BELDEN

ZERO TRUST NETWORK ACCESS

Smartly Simple in Today's Mobile World

macmon sdp

Secure Defined Perimeter

belden.com

ZERO TRUST NETWORK ACCESS WITH BELDEN

Zero Trust Network Access (ZTNA) is becoming more and more important in IT as well as in OT. ZTNA is based on the philosophy of not trusting a device or a user until it is definitively authenticated. As our working environment is increasingly reshaped by mobile working, digitalization, the Internet of Things and the outsourcing of various services to the cloud, ZTNA must continue to be a key component of integrative security in IT and OT solutions in the future.

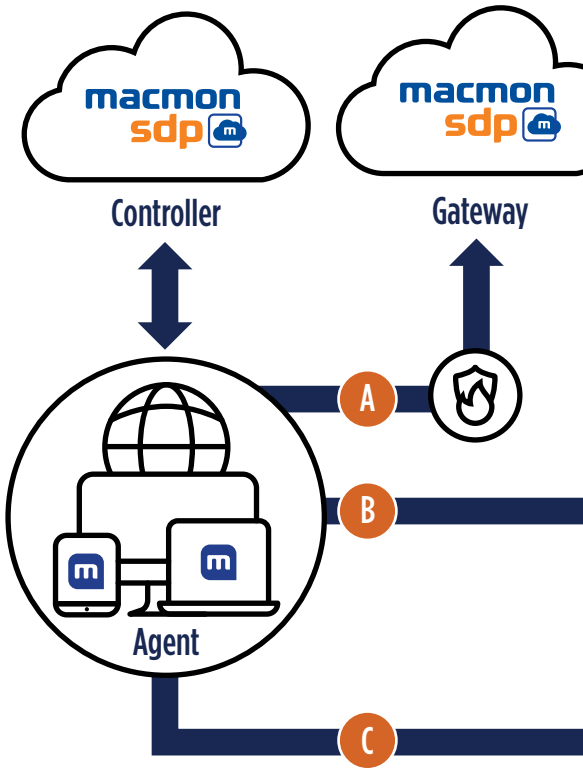
Belden macmon SDP and How it Works

macmon SDP has a very simple operating principle that makes it incredibly easy to use. With full transparency, the macmon SDP agent provides a highly secure authentication to the macmon SDP controller in order to check the identity of the user as well as the device and its security status.

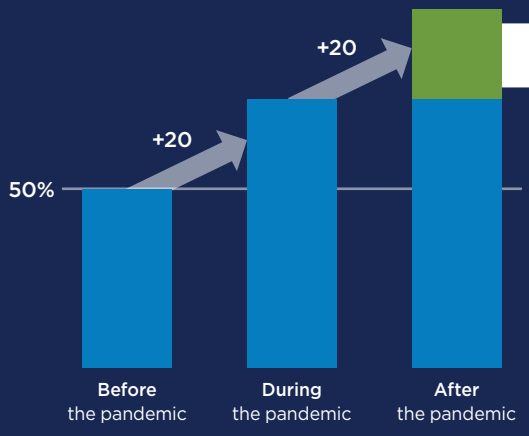
The SDP cloud controller is hosted in an ISO 27001–certified location in Berlin. Following successful authentication, the controller delivers the defined policy back to the agent via the encrypted connection. The policy contains all information about the accessibility of company resources. The system is also responsible for the intelligent control of the communication channels in order to avoid bandwidth constraints and to reduce latency as much as possible.

macmon SDP – Security in the Cloud

After successful authentication, the user has access to all the necessary resources. The user can either access the resources directly via Single Sign-on in the case of cloud applications, or via the macmon SDP cloud gateway resources in cloud data centers. Local resources in the company network can also be accessed directly via a local SDP gateway. To provide secure communication, there are encrypted tunnels which, depending on the configuration, make only specific resources accessible. All cloud strategies are supported, including hybrid cloud, leaving companies free to pursue their roadmaps for migrating services.



Secure and Direct Communication with

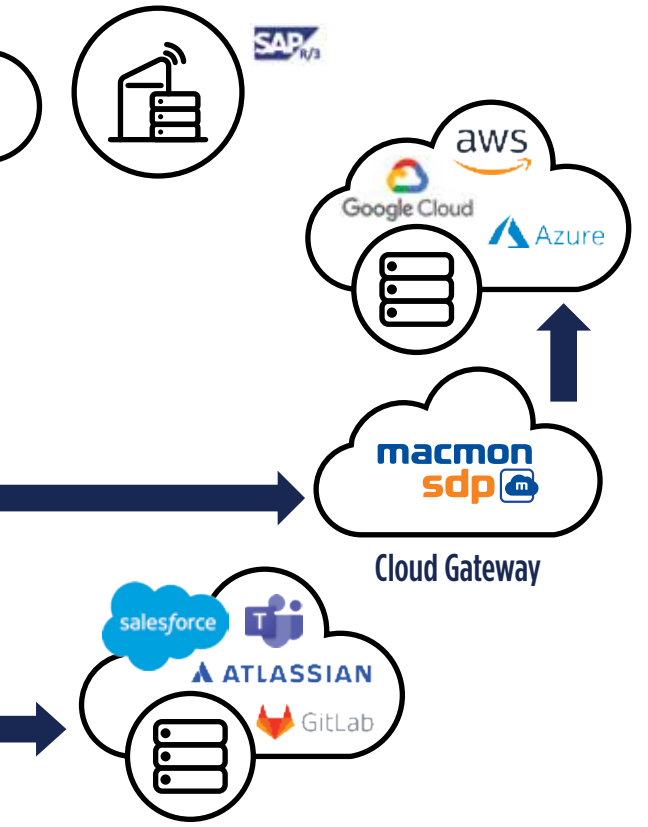


The Remote Work Trend

accelerated by the COVID-19 pandemic

According to a survey of HR managers carried out by the **Ifo Institute on behalf of Randstad Germany**, 80% of the workforce was able to work from home from the second quarter of 2020.

