Cisco AMP vs. Palo Alto Networks

Überblick

Cisco Advanced Malware Protection (AMP) ist die einzige Lösung, die über die Point-in-Time-Erkennung von Malware hinausgeht und durch kontinuierliche Analysen Retrospective Security ermöglicht. Folglich ist AMP die einzige Lösung, die Schutz über das gesamte Angriffskontinuum hinweg bietet – vor, während und nach einem Angriff. AMP bietet die kontextbezogene Datenerfassung und Transparenz, die auf dem Endgerät, Mobilgeräten, im Netzwerk und auf E-Mail- und Web Security-Appliances benötigt werden, um einen Angriff unter Kontrolle zu bekommen, einzugrenzen und zu beseitigen, bevor er Schaden anrichten kann.

Palo Alto Networks bietet Advanced Endpoint Protection (Traps genannt – aufgrund der Übernahme von Cyvera) und WildFire, ihr Produkt für erweiterten Malware-Schutz, an, beides als Abonnement-Add-On für eine PAN NGFW. Die standardmäßige Bereitstellung von WildFire ist ein Public Cloud-Service mit einer privaten Option über deren WF-500-Appliance.

WildFire identifiziert nur bekannte Malware und besitzt nur begrenzte Cloud-Informationen und bietet keine Problembehebung oder retrospektive Funktionen, keinerlei Transparenz nach einem Angriff, keine Informationen zur horizontalen Ausbreitung, zu Endgeräten oder Mobilgeräten, ausführbaren oder binären Dateien. Wenn also eine Bedrohung auftritt, liefert PAN keinerlei Informationen zur Reichweite des Angriffs. Während Cisco AMP laut einem Test von NSS Labs in Sachen Bedrohungserkennung führend ist, ist WildFire ungeprüft.

Traps identifiziert 23 der bekannten Exploit-Pfade, die von Angreifern gegen Windows verwendet werden. Bei Traps muss erst ein Angriff gegen einen Windows-Client ausgeführt werden, damit er erkannt werden kann. Traps ermöglicht die Sammlung von forensischen Beweisen nur zum Zeitpunkt der Verhinderung. Daher können der Zweck des Angriffs oder dessen gesamter Ablauf nicht vollständig aufgedeckt werden. Traps schützt vor Windows-Exploits, nicht vor Malware. Schutz vor Malware, über eine einfache Richtlinie hinaus, wird weiterhin von der WildFire-Cloud übernommen. Traps erfordert ein dediziertes/separates Management-System – keine Integration in vorhandene PAN-Management-Tools.

Vorteile von Cisco AMP	
Beispiellose Transparenz und Kontrolle	Bestimmung von Eintrittspunkt und Ausbreitung, Bestätigung, Analyse und Beseitigung von Malware über Netzwerk und verteilte Endgeräte hinweg
Kurze Wiederherstellungszeiten	Integrierte Problembehebung ermöglicht eine drastische Reduzierung der Zeit von der Entdeckung bis zur Eindämmung
Durchgängige Analysen	AMP ist die einzige Lösung, die nach einer ersten Point-in-Time-Einstufung kontinuierlich Datenverkehr und Dateien überwacht, die das Netzwerk durchlaufen. Dies aktiviert die Retrospective Security-Tools von AMP.
Retrospective Security	Über retrospektive Warnmeldungen werden Ihre Kunden informiert, wenn sich die Einstufung ändert. Indications of Compromise informieren über Muster von verdächtigen Aktivitäten.
Prävention von Angriffen	Schutz vor Exploits, die auf Schwachstellen zurückzuführen sind und zu Infektionen führen können
Wertvorteil	Kostengünstige Optionen für Netzwerke und Endgeräte

Wichtigste Einwände

Transparenz

Palo Alto Networks
Nur Point-in-Time-Erkennung
Bewertung einer Datei nur zu einem bestimmten Zeitpunkt über eine Netzwerkübersicht. Keinen Einblick in Nicht-Windows-Endgeräte oder mobile Geräte.

Cisco AMP
Point-in-Time-Schutz + kontinuierliche Analysen
Verbesserte Transparenz vor, während und nach einem Angriff
- Ermöglicht Retrospective Security mit AMP für Endgeräte, Netzwerk oder AMP für ASA mit FirePOWER Services

Ursachenanalyse

Palo Alto Networks
Weiteres Produkt erforderlich
WildFire und Traps liefern keine Erkenntnisse zur Ursache eines Angriffs.
Nach einem Angriff findet keine Identifizierung statt.

