DTS SSE

A globalized business world requires secure access to applications and data – both in the cloud and in local environments. At the same time, hybrid working models require flexible and scalable security solutions. Traditional, inflexible security architectures and isolated island solutions are no match for the dynamic threat landscape.

THREAT DEFENSE & ACCESS CONTROL

With the modern DTS Security Service Edge (SSE) platform, we provide you with consistent security measures for all your internet and SaaS traffic as a German "all-in-one" enabler, regardless of where users are located or how they access the internet. All data traffic is centrally checked, filtered, and protected by policies.

Key elements of the security architecture include a secure web gateway, internet firewall and URL filtering, intrusion prevention and threat prevention, as well as DNS protection. More extensive service upgrades also include advanced threat prevention via remote browser isolation and sandboxing, as well as cloud access security brokers and data loss prevention. In addition, mechanisms for IoT & OT security, AI security for users and applications, as well as identity security are possible.

Furthermore, all locations are directly connected to the cloud, so that all Internet traffic is centrally checked and protected by the security platform. This eliminates the need to provide individual security solutions or additional cloud services, which reduces costs and complexity.

DTS REMOTE USER ACCESS - ZTNA

For ideal connection to corporate networks without a physical connection, networking is established via client for managed devices and browser extension for unmanaged devices. The zero trust architecture supports all users everywhere and checks all data traffic. Session-based access policies are continuously enforced. Every connection is subject to advanced threat prevention and data protection measures.

PROOF OF CONCEPT

We offer an initial proof of concept. The process begins with a briefing and a rudimentary technical implementation. This is followed by a test phase to map real-world usage scenarios and obtain a meaningful picture of the functionality. Upon completion, a joint evaluation takes place – as a sound basis for further decisions.

AT A GLANCE
- Secure, global access control in accordance with zero trust for applications and data – regardless of location, user, or device
- Comprehensive security in one platform, with holistic protection mechanisms for modern cyber threats
- Centralized management and reduced operational workload, including through consistent policies
- Optimized remote and hybrid work access with demand-oriented service added value, e.g., DTS Remote User Access – ZTNA & proof of concept