



Browser based Remote Desktop White Paper

WebConnect World SL | v 1.0.0, Januar 27, 2023

Content

| | | |
|---|-----------|--|
| 1. Editorial | 5 | |
| 2. Management summary | 7 | |
| 3. Work remotely | 11 | |
| 3.1. Homeoffice und Remote-Arbeit – Herausforderung für Sicherheit und Administration | 11 | |
| 3.2. VPN – Verbindung mit Schwächen | 12 | |
| 3.3. Sichere Lösung: WebConnect | 14 | |
| 4. Warum WebConnect? | 16 | |
| 4.1. Für Unternehmen | 16 | |
| 4.2. Für Datacenter und Cloudanbieter | 17 | |
| 5. So funktioniert WebConnect | 19 | |
| 6. WebConnect Funktionalität | 23 | |
| 6.1. Die wichtigsten Funktionen von WebConnect | 23 | |
| 6.1.1. Protokolle | 23 | |
| 6.1.2. Shared-Monitor RDP mit mehreren Teilnehmern | 23 | |
| 6.1.3. Multi-Monitor und Co-Monitor | 24 | |
| 6.1.4. Multi-Verbindung | 25 | |
| 6.1.5. Shared-Drive mit Dateimanager | 25 | |
| 6.1.6. Private-Drive mit Dateimanager | 25 | |
| 6.1.7. Remote drucken | 25 | |
| 6.1.8. Webcam und Mikrofon | 26 | |
| 6.1.9. SmartCard Weiterleitung | 26 | |
| 6.1.10. Wake-on-LAN | 26 | |
| 6.1.11. Mobile apps | 26 | |
| 6.1.12. Unterstützung von Philips SpeechMike | 27 | |
| 6.1.13. RDP-Sitzungen mit Videobearbeitung | 27 | |
| 6.1.14. Benutzerverwaltung | 27 | |
| 6.1.15. Verbindungsverwaltung | 27 | |
| 6.2. Geplante Funktionen für das 4. Quartal 2022 | 28 | |
| 6.2.1. Shared Drive mit Online-/–Offline-Synchronisation | 28 | |
| 6.2.2. USB-Weiterleitung in der RDP Sitzung im Browser | 28 | |
| 6.2.3. WebMeet-Video-Meeting mit Whiteboard und Chat | 29 | |
| 7. WebConnect: Funktions-Übersicht | 31 | |
| 7.1. WebConnect: Funktions-Übersicht | 31 | |
| 7.2. Die im Browser unterstützten Protokolle | 31 | |
| 7.3. Sicherheit und Datenschutz | 32 | |
| 7.4. Nutzer- und Verbindungsverwaltung | 32 | |
| 7.5. Eigenschaften | 33 | |
| 7.6. Ansicht | 33 | |
| 7.7. Zusammenarbeit | 34 | |
| 7.8. Peripherie | 34 | |
| 7.9. Mobile app | 34 | |
| 9. Sicherheit | 38 | |
| 9.1. Verbindung & Verschlüsselung | 38 | |
| 9.2. Authentifizierung | 39 | |
| 9.3. Datenschutz & Compliance | 39 | |
| 9.4. Netzwerksicherheit | 39 | |
| 10. Webconnect: Lizenzierung | 41 | |
| 11. Über WebConnect | 44 | |
| Anlagen | 46 | |
| 1. WebConnect bringt Datacenter auf Azure-Level | | |
| 2. WebConnect-RDP im Browser oder RDP mit VPN | | |
| 3. Externe Geräte mit Wake-on-LAN einschalten | | |
| 4. Remote Zugänge sicher verwalten | | |
| 5. WebConnect und / oder andere IT-Lösungen | | |
| 6. Lizenzen und Preise | | |

Wir bringen die Zukunft zu Ihnen. Egal wo auch immer Sie sind.

1. Editorial



Wir bringen die Zukunft zu Ihnen. Egal wo auch immer Sie sind.

Ideen, die die Arbeitswelt revolutionieren, werden im Herzen von Madrid geboren. Gegründet vom CEO Saber Maram sind wir auf Datenschutz, Sicherheit und Kommunikation spezialisiert. Wir entwickeln eigene Produkte und beraten Kunden im Bereich F&E.

„Der wahre Luxus im Leben ist ein kurzer Arbeitsweg. Wir helfen Menschen, ihre Lebensqualität zu verbessern, und Unternehmen, nachhaltiger und flexibler zu werden.“

Saber Maram, CEO WebConnect World SL

Management summary

WebConnect verwendet kein VPN, erreicht aber dennoch hohe Leistungen Sicherheit mit hoher Leistung.

2. Management summary

Homeoffice und flexibles Arbeiten aus der Ferne gehören mittlerweile zum Alltag in Unternehmen. Um eine sichere Verbindung zum Firmennetzwerk zu gewährleisten, setzen Firmen meist auf einen verschlüsselten VPN-Tunnel (Virtual Private Network). Doch bei einer großen Belegschaft ist das VPN schnell überlastet und bremst den Geschäftsbetrieb aus. Zudem können die Konfiguration und permanente Überwachung der VPN-Verbindungen im Unternehmen für die Administratoren sehr aufwändig sein.



Hier setzt WebConnect mit einem neuartigen Konzept für den sicheren Fernzugriff auf Desktops und die Einwahl in das Firmennetzwerk an. WebConnect nutzt kein VPN, erreicht aber trotzdem hohe Sicherheit bei hoher Leistung. Dazu baut WebConnect über den Browser alle Verbindungen direkt zwischen Client und Remote-Gerät als Tunnel mit https-Verschlüsselung auf. Die Lösung nutzt ein SSLZertifikat pro Gerät über https und Secure WebSocket mit Verschlüsselung über TLS 1.3. Eine ähnliche Methodik kommt auch im Bankenwesen zum Einsatz.



Mitarbeiter können dank WebConnect sogar mit ihrem Smartphone über den Browser verschlüsselt auf jeden realen oder virtuellen PC im Büronetzwerk sowie verbundene Drucker, Scanner, Kartenlesegeräte oder Webcams zugreifen. Zusätzliche Softwareinstallationen und umständliches Einrichten eines VPNs gehören damit der Vergangenheit an. WebConnect bietet eine Vielzahl von Einstellungen, mit denen Firmen ihre Sicherheitsanforderungen sowie Rollen-Rechte-Konzepte verfeinern und Zugriffsrechte individuell oder gruppenbezogen zuweisen können.



WebConnect bietet darüber hinaus Funktionen wie Web Meet für die optimierte Zusammenarbeit in Videokonferenzen (Collaboration-Mode). Die Teilnehmer können hier während der RDP-Sitzung gemeinsam auf Maus und Tastatur zugreifen, Dokumente bearbeiten und auf das Whiteboard zugreifen. WebConnect sorgt als Host für die sichere Verbindung der Videokonferenz und damit den notwendigen Datenschutz. Sehr nützlich ist etwa ein geteiltes (Shared Drive) oder ein persönliches (WebConnect Drive) privates Cloud-Verzeichnis für die sichere Ablage von Daten als Alternative zum externen Cloud-Speicher – letzteres jetzt auch mit automatisierter Synchronisation über WebConnect mit allen eingesetzten Geräten. WebConnect erlaubt es zudem, auf dem Remote-PC gespeicherte Dokumente direkt auf dem lokalen Drucker auszudrucken beziehungsweise Dokumente von zuhause aus an den Drucker im Büro zu schicken und dort auszudrucken.

WebConnect gibt es in zwei Varianten: WebConnect Plug & Play und WebConnect Enterprise. WebConnect Plug&Play funktioniert über die bereits fertig konfigurierte WebConnect Box (Hardware), die einfach mit dem Netzwerk verbunden wird, und ist optimiert für bis zu 20 gleichzeitige RemoteVerbindungen. WebConnect Enterprise ist für mehr als 20 gleichzeitige Verbindungen konzipiert und eignet sich daher sehr gut für große Netzwerke und Cloud-Anwendungen. Bei dieser Version wird die WebConnect-Software im Netzwerk auf einer virtuellen Maschine (VM) mit dem Betriebssystem Linux installiert.

Remote arbeiten

Ziel ist es, dass jeder Mitarbeiter seine Tätigkeiten über das Internet und damit ortsunabhängig ausüben kann.

3. Work remotely

3.1. Homeoffice und Remote-Arbeit – Herausforderung für Sicherheit und Administration

Die Corona-Pandemie hat die Welt in einen Ausnahmezustand versetzt und auch die Art und Weise des Arbeitens massiv verändert. Homeoffice und flexibles Arbeiten gehören mittlerweile zum normalen Geschäftsalltag. Vor Corona war das Arbeiten von zuhause nur einem kleinen Personenkreis vorbehalten oder in Ausnahmefällen gestattet. Doch flexibles Arbeiten ist nicht nur in Krisenzeiten wichtig, sondern auch im normalen Geschäftsalltag. Mitarbeiter wollen von zuhause oder mobil auf Anwendungen und Daten des Unternehmens zugreifen oder an Videokonferenzen teilnehmen. Eine weitere Anforderung ist eine Remote-Desktop-Verbindung mit dem direkten Zugriff auf den im Büro befindlichen Rechner – auch vom Smartphone aus. Ziel ist es, dass jeder Mitarbeiter seine Tätigkeiten über das Internet und damit ortsunabhängig ausüben kann.



Was bedeutet das für die IT-Abteilung? Sie muss entsprechend Netzwerkkapazitäten für alle Mitarbeiter bereitstellen sowie für Sicherheit und Datenschutz sorgen. Letzteres kann eine große Herausforderung darstellen. Denn oft sind die im Homeoffice eingerichteten Arbeitsplätze nicht im gleichen Umfang abgesichert wie die Rechner im Büro. Durch die Vielzahl der digitalen Anwendungen, Datenzugriffe und Endgeräte gibt es auch mehr Gefahrenquellen für Sicherheitslecks. Die IT sollte daher alle Geräte unter einer einheitlichen Verwaltungs-Oberfläche zusammenführen und Tools zum Management der Endgeräte, Software und Nutzer, zur Verschlüsselung der Daten oder für sichere Backups einsetzen.

Neben der reinen technischen Sicherheit geht es darum, eine verbindliche Compliance und Governance zu definieren, damit sich auch die Mitarbeiter an die notwendigen Regeln halten und Daten nicht außerhalb der sicheren Umgebungen nutzen. Zu empfehlen ist hier das Zero-Trust-Prinzip nach dem Grundsatz: „Traue keiner Software und auch keinem Mitarbeiter und gewähre nur diejenigen Rechte, die eine Lösung und ein Mitarbeiter zum Erledigen seiner Aufgaben braucht.“

Um eine sichere Verbindung zum Firmennetzwerk zu gewährleisten, setzen Firmen meist auf einen verschlüsselten VPN-Tunnel (Virtual Private Network). Doch bei einer großen Belegschaft kann das VPN schnell überlastet sein und den Geschäftsbetrieb ausbremsen.