Cisco AMP
Kontextinformationen für alle Dateien/Aktivitäten
- Speicherung des Kontexts für spätere Analysen
- Parent-Child-Beziehungen erleichtern die Ursachenidentifikation

Bestimmung der Reichweite

Palo Alto Networks
eingeschränkte Transparenz
WildFire-Informationen zur Reichweite sind begrenzt auf Befehls- und Kontrollstrukturen – Traps liefert keine zusätzlichen Informationen.

Cisco AMP
Beispiellose Transparenz; liefert Echtzeitergebnisse
Findet alle betroffenen Hosts mithilfe von Datei-Hashwerten oder eines anderen Attributs innerhalb von Sekunden; verwendet Device und File Trajectory um den Ursprung einer bösartigen Datei zu ermitteln und herauszufinden, wo sie sich befindet und was sie tut.

Problembehebungsfunktionen

Palo Alto Networks
Erfordert ein weiteres Tool oder zusätzliches Incident Response-Team
Mehr Zeitaufwand, Komplexität und Kosten

Cisco AMP
Integrierte Problembehebung
Beendet Outbreaks im ganzen Unternehmen mit einem einfachen, dynamischen Richtlinien-Update.

Produktangebote

Cisco	Palo Alto Networks
AMP für WSA	Direkter Vergleich
AMP für ESA	WildFire-Plattform
AMP für Endgeräte	Traps-Plattform
AMP für Netzwerke	Firewall (PA-Serie) Virtualisierte PA-Firewall (VM) PA-7050 Firewall NGFW-Management-Systeme
AMP für ASA mit FirePOWER Services	

Zentrale Funktionen im Vergleich

Funktion	Cisco AMP	Palo Alto
File Trajectory	★★★★★	-
Outbreak-Kontrolle	★★★★★	-
Dateianalyse	★★★★★	★★★
Malware-Erkennungs-Engine	★★★★★	★
Berichtsfunktionen	★★★★★	★★
Quarantäne-Funktion	★★★★★	★
Infektions-Geolokation	★★★★★	★
Widerstandsfähig gegen Sandbox-Umgehungen	★★★★★	-
SSL-Überprüfung	★★★★★	★★
Cloud-basierte Analysen	★★★★★	★★
Effektivität der Absicherung*	99 %	Nicht geprüft
Gesamtbetriebskosten pro geschätztem Mbit/s*	ca. 230 USD	Nicht geprüft

*(NSS Labs, Breach Detection Systems SVM, 2014)

Comstor – Ihr Ansprechpartner:
t: +49 (0) 30 34603 - 331
e: security.de@comstor.com

