

## DTS Connectivity

# Connectivity

*Nothing describes the complex requirements of a modern network infrastructure better than “edge-to-cloud”. End-to-end networking of all data points, machines, IT systems and users is crucial for providing information without disruptions and for processing it quickly. There is also cyber security to consider, which on the one hand is important, but on the other hand increases complexity and in turn brings new challenges. How do you reconcile performance and security? How do you ensure the necessary, secure connectivity of all relevant systems, whether at the edge, in your own data center or in the cloud?*

- Secure, mobile, high-performance, stable networking
- Decades of experience as an ISP & CSP
- Over 20 years' experience as an ISP & data center operator
- Consulting & experience in multi-cloud environments
- 2 data centers of our own
- Leading solutions, long-term partners, customized scenarios
- Leading cyber security

With decades of experience as an Internet Service Provider (ISP) and Cloud Service Provider (CSP), we know exactly what is required of state-of-the-art network infrastructures. We specialize in meeting those requirements around the clock. In doing so, we draw on the leading solutions of our long-term partners to design, implement and operate customer-specific scenarios.

At the edge at one end, we ensure secure, mobile networking of employees, endpoints and machines. In particular, the requirements of high-performance and stable networking are immensely important here, as this is the only way to ensure the company's productivity through smooth communication.

In addition, our focus as an ISP is on transferring the information generated at various points as quickly as possible and sending the data to the central IT systems for further processing. This is only possible with individual WAN networks, with a focus on availability and performance.

At the other end, our solutions ensure secure, high-performance processing and storage of data in central IT systems, whether in the private or public cloud. The data must also be protected from unwanted changes and unauthorized access, which is why we make use of web application firewalls (WAF), SSL encryption, DDoS protection and other security technologies in this context.