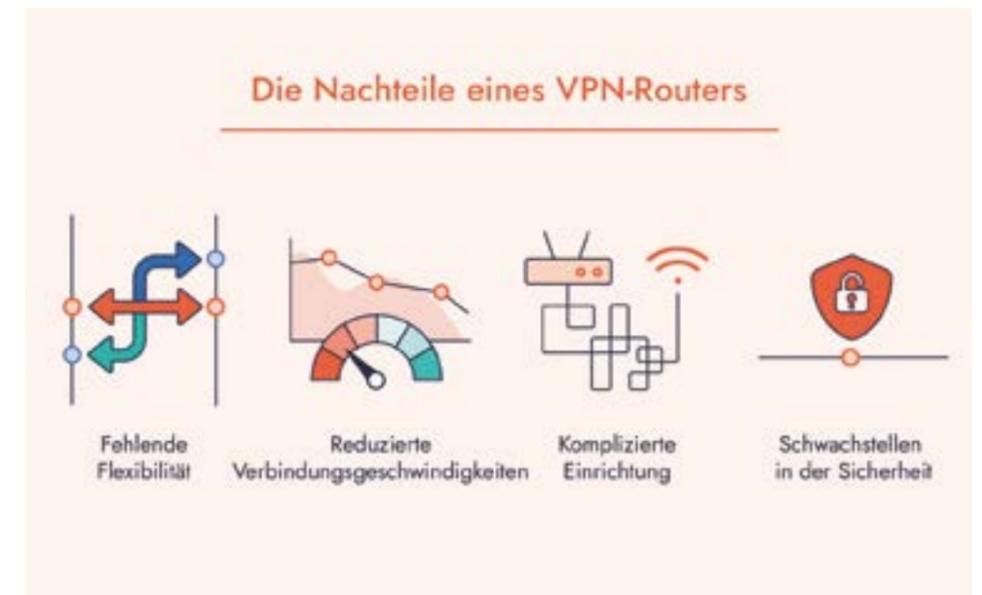
3.2. VPN – Verbindung mit Schwächen

Die Arbeitsweise eines VPNs ist im Prinzip sehr einfach. Man erzeugt über Verschlüsselung ein kleines Netzwerk innerhalb eines großen Netzes, das nur mit den passenden Adressen und Passwörtern zugänglich ist. Das heißt nur berechtigte Benutzer können miteinander kommunizieren. Ein VPN stellt somit eine Art überwachte private Leitung innerhalb des Internets her. Es verbindet Rechner oder Netzwerke miteinander, indem es andere Netzwerke als Transportweg benutzt. Dafür ist es meistens notwendig, einen VPN-Client auf dem Rechner zu installieren und einzurichten.

Alle Daten und Anfragen, die der Client an das Internet sendet, werden zunächst an den VPN-Server geleitet, verschlüsselt und dann erst ins Web weitergesendet. Die Verschlüsselung findet dabei in Echtzeit statt und verhindert Eingriffe von außen. Die Daten, die zurückgesendet werden, werden ebenfalls erst vom Server empfangen, verschlüsselt und dann an den Client geschickt. Der VPN-Client entschlüsselt diese dann abschließend wieder. Dieses Verfahren wird auch als Tunneling bezeichnet, da die zu schützenden Daten wie durch einen Tunnel fließen. Grundsätzlich wird dabei die IP-Adresse des Clients verschleiert und stattdessen die des VPN-Servers angezeigt – die Zielsever können damit die wahre Quelle der Anfrage nicht verfolgen oder protokollieren.

Doch der Einsatz von VPN ist nicht selten mit unerwünschten Nebenwirkungen verbunden. Die Kapazität der VPN-Gateways in den Firmen ist oft begrenzt und selten dafür ausgelegt, alle Mitarbeiter anzubinden, sondern lediglich einen Teil der

Belegschaft. Durch die hohe Auslastung wird der Zugriff langsam, beschwerlich oder bricht zeitweise ganz zusammen. Die Internetgeschwindigkeit hängt beispielsweise auch von der Art der Verschlüsselung und der Entfernung des Clients vom VPN-Server ab. Seien wir ehrlich: Kein Mitarbeiter will lange warten, bis sich Anwendungen oder Websites laden. Ein weiteres Problem: Fällt die VPN-Verbindung oder der VPN-Service



komplett aus und ist eine Neu-Einwahl erforderlich, fällt für diesen Zeitraum auch die Verschlüsselung aus. Damit wird die echte IP-Adresse enthüllt und der Mitarbeiter ist nicht mehr anonym im Internet unterwegs.

Um den VPN-Datenverkehr zu verringern, stellen manche Firmen in der Folge zum Beispiel auf SplitTunneling um. Dabei werden nur diejenigen Verbindungen durch den VPN-Tunnel geleitet, die Systeme am anderen Ende des VPN-Tunnels als Ziele haben. Für alle anderen Verbindungen wird der VPN-Tunnel ignoriert. Dadurch reduziert sich zwar das Datenvolumen am zentralen VPN-Endpunkt in der Firma, das Sicherheitsniveau aber sinkt.

Zudem können die Konfiguration und permanente Überwachung der VPN-Verbindungen im Unternehmen für die Administratoren sehr aufwändig sein. Sie müssen die vom VPN genutzte Bandbreite sowie die Integrität Ihres WAN und Ihres Netzwerkes immer im Auge behalten. Es geht darum, alle VPN-Verbindungen zu überwachen, Bandbreiten-Probleme zu identifizieren und bei Bedarf zusätzliche Kapazität zu ergänzen, damit bei den Nutzern keine Probleme auftreten.

Die Nutzer selbst sind auch gefordert. Sie müssen ihr Heimnetzwerk und ihr Gerät im Homeoffice mit einer Endpoint-Protection-Lösung absichern. Denn das beste VPN nützt nichts, wenn das Endgerät bei einem Mitarbeiter zu Hause infiziert ist. Der Angreifer hat dann mehr oder weniger schon Zugang zum Unternehmens-Netzwerk.

3.3. Sichere Lösung: WebConnect

Doch es gibt gute Alternativen zu VPN. Eine davon ist WebConnect, eine Lösung für den sicheren Fernzugriff auf Desktops und die Einwahl in das Firmennetzwerk. Das Besondere: WebConnect baut alle Verbindungen direkt zwischen Client und Remote-Gerät als Tunnel mit https-Verschlüsselung auf – das alles über den Browser und ohne Installation auf dem Client. Es gibt keine Server oder Knotenpunkte Dritter auf dem Weg. Dabei ist kein Gerät direkt erreichbar, der Verbindungsaufbau erfolgt über Nutzernamen und Passwörter. Zusätzlich ist 2-Faktor-Authentifizierung Standard bei WebConnect. Auf dem Zielgerät sind ebenfalls Nutzernamen und Passwörter zu verwenden. Damit sorgt die Lösung für Datenschutz und Sicherheit.



WebConnect setzt kein VPN ein, erreicht aber trotzdem hohe Sicherheit bei hoher Leistung. Dazu nutzt die Lösung ein SSL-Zertifikat pro Gerät über https und Secure WebSocket mit Verschlüsselung über TLS 1.3. Eine ähnliche Methodik kommt auch im Bankwesen zum Einsatz. Ein SSL-Zertifikat ist eine kleine Datendatei, die einen kryptografischen Schlüssel digital an die Details einer Organisation bindet. Wenn es auf einem Webserver installiert ist, aktiviert es das Sicherheitsschloss sowie das https-Protokoll und ermöglicht sichere Verbindungen von einem Webserver zu einem Browser. WebSocket ermöglicht als effizientes, bidirektionales Übertragungs-Protokoll moderne Webanwendungen, die sehr viel schneller agieren, als man es von der traditionellen HTTP-Kommunikation her kennt.

WebConnect bietet eine Vielzahl von Einstellungen, mit denen Firmen ihre Sicherheitsanforderungen und Rollen-Rechte-Konzepte individuell verfeinern können. Administratoren sind so in der Lage, einzelnen Nutzern, Nutzergruppen und Verbindungsprofilen auf demselben Gerät entsprechende Zugriffsrechte oder Zeitbeschränkungen zuzuweisen sowie jederzeit anzupassen.

Warum WebConnect?

WebConnect bietet ein neuartiges Konzept für Remote Working – Remote Desktop im Browser.

4. Warum WebConnect?

4.1. Für Unternehmen

WebConnect ist als sichere und einfache Alternative zu VPN die ideale Lösung für Freiberufler sowie Unternehmen.



- Mit WebConnect jede Verbindung im Browser
- WebConnect funktioniert überall, wo Internet verfügbar ist
- WebConnect ist komplett konform mit der DSGVO:
 - WebConnect hat keine zentrale Kunden- und Geräteverwaltung
 - Alle Zugangsdaten befinden sich ausschließlich innerhalb der jeweiligen Installation
 - Alle Daten sind das alleinige Eigentum des Kunden

- Produktive Benutzererfahrung auf jedem browserfähigen Gerät
- Sofort loslegen ohne Client-Installation
- Keine Zusatz-Software für VPN oder RDP-Verwaltung notwendig
- Sicherer Remote-Zugriff ohne VPN (Nutzername und Passwort, 2FA, direkter Tunnel zwischen Client und Remote-Gerät, fail2ban)
- Flexibilität: Arbeiten unabhängig von Ort und Zeit
- Geteilte RDP-Verbindungen für die zeitgleiche Arbeit an gemeinsamen Projekten
- RDP-Sitzungen mit bis zu 60 FPS z.B. für Videobearbeitung
- Privates Cloud-Verzeichnis in der WebConnect Installation
- Vorteile für Administratoren
 - Einfache Konfiguration und Administration
 - Unbegrenzte gleichzeitige Verbindungen
 - Einfache Vergabe von Zugriffsrechten
- Niedrigere Kosten durch geringeren Einrichtungs- und Administrationsaufwand

4.2. Für Datacenter und Cloudanbieter

WebConnect bietet ein neuartiges Konzept für das Remote-Arbeiten - Remote Desktop im Browser: Cloud Service Provider können ihren Kunden einen RDP-Zugang zur Verfügung stellen - schnell und einfach über den Browser, weltweit erreichbar ohne VPN.

- Verschlüsselt: SSL-Zertifikat (HTTPS), Secure Websocket über HTTPS, zusätzlicher Schutz durch TLS 1.3
- MFA (Multi-Faktor-Authentifizierung): Zugangsauthentifizierung mit Passwort und 2FA-App
- Das vielfältige Rollen-Rechte-Konzept unterstützt eine Zero-Trust-Sicherheitsarchitektur
- Session Time-out Funktionalität bei Inaktivität
- Fail-to-Ban
- Zero Knowledge - 100% Datenschutz
- Kein Server oder Knotenpunkte Dritter

So funktioniert WebConnect

WebConnect ist immer eine „On-Premise“-Installation.

5. So funktioniert WebConnect

WebConnect wird immer im Netzwerk des Kunden installiert. Als Gateway-Lösung stellt sie die Verbindung zwischen dem Benutzer und dem Remote-Gerät her. Aus Gründen der Sicherheit und aus Datenschutzgründen werden keine Benutzer- oder Verbindungsdaten auf Servern von WebConnect gespeichert. WebConnect ist immer eine „**On-Premise**“ Installation.