Cisco AMP vs. Palo Alto Networks

Wettbewerbsstrategie

- Wir sollten uns IMMER auf die Einkäufer von Sicherheitslösungen konzentrieren und mit der Prävention von Sicherheitsrisiken beginnen. Stellen Sie daher sicher, dass Sie sich an einen SecOPS-Beteiligten wenden, um das bedrohungsorientierte Angebot zu betonen. PAN zielt darauf ab, Sicherheit „einfach" zu machen und hat es auf Netzwerkmitarbeiter abgesehen, die sich nun um die Sicherheit kümmern und nicht mit der Komplexität eines wahren bedrohungsorientierten Sicherheitssystems vertraut sind. PAN verwendet daher keine erweiterten Funktionen, die nötig wären, um Schutz gegen moderne Bedrohungen zu bieten.
- Echte Sicherheitslösungen wie Cisco AMP bieten Schutz vor, während und nach einem Angriff. Palo Alto platziert die Firewall als Grundlage ihrer Sicherheitslösung. Eine Firewall ist hauptsächlich ein „Richtlinienkontrollgerät", das sich vor allem auf den Zeitraum vor einem Angriff konzentriert.
- Cisco ist sich im Klaren, dass keine Point-in-Time-Technologie alleine hundertprozentig vor Bedrohungen schützen kann. AMP bietet umfassende Transparenz, damit Ihre Kunden bei einem Angriff die Bedrohung schnell beseitigen können. PAN ist überzeugt, dass eine Point-in-Time-Firewall und ein Add-On-Agent nur für Windows zu hundert Prozent effektiv ist. So etwas wie eine einzige Lösung zur Erkennung von Bedrohungen existiert nicht.
- Cisco AMP bietet kontinuierliche Analysen, Ursachenidentifikation, Reichweitenbestimmung in Echtzeit und integrierte Problembehebung. PAN WildFire Traps und NGFW bieten nichts davon.
- PAN verfügt weder über korrelierte Endgerätetransparenz noch über eine Funktion zur Nachverfolgung eines Ausbruchs. Daher gibt es im Falle eines Angriffs keine Möglichkeiten zur Eindämmung. Beim 24. Angriffstyp oder einem Angriff auf eine Nicht-Windows-Plattform erweist sich die Traps-Plattform als nutzlos und vermittelt Kunden ein falsches Gefühl von Sicherheit.
- Betonen Sie die Dominanz von Cisco/Sourcefire bei NSS-Tests im Bereich Drittanbieterlösungen für Firewalls, bei denen Cisco PAN durchgehend in allen Bereichen schlägt: Schutz, Leistung und Gesamtbetriebskosten. WildFire ist als Client zur Bedrohungserkennung ungeprüft. NGFW-Tests von NSSL Labs haben erneut die Dominanz über PAN bewiesen.
- VERMEIDEN Sie es, sich auf einen Kampf um Ausschreibungen einzulassen – PAN sind die Meister darin und sie besitzen Funktionen in ihrer Benutzeroberfläche, die nur dem Zweck dienen, ein Kontrollkästchen auf einem Ausschreibungsformular aktivieren zu können.
- Obwohl PAN für Netzwerk- und Firewall-Funktionen beliebt ist, ist der Malware-Schutz mit WildFire sehr ineffizient. Es können nur kleine 32-Bit-Binärdateien bearbeitet werden, es gibt zahlreiche Sicherheitsbedenken und er wurde von keinem Drittanbieter geprüft. Die meisten Kunden, die PAN verwenden, nutzen daher für die Erkennung von Sicherheitsrisiken auch ein anderes Tool wie FireEye.
- Obwohl das Advanced Endpoint-Tool vorgibt, zukunftssicher zu sein, werden nur 30 % der heute weltweit genutzten Endgeräte abgedeckt. Es ist davon auszugehen, dass künftig mehr und mehr primäre Clients keine Windows-Plattformen sind. Ausschließlicher Schutz für Windows ist ein Nachteil von Palo Alto.

Vorteile von Cisco AMP

Kontinuierliche Analysen und Retrospective Security
Cisco AMP verwendet kontinuierliche Analysen, um Dateien zu überwachen, selbst wenn diese bereits untersucht und als „gut" eingestuft wurden. AMP führt retrospektive Überprüfungen durch und informiert den Kunden, wenn der Status einer „guten" Datei sich ändert. Die Kombination von AMP aus Cisco-Sourcefire Collective Security Intelligence, Point-in-Time-Schutz und integrierter Retrospective Security durch kontinuierliche Analysen bietet Schutz über das gesamte Angriffskontinuum hinweg und schützt dort, wo herkömmliche Point-in-Time-Systeme versagen.

Palo Alto bietet nur Point-in-Time-Erkennung während eines Angriffs. Bei Point-in-Time-Erkennungsmethoden wird die Datei nur einmal überprüft (erste Beobachtung). Erfolgt keine Verurteilung, geht es über den Ereignishorizont hinaus, ohne das Gesehene gespeichert zu haben. Wenn dies geschieht, kann eine einfache Point-in-Time-Lösung nichts tun, um den Benutzer vor Angriffen zu schützen, die polymorph sind oder Standby-Techniken verwenden. Traps lässt Point-in-Time auf eine neue Weise beängstigend wirken; es ist ein Angriff erforderlich, damit Daten am Windows-Endgerät gesammelt werden können. Dies bedeutet, dass sich das Ausmaß des Sicherheitsrisikos nicht verbessert hat, wenn die Bedrohung der Firewall entgeht.

Überlegene Malware-Erkennung
Cisco AMP verwendet ein proprietäres Cloud-basiertes Erkennungssystem, das Big Data-Analysen verwendet, um den Status einer Datei zu bestimmen. Dieses Erkennungssystem umfasst Techniken für maschinelles Lernen, die mehr als 400 Funktionen jeder einzelnen Datei bewerten. NSS Labs hat AMP aufgrund der Überlegenheit auf sieben verschiedenen Ebenen der Malware-Erkennung zu einer führenden Lösung im Bereich Sicherheitseffektivität ernannt.

