BELDEN

ZERO TRUST NETWORK ACCESS

Einfach gelebt in einer mobilen Welt

macmon sdp

Secure Defined Perimeter

belden.com

ZERO TRUST NETWORK ACCESS MIT BELDEN MACMON SECURE

Zero Trust Network Access (ZTNA) gewinnt sowohl in der IT als auch in der OT immer mehr an Bedeutung. ZTNA fußt auf der Philosophie, weder einem Gerät noch einem Benutzer einen Vertrauensvorschuss zu geben, bevor es sich nicht sicher authentifiziert hat. Der Wandel der Arbeitswelt, der sich durch mobiles Arbeiten sowie in der fortschreitenden Digitalisierung, dem Internet of Things sowie dem Auslagern verschiedener Dienste in die Cloud immer weiter verfestigt, sind Gründe dafür, dass ZTNA auch in Zukunft ein wichtiger Bestandteil integrativer IT und OT-Security- Lösungen sein muss.

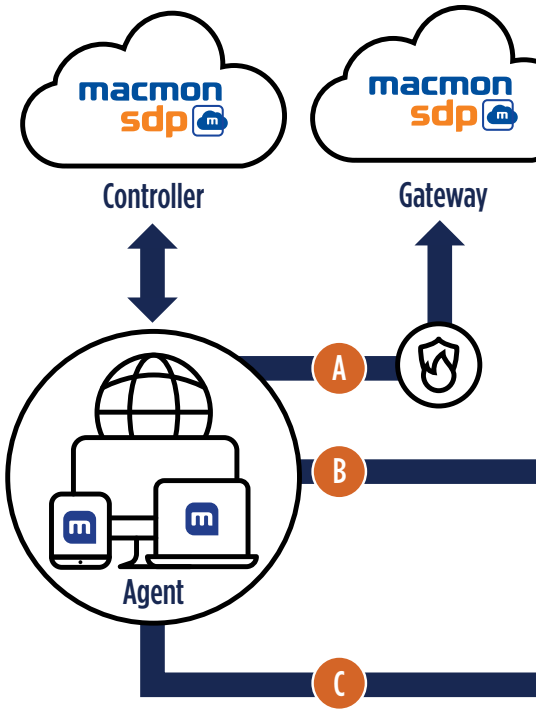
Belden macmon SDP – so funktionierts

Die Funktionsweise und vor allem die Nutzung von macmon SDP ist denkbar einfach. Der macmon SDPAgent übernimmt transparent eine hochsichere Authentifizierung gegenüber dem macmon SDP Controller, um die Identität des Benutzers sowie des Gerätes und dessen Sicherheitszustand zu prüfen.

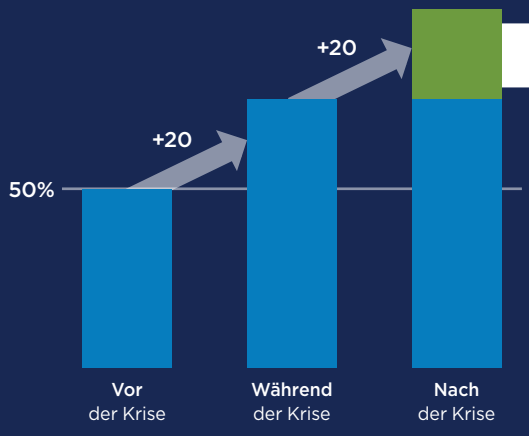
Der SDP-Controller befindet sich in einer ISO 27001 zertifizierten deutschen Cloud in Berlin und liefert über die verschlüsselte Verbindung nach erfolgreicher Authentifizierung die definierte Policy zurück an den Agenten. Die Policy enthält alle Information über die Erreichbarkeit der Unternehmensressourcen. Das System übernimmt außerdem die intelligente Steuerung der Kommunikationswege, um Bandbreitenengpässe zu vermeiden und möglichst geringe Latenzen zu gewährleisten.

macmon SDP – Sicherheit in der Cloud

Nach erfolgreicher Authentifizierung erreicht der Nutzer alle erforderlichen Ressourcen. Entweder direkt per Single Sign-on bei Cloud-Applikationen oder über das macmon SDP Cloud Gateway Ressourcen in Cloud-Rechenzentren. Darüber hinaus können auch lokale Ressourcen im Firmennetzwerk über eine direkte Verbindung durch ein lokales SDP Gateway erreicht werden. Zur Absicherung der Kommunikation bestehen jeweils verschlüsselte Tunnel, die je nach Konfiguration nur gezielt Ressourcen erreichbar machen. So werden zudem sämtliche Cloud Strategien, wie auch „Hybrid Cloud“ unterstützt und Unternehmen können ihre Roadmaps zum Migrieren von Services bedenkenlos verfolgen.