Alle Zugangsdaten der Nutzer und alle Verbindungsdaten sind verschlüsselt sowie nur in dieser Installation gespeichert. Zu keinem Zeitpunkt erhält WebConnect selbst Kenntnis dieser Daten oder kann darauf zugreifen.

Das WebConnect Gateway ist die einzige Verbindung zwischen den Remote-Geräten und den Nutzern, die auf diese Geräte zugreifen wollen. Zwischen dem WebConnect Gateway und dem Nutzer wird eine direkte HTTPS-Verbindung aufgebaut. Erst das WebConnect Gateway selbst baut dann eine Verbindung zum Remote-Gerät mit dem gewünschten Protokoll (RDP, VNC, SSH, Telnet oder Kubernetes) auf.

Die meisten Remote-Anbieter arbeiten mit zentralen Verbindungsservern. Hier wird mit Ende-zu-Ende Verschlüsselung geworben, nur ist der Schlüsselinhaber immer der Anbieter. WebConnect besitzt niemals die Schlüssel der Kunden. Die HTTPS-Verbindung wird direkt zwischen dem beim Kunden installierten WebConnect Gateway und dem Browser beim Benutzer aufgebaut. Nur diese beiden Geräte kennen den Schlüssel. Die Verbindung läuft nicht über WebConnect Server, sondern direkt.



WebConnect ermöglicht in der RDP-Verbindung Dienste, die sonst nur in einer direkten RDP-Verbindung möglich sind. So werden Funktionen wie direktes Drucken,

mehrere Monitore, geteilte RDP-Verbindungen und Videoübertragungen bis zu 60 FPS ermöglicht.

Mit WebConnect ist kein VPN notwendig. Das erleichtert die Verwendung für Benutzer erheblich. VPNs sind häufig aufwendig zu administrieren und es gibt viele Anwendungsfälle, in denen VPN-Verbindungen nicht aufgebaut werden können, da die dafür notwendigen Ports blockiert sind (Hotels, Konferenzräume etc.). Da WebConnect per HTTPS verbindet, ist nur der entsprechende HTTPS-Port notwendig, der nahezu überall frei verfügbar ist.



Da für die Grundfunktionen von WebConnect keinerlei Client Installationen notwendig sind, lässt sich jederzeit auch ein öffentlicher PC für kurzfristig notwendige Arbeiten verwenden. Die Verbindung wird auch von dort im Browser aufgebaut und hinterlässt keinerlei Daten. Es wird nichts auf dem lokalen Gerät gespeichert, da ausschließlich auf dem Remote-Gerät gearbeitet wird.

Mit WebConnect ist sowohl verteiltes Arbeiten von jedem Ort der Welt als auch verteiltes Arbeiten innerhalb moderner Büroumgebungen möglich. Sind die Basisarbeitsplätze werden im Datacenter des Bürogebäudes eingerichtet, kann man mit der WebConnect-Installation mit jedem Endgerät von jedem Platz im Büro gearbeitet werden.

Feste Arbeitsplätze gehören der Vergangenheit an. Remote ist jetzt überall. Teams arbeiten flexibel zusammen, egal ob im Konferenzraum oder im Freibereich – Arbeitsplätze sind dort, wo es für die Nutzer und die Arbeit am effektivsten ist.

Mit WebConnect müssen keine Anwendungen und keine Daten mehr lokal vorgehalten werden. Alles verbleibt ausschließlich und gesichert im Unternehmen. Gearbeitet wird nur im Unternehmen, ohne das der Nutzer im Unternehmen vor Ort anwesend sein muss. Mit WebConnect ist die Flexibilisierung der Arbeitswelt im Unternehmen angekommen.

Alles das ohne große Investitionen in Netzwerke, in VPN, in Infrastruktur. WebConnect wird einfach im internen Netz angeschlossen – und jedes Gerät ist automatisch ein flexibler „Fernarbeitsplatz“. Mit WebConnect geht jedes Unternehmen in die Cloud, ohne in Cloud Infrastruktur investieren zu müssen. Die Niederlassung fungiert direkt als Cloud und alle Daten verbleiben im Unternehmen.



WebConnect Funktionalität

WebConnect ist Remote-Arbeiten im Browser. Alles findet im Browser statt.

6. WebConnect Funktionalität

WebConnect ist Remote-Arbeiten im Browser. Alles findet im Browser statt. Damit kann WebConnect ohne Client-Installation von jedem browserfähigen Endgerät unabhängig vom Betriebssystem verwendet werden.

WebConnect ist Remote-Arbeiten im Browser. Alles findet im Browser statt. Damit kann WebConnect ohne Client-Installation von jedem browserfähigen Endgerät unabhängig vom Betriebssystem verwendet werden.

6.1. Die wichtigsten Funktionen von WebConnect

6.1.1. Protokolle

WebConnect unterstützt die folgenden Protokolle direkt im Browser:
RDP, VNC, SSH, Telnet, Kubernetes.



6.1.2. Shared-Monitor RDP mit mehreren Teilnehmern

Zeitgleiche Arbeit an gemeinsamen Projekten mit beliebig vielen Nutzern und besonderem Augenmerk auf den Schutz von wichtigen Daten. Dank WebConnect ist es möglich, über geteilte RDP-Verbindungen im eigenen Netzwerk ohne Zugriff auf Fremdsysteme Dokumente zu teilen. Alle Teilnehmer können gleichberechtigt auf dem Bildschirm arbeiten und so Dokumente gemeinsam erstellen und optimieren. Shared Monitor bietet auch Links für Gäste, die nur über Besucher Rechte verfügen. Diese Gäste können die RDP-Sitzung verfolgen, aber nicht selbst interagieren.

6.1.3. Multi-Monitor und Co-Monitor

WebConnect unterstützt bis zu drei Monitore in Browser-Tabs. Jeder Monitor befindet sich in einem eigenen Browser-Tab, der beliebig positioniert und bewegt werden kann. Wie bei „echten“ Monitoren lassen sich Elemente von einem Tab in den nächsten Tab verschieben.

Mit Co-Monitor ist es möglich, dass sich Nutzer mit demselben Konto auf 2 Geräten anmelden. Auf dem 2. Gerät wird hier ein Button „CoMonitor“ zu aktiven Verbindungen angeboten. Dieser Button öffnet die RDP-Verbindung als identische Kopie. Damit lassen sich alle Anwendungen auf beiden Geräten gleichberechtigt bedienen. Diese Funktion kann zum Beispiel verwendet werden, um auf einem PC oder MacBook zu arbeiten und für das einfache Signieren von Dokumenten ein Tablett zu nutzen.



6.1.4. Multi-Verbindung

Es können bis zu 6 gleichzeitige Verbindungen in einem Browser geöffnet werden. Die Verbindungen werden als Thumbnails im Fuß-Bereich des Browsers angezeigt. Durch Klick auf diese ist ein bequemer Wechsel zwischen den Verbindungen möglich. Mit dieser Funktion lassen sich einfach und effektiv mehrere Geräte gleichzeitig steuern und überwachen. Ideal ist diese Funktion für administrative Arbeiten.

6.1.5. Shared-Drive mit Dateimanager

Shared-Drive ist ein gemeinsamer Ordner für alle Nutzer einer WebConnect-Installation. Er befindet sich innerhalb der Installation und ist von jedem Ort als angemeldeter Benutzer erreichbar. Im SharedDrive können Benutzer Daten bequem austauschen, da jeder Nutzer gleichberechtigt Zugriff auf diese Dateien hat. Damit sind keine öffentlichen Cloud-Verzeichnisse für den Austausch von Dateien mehr notwendig. Als Dateimanager steht ein moderner Filemanager zur Verfügung.

6.1.6. Private-Drive mit Dateimanager

Neben dem Shared-Drive wird auch ein Private-Drive angeboten. Auf dieses Verzeichnis hat nur der angemeldete Nutzer selbst Zugriff. Auch Administratoren können dieses Verzeichnis nicht einsehen. Im Private-Drive können Nutzer Daten speichern, die sie remote benötigen. Auch im Private-Drive steht der komfortable Filemanager für die Verwaltung zur Verfügung. Der Private-Drive ist mit einem privaten Cloud-Verzeichnisvergleichbar, das aber im Unterschied zu Cloud-Diensten keine Server Dritter verwendet. Alle Dateien bleiben immer unter der Kontrolle und im Besitz des Nutzers.



6.1.7. Remote drucken

WebConnect erlaubt es im Standard, Dokumente in PDF zu drucken. Zusätzlich hat WebConnect ein Add-On entwickelt, das es ermöglicht sämtliche lokalen und Netzwerkdrucker direkt mit allen Einstellungen anzusprechen und remote jedes Dokument direkt zu drucken. Das kann der freigegebene Drucker im Hotel oder einer Konferenz sein, genauso wie die Netzwerkdrucker im Büro, wenn man Kollegen gedruckte Dokumente zur Verfügung stellen will.

Das WebConnect Add-On gibt es als Dienst für Windows und für MacOS.

6.1.8. Webcam und Mikrofon

Da WebConnect sich direkt mit dem Arbeitsplatz verbindet, lassen sich Video-Calls bequem von zuhause aus über die vorinstallierte Firmenanwendung führen. Die Lösung unterstützt am lokalen Gerät angeschlossenen WebCams und Mikrofone. Es gibt keine Einschränkungen auf bestimmte Webcam-Modelle oder Auflösungen. Auch das Audiosignal des Remote-Gerätes wird ohne Einschränkung übertragen.

6.1.9. SmartCard Weiterleitung

Häufig gibt es die Anforderung sich bei bestimmten Programmen oder Diensten per SmartCard zu authentifizieren. Ein Beispiel in Deutschland ist der beA Dienst als elektronisches Anwaltspostfach. Das WebConnect AddOn, das auch das Remote-Drucken ermöglicht, stellt auch eine Funktion bereit, die es erlaubt SmartCard Reader am lokalen Gerät zu verwenden und sich damit auf dem Remote-Arbeitsplatz zu verifizieren. Alle Daten werden direkt übertragen, als ob man vor Ort tätig ist.

6.1.12. Unterstützung von Philips SpeechMike

Mitarbeitern, die viel diktieren und Spracherkennungs-Software in ihrem Arbeitsalltag einsetzen, ermöglicht WebConnect grenzenlose Mobilität. Wenn sie Philips SpeechMike mit Ihrem lokalen Gerät verbinden, können sie von überall in ihr Remote-Gerät diktieren. Die Dateien stehen der Spracherkennungssoftware dann unmittelbar zur Weiterverarbeitung zur Verfügung.



6.1.10. Wake-on-LAN

Energieeffizientes Arbeiten ist ein wichtiges Thema, um Betriebskosten zu senken und umweltbewusst zu handeln. WebConnect unterstützt Wake-on-LAN. Damit kann man entfernte Geräte einfach ausschalten oder in den Stromsparmodus schicken, wenn man diese nicht benötigt. Muss der Nutzer jetzt an diese Geräte, um bestimmte Programme zu starten oder an Daten zu kommen, lässt sich mit Wake-on-LAN ein Aufwecksignal an das Remote-Gerät senden.

