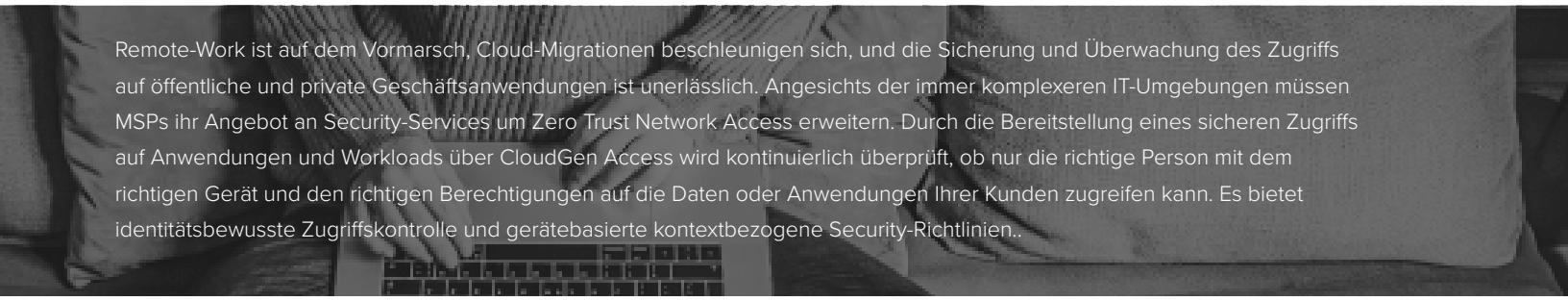
Barracuda CloudGen Access für MSP

Schützen Sie Ihre Kunden mit Zero Trust Network Access



Remote-Work ist auf dem Vormarsch, Cloud-Migrationen beschleunigen sich, und die Sicherung und Überwachung des Zugriffs auf öffentliche und private Geschäftsanwendungen ist unerlässlich. Angesichts der immer komplexeren IT-Umgebungen müssen MSPs ihr Angebot an Security-Services um Zero Trust Network Access erweitern. Durch die Bereitstellung eines sicheren Zugriffs auf Anwendungen und Workloads über CloudGen Access wird kontinuierlich überprüft, ob nur die richtige Person mit dem richtigen Gerät und den richtigen Berechtigungen auf die Daten oder Anwendungen Ihrer Kunden zugreifen kann. Es bietet identitätsbewusste Zugriffskontrolle und gerätebasierte kontextbezogene Security-Richtlinien..

Schnell einsatzbereit, leicht zu bedienen und einfach zu verwalten

Eine mehrmandantenfähige Lösung, die einfach einzurichten und zu verwalten ist. Bietet globale Zugriffskontrollrichtlinien für öffentliche, private und hybride Umgebungen, um einen sicheren Zugriff auf Apps, Web und Workloads zu gewährleisten.

Gewinnen Sie wertvolle Einblicke und volle Transparenz in die Ressourcenzugriffsströme Ihrer Kunden und mindern Sie so Sicherheits- und Compliance-Risiken. Erstellen Sie ein klares System der Aufzeichnung, das Berichte über den Systemzugriff im gesamten Unternehmen liefert. Verwalten, verfolgen und überprüfen Sie das “Wer”, “Was” und “Wann” von privilegierten Zugriffen mit einem einzigen Produkt.

Schneller, sicherer Remote Access auf Unternehmensressourcen

Zero Trust Network Access (ZTNA) ist die moderne Alternative zu VPN. Barracuda CloudGen Access ist eine mandantenfähige Lösung, die den Zugriff auf Unternehmensanwendungen für die Mitarbeiter, Auftragnehmer und Partner Ihrer Kunden mit unübertroffener Geschwindigkeit rationalisiert. Sorgen Sie im Vergleich zu VPN- oder MDM-Lösungen für überlegene Data Security und wahren Sie die Privatsphäre der Benutzer.