Sichere und direkte Kommunikation mit

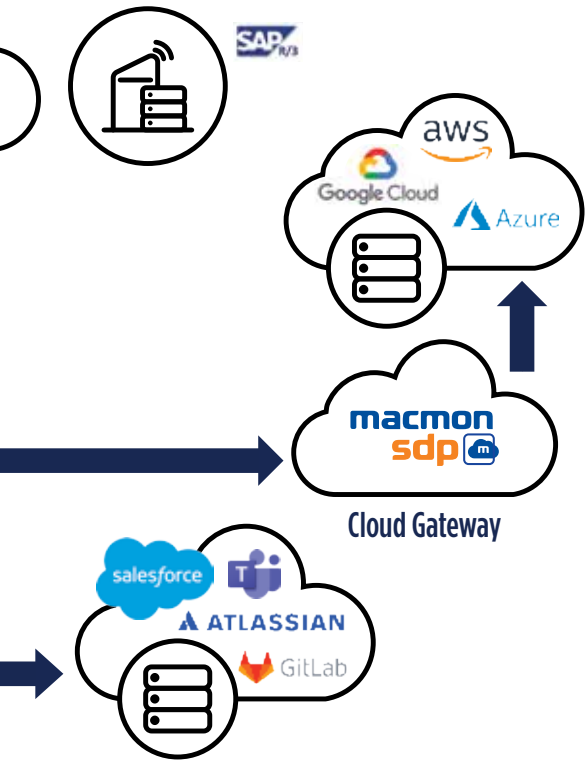


DER TREND ZUM HOMEOFFICE

beschleunigt durch die Corona-Krise

Laut der **Randstad-ifo-Personalleiterbefragung** aus dem zweiten Quartal 2020, könnten 80 % der Belegschaften von Zuhause aus arbeiten.

Quelle: Corona-Krise: Anteil der Belegschaft, der im Homeoffice arbeitete, aktuell arbeitet oder theoretisch arbeiten könnte in Deutschland im 2. Quartal 2020, Statista Research Department, 03.08.2020.



A **traditionellen lokalen Ressourcen im Firmennetzwerk**

B **Ressourcen in der Private Cloud**

C **Ressourcen in der Public Cloud**

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, während weniger sensible Ressourcen validen Benutzern auch mit fremden Geräten zur Verfügung stehen.

macmon secure trägt mit seiner bewährten Network-Access-Lösung schon seit 2003 dem ZTNA-Ansatz Rechnung, indem macmon NAC nur definierten Geräten Zugang zum Netzwerk erlaubt. Mit macmon SDP kann macmon den Schutz nun auch auf sämtliche Cloud-Dienste ausdehnen.

TIPP: Sie planen schon länger die Einführung eines Federation Services für Single Sign-on im eigenen Netzwerk?

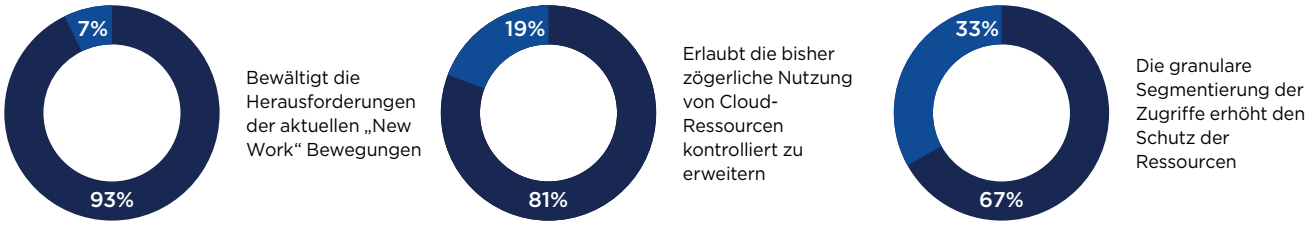
macmon SDP bietet Federation Services per SAML und OpenID inklusive und agiert damit auch als Identity-Access-Management-Lösung. Da die Kommunikation ausschließlich über den Client-Browser erfolgt ist keine Verbindung zwischen dem Cloud-Service und Ihren internen Systemen notwendig, so dass Single Sign-on nicht nur für Cloud-Applikationen verfügbar ist, sondern bedenkenlos auch für Ihre internen Ressourcen!