6.1.13. RDP-Sitzungen mit Videobearbeitung

Durch Frameraten zwischen 60 und (Frames pro Sekunde) bei minimaler Verzögerung setzt WebConnect neue Standards beim Streaming von Videodateien. Damit können Grafiker, Industriedesigner und andere Mitarbeiter aus der Ferne auf ihre hoch performanten Prozessrechner und die darauf installierten Programme zugreifen und gemeinsam an ihren Projekten arbeiten.

6.1.11. Mobile apps

Selbstverständlich funktioniert WebConnect auch mobil im Browser. Um aber der eingeschränkten Bildschirmgröße gerecht zu werden hat WebConnect Apps für iOS und Android entwickelt, die aufstörende Browser-Elemente verzichten. Mobile WebConnect-Apps sind optimiert für mobile Geräte mit iOS und Android Betriebssystemen.



6.1.14. Benutzerverwaltung

All user data is stored exclusively in the local application. There is no central WebConnect user database. This decentralised user management of all WebConnect installations increases security for customers, as there are no centralised opportunities for attack.

Alle Nutzerdaten werden ausschließlich in der lokalen Anwendung gespeichert. Es gibt keine zentrale WebConnect-Nutzerdatenbank. Diese dezentrale Benutzerverwaltung aller WebConnect-Installationen erhöht die Sicherheit für die Kunden, da es keine zentralen Angriffsmöglichkeiten gibt.

6.1.15. Verbindungsverwaltung

In der WebConnect-Verbindungsverwaltung werden alle Geräte angelegt. Es können auch unterschiedliche Profile für gleiche Geräte angelegt werden, um die Einstellungen für spezielle Nutzungssituationen anzupassen. In den Verbindungsprofilen ist es bereits möglich, die Zugangsdaten zum Gerät zu hinterlegen. Sicherer ist es jedoch diese erst bei der Verbindung abzufragen, da damit ein weiteres Sicherheitslevel aufgebaut wird, das von WebConnect unterstützt wird.



6.2. Geplante Funktionen für das 4. Quartal 2022

6.2.1. Shared Drive mit Online-/Offline-Synchronisation

Dropbox, Microsoft One Drive oder Google Drive, jeder kennt diese und andere Dienste und nutzt sie privat oder beruflich. Alle diese Dienste liegen hier auf den Servern der Anbieter und es ist nicht klar, was mit den Daten passiert. In der Regel kennt der Nutzer noch nicht einmal den geografischen Speicherplatz. Konten können von einem Tag auf den anderen willkürlich gesperrt werden, Daten können unberechtigt abgerufen werden. Die KI großer Unternehmen analysiert die Daten auf mögliche Verstöße gegen die AGB. Hinzu kommt die Gefahr von gezielten Hackerangriffen gegen diese Provider.

Die neue Online-/Offline-Synchronisation von WebConnect verlegt die Cloud in das eigene Netzwerk. Die Daten werden auf den vom Benutzer freigegebenen Geräten offline bereitgehalten und synchronisiert, wenn die jeweiligen Geräte online im Netz sind. Alle Daten werden DSGVO-konform gespeichert und können entsprechend der strengen Anforderungen einiger Berufsgruppen, wie Ärzten, Anwälten, oder Steuerberatern sicher unter der eigenen Kontrolle verwaltet werden.

Der neue WebConnect Shared-Drive wird der sichere Speicherplatz der Zukunft, in dem der Nutzer die Hoheit über seine Daten zurückgewinnt.



6.2.2. USB-Weiterleitung in der RDP Sitzung im Browser

WebConnect leitet alle USB-Geräte vom lokalen Arbeitsplatz in die entfernte RDP-Remote-Sitzung weiter. Schon jetzt werden Drucker, WebCams und SmartCard Lesegeräte von WebConnect in der Remote-RDP-Sitzung unterstützt. Mit der kommenden generellen USB-Weiterleitung wird der USB-Anschluss komplett in die Arbeitssitzung weitergeleitet. Damit spielt das angeschlossene Gerät keine Rolle mehr.



6.2.3. WebMeet-Video-Meeting mit Whiteboard und Chat

WebMeet ist ein eigener Video-Meeting Server in der WebConnect Installation. Da alle Video-Verbindungen, Chats und Whiteboard Arbeiten ausschließlich Peer2Peer stattfinden, gibt es keine Server in der Mitte, die Daten verwalten oder verarbeiten. Die Video-Meetings sind damit DSGVO-konform.

WebMeet ist optimiert für bis zu 6 Teilnehmer in einem Gespräch. Es können alle Benutzer der WebConnect Installation miteinander kommunizieren.

WebMeet ist optimiert für bis zu 6 Teilnehmer in einem Gespräch. Es können alle Benutzer der WebConnect Installation miteinander kommunizieren.

Mit WebMeet und einer Shared-RDP-Verbindung ist eine effektive und professionelle Zusammenarbeit in einer absolut gesicherten Umgebung möglich. Die eingesetzten Technologien verhindern das Abhören und Mitschneiden durch Unbefugte.

Mit WebMeet und einer Shared-RDP-Verbindung ist eine effektive und professionelle Zusammenarbeit in einer absolut gesicherten Umgebung möglich. Die eingesetzten Technologien verhindern das Abhören und Mitschneiden durch Unbefugte.

WebConnect: Funktions-Übersicht

Hallo Web Connect.
Ihre private Cloud.

7. WebConnect: Funktions-Übersicht

7.1. WebConnect: Funktions-Übersicht

- **Alles im Browser:** Zugriff von jedem browserfähigen Endgerät – sofort loslegen ohne Client- Installation
- **Wake-on-LAN:** Ausgeschaltete Desktops aus der Ferne aktivieren
- **Videoptimiert:** Übertragungsrate 60 Frames pro Sekunde (FPS)
- **Remote USB:** Alle USB-Geräte von überall nutzen
- **Protokolle:** RDP, VNC, SSH, Telnet, Kubernetes
- **Sicherheit:** 2-Faktor-Authentifizierung & https-Verschlüsselung
- **Shared-RDP-Connections:** Team Arbeit auf einem Screen
- **Shared Drive:** Die Alternative zum externen Cloud-Speicher
- **Online / Offline Synchronisation** (4. Quartal 2022)
- **WebMeet** (4. Quartal 2022)
- **Optimiert für mobile Geräte:** Apps für Android & iOS

7.2. Die im Browser unterstützten Protokolle

- RDP
- VNC
- SSH
- TelNet
- Kubernetes

7.3. Sicherheit und Datenschutz

- Zero-Trust-Politik
- Keine zentrale Datenbank (Zero Knowledge – keine Daten beim Betreiber)
- Alle Benutzerdaten verschlüsselt in der Kundeninstallation
- Login direkt in der Installation
- Benutzername und Passwort
- 2FA (optional)
- Fail to Ban
- Zusätzlich Login in der Verbindung
 - Je nach Gerätekonfiguration:
 - Benutzername und Passwort
 - SmartCard (optional)
 - 2FA (optional)
- Peer to Peer (direkte Verbindung zur Installation ohne Drittanbieter)
- Verschlüsselung: Secure websocket auf https, TLS 1.3
- Sicherer Remote Zugriff: sicherer unbeaufsichtigter Zugriff

7.4. Nutzer- und Verbindungsverwaltung

- Unbegrenzte Benutzerkonten anlegen
- Anzahl gleichzeitige Benutzer je nach gewähltem Tarif
- Datenvermeidung durch ein Minimum an notwendigen Daten für den Betrieb von WebConnect
- Anlage von Benutzergruppen mit definierten Benutzern und Geräten
- Zugriffsrechte, um unterschiedliche Zugriffsebenen zu verwalten
- Geräte bestimmten Benutzern zuzuweisen.
- Zugangsbeschränkungen mit Datum und Uhrzeit
- 2FA für alle Benutzer verpflichtend anschalten
- In der Verbindung definieren, dass Benutzer sich auch dort per Benutzername und Passwort legitimieren müssen
- Unbegrenzte Verbindungen anlegen
- Passwort abgelaufen: Funktion, um Benutzer zu zwingen ein neues Passwort zu setzen

- Backup: Export und Import von Benutzer, Gruppen, Verbindungen und anderen Einstellungen
- E-Mail-Einladung für neue Nutzer (optional)
- Notizen-Seite für Administratoren
- Verbindungsverlauf
- Speicherplatz Anpassung in VM-Installationen
- Ethernet-Port-Erkennung in VM-Installationen

7.5. Eigenschaften

- Alles im Browser (Keine Installation einer Sender- oder Empfänger-Software)
- Streaming bis zu 60FPS mit RDP im Browser
- Cross Plattform Access
- Wake On Lan (Aufwecken, Neustart von Geräten)
- Bis zu 6 gleichzeitige Verbindungen im Browser mit einfachem Wechsel über Kacheln
- Shared drive inkl. Filemanager
- Spezielle Tastatur-Shortcuts für Anwendungen in Windows-RDP von MacOS oder Windows
- Private Drive (Networkdrive mit WebDAV)
- Einstellungen für Tastatur-Setup
- Remote Audio
- USB-Weiterleitung in der RDP-Sitzung im Browser (4. Quartal 2022)

7.6. Ansicht

- Fullscreen Mode in jeder Verbindung
- Bildschirm resize: Bildschirm passt sich automatisch der Browsergröße an
- Multimonitor im RDP mit bis zu 3 gleichzeitigen Bildschirmen in Browser Tabs
- Dark- und Light-Theme
- Individuelles Hintergrundbild
- CO-Monitor

7.7. Zusammenarbeit

- Shared-RDP-Verbindungen mit gleichberechtigter Zusammenarbeit
- Reiner Lesemodus in Shared-RDP-Verbindungen
- Shared Drive inkl. Filemanager
- Shared Drive mit Online-/–Offline-Synchronisation (4. Quartal 2022)
- WebMeet-Videomeeting bis zu 6 Personen in einer Sitzung (4. Quartal 2022)
- WebMeet-Text-Chat (4. Quartal 2022)
- WebMeet-Whiteboard (4. Quartal 2022)
- WebMeet whiteboard (4th quarter 2022)

7.8. Peripherie

- Drucker-Redirect im Browser-RDP für lokale und Netzwerkdrucker
- SmartCard-Redirect im Browser-RDP (z.B. für Remote-Login in das elektronische Anwaltspost-fach bEA)
- Unterstützung für Philip- Speechmike im Browser-RDP
- Umleitung von WebCam und Audio im Browser-RDP

7.9. Mobile app

- Optional iOS und Android Apps
- QR Code in WebConnect zur einfachen Einrichtung der iOS und Android App

Vergleichsmatrix

Vergleichen Sie uns mit der Konkurrenz und finden Sie heraus, warum wir die beste Wahl sind.



