Endpunktschutz mit Cortex XDR

Ein einheitlicher, über die Cloud bereitgestellter Agent mit Erkennungs- und Abwehrfunktionen sichert Ihre Endpunkte gegen bisher unbekannte Angriffe.

Vorteile

- Malware-Abwehr basierend auf Verhaltensanalysen und KI-gestützten lokalen Prüfmechanismen
- Blockierung von Exploits, die für Hackereinbrüche eingesetzt werden
- Einheitlicher Schutz durch zentralisierte Erkennungs- und Abwehrfunktionen, die das gesamte Netzwerk sowie alle Endpunkte und Cloud-Ressourcen abdecken
- Einfacher Betrieb dank cloudnativer Bereitstellungs- und Managementprozesse

Branchenführende Erfassung aktueller Angriffsmethoden, belegt durch Tests von MITRE

Komplexe Malware und skriptbasierte Angriffe stellen ein hohes potenzielles Risiko für Ihr Unternehmen und Ihren Geschäftsbetrieb dar, werden jedoch durch herkömmliche Antivirusprodukte nicht erkannt. Deshalb benötigen Sie eine Lösung, die Ihre Endpunkte effektiv gegen derartige Angriffe sichert und die eigenen Schutzfunktionen mithilfe von künstlicher Intelligenz kontinuierlich an neue Bedrohungen und Angriffsmethoden anpasst.

Genau hier kommt der leistungsstarke Agent von Cortex XDR ins Spiel. Er schützt Ihre Endpunkte vor Zero-Day-Malware, dateilosen oder skriptbasierten Angriffen und anderen Hackeraktivitäten, indem er eingehende Dateien vor und nach der Ausführung analysiert. Da der Agent aus der Cloud bereitgestellt wird, bietet er Ihren Endpunkten sofortigen Schutz vor komplexen Bedrohungen und beginnt unmittelbar mit der Erfassung von sicherheitsrelevanten Daten zur Verbesserung der Erkennungs- und Abwehrmechanismen.

Effektiver Schutz vor Zero-Day-Malware, Ransomware und dateilosen Angriffen

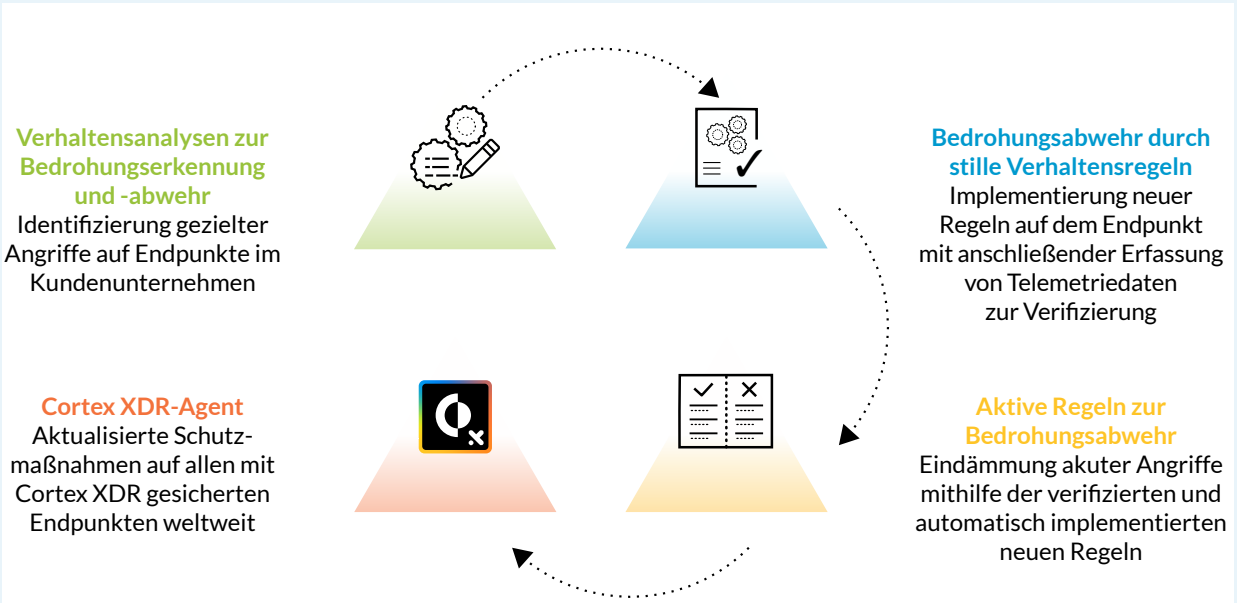
Der einheitliche Agent von Cortex XDR deckt sämtliche Angriffsvektoren mit vielfältigen Sicherheitsfunktionen und mehreren einander ergänzenden Engines ab:

