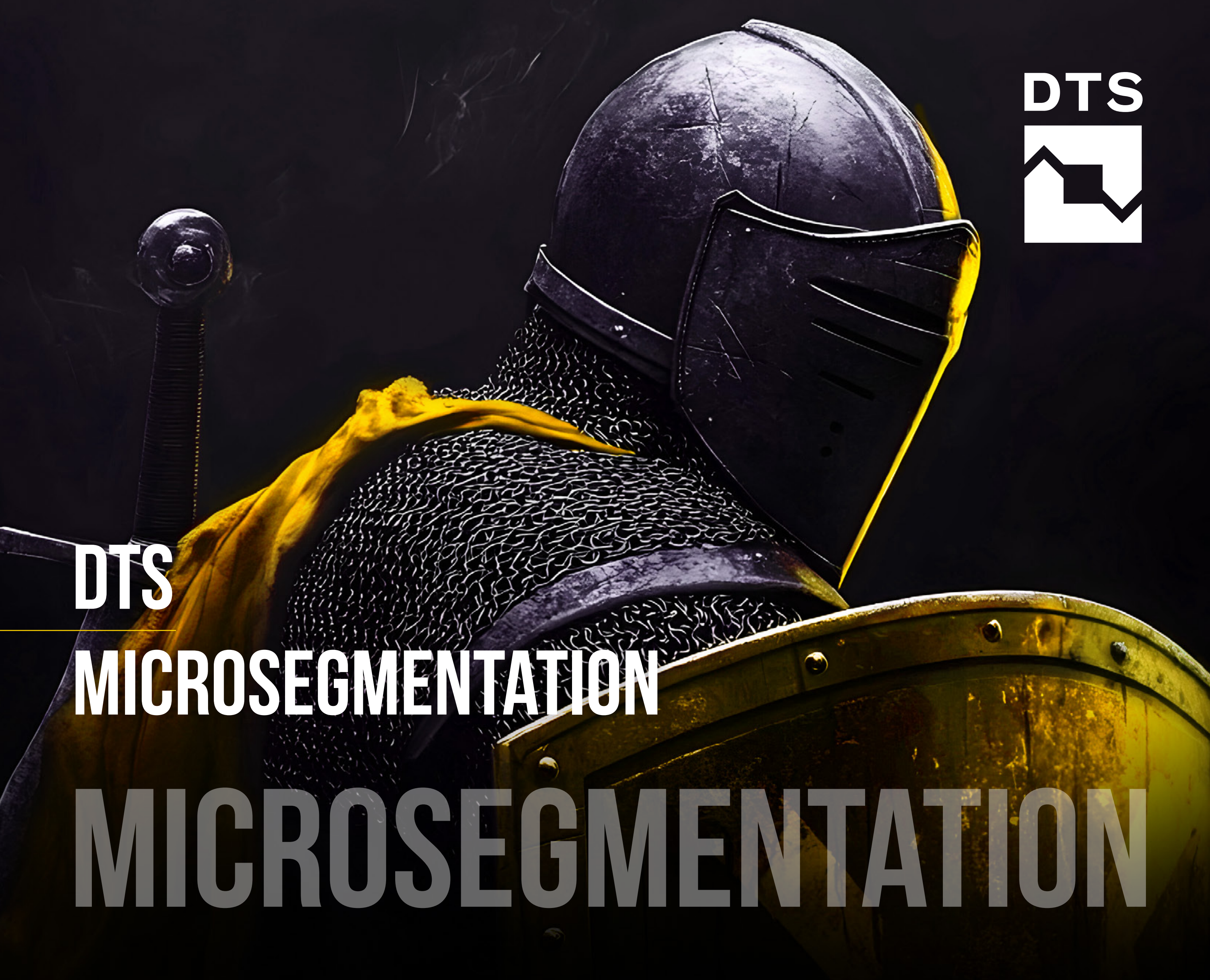

DTS MICROSEGMENTATION

MICROSEGMENTATION

ZERO TRUST STARTS IN THE NETWORK - PROTECT IT, WHAT REALLY COUNTS!

You want to prevent unauthorized data traffic and increase your security by preventing intruders from entering your network? Conventional security tools such as firewalls are designed to monitor and block traffic flowing into your network from outside. Worryingly is the fact that 70% of organizations have not implemented effective network segmentation in place.

