TRAPS

Omicron Seit 1995

paloalto NETWORKS®

Advanced Endpoint Protection

Traps™, die Advanced Endpoint Protection von Palo Alto Networks®, ersetzt ältere Antivirussysteme durch multimethodische Präventionsmechanismen, die in einen einzelnen, einfachen Agenten integriert sind, der Endpunkte vor bekannter und unbekannter Malware und Exploits schützt. Ob eigenständig oder als Teil der Palo Alto Networks-Next-Generation-Sicherheitsplattform implementiert, stoppt Traps zielgerichtete und technisch ausgereifte Bedrohungen wie Ransomware, ohne dafür Signaturen zu betrachten.

Trotz ihren fortlaufenden Investitionen in ältere und zukunftsweisende Antiviruslösungen erleben Unternehmen verstärkt Sicherheitsverletzungen und Ransomware-Angriffe. Die Sicherheitsbranche insgesamt und im Speziellen ältere Antivirussysteme hatten große Schwierigkeiten, bzw. waren immer häufiger nicht in der Lage, die Sicherheitsverletzungen erfolgreich abzuwehren, die von Endpunkten ausgingen.

Die Versuche, die Effizienz von Antivirussystemen zu verbessern und den Schwerpunkt der Sicherheitsbranche auf die Bereiche Ermittlung und Antwort zu verlagern, führten lediglich zu einer schrittweisen Verbesserung des Endpunktschutzes. Dabei wurden zusätzliche Schwachstellen geschaffen, die die Effizienz der Systeme im Hinblick auf die Vermeidung von Sicherheitsverletzungen einschränken.

Traps sichert Endpunkte über einen einmaligen multimethodischen Präventionsmechanismus. Sicherheitsverletzungen und Ransomware-Angriffe, die auf Malware und Exploits setzen, ob bekannt oder unbekannt, werden blockiert, bevor sie in macOS®- oder Windows®-Endpunkte wie zum Beispiel Laptops, Desktops und Server eindringen.

Multimethodischer Malware-Schutz

Traps verhindert die Ausführung schädlicher ausführbarer Dateien, DLLs und Office-Dateien mittels eines einmaligen multimethodischen Schutzansatzes, bei dem einerseits die Angriffsfläche verkleinert und andererseits die Präzision des Malware-Schutzes verbessert wird. Für diesen Ansatz werden mehrere Schutzmethoden vereint, um die Infektion von Endpunkten durch bekannte und unbekannte Malware unmittelbar zu verhindern:

1. **WildFire – Threat Intelligence:** Traps nutzt die gesammelten Informationen von Palo Alto Networks WildFire™, dem cloudbasierten Bedrohungsanalyseservice. Bei WildFire handelt es sich um das weltweit größte verteilte Sensorsystem, das den Schwerpunkt auf die Ermittlung und Vermeidung unbekannter Bedrohungen legt. Dabei leisten über 17.000 Kunden aus Unternehmen, Regierungen und Dienstanbietern einen Beitrag zur kollektiven Immunität aller anderen Benutzer, und zwar über Endpunkte, Netzwerk und Cloudanwendungen hinweg.
2. **Lokale Analyse mithilfe von maschinellem Lernen:** Diese Methode liefert sofort ein Verdikt zu sämtlichen unbekannten ausführbaren Dateien, DLLs oder Office-Dateien, bevor deren Ausführung gestattet wird. Traps untersucht im Bruchteil einer Sekunde Hunderte von Dateieigenschaften, ohne sich rein auf Signaturen, Scans oder Verhaltensanalysen zu verlassen.
3. **WildFire-Inspektion und -Analyse:** Zusätzlich zur lokalen Analyse setzt Traps auf WildFire, um eine umfassende Inspektion unbekannter Dateien durchzuführen, die über das reine maschinelle Lernen hinausgeht. Wird eine neue Bedrohung ermittelt, werden in nur fünf Minuten die Verhinderungsmechanismen für die gesamte Palo Alto Networks-Next-Generation-Sicherheitsplattform implementiert, alle Traps-Kunden eingeschlossen, und das ganz ohne menschliche Interaktion. WildFire kombiniert die Vorteile von vier unabhängigen Technologien für die realistische und gegenüber Ausweichmanövern nicht anfällige Entdeckung, die auf dynamische und statische Analysen, maschinelles Lernen und Bare-Metal-Analysen setzt.
4. **Granularer Schutz von untergeordneten Prozessen:** Traps bietet feinabgestimmte Steuerungsmechanismen für die Ausführung legitimer Prozesse, wie zum Beispiel Scriptmodule oder Befehls-Shells, die auch missbräuchlich eingesetzt werden können. Diese Technologie wird von Ransomware und anderen fortschrittlichen Bedrohungen eingesetzt, um herkömmliche Schutzmaßnahmen zu umgehen.
5. **Verhaltensbasierter Ransomware-Schutz:** Zusätzlich zum vorhandenen multimethodischen Schutz, einschließlich Exploit-Schutz, lokaler Analysen und WildFire, überwacht Traps das System auf das Verhalten von Ransomware und blockiert den Angriff sofort, wenn dieser erkannt wird, und verhindert die Entschlüsselungen von Kundendaten.