- **KI-gestützte Analysefunktionen:** Der Agent nutzt ein lokales, auf einem umfangreichen Datensatz aus verschiedenen Quellen basierendes Modell für das maschinelle Lernen, um Malware noch vor der Ausführung zu blockieren. Dieses Modell fußt auf einem einzigartigen agilen Framework und kann daher kontinuierlich aktualisiert und auf den aktuellen Stand gebracht werden.
- **Integration in den cloudbasierten Malware-Schutz WildFire®:** Die Kombination der beiden Lösungen ermöglicht die detaillierte Analyse unbekannter Dateien und den automatischen Austausch der sicherheitsrelevanten Daten, die von den Endpunktagenten von Palo Alto Networks, Ihren Next-Generation Firewalls und den Überwachungstools für Ihre Cloud-Umgebungen erfasst wurden.
- **Verhaltensanalysen:** Der Agent erkennt und blockiert auch die am besten getarnten Bedrohungen, indem er Ereignissequenzen identifiziert, die auf Malware und dateilose Angriffe hinweisen. Die dafür genutzte Engine überprüft das Verhalten miteinander zusammenhängender Prozesse, um Angriffe aufzudecken, die aus einer Kette vermeintlich unverdächtiger Aktivitäten bestehen.

- **Verhaltensbasierter Schutz vor Ransomware:** Der Agent schützt Ihre Endpunkte vor Ransomware, indem er Prozesse identifiziert, die auf die Änderung oder Verschlüsselung von Dateien zielen. Das bietet zusätzliche Sicherheit bei Angriffen mit getarnter Ransomware.
- **Verhinderung des Diebstahls von Anmeldedaten:** Der Agent verhindert den Einsatz von Tools wie Mimikatz, mit denen externe Angreifer oder böswillige Insider Systempasswörter stehlen können. Dadurch wird der Missbrauch von Anmeldedaten und die unbefugte Erlangung erweiterter Zugriffsrechte unterbunden.
- **Regelmäßige und anlassbezogene Malware-Scans:** Durch die Aufdeckung inaktiver Malware in schädlichen ausführbaren Dateien, DLLs und Office-Makros lassen sich Bedrohungen beseitigen, bevor sie Schaden anrichten können.

Effektiver Schutz durch hochpräzise Verhaltensanalysen

Im Rahmen des Features „Behavioral Threat Protection" erstellen die Forscher von Cortex XDR Regeln, die auf Ergebnissen aus der Bedrohungsforschung sowie aktuellen Telemetrie- und Bedrohungsdaten aus Kundennetzwerken basieren und dann zur Aktualisierung aller weltweit implementierten Agenten genutzt werden. Da jede neue Regel zunächst „stummgeschaltet" ist, kann die Bereitstellung schnell und unter Beibehaltung einer außergewöhnlich niedrigen Fehlalarmquote erfolgen.



Früh greifende Maßnahmen zur Unterbindung von Exploit-Angriffen

Angreifer nutzen oft Schwachstellen von Betriebssystemen und Anwendungen aus, um Endpunkte unter ihre Kontrolle zu bringen und mit Malware zu infizieren. Hier erweist es sich als großer Vorteil, dass der Agent von Cortex XDR derartige Aktivitäten auch ohne Abgleiche mit einer Signaturdatenbank erkennen und unterbinden kann, sodass auf Exploits basierende Bedrohungen schon in den frühen Phasen des Angriffszyklus gestoppt werden.

