DTS Cyber Security

What is effective cyber security? A cyber security strategy is only effective if it can withstand modern cyber attacks. This means it involves more than implementing firewalls, endpoint protection or patching. The „right" cyber security is built on a foundation of prevention, information sharing, automation and as a unit with fixed processes, policies, and expert knowledge, it ensures the greatest possible security - it is integrated.

For the entire cyber security lifecycle, you should have a partner at your side who is specialized on the one hand and can develop an individual solution together with you on the other hand, no matter where you are on your way to increased cyber security. We design integrated solutions, identify potential threats and vulnerabilities, protect IT landscapes and complete your solutions with our DTS Services. The special feature here is that the leading solutions are linked and intertwined. This creates a complete security solution. Our solutions are complemented by our Security Operations Center (SOC), which is active at several locations throughout Europe. As a central 24/7 security control center, it continuously protects infrastructures and data - manned by highly qualified German and English-speaking security experts.

We see. We do. Safe! DTS helps you with integrated cyber security, no matter where you are on your cyber security journey.

At a glance:

- Complete visibility of your entire infrastructure & users
- Minimize the attack surface with state-of-the-art architectures
- Full prevention of known threats
- Detection of new, unknown threats through automated real-time protection
- Managed Services: You save resources, time & money
- Consulting & support in German & English

What does integrated cyber security mean at DTS?
The question these days is no longer whether you will become a victim of a cyberattack, but when you will - and whether you will even register it.

The holistic nature of an effective cyber security strategy extends from the first prevention-first measures to each individual device and user. BYOD and IoT devices can make such a measure a real challenge. To cover all possible gaps in the attack surface, every device, as well as every user, should be identified and authenticated across the organization's network, endpoint, cloud and SaaS applications. A DTS zero-trust architecture ensures identity-based access with dynamically provisioned connectivity.

DTS has made it its business to create such a cyber security platform for its customers. In order to be able to implement integration and automation as the foundations of our cyber security strategy, we work together with selected, leading partners. This focus on a few, strategic partners enables us to have a deep product knowledge, which is essential for the operation of cyber security and managed services based on these technologies. Our cyber security strategy to protect your data and know-how is based on several principles:

I. Prevention-First as the basis
The flip side of the ever-decreasing cost of computing power is the opportunity for cybercriminals and attackers to conduct automated and sophisticated attacks at ever-lower costs. Focusing on a prevention-first approach allows attacks to be reduced to a manageable level, enabling you to focus on the most serious attacks. To establish the approach, you need interlocking technologies, automations and compliance requirements, as well as architectures, such as the zero-trust model, to implement all protection mechanisms. This is because a holistic platform can only be established and further developed if the individual mechanisms interlock smoothly.

II. Zero-Trust architecture
The holistic nature of an effective cyber security strategy extends from the first prevention-first measures to each individual device and user. BYOD and IoT devices can make such a measure a real challenge. To cover all possible gaps in the attack surface, every device, as well as every user, should be identified and authenticated across the organization's network, endpoint, cloud and SaaS applications. A DTS zero-trust architecture ensures identity-based access with dynamically provisioned connectivity.

III. Detection & respond as a component
Good prevention provides basic protection by making it more difficult for attackers to compromise the company. As attacks become more sophisticated, it is impossible today to prevent all attacks with certainty. For this reason, it is necessary to prepare for emergencies. The following steps are necessary:

a) Detection of the attack and assessment of the threat situation

b) Reacting to the threat in a timely manner (Response)

In order to carry out these essential steps, professional and qualified personnel are required. They assess the nature of the attack, recommend and initiate follow-up measures.

IV. Expert personnel & processes as a module
Another key point for a successful security strategy is organizational processes and the right team. The rapid adaptation of attackers to the security architecture requires the defense side to quickly adapt technologies, processes and rule sets. But finding and retaining trained employees is not as easy as it sounds.

For this reason, we offer 24/7 support from our experienced and certified engineers, as well as from our information security consultants. The focus of DTS in the area of cyber security strategy and unique positioning in the

partner landscape allows us to gain exceptional technical expertise for our solutions and services and thus define our own best practices.

As one of the leading managed service providers for our partners in Europe, we use our knowledge and experience from the field. This allows us to focus on maximum usability and effectiveness of the solutions effectiveness of the solutions in subsequent operation.

V. With a clear solution vision for a one-vendor strategy
With a focus on a clear solution vision for every customer and every challenge, we rely on a one-vendor strategy. Together with the underlying platform strategy and our many years of expertise, this gives us a unique positioning in the field of cyber security to provide the right answer to the cyber threats of today and tomorrow, from midmarket to enterprise. We exclusively offer holistic solutions from a single source.

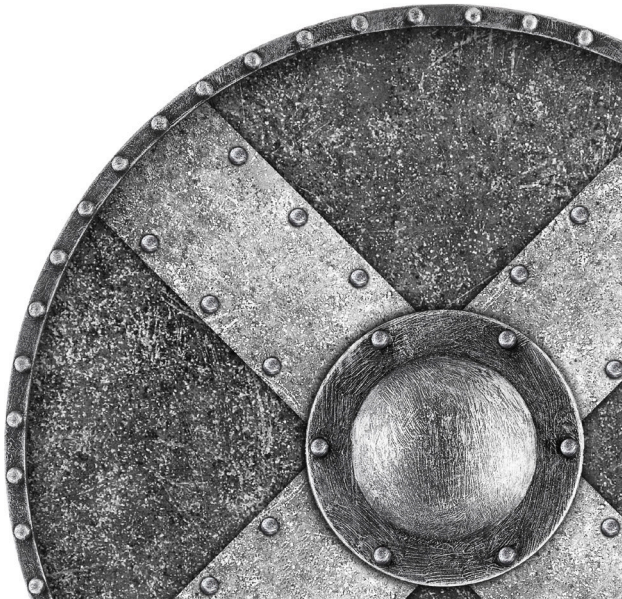
VI. DTS as Vendor
In addition, we are a „vendor“ ourselves. We design and develop our own IT security software solutions, which in turn fit ideally into our clear solution vision. The versatility ranges from Identity & Access Management and Network Access Management to the great to the great DTS Cockpit as a real market innovation.

