



Secure Defined Perimeter

Mobiles Arbeiten und New Work - Sicherer Zugriff auf alle Unternehmensressourcen

PRODUCT BULLETIN



Die Funktionsweise und vor allem die Nutzung von Belden macmon Secure Defined Perimeter (SDP) ist intuitiv und einfach. Der macmon SDP-Agent übernimmt transparent eine hochsichere Authentifizierung gegenüber dem macmon SDP-Controller, um die Identität des Benutzers sowie des Gerätes und dessen Sicherheitszustand zu prüfen.

Der SDP-Controller befindet sich in einer ISO 27001 zertifizierten deutschen Cloud und liefert über die verschlüsselte Verbindung nach erfolgreicher Authentifizierung die definierte Policy zurück an den Agenten, damit der Remote-Nutzer auf genau seine Ressourcen im Unternehmen zurückgreifen kann.

Vorteile von macmon SDP

- Hosted in Deutschland, mit deutschem Support und DSGVO-konform
- Zeitsparen durch Single Sign-on
- Unterstützung aller Netzwerke
- ISO 27001 zertifiziertes Rechenzentrum
- 2-Faktor- oder Mehr-Faktor-Authentifizierung
- Keine initiale Investition in Hardware notwendig
- Minimaler Pflegeaufwand und geringe Kosten durch SaaS (Software as a Service)
- Inklusive Cloud Identity Provider / Identity Access Management (IAM)
- Verhinderung von Account-Hijacking
- Hoch skalierbar für jede Anzahl an Nutzern

Eine Lösung auf Zugriffe aller Art von Unternehmensressourcen



Next Generation VPN

Lokale Ressourcen im Firmennetzwerk können über eine direkte Verbindung durch ein lokales SDP Gateway erreicht werden.



Private Cloud Protection

Über das macmon SDP Cloud Gateway können Ressourcen in privaten Rechenzentren erreicht werden.



Public Cloud Protection

Zugriff auf Ressourcen in der Public Cloud mit dem macmon SDP Controller und mit Single Sign-on.

Mobiles Arbeiten & New Work - Sicherheit für Netzwerke und Clouds

Die Berufswelt ändert sich. Digitales Arbeiten ermöglicht Mitarbeitern heute verstärkt, mobil von überall und mit verschiedenen Endgeräten fürs Unternehmen tätig zu sein. Natürlich benötigen die „New Worker“ dabei sicheren Zugriff auf alle Unternehmensressourcen. Auch eine reibungslose Kommunikation mit dem Team muss gewährleistet sein, um optimal und ohne Einschränkung die eigenen Projekte abwickeln zu können. Dies stellt die IT-Abteilung vor große Herausforderungen: Zum einen muss sie einwandfrei Prozesse abbilden können, sodass Arbeitsabläufe digital funktionieren und gleichzeitig die Performance des Unternehmensnetzwerks hochperformant bleibt. Zum anderen müssen Daten jederzeit sicher und geschützt sein und das unter Einhaltung von Securityrichtlinien auch außerhalb des Unternehmensnetzwerks, in der Cloud. Keine leichte Aufgabe.

Zero Trust Network Access mit Belden

Zero Trust Network Access (ZTNA) ist die Antwort auf die Herausforderung der IT-Abteilung. ZTNA fußt auf der Philosophie, weder einem Gerät, noch einem Benutzer einen Vertrauensvorschuss zu geben, bevor es sich nicht sicher authentifiziert hat. Dadurch minimiert der moderne ZTNA-Ansatz signifikant die Angriffsvektoren.



Komfortable und einfache Bedienung

- **Maximale Sicherheit durch granulare Zugriffssteuerung.** Je Unternehmensressource kann unterschieden werden, ob die Verfügbarkeit nur bei voller Konformität der Identitätsmerkmale und Sicherheitskonfiguration gewährt wird oder auch bereits bei eingeschränkter. So können z.B. sensible Bereiche nur für einen eingeschränkten Kreis an Benutzern mit definierten Endgeräten erreichbar sein.
- **Einfaches Onboarding neuer Mitarbeiter.** Neue Mitarbeiter können dank dem Belden macmon SDP-Agenten auf ihren Endgeräten direkt auf alle Ressourcen, die Ihnen von der IT-Abteilung zur Verfügung gestellt werden, zugreifen. Alle Apps und Zugänge stehen auf einen Blick den Mitarbeitern zur Verfügung. Besonders ein Mehrwert für neue Mitarbeiter, da hier die schwierige Suche nach Zugriffen und Zugängen entfällt.
- **Zeit sparen durch Single Sign-on.** Belden macmon SDP bietet Federation Services per SAML und OpenID inklusive und agiert damit auch als Identity-Access-Management-Lösung. Da die Kommunikation ausschließlich über den Client-Browser erfolgt ist keine Verbindung zwischen dem Cloud-Service und Ihren internen Systemen notwendig, so dass Single Sign-on nicht nur für Cloud-Applikationen verfügbar ist, sondern bedenkenlos auch für Ihre internen Ressourcen.

Entscheider in den Bereichen IT & Security berichten von folgenden Vorteilen während und nach der Einführung von SDP:

- Bewältigt die Herausforderungen der aktuellen „New Work“-Bewegungen
- Erlaubt die bisher zögerliche Nutzung von Cloud-Ressourcen kontrolliert zu erweitern
- Die granulare Segmentierung der Zugriffe erhöht den Schutz der Ressourcen
- Minimaler Pflegeaufwand und Entlastung der IT-Abteilung
- Einsparung von Kosten und Ressourcen, da administrative Prozesse entfallen und mehrere Sicherheitslösungen durch ein einziges Tool zur Verfügung gestellt werden