| | WebConnect | Anydesk | Teamviewer | Microsoft Browser RDP | Microsoft RDP + VPN |
|--|---------------|---------------|-----------------|-----------------------|---------------------|
| Performance / Preis | | | | | |
| Framerate | bis zu 60 fps | bis zu 60 fps | bis zu 60 fps | bis zu 60 fps | bis zu 60 fps |
| Preis | 10 € p.m. | ab 9.9 € p.m. | ab 298.8 € p.a. | - | - |
| Browserbasiertes Remote Desktop | ✓ | ✗ | ✗ | ✓ | ✗ |
| Features | | | | | |
| Aktivitäts Dashboard | ✓ | ✗ | ✗ | ✗ | ✗ |
| API | ✓ | ✓ | ✓ | ✗ | ✗ |
| App | ✓ | ✓ | ✓ | ✗ | mit 2 Apps |
| Bildschirm teilen / Shared Screen | ✓ | ✓ | ✓ | ✗ | ✗ |
| Benötigt Client Software | ✗ | ✓ | ✓ | ✗ | mit 2 Apps |
| Drag & Drop | ✓ | ✗ | ✓ | ✗ | ✓ |
| Filesharing (direkt) | ✓ | ✓ | ✓ | ✗ | ✓ |
| Filesharing (offline/online sync alias OneDrive) | ✓ | ✗ | ✗ | ✗ | ✓ |
| Generic USB redirection | ✓ | ✗ | ✗ | ✗ | ✓ |
| Integration Active Directory (LDAP) | ✓ | ✗ | ✗ | ✓ | ✓ |
| Kein Dritts | ✓ | ✗ | ✗ | ✗ | ✓ |
| Lokale Nutzerdatenbank | ✓ | ✗ | ✗ | ✗ | ✓ |
| Kommentare/Notizen | ✓ | ✗ | ✗ | ✗ | ✗ |
| Kundenspezifisches Branding | ✓ | ✓ | ✓ | ✗ | ✗ |
| Live Chat | ✓ | ✗ | ✓ | ✗ | ✗ |
| MFA (Multi Factor Authentifizierung) | ✓ | ✗ | ✓ | ✗ | ✗ |
| Mobiler Zugriff | ✓ | ✓ | ✓ | ✓ | ✓ |
| Nutzerverwaltung | ✓ | ✗ | ✗ | ✓ | ✓ |
| Personalisierung | ✓ | ✗ | ✓ | ✗ | ✗ |
| Präsentations-Streaming | ✓ | ✗ | ✓ | ✗ | ✗ |
| Remote-Drucker als PDF | ✓ | ✓ | ✓ | ✗ | ✓ |
| Remote-Drucken auf lokalem Printer | ✓ | ✗ | ✗ | ✗ | ✓ |
| Remote-Zugriff/-Kontrolle | ✓ | ✓ | ✓ | ✓ | ✓ |
| Sicheres Login | ✓ | ✗ | ✗ | ✓ | ✓ |
| Unbeaufsichtigter Zugang | ✓ | ✓ | ✓ | ✓ | ✓ |
| Videokonferenzen | ✓ | ✗ | ✓ | ✗ | ✗ |
| Umschaltung zwischen mehreren Monitoren | ✓ | ✓ | ✓ | ✗ | ✓ |
| Gleichzeitiger Zugriff auf mehrere Monitore | ✓ | ✗ | ✗ | ✗ | ✓ |
| Zugriffskontrollen / Berechtigungen | ✓ | ✓ | ✓ | ✓ | ✓ |
| Wake on Lan | direkt | 2 Gerät | 2 Gerät | ✗ | ✗ |
| Mehrere Sitzungen in einer Session | ✓ | ✓ | ✓ | ✗ | ✗ |
| Fail-to-ban | ✓ | ✗ | ✗ | ✗ | ✓ |
| Gruppenmanagement | ✓ | ✗ | ✗ | ✗ | ✓ |
| Live Display Update Resize | ✓ | ✗ | ✗ | ✓ | ✗ |
| Real RDP (Nativer Remote Desktop) | ✓ | ✗ | ✗ | ✓ | ✓ |
| Smart Card Redirection | ✓ | ✗ | ✗ | ✗ | ✓ |
| Phillips Speech Mike Redirection | ✓ | ✗ | ✗ | ✗ | ✓ |
| Self Administered | ✓ | ✓ | ✓ | ✗ | ✗ |

Sicherheit

Die sichere Zwei-Faktor-Authentifizierung stellt von überall aus sofort eine Verbindung zu Ihrer Workstation her.

9. Sicherheit

Sichere und einfache Alternative zu VPN:
WebConnect bietet ein neuartiges Konzept für das Remote-Arbeiten – eine ähnliche Methodik wie im Bankenwesen.



9.1. Verbindung & Verschlüsselung

- Kein Server oder Knotenpunkte Dritter
- WebConnect funktioniert als Application Gateway
- Sichere HTTPS-Verschlüsselung (abhörsicheres Protokoll, dass Daten zwischen Browser und WebConnect in beiden Richtungen verschlüsselt überträgt)
- SSL Zertifikat (HTTPS) / Secure Web Socket über HTTPS
- Keylänge SSL: RSA 2048
- Zusätzlicher Schutz durch TLS 1.3 (Transport Layer Security)

9.2. Authentifizierung

- MFA (Multi-Factor-Authentication): Zugangsauthentifizierung mit Passwort sowie 2FA-App
- Authentifizierung am Zielgerät mit Username und Passwort
- Alle Benutzerdaten liegen ausschließlich und verschlüsselt in der WebConnect-Installation (keine zentrale Zugangsdatenbank auf WebConnect Servern)
- Sperre mit gestaffelten Zeitintervallen bei Mehrfach-Falschlogin (Fail to Ban)

9.3. Datenschutz & Compliance

- Zero Knowledge / 100% Datenschutz: Keine Daten beim Hersteller, alle Daten im Besitz des Kunden
- Produkt installiert beim Kunden
- Security by Design
- DSGVO-konform, da alle Nutzerdaten ausschließlich beim Nutzer gespeichert sind.

9.4. Netzwerksicherheit

- Verstecken des Zugangs durch Portweiterleitung. Nur WebConnect ist mit der öffentlichen IP des Netzwerks erreichbar.
- Höhere Verfügbarkeit als bei VPN. WebConnect nutzt Port 443 (HTTPS) für den Verbindungsaufbau, der in vielen Netzen (z.B. Flughäfen, Konferenzzentren) als einziger Port offen ist.
- Keine Öffnung von Firewall zusätzlichen Ports außer 443 oder Portforwarding notwendig.
- Das vielfältige Rollen-Rechte-Konzept unterstützt eine Zero-Trust-Sicherheitsarchitektur
- Session Time-out Funktionalität bei Inaktivität

WebConnect Plug & Play WebConnect Enterprise

10. Webconnect: Lizenzierung

WebConnect Plug&Play

Die Plug&Play-Lösung funktioniert über den bereits fertig konfigurierte WebConnect Co-Router (Hard-ware), der einfach mit dem Netzwerk verbunden wird. Alles, was Firmen für den Zugriff auf ihre Desk-tops benötigen, sind ein Webbrowser und der WebConnect Co-Router im Netzwerk. Für den Betrieb ist in der Regel lediglich ein Portforwarding des Port 443 (HTTPS) auf den WebConnect Co-Router im Netzwerk einzutragen. WebConnect kontrolliert automatisch alle Sicherheitsregeln. Mit dem WebConnect Co-Router ist es nicht notwendig, ein komplexes VPN einzurichten, um Geräte von außen zu erreichen.

Denn nur der WebConnect Co-Router ist mit der öffentlichen IP des Netzwerkes erreichbar, alle anderen Netzwerkgeräte sind weiter hinter internen IP-Adressen versteckt und nicht direkt zugänglich. Der WebConnect Co-Router erlaubt als eine Art Gateway den einfachen und sicheren Zugriff von außen unabhängig vom Betriebssystem und Gerät. Selbst mobile Geräte, die sich meist nur mühsam ins VPN einbinden lassen, sind bei WebConnect Standard.

WebConnect Plug&Play ist optimiert für bis zu 20 gleichzeitige Remote-Verbindungen.

WebConnect Enterprise

Die Enterprise-Lösung ist für mehr als 20 gleichzeitige Verbindungen konzipiert und eignet sich daher sehr gut für große Netzwerke und Cloud-Anwendungen. Bei dieser Version wird die WebConnect-Software im Netzwerk auf einer virtuellen Maschine (VM) mit dem Betriebssystem Linux (VM) installiert. Die VM wird innerhalb des entfernten Netzwerkes eingerichtet und ist daher - wie der WebConnect Co-Router - das einzige Gerät, das über eine öffentliche IP-Adresse sichtbar ist. Alle anderen entfernten Geräte mit internen IP-Adressen bleiben für den Zugriff ohne WebConnect unsichtbar. WebConnect Enterprise lässt sich innerhalb eines lokalen Netzwerkes als VM installieren, beispielsweise auf einem vorhandenen NAS (z. B. Synology). In der Cloud im Rechenzentrum sollten Firmen dafür eine kleine VM auswählen.

Die Installation der Enterprise-Lösung ist etwas aufwändiger als die der Plug&Play-Lösung, aber deutlich einfacher als die Einrichtung eines VPN mit all seinen Problemen. Die Enterprise-Lösung hat den gleichen Funktionsumfang wie die Plug&Play-Version, ist aber auch für große Teams konzipiert, die gleichzeitig auf das entfernte Netzwerk zugreifen.



Kapitel 11

Über WebConnect



11. Über WebConnect

WebConnect World SL mit Sitz in Madrid hat sich auf die Themen Datenschutz, Sicherheit und Kommunikation spezialisiert. Das Unternehmen entwickelt eigene Produkte und berät Kunden im Bereich Forschung & Entwicklung. Zentrales Produkt ist WebConnect für flexibles und sicheres Arbeiten von überall auf der Welt. Die Lösung bietet ein neuartiges Konzept für den sicheren Fernzugriff auf Desk-tops und die Einwahl in das Firmennetzwerk – als sichere und einfache Alternative zu VPN. Der Vertrieb von WebConnect erfolgt über Reseller und verschiedene Partner-Programme. Weitere Informationen erhalten Sie unter <https://webconnect.pro/de/>.



Resources

Website

<https://webconnect.pro>

Brand Guidelines

https://webconnect.pro/wp-content/uploads/2022/08/Brand_Guidelines_V3.pdf

Help center

<https://webconnect.pro/de/hilfezentrum/>

Anlagen

1. **WebConnect bringt Datacenter auf Azure-Level**
2. **WebConnect-RDP im Browser oder RDP mit VPN**
3. **Externe Geräte mit Wake-on-LAN einschalten**
4. **Remote Zugänge sicher verwalten**
5. **WebConnect und / oder andere IT-Lösungen**
6. **Lizenzen und Preise**

WebConnect bringt Datacenter auf Azure-Level

WebConnect bringt Datacenter auf Azure-Level

Remote arbeiten von überall ist die Herausforderung der heutigen Zeit. Dieser Situation haben sich die Datacenter gestellt und bieten immer umfangreichere Büro-Lösungen in der Cloud an. Dazu gehört auch das gesamte Office-Software Portfolio von Microsoft. Auch Microsoft hat daher das Potential dieses Marktes erkannt und steht jetzt mit anderen Datacenter-Anbietern im Wettbewerb um Kunden.

