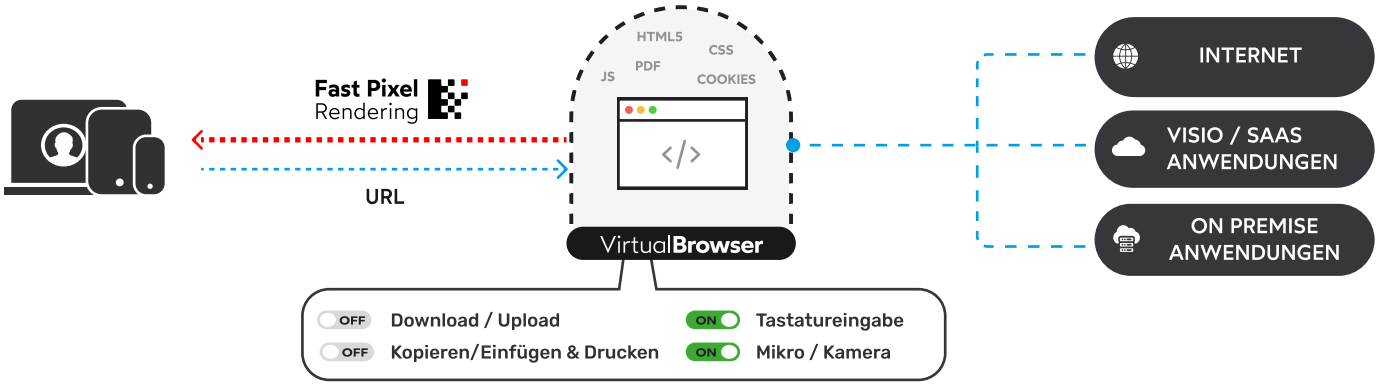
"Organisationen, die Internet-Browsing isolieren, verzeichnen rund 70 % weniger Angriffe, die Endnutzergeräte kompromittieren."

Innovation Insight for Remote Browser Isolation

Gartner

1. Osterman Research. "Why You Should Seriously Consider Web Isolation Technology." December 2018.

Proaktives Cybersicherheitsmodell
zum Schutz von Internet-Browsing



Erweiterte Schutzfunktionen

Proaktive Navigationssicherheit

VirtualBrowser verlagert das Browsing vollständig in eine isolierte Remote-Umgebung – physisch getrennt vom Endgerät.

Granulare Zugriffskontrolle

Mit VirtualBrowser lassen sich Zugriffsrichtlinien und Nutzeraktionen präzise steuern: Tastatureingaben, Copy/Paste, Downloads/Uploads, Drucken usw.

Gerätemanagement (Kamera, Mikrofon)

Einfache Verwendung gängiger Videokonferenzlösungen (Teams, Zoom, Gmeet, Webex) ohne technische Hürden wie das Öffnen bestimmter Netzwerkports.

Einzigartige Rendering-Technologie

Im Gegensatz zu den meisten traditionellen RBI-Lösungen, die auf einer lokalen Rekonstruktion des „Document Object Model" (DOM) basieren und somit ein Restrisiko für schädlichen Code darstellen, setzt VirtualBrowser auf ein deutlich sichereres Verfahren: **„Pixel Pushing"**.

Sämtlicher Code – HTML, CSS, JavaScript, Cookies oder Dokumentenansichten – läuft ausschließlich in einer isolierten Remote-Umgebung. Dem Nutzer wird lediglich ein sicherer Videostream übertragen.

Gestützt auf über 10 Jahre Expertise hat VirtualBrowser die innovative **Fast Pixel Rendering (FPR)-Technologie** entwickelt, die ein flüssiges und optimiertes Browsing-Erlebnis bietet.

URL-Kategorisierung

Passen Sie die URL-Kategorien an und verwenden Sie sie in Ihren Navigationsregeln.

Benutzerauthentifizierung

Ermöglichen Sie Ihren Nutzern eine einfache Authentifizierung über Ihre Anmeldedaten (SAML/LDAP).

Anonyme Navigation

Schützen Sie Ihre Nutzer vor bösartigen Trackern und Fingerprinting.

Überall, für jeden, ohne Grenzen

Kompatibilität

Funktioniert nativ auf jeder Webseite und in jedem Browser.

Nahtlose Nutzung

Bereitstellung ohne Agent und ohne Plug-ins – ganz ohne zusätzlichen Installations- oder Change-Management-Aufwand.

Technische Spezifikationen

Funktionsweise

Der Nutzer stellt über seinen lokalen Browser eine Navigationsanfrage. Wie der RBI-Prozess im Einzelnen abläuft, hängt von den Weiterleitungsregeln in Ihrem Unternehmen ab. Grundsätzlich sieht er so aus:

1. **Abfangen der Browseranfrage durch den VirtualBrowser-Server**
2. **Explizite oder transparente Nutzerauthentifizierung und Start von VirtualBrowser**
3. **Erstellung eines Nutzer-Containers auf dem VirtualBrowser-Server**
4. **Nutzer surft im Web**
5. **Interaktion wird im Container abgefangen und an die Zielseite weitergeleitet**
6. **Seite wird dem Nutzer per Audio- und Video-Streaming dargestellt**
7. **Sitzung wird beendet**
8. **Container wird zerstört**

Drei Konfigurationsmodi

Lokale Prox proxy chaining:
Der Proxy des Kunden fängt Verbindungen ab und entscheidet – basierend auf definierten Kriterien wie Kategorien oder Nutzern – ob Datenverkehr ganz oder teilweise an VirtualBrowser weitergeleitet wird. Die Möglichkeiten richten sich nach den Funktionen Ihres Proxyservers.

Proxy-Stationen:
Der VirtualBrowser-Server fungiert als Desktop-Proxy, fängt alle Verbindungen ab und leitet sie an VirtualBrowser weiter. Browsing-Regeln werden in der VirtualBrowser Management Platform festgelegt.

Expliziter Modus:
Nutzer geben im Browser die URL des VirtualBrowser-Servers ein und authentifizieren sich. Anschließend können sie sicher auf beliebige Webseiten zugreifen, da Inhalte über den Remote-Server geladen werden. Dieser Modus ermöglicht zudem einen geschützten Zugriff auf Unternehmensanwendungen – auch bei BYOD oder nicht vertrauenswürdigen Geräten.

Hosting

On-Premise

- VirtualAppliance: Bereitstellung in unter 10 Min.
- Einzel- oder Clusterarchitektur
- Sicherer externer Zugriff auf sensible Unternehmensanwendungen

SaaS

- Betrieb zu 100 % durch VirtualBrowser
- Hosting in Europa
- SAML-Authentifizierung
- Geteilter oder dedizierter Server
- GPU-Hardwarebeschleunigung

Einfache Bereitstellung

Intuitive Konfiguration und schnelle Integration in Ihre Infrastruktur.

Nahtlose Benutzererfahrung

Flüssiges Browsing ohne Kompromisse bei Sicherheit und Performance.

Support & Updates

Regelmäßige Aktualisierungen, um neue Sicherheits-anforderungen abzudecken.

Kosten-ersparnis

Minimierung der Kosten für den Betrieb von Sicherheitslösungen.