Mehrwerte von macmon SDP im Vergleich mit VPN

- Exakte Netzwerk-Segmentierung
- Individuelle Festlegung von Richtlinien auf Benutzer- und Geräteebene
- Dank SaaS – minimaler Pflegeaufwand und geringe Betriebskosten
- IInklusive Cloud Identity Provider / Identity Access Management (IAM)
- „Split-Tunneling“ out of the Box
- Verhinderung von „Account hijacking“
- Nahtlose Integration von Cloud Ressourcen und Reduzierung des Traffics
- Umfassende Übersicht zur Nutzung der einzelnen Ressourcen
- Hoch skalierbar für jede Anzahl an Nutzern

Vorteile von ZERO TRUST

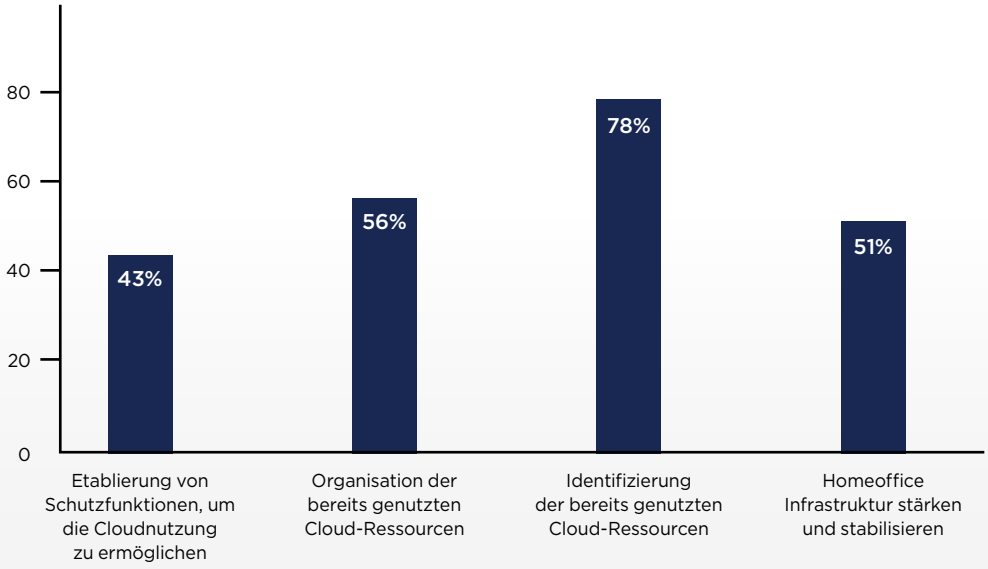
Entscheider in den Bereichen IT & Security berichten von folgenden Vorteilen während und nach der Einführung von SDP:



Vorteile von macmon SDP

- Globale Verfügbarkeit
- Hosted in Deutschland
- DSGVO Konform
- Exzellenter Support
- Unterstützung aller Netzwerke
- ISO 27001 zertifiziertes Rechenzentrum
- Software as a Service (SaaS) Lösung
- Unterstützung von „Zero Trust“ mit NAC seit über 15 Jahren

Die größten Cloud-IT-Herausforderungen für Unternehmen



macmon sdp

Secure Defined Perimeter

DEUTSCHLAND

Sitz der Gesellschaft

macmon secure GmbH

Alte Jakobstr. 79-80 | 10179 Berlin Deutschland
Tel.: +49 30 2325 777-0
nac@macmon.eu
www.macmon.eu