Warum ist Microsoft Azure hier im Vorteil?



Der Unterschied liegt in der letzten Meile, in der Art des Zugriffes auf die Anwendungen, um dem Nutzer das beste Arbeitsumfeld zu schaffen. Datacenter können genau wie Microsoft Office, Teams, SharePoints und andere Lösungen anbieten, aber Microsoft lizenziert nicht den einfachen komfortablen Browser-Zugang auf den RDP des Remote-Rechners. Diesen vermarktet Microsoft exklusiv in der Azure Cloud und schafft sich damit den entscheidenden Marktvorteil.

| | Datacenter | Azure |
|---------------------------|------------|-------|
| Office, Teams, SharePoint | ✓ | ✓ |
| VPN | ✓ | ✓ |
| RDP im Browser | ✗ | ✓ |

Kunden wollen es einfach haben. Sie wollen von überall und mit jedem Gerät auf das Firmennetzwerk zugreifen und ein perfektes Bildschirm-Erlebnis beim Arbeiten. Das können Datacenter so nicht anbieten. Sie müssen den Zugang per VPN aufbauen. Das ist allerdings supportanfällig und erfordert immer Administratoren für die Einrichtung und Verwaltung. Microsoft Azure bietet den Zugang per Browser von überall mit jedem Gerät.

Mit WebConnect jedes Datacenter zum Azure-Wettbewerber ausbauen

Hier setzt WebConnect an. WebConnect bietet Datacentern genau diese fehlende letzte Meile mit Funktionen, die das Datacenter leistungsfähiger als Azure macht.



WebConnect wird als Software in der Kunden-Cloud installiert und bildet das Gateway zwischen dem Kunden und der Cloud. Der Kunde kann seine Cloud-Rechner per Browser bedienen. Die Verbindung wird über HTTPS direkt zwischen dem Kunden und der Cloud (Peer-to-Peer) aufgebaut, die RDP-Verbindung erfolgt über WebConnect.

| | Datacenter | Azure |
|---------------------------|------------|-------|
| Office, Teams, SharePoint | ✓ | ✓ |
| VPN | ✓ | ✓ |
| RDP im Browser | ✓ | ✓ |

WebConnect unterstützt jeden Arbeitsplatz mit Browser und bietet mobile Apps mit optimierten Bildschirmen für Smartphone und Tablet. Einfache Geräteverwaltung sowie, umfangreiche Kunden- und Rechte-Verwaltung runden das Produkt ab.

Mit WebConnect das Datacenter von Azure abheben

Alle Zugangsdaten liegen bei WebConnect ausschließlich in der lokalen Kunden-Installation, bei Azure liegen diese in der zentralen Microsoft-Datenbank.

Alle Daten und Anwendungen des Kunden liegen in dem Datacenter seines Vertrauens, während bei Azure die Daten alle in den Händen eines multinationalen Unternehmens mit Sitz in den USA liegen.

Während WebConnect mit mehreren Installationen Zugangs- und Geräte-Daten dezentral speichert und sichert, liegen die Zugangsdaten bei Azure immer in der zentralen Microsoft-Datenbank.

Bei WebConnect wird der Zugang mit Nutzernamen und Passwort, mit 2FA und mit Fail to Ban abgesichert. Zero-Trust ist das Grundprinzip für alle Nutzer.

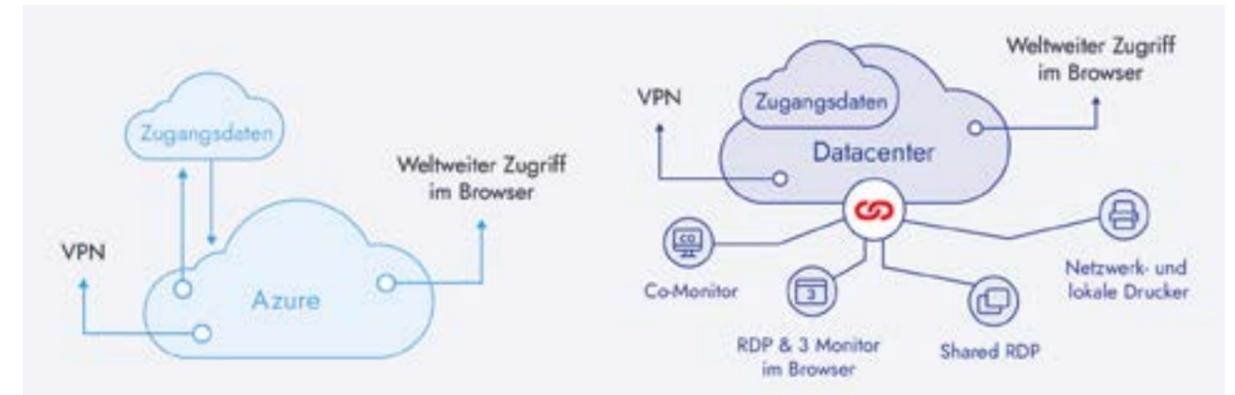
Mit WebConnect lässt sich jede RDP-Verbindung auf bis zu 3 Monitore in Browser-Tabs erweitern.

WebConnect steuert sämtliche lokalen und Netzwerk-Drucker direkt an und übernimmt alle bestehenden Drucker-Einstellungen.

Mit WebConnect kann der Nutzer seine RDP-Verbindung auf einem zweiten Gerät (Co-Monitor) anzeigen und bedienen, zum Beispiel für digitale Unterschriften per Tablet während der Dokumenten-Bearbeitung auf dem PC.

Mit WebConnect kann der Nutzer weitere Nutzer in seine RDP-Sitzung (Shared-RDP) einladen, und alle Nutzer können gemeinsam auf dem RDP-Bildschirm im Browser arbeiten

Mit WebConnect kann der Nutzer weitere Nutzer als reine Zuschauer in seine RDP-Sitzung einladen und diesen Präsentationen zeigen oder sie einfach nur der Arbeit zuschauen lassen.



| | Datacenter | Azure |
|---|------------|-------|
| Zugangsdaten | Lokal | Cloud |
| Kundendaten und Anwendungen | Lokal | Cloud |
| Zugangsdaten in dezentralen Installationen | Dezentral | Cloud |
| Nutzernamen | ✓ | ✓ |
| Passwort | ✓ | ✓ |
| 2FA | ✓ | ✓ |
| Fail to Ban | ✓ | ✗ |
| RDP mit 3 Monitoren in Browser Tabs | ✓ | ✗ |
| Netzwerk und lokale Drucker im Browser RDP | ✓ | ✗ |
| Co-Monitor – RDP auf 2. Gerät | ✓ | ✗ |
| Shared-RDP – RDP mit mehreren Anwendern | ✓ | ✗ |
| RDP im Browser als Ansicht mit Nutzern teilen | ✓ | ✗ |

WebConnect und Datacenter - die echte Alternative zu Microsoft Azure

WebConnect World SL

WebConnect World SL mit Sitz in Madrid hat sich auf die Themen Datenschutz, Sicherheit und Kommunikation spezialisiert. Das Unternehmen entwickelt eigene Produkte und berät Kunden im Bereich Forschung & Entwicklung. Zentrales Produkt ist WebConnect für flexibles und sicheres Arbeiten von überall auf der Welt. Die Lösung bietet ein neuartiges Konzept für den sicheren Fernzugriff auf Desktops und die Einwahl in das Firmennetzwerk – als sichere und einfache Alternative zu VPN. Der Vertrieb von WebConnect erfolgt über Reseller und verschiedene Partner-Programme. Weitere Informationen erhalten Sie unter <https://webconnect.pro/de/>.

WEBCONNECT

WebConnect-RDP im Browser oder RDP mit VPN

WebConnect-RDP im Browser oder RDP mit VPN

- Was unterscheidet die beiden Lösungen?
- Wie soll man sich als Unternehmen entscheiden?
- Welche Vorteile ergeben sich für die Mitarbeiter?
- Sind beide Lösungen sicher?

WebConnect-RDP im Browser

WebConnect bietet RDP im Browser auf jedem Endgerät. Die Verbindung erfolgt direkt per HTTPS und TLS 1.3 vom Remote-Arbeitsplatz zur WebConnect-Installation. Benötigt wird hierfür der Port 443 (HTTPS). Je nach Netzwerkkonfiguration ist am Router eine Portweiterleitung auf den Port 443 der WebConnect-Installation einzurichten.



WebConnect benötigt keine Client-Software.

Da der Remote-Arbeitsplatz nicht zum Bestandteil des entfernten Netzwerkes wird, ist es einfacher, dieses gegen Schadsoftware und ungewollte Zugriffe zu sichern.

WebConnect passt den RDP-Desktop immer an das Browserfenster an. Es entfallen die manuellen Einstellungen von Bildschirmgrößen, unabhängig davon, ob auf dem Tablet oder einem 4K-Monitor gearbeitet werden soll.

WebConnect benötigt keinen physischen Monitor am entfernten Arbeitsplatz. Es erzeugt automatisch bis zu 3 gleichzeitige virtuelle Monitore, die zum Arbeiten gleichzeitig in 3 Browser-Tabs angezeigt werden. Elemente lassen sich zwischen den Bildschirmen verschieben.

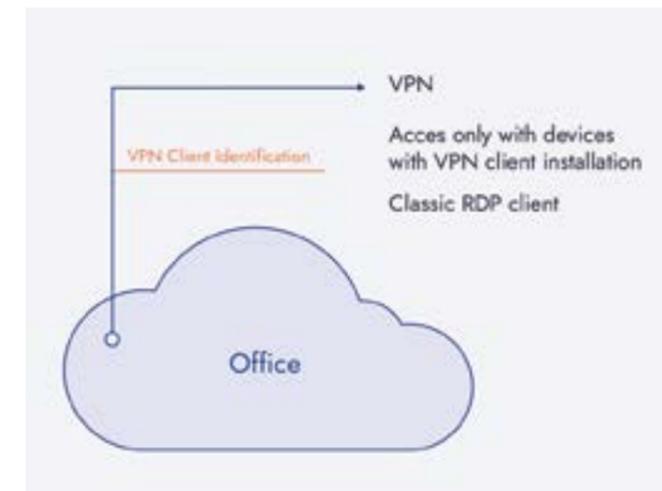
Mit WebConnect ist der Mitarbeiter komplett ortsunabhängig, da er über Browser und HTTPS überall dort arbeiten kann, wo das Internet zur Verfügung steht.

WebConnect ist einfach zu administrieren..

RDP mit VPN

VPN benötigt eine VPN-Installation auf dem Client und im Unternehmen, die für jede Verbindung einen Tunnel zwischen den Geräten aufbaut.

Mit VPN wird RDP über den klassischen RDP-Client aufgebaut.



Der Remote-Arbeitsplatz wird fester Bestandteil des Firmennetzwerkes mit allen Risiken, die sich auf dem Remote-Arbeitsplatz ergeben (Viren, Malware, etc.).

Der klassische RDP-Client passt bei Größen-Änderungen nicht automatisch dem Bildschirm des Remote-Arbeitsplatzes an.

