DTS
ENDPOINT SECURITY

ENDPOINT SECURITY

Cyberattacks affect companies of all sizes and in every industry - and the number is increasing every day: up to 144 million new malware programs per year, over 390000 variants per day, 16000 viruses or trojans per second. The figures from recent years show a threatening development. In addition, as digitalization progresses, there are more and more vulnerabilities in programs. Conventional antivirus solutions and their protection methods are not equal to these challenges. With Cortex XDR Prevent & Pro from Palo Alto Networks, we offer next-level detection & response as a true, sustainable further development of "antivirus". The innovative security strategy enables integrated end-point security and complete protection against known and unknown, highly advanced attacks.

- Preventive & continuous endpoint security
- Effective protection against (zero-day) exploits, (zero-day) malware, ransomware, fileless attacks and much more
- Comprehensive, pinpoint data collection & behavior analysis
- Lightning-fast, proactive detection & defense against previously unknown threats
- AI & cloud-based analyses
- Blocks attacks with behavior-based threat protection
- Incident investigation with additional response options
- Management & control of peripheral devices
- Cloud-based detection & response
- DTS Managed Services: Helpdesk, health checks, deployment & configuration

The Cortex XDR platform aims to correlate data from different data sources to more effectively detect and stop targeted attacks. By using machine learning, Cortex XDR continuously forms a baseline of user and device behavior to detect anomalies that could be signs of attacks.

Cortex XDR Prevent Prevent provides optimal protection for endpoints and includes device control, disk encryption and host firewall functions. It also includes an incident engine, integrated response capabilities and an optional threat intelligence feed.

Cortex XDR Pro offers the same protection as Cortex XDR Prevent, but for endpoints, networks, cloud resources and third-party products. It also includes features for behavioral analysis, rule-based detection, accelerated investigation and optional managed threat hunting.

Both versions include the storage of warning messages for 30 days and optional extended data retention. The Pro version also includes XDR data retention for endpoint and network data for 30 days.

ARCHITECTURE OF CORTEX XDR

The architecture of Cortex XDR includes several standard components. Both editions are based on the Cortex Data Lake and are designed to correlate log data across devices. The Cortex Data Lake is a storage resource for cloud-based logging that is designed to store your log data from all sources. The Data Lake centralizes your data and allows the XDR engine to correlate events and create alerts. Cortex XDR also offers a UI user interface that provides complete insight into your data lake. The UI allows you to sort and investigate alerts, take action and define your detection and response policies.

The extended platform components also include the analysis engine and the Cortex XDR agents. The analytics engine is a security service that uses network and endpoint data to detect and respond to threats. It applies behavioral analysis to identify both known and unknown threats by comparing them to known and accepted user or device behaviors. The Cortex XDR agents are installed on endpoints and are used to collect and forward data. These agents can also perform local analysis and utilize WildFire threat data for better threat detection. All collected data is sent to the data lake for joint analysis.

All in all, Cortex XDR offers several unique key features designed to secure an organization's networks and devices. Endpoint protection is a fully comprehensive defense against malware, fileless attacks, ransomware and exploits. All downloaded files are examined by an analysis engine with AI functions. The additional behavioral analysis helps to identify and stop malicious data transfers or processes. Companies can also integrate the Palo Alto Networks WildFire Malware Prevention Service to increase security and protection.

SECURE MANAGEMENT OF USB DEVICES

Cortex XDR includes device control, a function that monitors and secures USB access to devices. The function is agentless. It allows organizations to restrict device usage based on endpoint, type, manufacturer or active directory identities. Device control also makes it possible to restrict read and write permissions per USB device ID.

In addition, the protection of endpoint data is made possible with host firewall and hard disk encryption. Firewalls and disk encryption protect endpoints from malicious traffic and reduce the damage caused when attackers sometimes bypass firewalls. The Cortex XDR Firewall provides controls for inbound and outbound communication. Hard disk encryption can be integrated directly into BitLocker and companies can encrypt and decrypt data on end devices.

DTS MANAGED SERVICES

We also offer 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. In addition, regular health checks ensure that the configuration is optimally adapted to your environment. As an Elite Authorized Support Center, we provide first and second level support in the form of 9/5 or 24/7 telephone support. You benefit from the support of our technical experts via the DTS Helpdesk for all issues.

DTS Systeme GmbH
+49 5221 1013-000

DTS Systeme Münster GmbH
+49 251 6060-0

dts.de
info@dts.de