DTS
Endpoint Security

Endpoint Security

Cyber attacks affect companies of all sizes and in every industry – and they are increasing every day: up to 144 million new malware programs per year, more than 390,000 variants per day, 16,000 viruses or Trojans per second. The figures from recent years show a threatening development of malware. In addition, as digitalization progresses, there are ever more vulnerabilities in programs. Common antivirus solutions and their methods of protection against malware and exploits are not up to this challenge. With Cortex XDR Prevent and Cortex XDR Pro from Palo Alto Networks, we offer next-level detection and response – the only true, sustainable evolution of "antivirus". Only this innovative security strategy will meet the complex requirements of today and tomorrow.

- First-class endpoint protection against cyber attacks
- Analytics to detect stealth & unknown threats
- Lightning fast investigation & defense
- Full transparency through seamless data acquisition
- Proaktive Bedrohungserkennung mit leistungs-starken Suchfunktionen
- Proactive threat detection with powerful search capabilities
- USB device management & control
- Effective endpoint protection through host firewalls & hard drive encryption

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

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

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

Cortex XDR architecture

The Cortex XDR architecture includes several standard components. Of course, both editions are based first and foremost on the Cortex Data Lake and are designed to correlate log data across devices.

The Cortex Data Lake is a cloud-based logging storage resource designed to store your logging data from all sources. The data lake centralizes your data and enables the XDR engine to correlate events and generate alerts. Cortex XDR also offers a UI that provides complete visibility for your data lake. From this interface, you can sort and investigate alerts, take remedial action and define your detection and response policies.

Advanced platform components also include the analytics engine and 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 analytics to identify both known and unknown threats by comparing them to known and accepted user or device behaviors. Cortex XDR agents are installed on endpoints and are used to collect and forward data. These agents can also perform local analysis and use WildFire threat data to better detect threats. All collected data is sent to the data lake for shared analysis.

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

Secure USB device management

Cortex XDR includes Device Control, a feature that monitors and secures USB access to devices. The function is agentless. It allows organizations to restrict device usage based on endpoint, type, manufacturer and Active Directory identities. Device Control also allows companies to restrict read and write permissions according to USB device ID.

Endpoint data protection is also enabled with host firewall and hard disk encryption. Firewalls and hard disk encryption protect endpoints from malicious traffic and reduce the damage caused if attackers occasionally bypass firewalls. The Cortex XDR Firewall provides controls for incoming and outgoing communications. Disk encryption can be integrated directly with BitLocker, and organizations can encrypt and decrypt data at endpoints.