BELDEN

Secure Defined Perimeter

Mobile Work and New Work - Secure Access to All Company Resources

PRODUCT BULLETIN

macmon sdp

Belden's macmon Secure Defined Perimeter (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 controller is hosted in an ISO 27001-certified German cloud. 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 so that the remote user can access exactly his resources.

macmon SDP Benefits

- Hosted in Germany, GDPR-compliant, outstanding support
- Save time through Single Sign-on
- Support of all networks
- Data center certified to ISO 27001
- 2-factor or multi-factor authentication
- No initial investment in hardware necessary
- Minimal maintenance effort and reduced costs through SaaS (Software as a Service)
- Includes Cloud Identity Provider / Identity Access Management (IAM)
- Prevents account hijacking
- Highly scalable for any number of users

One Solution for Access to All Company Resources

Next Generation VPN

Local resources in the company network can be accessed directly via a local SDP gateway.

Private Cloud Protection

Resources in private data centers can be accessed via the macmon SDP Cloud Gateway.

Public Cloud Protection

Resources in the public cloud can be accessed with macmon SDP Controller and Single Sign-On.

Mobile Work & New Work – Security for Networks and Clouds

The world of work is changing. Digital work is enabling more and more employees to work from anywhere and with different endpoints, a phenomenon known as “New Work.” To do this, employees need secure access to company resources. They also need to be able to communicate seamlessly with their team, so that they can complete their projects successfully and without restrictions. This poses major challenges for the IT department: On the one hand, the processes need to be smooth in order for the workflows to function digitally and the performance of the company network to remain stable. On the other hand, data must be secure and protected at all times in compliance with security policies, even outside the corporate network, i.e. in the cloud. Not an easy task!

Zero Trust Network Access with Belden

Zero Trust Network Access (ZTNA) is the answer to the IT department’s challenges. ZTNA is based on the philosophy of not trusting a device or a user until it is definitively authenticated. As a result the modern ZTNA approach significantly minimizes attack vectors.

Convenient and Easy to Use

- **Granular access control for maximum security.** For each company resource, you can define whether identifying features and security configurations must be met in full or only in part. For example, sensitive areas can be made accessible only to a restricted group of users with defined endpoints.
- **Easy onboarding of new employees.** With the macmon SDP agent, new employees can access all resources provided by the IT department directly from their endpoints. Employees have access to all their apps and accounts at a glance. This is especially beneficial for new employees, since they do not have to go searching for the right accounts and access points.
- **Save time through Single Sign-on.** Belden 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.

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

- The challenges associated with New Work trend will be handled
- The rather hesitant use of cloud resources can be expanded in a controlled manner
- The granular segmentation of access increases the security of the resources
- Minimal maintenance and less work for the IT department
- Costs and resources are minimized by eliminating administrative processes and providing a single tool for multiple security solutions