Source: coronavirus pandemic: Proportion of the workforce who already worked from home, currently work from home or could theoretically work from home in Germany in the 2nd quarter of 2020, Statista Research Department, August 3rd, 2020.



A **Traditional local resources in the company network**

B **Resources in the private cloud**

C **Resources in the public cloud**

Maximum Security Thanks to Granular Access Control

It is possible to specify access requirements for each company resource and define whether identifying features and security configurations must be met in full or in part. For example, sensitive resources can only be accessed by a limited group of users with defined endpoints, while less sensitive resources are also available to authenticated users with third-party devices.

macmon secure adopted the ZTNA approach in 2003 with its successful Network Access Control solution designed only to allow designated users to access the network. Thanks to macmon SDP, macmon is now able to extend the same level of protection to all cloud services.

TIP: Have you planned for quite a while to introduce a federation service that enables Single Sign-on in your network?

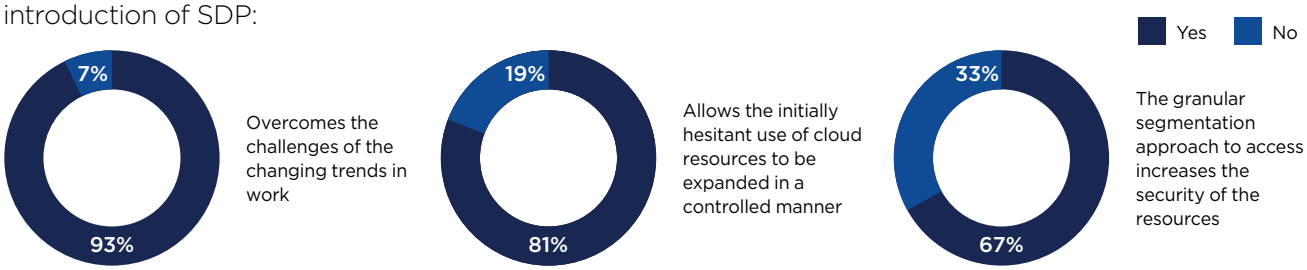
macmon SDP offers federation services via both SAML and OpenID and thus also functions as an identity access management solution. Since all communication takes place via the client browser, no connection between the cloud service and your internal systems is necessary. This means Single Sign-on is not only available for cloud applications, but also for your internal resources!

Advantage of macmon SDP over VPN

- Exact network segmentation
- Individual policies can be defined at user level and device level
- Minimal maintenance and low operating costs thanks to SaaS
- Includes Cloud Identity Provider / Identity Access Management (IAM)
- “Split tunneling” out of the box
- Prevention of “account hijacking”
- Seamless integration of cloud resources and reduced traffic
- Comprehensive overview of the use of the individual resources
- Highly scalable for any number of users

Advantages of ZERO TRUST

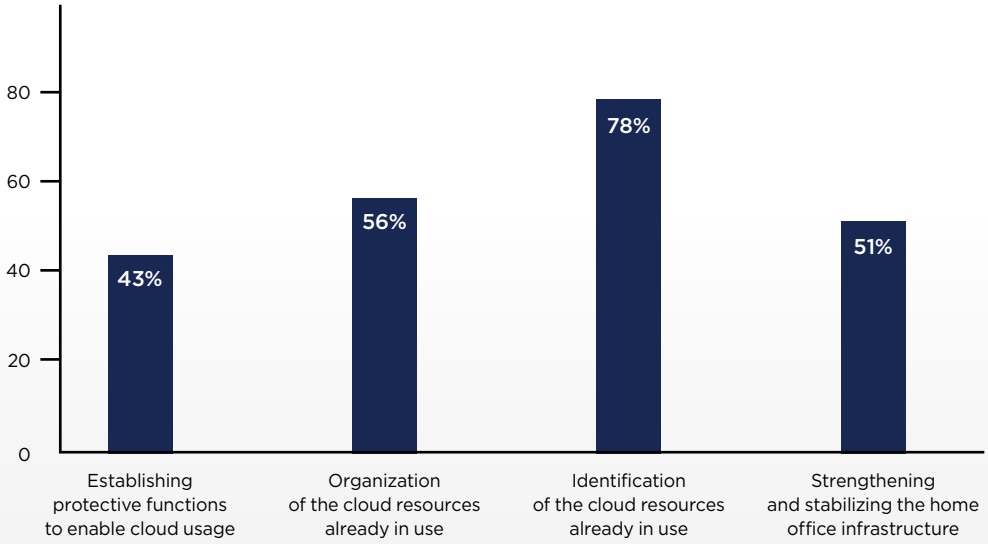
Decision-makers in the fields of IT & security report the following advantages during and after the introduction of SDP:



Advantages of macmon SDP

- Global availability
- Hosted in Germany
- GDPR-compliant
- Outstanding support
- Support of all networks
- Data center certified to ISO 27001
- Software as a Service (SaaS) solution
- Supporting Zero Trust with NAC for over 15 years

The biggest cloud computing challenges for companies



macmon sdp

Secure Defined Perimeter

GERMANY

Headquarters

macmon secure GmbH

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