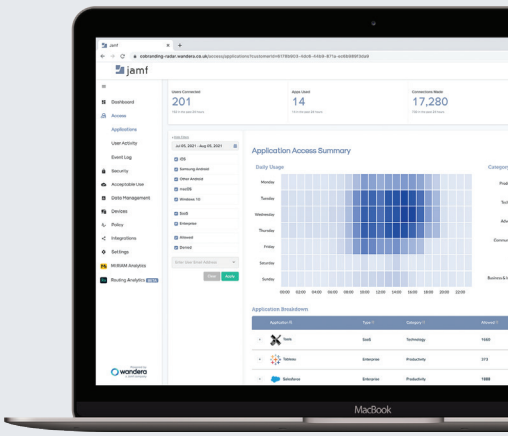
jamf

JAMF PRIVATE ACCESS

Ermöglichen Sie einen schnellen, einfachen und sicheren Zero-Trust-Netzwerkzugriff auf alle Unternehmensressourcen.



Stellen Sie Teams die Flexibilität bereit, jederzeit und von überall aus zu arbeiten, indem sie sichere Verbindungen mit den benötigten Anwendungen herstellen.

Private Access verwendet Identitäts- und App-zentrische Richtlinien, um Produktivität zu verbessern und um gleichzeitig einzuschränken wie einfach Benutzer auf Daten und Apps zugreifen können.

Starke Sicherheit

Private Access basiert auf einem Cloud-basierten softwaredefinierten Perimeter (SDP), der für sichere, isolierte Verbindungen mit jeder Anwendung sorgt. Mithilfe der Durchsetzung des Least-Privilege-Prinzips und Tests der Geräteaufstellung in Echtzeit wird der Zugriff auf jede Anwendung nur für bestimmte autorisierte Benutzer gewährt.

Verbesserte Verwaltbarkeit

Private Access verwendet eine völlig Cloud-basierte Architektur, ohne dass Vor-Ort-Server verwaltet werden müssen. Private Access ist effizient und vermeidet den Bedarf eines Tunnels für den gesamten Traffic, der unnötig teuer wäre. Gleichzeitig wird die Sichtbarkeit und Kontrolle auf die Elemente, auf die zugegriffen wird, zu verlieren (d. h. Richtlinie ohne Routing) nicht beeinträchtigt.

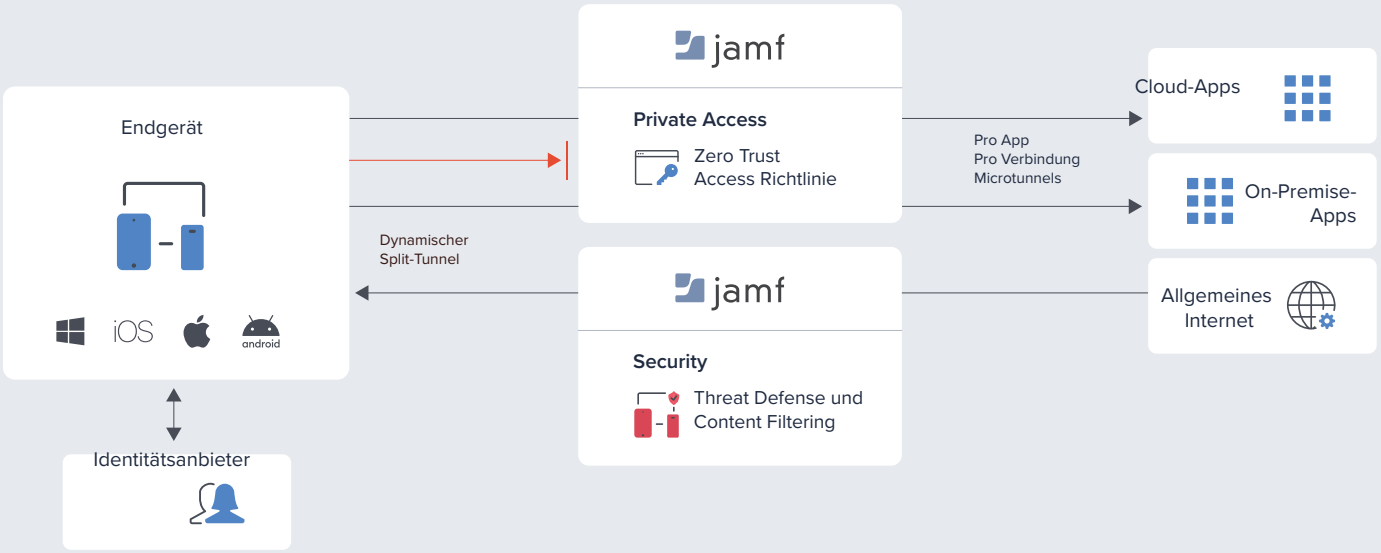
Intuitive Benutzererfahrung

Private Access verwendet ein Protokoll, das speziell für die schnelle und sichere Fernarbeit entwickelt wurde. In Verbindung mit der Skalierbarkeit unserer Cloud und der Fähigkeit, unnötige Traffic-Rücksendungen zu vermeiden, genießen Benutzer eine nahtlose Zugriffserfahrung ganz ohne Latenzprobleme. Dieser Dienst ist effizient und geht elegant mit Netzwerkübergängen um, sodass der Benutzer ohne Unterbrechungen zwischen dem Mobilnetz und WLAN wechseln kann.

jamf

Architektur

In der Cloud entwickelt, kann die Lösung skaliert werden, um Zugriff auf jede Anwendung zu bieten - egal ob diese in der Cloud gehostet oder sich in einem Servier vor Ort befindet.