Traps von PAN übernimmt nur die Prävention von Windows-Exploits und ist für Malware-Schutz auf WildFire angewiesen. WildFire von PAN wurde von keinem Drittanbieter geprüft. WildFire bewertet eine Datei auf der Grundlage von 130 verschiedenen Merkmalen, bei Cisco AMP sind es 400 Merkmale. PAN ist normalerweise vollständig IP-basiert- und bietet keine Retrospective Security, keine C&C-Protokolle, begrenzte Identifikation von Client-Anwendungen und weder ein Betriebssystem noch einen Router und Identifikation von mobiler Malware.

Umfassende Übersicht zur Bedrohungsausbreitung
Die AMP-Konsole bietet eine zentrale Übersicht zum Verhalten von Malware und Outbreaks über Netzwerke, Endgeräte, sichere Gateways, mobile Geräte und virtuelle Systeme hinweg. Mithilfe von Datenanalysen und Trajectory-Tools können Kunden die Ursache einer Infektion sowie Schweregrad und Ausbreitung eines Outbreaks im Netzwerk bestimmen.

PAN bietet keine kontextbezogene Transparenz. Es konzentriert sich hauptsächlich auf Netzwerkbedrohungen (da es sich lediglich um ein Firewall-Add-On handelt) und Windows-Exploits. Daher ist es für Bedrohungen von Endgeräten und mobilen Geräten blind.

Nachteile von Palo Alto

Palo Alto bietet begrenzte Bedrohungsinformationen und keinerlei Threat Management Workflow-Funktionen für ein SecOPS-Team und wird daher immer zuerst ihr NGFW-Produkt einführen, da es sich bei WildFire um ein Add-On für ihre Firewall handelt. Daher stammen Einwände von PAN üblicherweise aus der Firewall-Perspektive.

Cisco Management-Komplexität/Kein Unified Manager
PAN bietet einfaches, einheitliches Management in einer zentralen Benutzeroberfläche. Bei einer AMP-Lösung müssen Kunden mehr Benutzeroberflächen verwalten.

Antwort: Tatsächlich benötigt eine PAN-Lösung mehr Benutzeroberflächen als Cisco, um einen ähnlichen Funktionsumfang wie eine Cisco AMP-Lösung zu erzielen. Zum Beispiel 1) wenn ein Kunde AMP für Netzwerke bereitstellt, benötigt er 1 Schnittstelle, FireSIGHT Management Center. Um die Funktionen von AMP für Netzwerke bereitzustellen, müssen Kunden mit PAN 2 Benutzeroberflächen bereitstellen: PANOS und WildFire. 2) Wenn ein Kunde AMP für Netzwerke und Endgeräte bereitstellen möchte, kann er FireSIGHT Management Center und die FireAMP-Konsole bereitstellen. Um ähnliche Funktionen mit PAN zu erhalten, benötigt er PANOS, WildFire, Cyvera Client Agent, SIEM/Forensics und Schwachstellenmanagement. Und dennoch ist die AMP-Lö sung umfassender und zuverlässiger als PAN-Angebote.

AMP ist nur ein Forensik-Tool
AMP schützt Unternehmen nicht, es wird nur nach einem Angriff verwendet, um den Schaden zu beseitigen. PAN NGFW + WildFire bieten Schutz über eine einheitliche Architektur.

Antwort: In Wahrheit bietet AMP Schutz vor, während und nach einem Angriff. „Vor" mithilfe von zuverlässigen Bedrohungsinformationen, die von Cisco Collective Security Operations, Talos, ClamAV und SNORT Open Source-Communities stammen; „Während" mithilfe von Point-in-Time-Schutz mit Signaturen, adaptivem Sandboxing als Teil der ThreatGRID-Integration und IPS-/Firewallschutz mit AMP für Netzwerke oder AMP für ASA mit FirePOWER Services; und „Nach" mit umfassender Transparenz und Kontrolle über Bedrohungen im Netzwerk und sogar Fehlerbehebungen mit einem Klick bei AMP für Endgeräte.

PAN deckt nicht das gesamte Angriffskontinuum ab