Die Einrichtung eines VPN im Unternehmen und auf den Client Geräten ist aufwendig und erfordert ständige Kontrolle und Wartung.

VPN funktioniert nur dort, wo die entsprechenden ausgehenden Ports frei verfügbar sind. Das ist in vielen Hotels, auf Flughäfen, in Bahnhöfen, in Konferenzzentren und an vielen anderen Orten nicht der Fall oder muss extra angefragt und eingerichtet werden.

WebConnect World SL

WebConnect World SL mit Sitz in Madrid hat sich auf die Themen Datenschutz, Sicherheit und Kommunikation spezialisiert. Das Unternehmen entwickelt eigene Produkte und berät Kunden im Bereich Forschung & Entwicklung. Zentrales Produkt ist WebConnect für flexibles und sicheres Arbeiten von überall auf der Welt. Die Lösung bietet ein neuartiges Konzept für den sicheren Fernzugriff auf Desktops und die Einwahl in das Firmennetzwerk – als sichere und einfache Alternative zu VPN. Der Vertrieb von WebConnect erfolgt über Reseller und verschiedene Partner-Programme. Weitere Informationen erhalten Sie unter <https://webconnect.pro/de/>.

Externe Geräte mit Wake-on-LAN anschalten

Externe Geräte mit Wake-on-LAN anschalten

Die Herausforderung für Organisationen mit Remote-Arbeitsplätzen in der heutigen Zeit ist es möglichst energiesparsam zu wirtschaften und beispielsweise nicht genutzte Ressourcen abzuschalten.

Hierfür gibt es im IT-Netzwerk Lösungen wie Wake-on-LAN. Mit Wake-on-LAN ist es möglich ausgeschaltete Geräte innerhalb eines Netzwerkes anzuschalten. Dafür ist es notwendig, dass diese Geräte von einem anderen Gerät ein sogenanntes Magic Packet gesendet bekommen, das direkt an die Netzwerkkarte gesendet wird und bei entsprechender Konfiguration das Gerät startet.

Der Vorteil einer derartigen Konfiguration: Geräte verbrauchen nur dann Energie, wenn sie auch wirklich im Einsatz sind. Es gibt keinen Grund mehr, Geräte rund um die Uhr eingeschaltet zu lassen, um diese gelegentlich von außerhalb zu erreichen.

Wake-on-LAN mit WebConnect

WebConnect ist optimal vorbereitet für Wake-on-LAN, da es das Senden des Magic-Packets direkt in der Verbindung anbietet. Wenn WebConnect im Netzwerk installiert ist, ist es das einzige Gerät, das online erreichbar sein muss. Mit nur 8 Watt Verbrauch ist es dabei das effizienteste Gerät im Netzwerk.

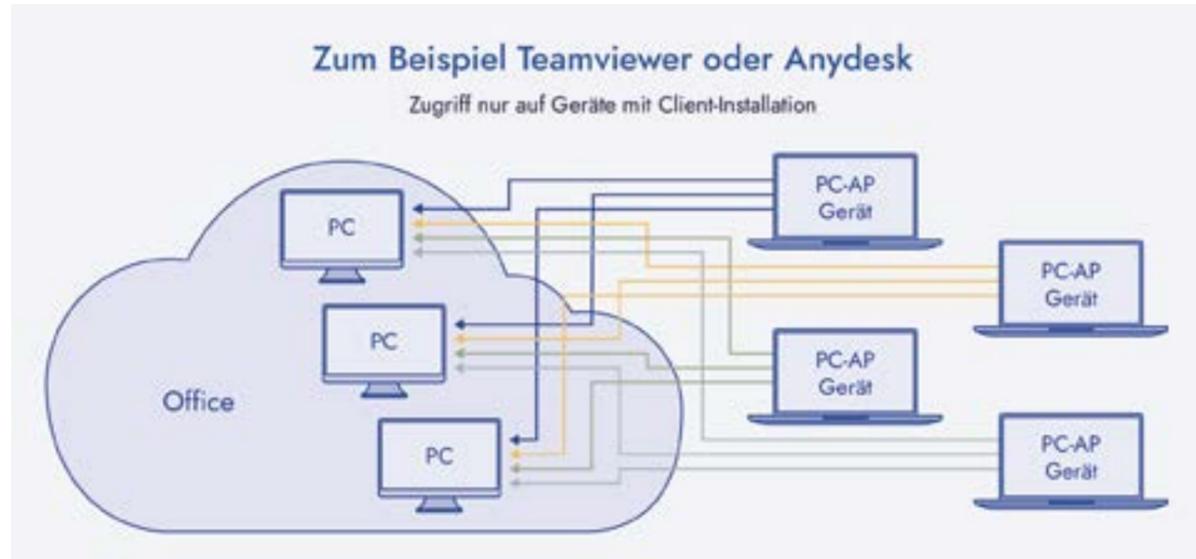


Alle Arbeitsplätze können im Stromsparmmodus oder ausgeschaltet sein. Der Benutzer verbindet sich bei WebConnect immer mit der lokalen Installation, die einen Arbeitsplatz direkt beim Start der Verbindung einschaltet. Hat der Benutzer seine Arbeit beendet, wird das Gerät einfach wieder ausgeschaltet.

Da WebConnect keinerlei Installationen auf dem sendenden oder empfangenden Gerät erfordert, gibt es hier auch keine Abhängigkeiten. Der Benutzer benötigt nur Nutzungsrechte zu den Geräten, die er verwenden darf.

Wake-on-LAN mit Teamviewer, Anydesk und anderen Lösungen

Bei Lösungen dieser Art gibt es keine zentrale Einheit innerhalb des IT-Netzwerkes der Organisation. Es ist jeweils eine Installation auf dem lokalen und dem entfernten Arbeitsplatz erforderlich. Da Magic Packets nur innerhalb des Netzwerkes abgesendet werden können, ist es erforderlich, dass mindestens ein Gerät mit einer Installation im Netzwerk aktiv und erreichbar ist.



Diese Anwendungen müssen dann das Signal an den gewünschten Arbeitsplatz senden. Das Ganze muss also so eingerichtet werden, dass die Installation zunächst ein aktives Gerät findet, diesem den Befehl gibt das Signal zu senden und dann die Verbindung zu dem gewünschten Gerät aufbaut.

Hier ist einiges an Konfigurationen und Rechtemanagement zu beachten.

Bleibt kein einziges Gerät eingeschaltet, ist das gesamte Netzwerk nicht zu erreichen.

WebConnect World SL

WebConnect World SL mit Sitz in Madrid hat sich auf die Themen Datenschutz, Sicherheit und Kommunikation spezialisiert. Das Unternehmen entwickelt eigene Produkte und berät Kunden im Bereich Forschung & Entwicklung. Zentrales Produkt ist WebConnect für flexibles und sicheres Arbeiten von überall auf der Welt. Die Lösung bietet ein neuartiges Konzept für den sicheren Fernzugriff auf Desk-tops und die Einwahl in das Firmennetzwerk – als sichere und einfache Alternative zu VPN. Der Vertrieb von WebConnect erfolgt über Reseller und verschiedene Partner-Programme. Weitere Informationen erhalten Sie unter <https://webconnect.pro/de/>.

WEBCONNECT

Remote-Zugänge sicher verwalten

Remote-Zugänge sicher verwalten

Schon im internen Netzwerk ist es notwendig die Rechte der Nutzer an Dienste und Geräte zu binden. Mit der Erweiterung der Organisation aus dem physischen Räumen in die Remote-Arbeitswelt, steigen die Herausforderungen an die Administration weiter an. Die Systeme und Daten einer Organisation sind ein hohes und sensibles Gut. Es ist notwendig diese bestmöglich vor fremden Zugriffen zu schützen.

Remote-Zugänge mit WebConnect verwalten

WebConnect läuft als zentrales Zugangssystem für alle Zugriffe von außen und innen, die die Remote Browser Sitzungen verwenden wollen. WebConnect bietet eine umfangreiche Benutzer- und Verbindungsverwaltung, in der jeder Benutzer mit seinen Rechten eingerichtet wird und in der jedem Benutzer genau die Verbindungen zugeordnet werden, die er verwenden darf.

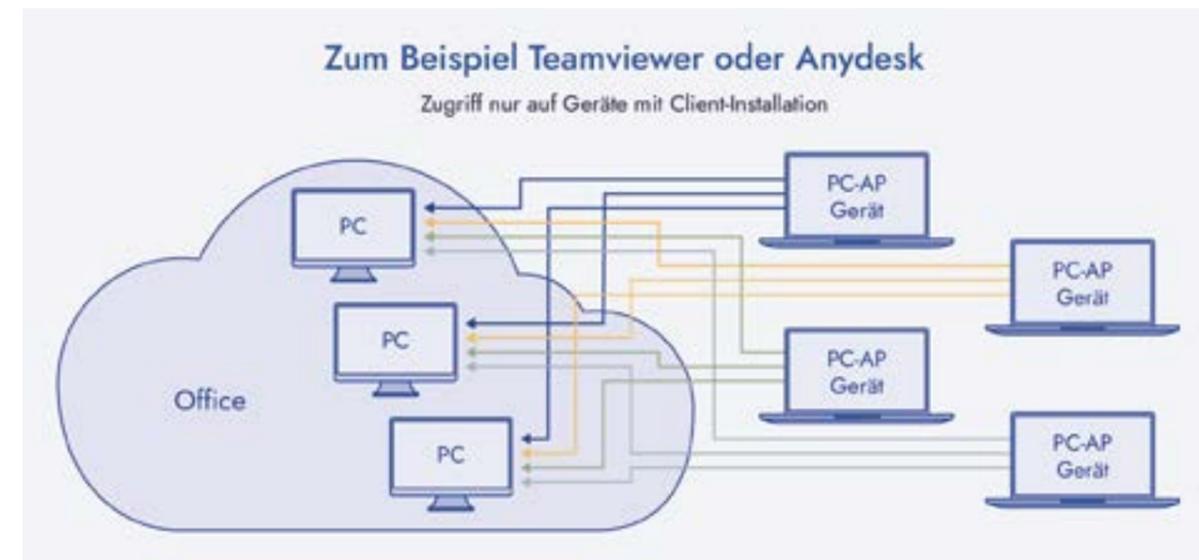


Jeder Benutzer muss sich zuerst an der WebConnect-Installation anmelden, bevor er überhaupt auf seine Geräte im Netz zugreifen kann. Ebenfalls muss er sich (je nach Konfiguration) auch an seinem Gerät anmelden. Es bestehen damit ausreichende Hürden, bevor ein Zugriff auf ein Gerät erfolgt. Wichtig: Alle diese Einstellungen stehen unter der ständigen Kontrolle der Administratoren, die jede Berechtigung zu jeder Zeit verändern oder entfernen können. Außerdem sehen die Administratoren wer gerade wo verbunden ist und war.

Kein Benutzer außerhalb des Netzwerks kann ohne Anmeldung bei WebConnect irgendein internes Gerät sehen. Diese sind hinter WebConnect versteckt und niemals öffentlich.