Darüber hinaus ermöglicht Traps Unternehmen die Ausführung von Anwendungen für Positiv- und Negativlisten, Definition von Richtlinien zur Einschränkung für die Anwendungsausführung sowie die Option, Malware unter Quarantäne zu stellen, damit die unbeabsichtigte Verbreitung verhindert wird.

Multimethodischer Exploit-Schutz

Um eine Anwendung erfolgreich zu manipulieren, muss ein Exploit stets eine Reihe dieser Exploit-Techniken verwenden. Anstatt sich auf die Millionen von individuellen Angriffen zu konzentrieren, legt Traps den Schwerpunkt auf die Kerntechniken von Exploits, die in der Regel bei allen derartigen Angriffen genutzt werden. Durch die Verhinderung eines Angriffs unterbricht Traps den Angriffsverlauf und macht die Bedrohung auf diese Weise unschädlich.

Der Exploit-Schutz von Traps setzt auf verschiedene Methoden:

1. **Vor-Exploit-Schutz:** Traps verhindert die Technologien zur Profilierung von Schwachstellen, auf die Exploit-Kits setzen, noch bevor diese einen Exploit-Angriff starten können. Durch das Blockieren dieser Technologien verhindert Traps, dass Angreifer verletzbare Endpunkte und Anwendungen ins Visier nehmen, die Angriffe werden somit im Keim erstickt.
2. **Technologiebasierter Exploit-Schutz:** Traps verhindert sowohl bekannte als auch Zero-Day-Exploits, indem die Exploit-Techniken blockiert werden, die Angreifer für die Manipulation von Anwendungen nutzen. Obgleich es Tausende von Exploits gibt, setzen alle auf eine kleine Anzahl an Exploit-Techniken, die sich nur selten ändern. Traps blockiert diese Techniken und verhindert auf diese Weise Exploit-Versuche, bevor diese Endpunkte kompromittieren können.
3. **Kernel-Exploit-Schutz:** Traps verhindert Exploits, die Schwachstellen im Betriebssystemkernel nutzen, um Prozesse mit eskalierten Privilegien auf Systemebene zu schaffen. Außerdem verhindert Traps Injektionstechnologien, bei denen Schadcode über den Kernel geladen und ausgeführt wird, wie das beispielsweise in den WannaCry- und NotPetya-Angriffen der Fall war. Auf diese Weise blockiert Traps technisch ausgereifte Angriffe, die auf das Betriebssystem abzielen bzw. davon selbst ausgehen.

Wirklicher Schutz für Mac

Traps sichert macOS-Systeme und ersetzt ältere Antivirussysteme durch einen multimethodischen Verhinderungsansatz, bei dem Endpunkte gegen bekannte und unbekannte Malware und Exploits abgesichert werden, bevor Systeme in Mitleidenschaft gezogen werden. Diese Herangehensweise steht vorhandenen signaturbasierten Antivirussystemen und Sicherheitslösungen der nächsten Generation für macOS gegenüber, die Sicherheitsverletzungen nicht durch das Blockieren von Malware und Exploits verhindern können und den Endpunkt so verwundbar machen.

Next-Generation-Sicherheitsplattform

Als elementarer Bestandteil der Next-Generation-Sicherheitsplattform erfolgt ein gegenseitiger Austausch der Informationen zu Bedrohungen zwischen Taps und WildFire. Jede Plattformkomponente (wie z. B. Firewalls der nächsten Generation und Traps), die für die globale Kundencommunity von Palo Alto bereitgestellt wird, tauscht auf fortlaufender Basis Informationen zu Bedrohungen mit WildFire aus. Die Kunden von Traps erhalten Zugriff auf diesen Pool an Informationen zu Bedrohungen sowie die vollständigen Malware-Analysefunktionen, die WildFire bietet.

