DTS
Advanced Endpoint Protection

Advanced Endpoint Protection

Cyber attacks affect companies of every size and in every industry - and the number is increasing every day. The figures from recent years show a threatening development of malware. In addition, as digitalization progresses, there are ever more vulnerabilities in programs. There is an enormous variety of products in the field of endpoint security. However, standard antivirus solutions and their protection methods are no longer up to this challenge.

We therefore offer you the unique DTS Advanced Endpoint Protection with our long-term partner Palo Alto Networks. Our managed service is designed to protect the endpoint fully and completely. In addition to defense against known threats, it includes protection against unknown and sophisticated attacks in particular. We provide you with the only true, sustainable evolution of antivirus software that meets the complex needs of today and tomorrow.

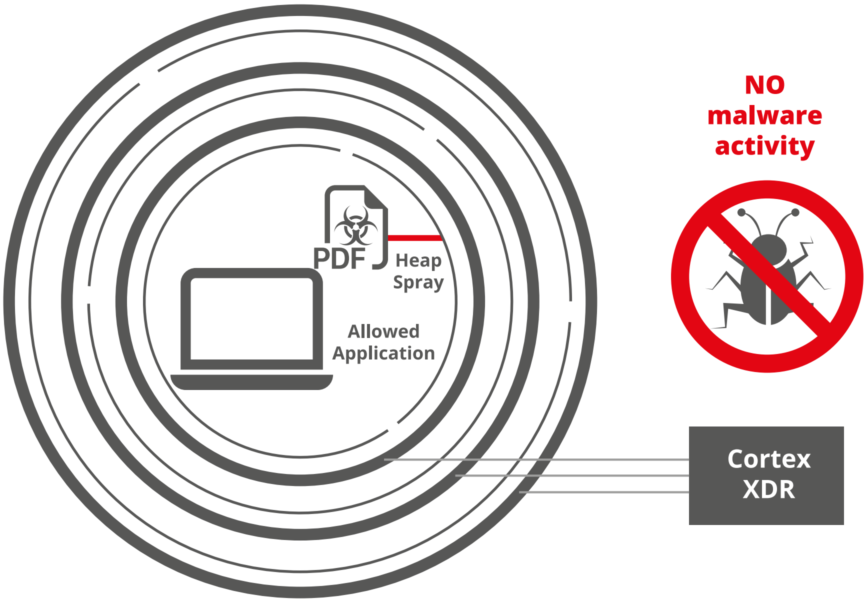
- Preventive & continuous endpoint security
- Protection against known exploits & zero-day exploits
- Effective protection against zero-day malware, ransomware & fileless attacks
- Integration with the Palo Alto Networks security platform
- Incident investigation with additional response capabilities (e.g. live terminal, endpoint isolation)
- Intelligent grouping of individual alarms
- Behavioral analysis
- Extensive data collection
- Cloud-based detection & response
- Peripheral device management & control
- DTS Helpdesk, health checks, provisioning & configuration

Cyber attacks can occur, for example, via websites or emails. Most endpoint security products only protect you from known malware at this point. But what is there to protect you against unknown malware or exploits? Palo Alto Networks' Cortex-XDR platform is the evolution of the Application Framework and aims to correlate data from multiple data sources to detect and stop targeted attacks more effectively.

This is based on the existing prevention products (sensors) from Palo Alto Networks, i.e. the firewalls and Prisma Access in the network area, Cortex XDR at the endpoint and Prisma Cloud and Prisma SaaS in the cloud. All information from these sensors is stored in the Cortex Data Lake in the form of logs. The Data Lake serves as a large, central data pool and Cortex XDR in turn accesses it.

Using machine learning, Cortex XDR continuously builds a baseline of user and device behavior to detect anomalous activity that could be a sign of attack. Cortex XDR combines the information of all sensors and thus functions from the areas of UBA, EDR, NTA & EPP in a single platform.

Thanks to the close connection to Palo Alto Networks prevention products, you can take immediate countermeasures to stop attacks in good time. All applications have vulnerabilities and bugs. Exploits use unpatched vulnerabilities to attack good and/or authorized applications. Cortex XDR's management is activated when an attempt is made to run an exploit and terminates the exploit immediately – before anything harmful can be done.



DTS managed services

We offer you this innovative solution as a DTS managed service. The service is provided by Cortex XDR Management, which serves as the central instance. The highly scalable, efficient agents are made available for various operating systems. Regular health checks also ensure that the configuration is optimally adapted to your environment. As an award-winning Elite Authorized Support Center, we provide first and second-level support in the form of 9/5 or 24/7 phone support. You benefit from the support of our technical experts via the DTS Helpdesk, which will deal with all your concerns.