Erforderlich

- Jede App (unterstützt On-Premise, Cloud, SaaS)
- Jedes Gerät (unterstützt alle modernen Betriebssysteme)
- Jeder Identitätsanbieter (mit Azure AD-Föderierung)

Nicht Erforderlich

- Es muss keine Hardware bereitgestellt werden
- Es müssen keine Gerätezertifikate verwaltet werden
- Es muss kein manuelles Traffic-Routing konfiguriert werden

Optional

- Endgeräteverwaltung zur Vereinfachung der Bereitstellung
- Zentralisierte Sicherheitsprotokollierung für verbesserte Sichtbarkeit und Reaktion
- Dedizierte Egress-IP-Adresse und Serverstandorte

Funktionen

Cloud-SDP

Private Access basiert auf einem Cloud-basierten softwaredefinierten Perimeter, der für sichere, isolierte Verbindungen mit jeder Anwendung sorgt. Mithilfe Least-Priviledge-Prinzips und Tests der Geräteaufstellung in Echtzeit wird der Zugriff auf jede Anwendung nur für bestimmte autorisierte Benutzer gewährt.

App Microtunnels

Private Access ist eine Lösung für den Zero-Trust-Netzwerkzugriff. Das Gerät und alle darauf ausgeführten Apps können jede Netzwerkinfrastruktur nutzen. Private Access verwendet Microtunnels auf Anwendungsebene, die über unsere Infrastruktur verlaufen und genaue Kontrolle - sowohl bei der Verbindungsherstellung als auch während der aktiven Sitzungen - ermöglichen.

Sitzungs-Reporting

Detailliertes Sitzungs-Reporting ermöglicht die Überwachung aktiver Benutzer und der von ihnen verwendeten Anwendung. Echtzeit-Statistiken bieten Einblicke in ungewöhnliche Aktivitäten, Sitzungsdauer oder Bandbreitenanforderungen. Umfassende Sichtbarkeit bietet Administratoren einen Audit-Trail, um auf unangemessene Inhalte zu prüfen, Malware zu erkennen und Datenlecks zu identifizieren.

Protokolle

Die meisten Endgeräte nutzen WLAN- oder Mobilfunkverbindungen, Benutzer und Anwendungen erfordern aber Leistungen, wie sie von einer Kabelverbindung erwartet werden. Mit Private Access ist die sichere Verbindungsherstellung schnell, vielseitig und einfach, indem ein nahtloser Service bereitgestellt wird, selbst wenn der Benutzer unterwegs arbeitet.

Identitätsbasierte Lösung

Private Access nutzt identitätsbasierte Richtlinien für die Zuweisung von Benutzer- und Anwendungsberechtigungen. Die Integration mit bestehenden Verzeichnisdiensten ermöglicht eine schnelle Bereitstellung und Verwaltung von Richtlinien. Die einzige Möglichkeit zur Herstellung eines Tunnels besteht darin, dass der Benutzer die entsprechenden Berechtigungen für die jeweilige Anwendung hat.

Dynamischer Split-Tunnel

Private Access verwendet ein intelligentes Tunneling-Protokoll, das nur den Traffic aus einer Anwendung auf dem Gerät des autorisierten Benutzers zur zugehörigen Anwendung auf der anderen Seite des Cloud-SDP leitet. Dadurch wird sichergestellt, dass die Microtunnel-Richtlinie der App korrekt durchgesetzt wird, während gleichzeitig eine optimale Benutzererfahrung bereitgestellt wird, weil kein Traffic unnötig über den gesicherten Anwendungstunnel geleitet wird.

Einzelpaket-Autorisierung

Verhindern Sie, dass Anwendungen von nicht authentifizierten Parteien entdeckt werden können. Einzelpaket-Autorisierung erfordert eine Identitätsüberprüfung von Benutzer und Gerät, bevor der Zugriff bereitgestellt werden kann. Das bedeutet, dass nur Verbindungsversuche von autorisierten Benutzern erkannt werden, wodurch Ihr Service allen anderen im Internet gegenüber „unsichtbar“ bleibt.

Adaptiver Zugriff

Private Access bietet Benutzer- und Geräterisikobewertungen in Echtzeit, die Routen beeinflussen und mithilfe von Drittanbieter-Integrationen als Signale genutzt werden können. Sollte sich der Risikostatus eines Geräts ändern, kann Private Access je nach Richtlinie in Echtzeit eine Sitzung beenden oder Routen verändern.

Jamf Private Access arbeitet nahtlos mit Ihren bestehenden IT-Tools und Geräten zusammen.

Integrationen mit Microsoft, Google, Cisco und anderen Anbietern helfen Ihnen, den Wert Ihrer bestehenden Technologie zu erweitern.

jamf

www.jamf.com

Um mehr darüber zu erfahren, wie Private Access Benutzer, Mobilgeräte und Organisationsdaten vor Cyberrisiken schützen kann, besuchen Sie bitte jamf.com/de.