Die automatische Umprogrammierung und Konvertierung von Threat Intelligence in Schutzmaßnahmen entzieht Angreifern die Grundlage, um ein System mit unbekannter und fortschrittlicher Malware zu infizieren. Ein Angreifer kann jede Art von Malware in einer Umgebung, in der Traps bereitgestellt wird, allerhöchstens einmal nutzen, und es bleiben ihm nur wenige Sekunden für einen Angriff, bevor dieser von WildFire unwirksam gemacht wird.

Traps nutzt Protokolle gemeinsam mit der Netzwerksicherheitsverwaltung von Panorama™ und bietet Sicherheitsteams so die Möglichkeit, Endpunktsicherheitsprotokolle im gleichen Kontext wie ihre Firewallprotokolle anzuzeigen. Auf diese Weise ist es einfacher, eigenständige Vorgänge, die im Netzwerk und für Endpunkte beobachtet werden, in einem Gesamtbild für Sicherheitsvorfälle in der gesamten Umgebung zusammenzuführen. So lassen sich Bedrohungen ermitteln, die anderenfalls unter Umständen unter dem Radar unentdeckt geblieben wären.

Preisgekrönt, in der Branche anerkannt und Compliance-fähig

Traps hat bereits mehrere Auszeichnungen erhalten, im Folgenden erhalten Sie einen Überblick über Auszeichnungen der letzten Zeit. Außerdem genießt Traps eine große Anerkennung in der Branche:

- **„100-Prozentige Erkennung realer Angriffe“** – Traps erkannte 100 % aller realen Angriffe und erhielt die beste Leistungsbewertung in einer von AV-Test im 3. Quartal 2017 in Auftrag gegebenen Bewertung.
- **„Visionär“** – Gartner bezeichnete Traps in seinem Bericht „Magic Quadrant for Endpoint Protection Platforms“ 2017 als „Visionär“.
- **„Gesamtsieger und Produkt des Jahres 2016“** – Traps erhielt die begehrte CRN-Auszeichnung zum Produkt des Jahres und stand dabei in Konkurrenz zu allen im Rahmen des Wettbewerbs evaluierten Sicherheitsangeboten für Endpunkte.
- **„Anerkanntes Produkt für Unternehmen“** – Die unabhängige Organisation AV-Comparatives, die Tests und Bewertungen von Antivirussoftware durchführt, verlieh Traps im erstmals durchgeführten „Vergleich von Sicherheitsprodukten der Zukunft“ seine Auszeichnung.
- **„Leistungsstarkes Tool“** – Forrester® Research bezeichnete Traps (V 3.3) in seinem Bericht „The Forrester Wave™: Endpoint Security Suites“ 4. Quartal 2016, als „Leistungsstarkes Tool“.

Traps ist außerdem anerkannt dafür, dass wir unsere Kunden dabei unterstützen, dass sie ihren Compliance-Anforderungen gerecht werden, indem sie ihr Antivirussystem austauschen. Coalfire®, Weltmarktführer im Bereich Cyberrisikomanagement- und Compliance-Services, führte eine unabhängige Bewertung von Traps durch, im Hinblick auf die Anforderungen, die vom PCI DSS (Payment Card Industry Data Security Standard, dem Regelwerk zur Abwicklung von Kreditkartentransaktionen) und der Sicherheitsregel des HIPAA (Health Insurance Portability and Accountability Act, dem US-Bundesgesetz zur Vertraulichkeit medizinischer Informationen) vorgegeben werden, sowie die Anforderungen der Regel zur Benachrichtigung bei Sicherheitsverletzungen des US-Bundesgesetzes HITECH (Health Information Technology for Economic and Clinical Health) aus dem Jahr 2009 und der Omnibus-Regel aus dem Jahr 2013.

Coalfire stellt in seinen Berichten fest, dass jedes Unternehmen, das derzeit auf ältere Antivirussysteme setzt, um die Anforderungen von PCI DSS oder HIPAA/HITECH zu erfüllen, diese Lösung vertrauensvoll durch Traps ersetzen kann, ohne dass die Compliance dabei gefährdet wird.

Systemanforderungen und Betriebssystemunterstützung

Traps unterstützt Endpunkte (Desktops, Server, Steuerungssysteme in der Industrie, virtuelle Desktopinfrastrukturkomponenten und eingebettete Systeme), die unter Windows- und macOS/Mac® OS X®-Betriebssystemen laufen. Eine vollständige Liste der Systemanforderungen und unterstützten Betriebssysteme finden Sie auf der Webseite zur Traps-Kompatibilitätsmatrix.

paloalto NETWORKS®

3000 Tannery Way
Santa Clara, CA 95054

Zentrale: +1/408/75 34 000
Vertrieb: +1/866/320/4788
Support: +1/866/89 89 087

www.paloaltonetworks.com