Remote-Zugänge mit Teamviewer, Anydesk und ähnlichen Lösungen

Bei Systemen wie Teamviewer ist das System anders aufgebaut. Jedes Gerät benötigt eine Software, die diesem eine Nummer und ein Kennwort zuteilt. Die Nummer bleibt immer gleich und ist im zentralen Server des Softwareanbieters mit der entsprechenden Zieladresse registriert. Wer diese Nummer kennt, kann das interne Zielgerät erreichen, ohne dass dafür irgendeine Anmeldung oder Legitimierung erfolgt. Erst auf dem Zielgerät erfolgt dann die Eingabe eines Kennwortes, das entweder in der lokalen Software fest eingestellt wird oder durch ein Zufallskennwort, das von einem Benutzer innerhalb der Organisation an den Remote Benutzer durchgegeben wird. Alternativ kann auch ein Benutzer im internen Netz direkt auf „Zugriff erlauben“ klicken.



Wird im internen Netz eine Software wie Teamviewer, Anydesk oder ähnliches installiert, verliert der Administrator die weitere Kontrolle über dieses Gerät und kann auch dessen Aktionen im Netzwerk nicht mehr nachvollziehen. Er übergibt diese in die Hoheit des jeweiligen Mitarbeiters, der jederzeit jeder Person Zugriff auf dieses Gerät und damit das Netz geben kann.

Da die Struktur der Nummern bekannt ist, können auch Externe versuchen, Geräte zu erreichen und das jeweilige Passwort zu übergehen. Damit öffnen sich Türen, die vorher mühsam mit Firewall & Co geschlossen wurden.

WebConnect World SL

WebConnect World SL mit Sitz in Madrid hat sich auf die Themen Datenschutz, Sicherheit und Kommunikation spezialisiert. Das Unternehmen entwickelt eigene Produkte und berät Kunden im Bereich Forschung & Entwicklung. Zentrales Produkt ist WebConnect für flexibles und sicheres Arbeiten von überall auf der Welt. Die Lösung bietet ein neuartiges Konzept für den sicheren Fernzugriff auf Desktops und die Einwahl in das Firmennetzwerk – als sichere und einfache Alternative zu VPN. Der Vertrieb von WebConnect erfolgt über Reseller und verschiedene Partner-Programme. Weitere Informationen erhalten Sie unter <https://webconnect.pro/de/>.

WebConnect und / oder andere IT-Lösungen

WebConnect und / oder andere IT-Lösungen

Eine Grundsatzentscheidung, vor der IT-Entscheider in IT-Projekten häufig stehen: Welches Projekt realisieren wir? Ersetzen wir System A mit System B? Wenn wir B einsetzen wollen, müssen wir uns aber von A trennen. Sollten wir nicht doch besser A beibehalten und auf B verzichten?

Bei dieser Entscheidungskreuzung hilft WebConnect. Da die Lösung IT-Welten verbindet, wird aus einem Oder ein Und. Damit können Firmen bestehende Investitionen erhalten und Ressourcen mit neuen Investitionen schonend ergänzen.

WebConnect und internes Netzwerk

Arbeitsplätze der Zukunft sind remote. Remote bedeutet aber nicht nur außerhalb der physischen Räumlichkeiten einer Organisation. Remote bedeutet einfach räumlich flexibel. Größere Einheiten haben heute einen Campus, kleinere haben schon immer eine Terrasse. Arbeit sollte dort stattfinden, wo sich Mitarbeiter wohlfühlen.

WebConnect funktioniert nicht nur von außerhalb über das Internet, sondern auch im internen Netzwerk. Und wenn es die IT-Politik der Organisation erfordert, lässt sich WebConnect sogar auf eine rein interne Nutzung beschränken.



WebConnect ist ein Add-On, das Arbeitsplätze mobil macht. Die übliche IT-Infrastruktur besteht in Firmen häufig aus Desktop-PCs, die an einen festen Arbeitsplatz gebunden sind. Die meisten dieser Desktop-PCs lassen sich aber auch so einstellen, dass Sie per RDP erreichbar sind. Hier zögern aber die meisten Firmen, weil der Aufbau von geregelten und gesicherten Zugriffsmöglichkeiten sehr aufwändig ist.

Hier schafft WebConnect Abhilfe. Die Installation im internen Netzwerk ist einfach und die Lösung ist vor allem einfach zu verwalten. Jeder berechnete Benutzer erhält einen Zugang mit Benutzername, Passwort und optional 2FA. Diesen Benutzern werden dann genau die Arbeitsplätze zugewiesen, auf die sie auch im normalen Betrieb zugreifen dürfen.

Ab diesem Zeitpunkt ist der Mitarbeiter maximal flexibel. Er kann sich per WebConnect einfach im Browser mit jedem Gerät an seinen Arbeitsplatz begeben. Das kann mit dem Tablet von der Terrasse oder dem Campus sein, mit dem Chromebook aus dem Besprechungsraum oder mit einem Laptop aktuellen Aufenthaltsort. Es ist sogar möglich, den eigenen Arbeitsplatz auf den Bildschirm eines an-deren Desktop-PCs zu holen.

WebConnect macht aus statischen Netzwerken flexible moderne Arbeitswelten ohne hohe Investitionen in den Umbau der vorhandenen und bewährten IT-Infrastruktur.

WebConnect und Cloud

Berater empfehlen häufig die Migration in die Cloud, um flexibel und remote zu arbeiten. Wenn aber alle Anwendungen in die Cloud verlagert werden, wandert die bestehende Hardware in den Elektroschrott. Cloud und internes Netz sind häufig Konkurrenten, die sich nicht vertragen.

Sehr viel kostengünstiger sind alternative Ansätze. WebConnect verwandelt das interne Netzwerk in eine private Cloud und schont Ressourcen. WebConnect in der Cloud erweitert diese um attraktive Funktionen, die Standard-Cloud-Installationen nicht anbieten. Beides lässt sich in der Arbeitswelt kombinieren.

WebConnect und Citrix

Normal würde man denken: WebConnect oder Citrix? WebConnect kann bestehende Citrix Systeme aber auch ergänzen und sinnvoll erweitern.

Mit WebConnect lassen sich innerhalb einer Citrix Infrastruktur weitere Geräte im System verwenden, die dann nicht dem Citrix-Lizenzmodul unterliegen. Damit ist es möglich, vor allem temporäre Arbeitsplätze kostengünstig zu integrieren.

WebConnect und Inhouse Softwarelösungen

Viele Organisationen haben hoch spezialisierte Unternehmenssoftware im Einsatz, die über viele Jahre entwickelt und maßgeschneidert wurden. Leider laufen die meisten dieser Softwarelösungen nur innerhalb eines geschlossenen Netzwerkes. Sie sind weder in der Cloud noch im Web nutzbar. Das stellt die IT-Verantwortlichen vor Herausforderungen, wenn sie Remote-Arbeitsplätze anzubieten wollen.

Mit WebConnect sind keine Änderungen an der bestehenden Lösung notwendig. Da WebConnect im internen IT-System installiert wird, verwandelt es das Haussystem in eine weltweit erreichbare private und geschützte Cloud.

WebConnect bildet dabei das Gateway zwischen dem World Wide Web und dem Haussystem und damit gleichzeitig die sichere Grenze zwischen drinnen und draußen.



Externe Benutzer sehen nur das WebConnect Gateway und verbinden sich mit einem Browser mit HTTPS und TLS 1.3 (Bankenstandard). Hier legitimieren sie sich mit Benutzername, Passwort und 2FA. Nur das WebConnect Gateway kennt die Geräte, die erreichbar sein sollen. Erst zwischen dem Gateway und dem internen Gerät wird die Remote-Verbindung aufgebaut, die dann im Browser über HTTPS angezeigt und bedient wird.

Da die externen Geräte bei WebConnect-Verbindungen nicht Bestandteil des internen Netzes werden, ist dieses besser vor Viren oder Malware geschützt. Ein weiterer Vorteil: Nutzer können ihre eigene bevorzugte Hardware verwenden und müssen nicht zwingend mit abgesicherter Hardware der Organisation ausgerüstet werden.

Mit WebConnect lässt sich jede bisher nur lokal verfügbare Desktop-Anwendung im Browser von jedem Ort der Welt bedienen, ohne dass die Software selber außerhalb der Organisation läuft. Die Anwendung läuft immer lokal, lediglich der Bildschirm wird im Browser mit HTTPS übertragen und bedient.

WebConnect World SL

WebConnect World SL mit Sitz in Madrid hat sich auf die Themen Datenschutz, Sicherheit und Kommunikation spezialisiert. Das Unternehmen entwickelt eigene Produkte und berät Kunden im Bereich Forschung & Entwicklung. Zentrales Produkt ist WebConnect für flexibles und sicheres Arbeiten von überall auf der Welt. Die Lösung bietet ein neuartiges Konzept für den sicheren Fernzugriff auf Desktops und die Einwahl in das Firmennetzwerk – als sichere und einfache Alternative zu VPN. Der Vertrieb von WebConnect erfolgt über Reseller und verschiedene Partner-Programme. Weitere Informationen erhalten Sie unter <https://webconnect.pro/de/>.

Lizenzen und Preise

Lizenzen und Preise

WebConnect wird als Plug& Play Version inklusive Hardware (Co-Router) und als Software-Image für die Installation auf Server-Hardware angeboten.

Installationspreis

Plug&Play

| | |
|--|----------------|
| Co-Router (MiniPC optimiert für bis zu 20 gleichzeitige Nutzer) | 150 Euro |
| Einkaufspreis für Reseller | 100 euros |
| Installationshilfe optional für Endkunden | 50 Euro |
| Server-Installation: (Hyper-V, Proxmox, Virtualbox, VMware, Synology Software-Download (Image mit Installationsdatei) | free of charge |

Das WebConnect Lizenzmodell beruht auf gleichzeitig aktiven Nutzern. Der Kunde kann die Anzahl der gewünschten maximal gleichzeitigen Verbindungen frei wählen und jederzeit anpassen.

Licence price

| | |
|---|---------|
| Je gleichzeitigem Nutzer (Verbindung) pro Monat | 10 Euro |
| Reseller erhalten auf den Lizenzpreis 50% Rabatt | |

Großabnehmer wie Datacenter oder Organisationen erhalten attraktive Staffel- und Pauschalpreise. Alle Preise zuzüglich ges. gültiger MwSt.

WebConnect World SL

WebConnect World SL mit Sitz in Madrid hat sich auf die Themen Datenschutz, Sicherheit und Kommunikation spezialisiert. Das Unternehmen entwickelt eigene Produkte und berät Kunden im Bereich Forschung & Entwicklung. Zentrales Produkt ist WebConnect für flexibles und sicheres Arbeiten von überall auf der Welt. Die Lösung bietet ein neuartiges Konzept für den sicheren Fernzugriff auf Desk-tops und die Einwahl in das Firmennetzwerk – als sichere und einfache Alternative zu VPN. Der Vertrieb von WebConnect erfolgt über Reseller und verschiedene Partner-Programme. Weitere Informationen erhalten Sie unter <https://webconnect.pro/de/>.

