DTS
Endpoint Security

Endpoint Security

Cyberangriffe treffen Unternehmen jeder Größe und in jeder Branche - und täglich werden es mehr: bis zu 144 Millionen neue Malware-Programme pro Jahr, über 390.000 Varianten am Tag, 16.000 Viren oder Trojaner pro Sekunde. Die Zahlen der vergangenen Jahre zeigen eine bedrohliche Entwicklung von Schadsoftware. Zudem gibt es im Zuge der fortschreitenden Digitalisierung kontinuierlich mehr Schwachstellen in Programmen. Gängige Antivirus-Lösungen und deren Schutzmethoden vor Malware und Exploits sind dieser Herausforderung nicht gewachsen. Mit Cortex XDR Prevent und Cortex XDR Pro von Palo Alto Networks bieten wir Ihnen ein Next Level Detection and Response – die einzig echte, nachhaltige Weiterentwicklung von „Antivirus". Nur diese innovative Sicherheitsstrategie wird den komplexen Anforderungen von heute und morgen gerecht.

- Erstklassiger Endpunktschutz gegen Cyberangriffe
- Analysen zur Erkennung getarnter & unbekannter Bedrohungen
- Blitzschnelle Untersuchung & Abwehr
- Volle Transparenz durch lückenlose Datenerfassung
- Proaktive Bedrohungserkennung mit leistungsstarken Suchfunktionen
- Verwaltung & Kontrolle von USB-Geräten
- Effektiver Schutz von Endpunkten durch Host-Firewalls & Festplattenverschlüsselung

Cortex XDR Prevent bietet optimalen Schutz für Endpunkte und umfasst Funktionen zur Gerätekontrolle, Festplattenverschlüsselung und Host Firewall. Außerdem enthält es eine Incident Engine, integrierte Reaktionsmöglichkeiten und einen optionalen Threat Intelligence Feed.

Cortex XDR Pro bietet den gleichen Schutz wie Cortex XDR Prevent, jedoch für Endgeräte, Netzwerke, Cloud-Ressourcen und Produkte von Drittanbietern. Es umfasst außerdem Funktionen für die Verhaltensanalyse, regelbasierte Erkennung, beschleunigte Untersuchung und optional verwaltetes Threat Hunting.

Beide Versionen beinhalten die Speicherung von Warnmeldungen für 30 Tage und eine optional erweiterte Datenaufbewahrung. Die Pro-Version umfasst außerdem die XDR-Datenaufbewahrung für Endpunkt- und Netzwerkdaten für 30 Tage.

Architektur von Cortex XDR
Die Architektur von Cortex XDR beinhaltet mehrere Standardkomponenten. Natürlich basieren beide Editionen zuallererst auf dem Cortex Data Lake und sind darauf ausgelegt, Protokolldaten geräteübergreifend zu korrelieren.

Der Cortex Data Lake ist dabei eine Speicherressource für die cloudbasierte Protokollierung, die für die Speicherung Ihrer Protokolldaten aus allen Quellen ausgelegt ist. Der Data Lake zentralisiert Ihre Daten und ermöglicht es der XDR-Engine, Ereignisse zu korrelieren und Warnmeldungen zu erstellen. Cortex XDR bietet zudem eine UI-Benutzeroberfläche die einen vollständigen Einblick in Ihren Data Lake bietet. Über diese Benutzeroberfläche können Sie Warnungen sortieren und untersuchen, Maßnahmen zur Behebung ergreifen und Ihre Erkennungs- und Reaktionsrichtlinien definieren.

Zu den erweiterten Plattformkomponenten gehören außerdem die Analyse-Engine und die Cortex-XDR-Agenten. Die Analyse-Engine ist ein Sicherheitsdienst, der Netzwerk- und Endpunktdaten nutzt, um Bedrohungen zu erkennen und darauf zu reagieren. Er wendet Verhaltensanalysen an, um sowohl bekannte als auch unbekannte Bedrohungen durch den Vergleich mit bekannten und akzeptierten Benutzer- oder Geräteverhaltensweisen zu identifizieren. Die Cortex-XDR-Agenten sind auf Endpunkten installiert und werden zum Sammeln und Weiterleiten von Daten verwendet. Diese Agenten können auch lokale Analysen durchführen und WildFire-Bedrohungsdaten zur besseren Erkennung von Bedrohungen nutzen. Alle gesammelten Daten werden an den Data Lake zur gemeinsamen Analyse gesendet.

Alles in allem bietet Cortex XDR mehrere, einzigartige Schlüsselfunktionen, die dazu dienen, die Netzwerke und Geräte eines Unternehmens zu sichern. Der Endpunktschutz ist eine vollumfassende Abwehr vor Malware, dateilosen Angriffen, Ransomware und Exploits. Alle heruntergeladenen Dateien werden von einer Analyse-Engine mit KI-Funktionen untersucht. Die zusätzlichen Verhaltensanalysen helfen dabei, bösartige Datenübertragungen oder Prozesse zu identifizieren und zu stoppen. Unternehmen können auch den Palo Alto Networks WildFire Malware Prevention Service integrieren, um die Sicherheit und den Schutz zu erhöhen.

Sichere Verwaltung von USB-Geräten
Cortex XDR enthält mit Device Control eine Funktion, die den USB-Zugriff auf Geräte überwacht und sichert. Die Funktion ist agentenlos. Sie ermöglicht es Unternehmen, die Gerätenutzung je nach Endpunkt, Typ, Hersteller oder Active-Directory-Identitäten einzuschränken. Die Gerätekontrolle ermöglicht es Unternehmen auch, Lese- und Schreibberechtigungen entsprechend der USB-Geräte-ID zu beschränken.

Zusätzlich wird der Schutz von Endpunktdaten mit Host-Firewall und Festplattenverschlüsselung ermöglicht. Firewalls und eine Festplattenverschlüsselung schützen Endgeräte vor bösartigem Datenverkehr und reduzieren den Schaden, der entsteht, wenn Angreifer mitunter Firewalls umgehen. Die Cortex XDR Firewall bietet Kontrollen für eingehende und ausgehende Kommunikation. Die Festplattenverschlüsselung kann direkt in BitLocker integriert werden, und Unternehmen können Daten auf Endgeräten ver- und entschlüsseln.

DTS Systeme GmbH
+49 5221 1013-000

DTS Systeme Münster GmbH
+49 251 6060-0

dts.de
info@dts.de