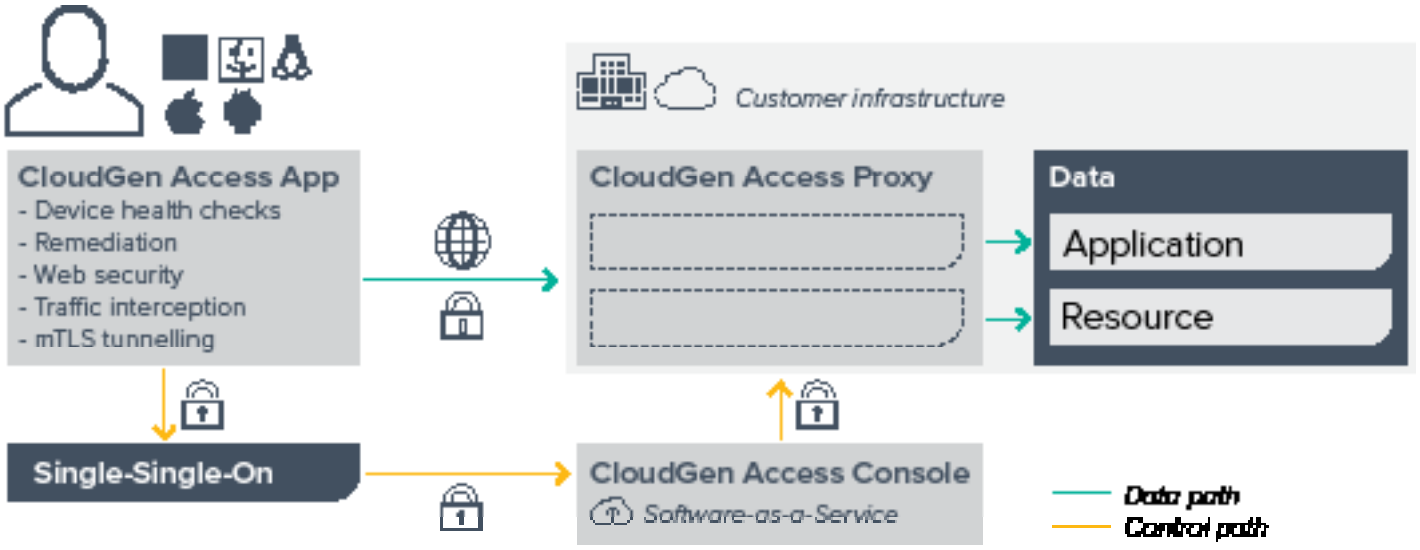
Erweitern Sie Ihr Security-Serviceangebot

Stärken Sie die Security-Position Ihrer Kunden und demonstrieren Sie Ihren Wert, indem Sie die sensiblen Daten Ihrer Kunden vor potenziell unsicheren oder gefährdeten Geräten schützen.

Geräten, indem Sie den Zugriff auf Kundenressourcen von diesen Endpunkten aus kontrollieren.

Solution Features

- Multi-Tenant
- Software-definiertes Perimeter (SDP)
- Mobil zuerst, BYOD zuerst
- Identitätsgesteuerter Zugriff und App-Segmentierung
- Wiederherstellungs-Engine (NAC)
- RBAC- und ABAC-basierte globale Richtlinien-Engine
- Leistungsstarke Konnektivität
- Skalierbarkeit über Cloud- und Hybrid-Infrastrukturen hinweg
- Optimierte Benutzerbereitstellung mit nur einem Klick
- Die Datenebene gehört dem Kunden
- Kompatibel mit allen Anwendungen, von Legacy bis SAML/https auf jeder Infrastruktur
- Keine Abhängigkeit von MDM
  - DNS Security
- - DNS-Filterung
- - DNS über TLS
- Eliminieren Sie Latenz durch lokale Inspektion
- Schützt vor Phishing und blockiert Bedrohungen auf Geräteebene
- Single-Sign-On Integrationen:
  - Azure AD
  - Okta
  - Ping-Identity
  - Google Suite
- - SAML



Technical Specs

CloudGen Access App

- Self-provisioning (onboarding)
- Konsistentes Look and feel
- Plattform übergreifend
- Integrierter DNS filter
- Integrierte Identität- und Geräte Gesundheitscheck
- Self-Service-Abhilfemaßnahmen
- Abfangen von Datenverkehr
- mTLS-Tunneling für Proxy Zugriff
- Sehr geringer Batterieverbrauch
- Geringer Speicherbedarf
- Verfügbar für:
  - Windows
  - macOS
  - Linux
  - iOS
  - Android

CloudGen Access Proxy

- Extrem einfache Einrichtung: automatisierte Bereitstellung mit nur einem Parameter
- Hört auf Anfragen, prüft Berechtigungen und vertritt entsprechend
- Erzwingt Authentifizierung und Autorisierung
- Verfügbar für:
  - Docker
  - Kubernetes
  - (schliesst AKS und GKE ein)
  - VMware
  - Amazon Web Services
  - Microsoft Azure
  - Bare metal

CloudGen Access Console

- Konfiguration von Proxies
- Konfiguration von Access Policies
- DNS Security und Track Access
- Security Events
- Supported policies:
  - Sperren von Jailbroken Geräten
  - Bildschirmsperre erforderlich
  - Firewall erforderlich
  - Erforderlich Antivirus
  - OS-Updates erforderlich machen
  - Re-Authentifizierung verlangen
  - Erfordert CloudGen Access-App aktualisiert
  - Verschlüsselung der Festplatte erforderlich