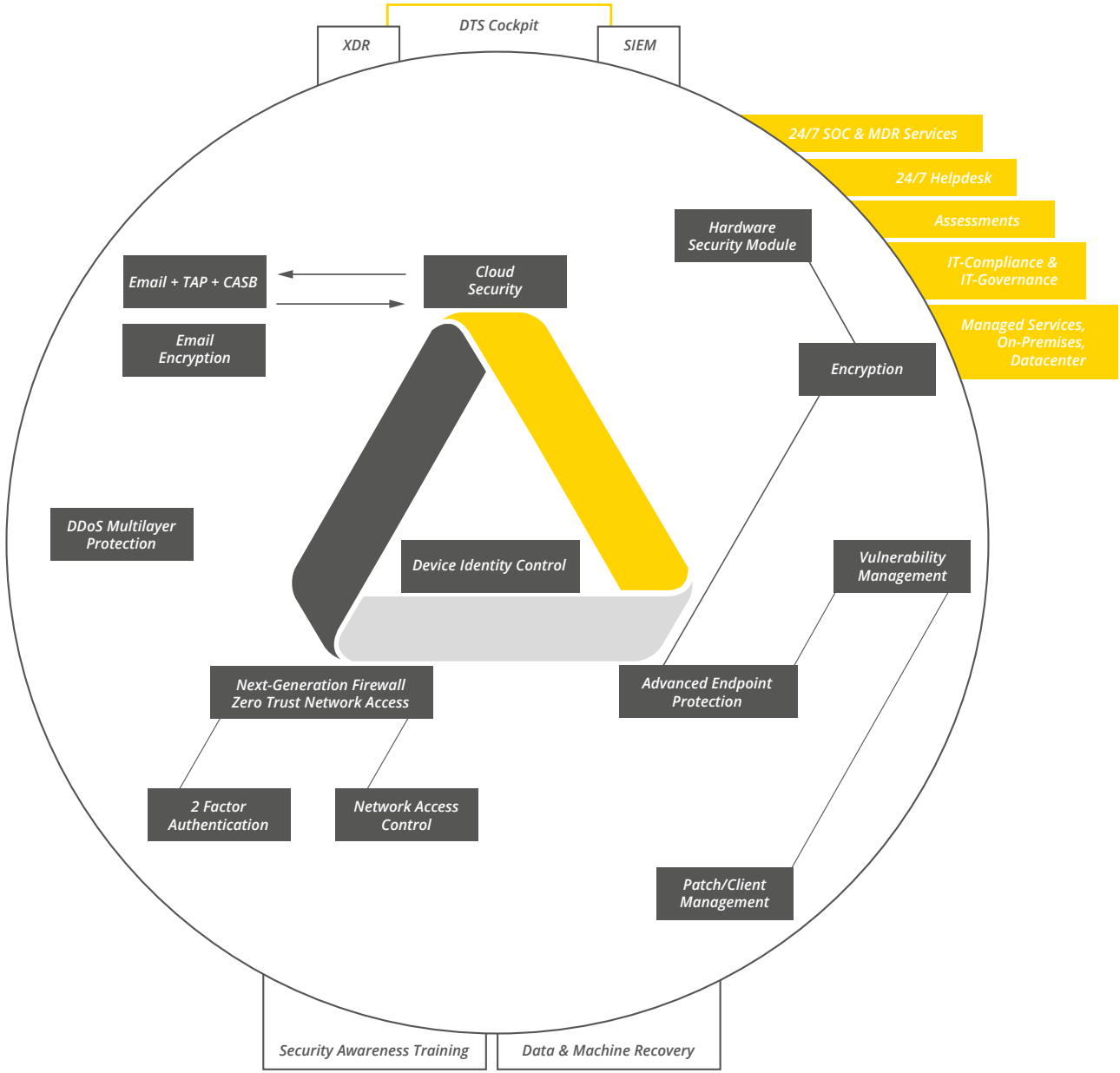
For example, we enable a complete 24/7 security information & operation service through Cockpit. Away from passive, decentralized data collection to active, centralized visibility and control: With Cockpit, we bundle and orchestrate all security solutions independently of manufacturers, fully map security landscapes, and enable automated, direct actions. All this is monitored and analyzed 24/7 by our DTS Security Operations Center. This is integrated vision, understanding and action in a cost-attractive service.

For this reason, we no longer see ourselves as just a service & IT security provider or reseller. We see ourselves as a software enabler - Cyber Security made by DTS!

DTS as your cyber security specialist

- Consulting by experts: BSI, DSGVO, KRITIS and much more
- Hybrid scenarios (on-premises, cloud)
- 24/7/365 monitoring & helpdesk
- Integrated cyber security approach
- Flexible & modular managed services
- Certified experience & expertise
- Clear solution vision & partnership-based collaboration
- End-to-end project support





DTS Systeme GmbH
+49 5221 1013-000

DTS Systeme Münster GmbH
+49 251 6060-0

dts.de
info@dts.de