Im Einzelnen kommen dabei drei verschiedene Methoden zum Einsatz:

- **Vorbeugende Schutzmechanismen** unterbinden die Ausspähung der Infrastruktur im Vorfeld eines bevorstehenden Angriffs und stoppen diesen damit präventiv.
- **Methodenbasierte Schutzmechanismen** wehren auf bekannten und unbekannten Exploits basierende Bedrohungen ab, indem sie gängige Angriffsmethoden zur Erzeugung von Pufferüberläufen sowie für das DLL-Hijacking blockieren.
- **Maßnahmen zum Schutz vor Kernel-Exploits** blockieren Schadprogramme, die Schwachstellen im Betriebssystem ausnutzen, um Prozesse mit erweiterten Systemprivilegien zu erstellen. Darüber hinaus verhindert der Agent von Cortex XDR Injektionen zum Laden und Ausführen von Schadcode aus dem Kernel und bietet damit auch vor jenen Kernel-Exploits Schutz, die beispielsweise bei den Angriffen mit WannaCry und NotPetya zum Einsatz kamen.

Schnelle Erkennung und Untersuchung von Bedrohungen

Der Agent von Cortex XDR sammelt detaillierte Endpunktdaten und leitet diese an die gleichnamige Enterprise-Sicherheitsplattform weiter, wo sie mit Informationen über den Status der Netzwerke und Cloud-Umgebungen zusammengeführt und zur Unterbindung raffinierter Angriffe genutzt werden. Zusätzlich bietet die Plattform von Cortex XDR eine Benutzeroberfläche zur zentralisierten Verwaltung von Warnmeldungen, Sicherheitsvorfällen und den auf dem Agenten implementierten Richtlinien.

Durch die Bündelung der verschiedenen Typen sicherheitsrelevanter Daten erhalten Kunden von Cortex XDR automatisch ein umfassendes Bild jedes Angriffs, das zum einen über den Ausgangspunkt und den Ablauf Auskunft gibt und zum anderen die Sichtung von Warnmeldungen und die Einleitung von Gegenmaßnahmen beschleunigt. Das ermöglicht schnellere forensische Untersuchungen und reduziert den Zeit- und Arbeitsaufwand in allen Phasen der Angriffsabwehr. Außerdem schafft Cortex XDR durch die enge Verzahnung mit Sicherheitspunkten ideale Voraussetzungen für eine schnellere Reaktion auf Vorfälle und die Anwendung des gewonnenen Wissens zur Erkennung zukünftiger ähnlicher Angriffe.

Rasche Reaktionen auf raffinierte Angriffe

Der Agent von Cortex XDR unterstützt ein breites Spektrum an Maßnahmen zur Eindämmung von Bedrohungen und versetzt Analysten in die Lage, reichhaltige Endpunktdaten für ihre forensischen Untersuchungen abzurufen.

Mit Cortex XDR können Analysten und Administratoren im Rahmen der Bedrohungsabwehr ...

- **Endpunkte isolieren,** indem jeglicher Netzwerkzugriff von und zu kompromittierten Endpunkten unterbunden wird (außer dem Datenverkehr mit der Managementkonsole von Cortex XDR), sodass diese nicht mit anderen Endpunkten kommunizieren und sie möglicherweise infizieren können.
- **Prozesse beenden,** um bereits laufende Malware an der weiteren Ausführung schädlicher Aktivitäten auf dem Endpunkt zu hindern.
- **die Ausführung weiterer Instanzen schädlicher Dateien unterbinden –** mithilfe einer Richtlinie, die die Datei auf eine Blacklist setzt.
- Schaddateien unter Quarantäne stellen **und sie aus ihren Arbeitsverzeichnissen entfernen, wenn Cortex XDR das nicht bereits** automatisch erledigt hat.
- **gerätespezifische Dateien abrufen,** um ein genaueres Bild von den untersuchten Endpunkten zu gewinnen.
- **über das flexible Live Terminal direkt auf Endpunkte zugreifen,** um dort Python-, PowerShell- oder Systembefehle oder -skripte auszuführen, die aktiven Prozesse zu analysieren und zu verwalten und vorhandene Dateien einzusehen, zu löschen, zu verschieben oder herunterzuladen.
- **offene APIs zur Integration von Drittanbietertools nutzen,** sodass Sicherheitsrichtlinien konsistent implementiert und die von den Agenten bereitgestellten Informationen standortunabhängig erfasst werden können.

