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. Zudem gibt es im Zuge der fortschreitenden Digitalisierung kontinuierlich mehr Schwachstellen in Programmen. Gängige Antivirus-Lösungen und deren Schutzmethoden sind diesen Herausforderungen nicht gewachsen. Mit Cortex XDR Prevent & Pro von Palo Alto Networks bieten wir ein Next Level Detection & Response als echte, nachhaltige Weiterentwicklung von „Antivirus". Die innovative Sicherheitsstrategie ermöglicht ganzheitliche Endpoint Security und vollständigen Schutz vor bekannten und unbekannten, hoch entwickelten Angriffen.

- Präventive & kontinuierliche Endpoint Security
- Effektiver Schutz vor (Zero-Day-)Exploits, (Zero-Day-) Malware, Ransomware, dateilosen Angriffen u. v. m.
- Umfangreiche, punktgenaue Datenerfassung & Verhaltensanalyse
- Blitzschnelle, proaktive Erkennung & Abwehr bislang unbekannter Bedrohungen
- KI & cloudbasierte Analysen
- Blockiert Angriffe mit verhaltensbasiertem Bedrohungsschutz
- Untersuchung von Incidents mit zusätzlichen Reaktionsmöglichkeiten
- Verwaltung & Kontrolle von Peripherie-Geräten
- Cloudbasierte Erkennung & Reaktion
- DTS Managed Services: Helpdesk, Health Checks, Bereitstellung & Konfiguration

Die Cortex-XDR-Plattform zielt darauf ab, Daten von verschiedenen Datenquellen miteinander zu korrelieren, um zielgerichtete Angriffe effektiver zu erkennen und zu stoppen. Durch die Nutzung von Machine Learning bildet Cortex XDR dabei kontinuierlich eine Baseline zum Nutzer- und Geräteverhalten, um Anomalien, die Anzeichen von Angriffen sein könnten, aufzudecken.

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 obendrein 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 zusätzlich die XDR-Datenaufbewahrung für Endpunkt- und Netzwerkdaten für 30 Tage.

ARCHITEKTUR VON CORTEX XDR

Die Architektur von Cortex XDR beinhaltet mehrere Standardkomponenten. Dabei basieren beide Editionen auf dem Cortex Data Lake und sind darauf ausgelegt, Protokolldaten geräteübergreifend zu korrelieren. Der Cortex Data Lake ist 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 die Benutzeroberfläche können Sie Warnungen sortieren und untersuchen, Maßnahmen 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 voll umfassende 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 auch, Lese- und Schreibberechtigungen je 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 MANAGED SERVICES

Wir bieten Ihnen die neuartige Lösung auch als DTS Managed Service an. Dabei erfolgt die Bereitstellung des Dienstes durch das Cortex XDR Management, welches als zentrale Instanz dient. Die hoch skalierbaren, effizienten Agenten werden für verschiedene Betriebssysteme zur Verfügung gestellt. Zudem sorgen regelmäßige Health Checks dafür, dass die Konfiguration optimal auf Ihre Umgebung angepasst ist. Als ausgezeichnetes Elite Authorized Support Center übernehmen wir den First- und Second Level Support in Form eines 9/5 oder 24/7 Telefon-Supports. Sie profitieren bei allen Anliegen von der Unterstützung unserer Fachexperten über den DTS Helpdesk.

Üwelches als zentrale Instanz dient. Die hoch skalierbaren, effizienten Agenten werden für verschiedene Betriebssysteme zur Verfügung gestellt. Zudem sorgen regelmäßige Health Checks dafür, dass die Konfiguration optimal auf Ihre Umgebung angepasst ist. Als ausgezeichnetes Elite Authorized Support Center übernehmen wir den First- und Second Level Support in Form eines 9/5 oder 24/7 Telefon-Supports. Sie profitieren bei allen Anliegen von der Unterstützung unserer Fachexperten über den DTS Helpdesk.

DTS Systeme GmbH
+49 5221 1013-000

DTS Systeme Münster GmbH
+49 251 6060-0

dts.de
info@dts.de