The solution? Microsegmentation. But not just any solution: DTS Microsegmentation. Agentless. Automated. Secure.

WHAT IS MICROSEGMENTATION?

Microsegmentation is an important key component of a Zero Trust architecture, which divides networks into finely granular, logically logically isolated segments. In contrast to conventional VLANs or firewalls, it not only restricts access from outside, but also access, but also controls the entire communication behavior within the network, regardless of infrastructure, location or user location or user identity. Microsegmentation allows each application, each system and each user only the communication that is necessary and permitted - everything else is blocked.

- Reduction of the attack surface by up to 90 % through adaptive Just-in-time access controls
- Clear separation of environments, applications & identities
- Performance optimization through inline/sidecar architecture
- Security policies per communication unit - not just per network segment
- Adaptive threat response via ML-supported risk analysis
- No need to change existing network topologies
- GDPR-compliant logging of all processes
- Zero Trust reality instead of buzzword - through continuous verification
- Automated segmentation of the defined workstations & servers
- Cost efficiency through automation & agentless implementation
- Dynamic policy management
- Jour fixes to support the continuous implementation of the solution
    - Regular check of active regulations
    - Dynamic inclusion of additional assets

WHAT DOES DTS MICROSEGMENTATION OFFER?

DTS Microsegmentation offers an innovative security solution for workstations and servers that automatically segments and secures network access. An intelligent, self-learning, agentless technology allows only the connections that are actually needed, without manual effort or complex configurations complex configurations. Automated policy management also enables a rapid response to incidents and thus strengthens the defense against cyber incidents. The MFA-enabled solution implements just-in-time access and thus offers an optimal approach to implementing a Zero Trust strategy.

WHAT MAKES DTS MICROSEGMENTATION DIFFERENT & BETTER?

Automated network segmentation: The system automatically learns about all network connections and creates precise security policies, which are applied to host-based firewalls. This enables complete segmentation within 30 days without the need for manual rule configurations. Even after the initial segmentation, the implemented solution can dynamically and automatically adapt to new devices and changing user behavior.

Agentless implementation: In contrast to conventional solutions, where software agents have to be installed on each device.

MFA-supported security: Modern microsegmentation includes a just-in-time MFA component. Sensitive ports are blocked by default blocked by default and can be temporarily opened after multifactor authentication. By using MFA at the port level, organizations can extend MFA protection to a variety of resources, including clients, servers, legacy applications, databases and OT/IoT devices, that were previously difficult to protect. This approach not only prevents lateral movement when credentials are compromised, but also provides additional protection for privileged access and makes unauthorized access much more difficult. This means that the Zero Trust principle can be optimally implemented, as every access is authorized and verified.

Immediate containment of threats: Microsegmentation creates isolated security zones around critical assets. This considerably reduces the radius of action of an attack by blocking lateral movement and preventing ransomware.

Rapid response to threats: A modern microsegmentation solution should enable a rapid response to incidents and be able to thwart attacks within 24 hours while maintaining network operations. In the implemented solution, the platform learns for example, learns 90% of network activity within 24 hours, creates and applies security policies to host-based firewalls and implements MFA for remote administration protocols.

DTS MICROSEGMENTATION SERVICE

Onboarding begins with the implementation of the solution. It automatically learns all network connections and creates precise security policies. This enables complete segmentation within 30 days without the need for manual configurations. DTS Microsegmentation Service accompanies the entire process, from capturing and selecting the assets to be integrated to activating the proposed security policies.

In addition, the DTS Microsegmentation Service supports the continuous implementation of the implemented solution and regularly checks whether all active rules still fit optimally and all relevant assets are covered. Regular jour fixes also ensure the continuous expansion of the expansion of the integrated asset base. The installation of updates and fixes as well as regular maintenance work are also part of the service. With this proactive support, DTS ensures that the processes run smoothly. This allows the implementing customers to concentrate on their core business.

While other solutions rely on agents, complex configurations or selective segmentation, DTS automates the entire process - across all systems and without any loss of performance. Our solution is not just a technical tool. It is a security layer that intelligently adapts to your IT reality.

DTS Microsegmentierung E 16052025