Konsistente Sicherheit durch einheitliche Richtlinien für Endpunkte, Netzwerke und Cloud-Umgebungen

Der Agent von Cortex XDR lässt sich mit WildFire, Next-Generation Firewalls und Prisma™ Access verzahnen und unterstützt dadurch die Einrichtung konsistenter Schutzmaßnahmen in der gesamten Unternehmensumgebung. Mit einer derart integrierten Infrastruktur können Sie das Sicherheitsniveau Ihres Unternehmens kontinuierlich heben und Angriffe mit Zero-Day-Exploits auf koordinierte Weise abwehren. Sobald eines der Produkte von Palo Alto Networks eine bisher unbekannte Malware-Variante identifiziert, werden die verdächtigen Dateien umgehend zur weiteren Analyse an WildFire übermittelt. Falls sich die vermeintliche Malware dort tatsächlich als Schadprogramm erweist, werden automatisch neue Sicherheitsrichtlinien erstellt und innerhalb von Minuten in Prisma Access sowie allen Next-Generation Firewalls und Endpunktagenten implementiert.

Verwaltung und Kontrolle von USB-Geräten

USB-Geräte sind in vielerlei Hinsicht nützlich, bergen jedoch auch Sicherheitsrisiken. Wenn unachtsame Mitarbeiter einen mit Malware infizierten USB-Stick in den entsprechenden Port ihres Computers stecken oder vertrauliche Daten auf mobilen Festplatten speichern, setzen sie ihr Unternehmen der Gefahr von Ransomware-Angriffen und Datenverlusten aus. Erschwerend kommt hinzu, dass raffinierte Angreifer selbst vermeintlich harmlose Geräte wie Tastaturen und Webcams mit Malware infizieren können. Deshalb bietet Ihnen Cortex XDR ein leistungsstarkes Kontrollmodul, das die Überwachung und Sicherung von USB-Geräten ermöglicht und ohne vorherige Installation zusätzlicher Endpunktagenten eingesetzt werden kann. Damit können Sie Richtlinien für Active Directory®-Gruppen und -Organisationseinheiten erstellen, die Nutzung bestimmter Gerätetypen einschränken und gerätespezifische Lese- und Schreibberechtigungen in Abhängigkeit des Anbieters oder Produkts sowie der Seriennummer festlegen. Auf diese Weise lässt sich verhindern, dass USB-Geräte zum Einfallstor für Angreifer und Cyberbedrohungen werden.

Mühelose Bereitstellung aus der Cloud

Der Agent von Cortex XDR kann über den cloud-nativen Managementdienst schnell auf sämtlichen Endpunkten installiert werden und kommt ohne unternehmensinterne Protokollierungs- und Verwaltungsserver aus. Dadurch verkürzt er die zum Schutz neuer Systeme benötigte Zeitspanne, vereinfacht die Sicherheitsprozesse und entlastet die für den IT-Betrieb zuständigen Teams. Zugleich profitieren die Endbenutzer von einer – im Vergleich zu alten Antivirusprodukten – verbesserten Performance und geringeren Latenz.

Unterstützung aller gängigen Betriebssysteme

Der Agent von Cortex XDR ist unter anderem für Windows®, macOS®, Linux und Android® ausgelegt und schützt daher sämtliche Endpunkte mit gängigen Betriebssystemen vor bekannten und unbekannten Angriffen. Dadurch hebt er sich von den nativen Sicherheitsfunktionen der verschiedenen Betriebssysteme ab, die keinen übergreifenden Schutz bieten und auf diese Weise die zügige, koordinierte Abwehr von Bedrohungen erschweren. Eine vollständige Liste der unterstützten Betriebssysteme finden Sie in der Kompatibilitätsmatrix von Palo Alto Networks.

Broker-Service für isolierte Netzwerke

Der On-Premises-Broker-Service ermöglicht die Sicherung von Geräten, die nicht direkt mit dem Internet verbunden sind. Die auf diesen Geräten installierten Cortex XDR-Agenten können den Broker-Service als Proxy für die Kommunikation mit dem Cortex XDR-Managementdienst nutzen und auf diese Weise sowohl aktuelle Richtlinien und Sicherheitsdaten erhalten als auch Daten mit WildFire und dem Cortex™ Data Lake austauschen.

CORTEX XDR™
BY PALO ALTO NETWORKS

Oval Tower, De Entrée 99-197
1101 HE Amsterdam
Niederlande

Telefon: +31 20 888 1883

www.paloaltonetworks.de

cortex-xdr-endpoint-protection-solution-guide-b-120319-de