Unternehmensvorteile

- **Befreien Sie Ihr Unternehmen von Kosten und Aufwand eines eigenständigen IPS.** Nutzen Sie die Vorteile von Snort und anderen leistungsstarken IPS-Funktionen, die in unsere NGFW eingebettet ist. So wird ein einheitliches Regelwerk mit grundlegenden Sicherheitsrichtlinien möglich.
- **Verbessern Sie die Erkennung von Angriffen, damit Ihre Organisation geschützt ist.** Überprüfen Sie Ihren gesamten Datenverkehr auf Bedrohungen – unabhängig von Port, Protokoll oder Verschlüsselung.
- **Verwalten Sie Sicherheitslücken und Patches mit geringerem Aufwand.** Blockieren Sie bekannte Malware, das Ausnutzen und C2 automatisch.
- **Nutzen Sie alle Vorteile der Erkennung und Abwehr von Bedrohungen** ohne Leistungsverlust.

Threat Prevention

Die herkömmliche Intrusion Prevention hat sich nicht mehr weiterentwickelt.

Organisationen haben mit ständigen Angriffen aus verschiedensten Motiven zu kämpfen, wie etwa Profit, Ideologie/Hacktivismus oder sogar interne Konflikte und Unzufriedenheit. Moderne Hacker sind finanziell und technisch hervorragend ausgestattet. Sie wenden schwer erkennbare Taktiken an, um in Netzwerke einzudringen, die sie dann mit hoher Frequenz professionell attackieren. Ihre Methoden erlauben ihnen zielgerichtete Angriffe mit raffinierten Abläufen – so gelingt es ihnen, in Organisationen einzudringen, sich unerkannt zu bewegen und wertvolle Daten zu stehlen. Dabei bleiben sie für die herkömmliche Abwehr unsichtbar.

Noch gravierender ist, dass herkömmliche Intrusion Prevention- oder Abwehrsysteme (IPS/Intrusion Detection System, IDS) noch immer Verteidigungsstrategien aus einer Zeit nutzen, in der die Bedrohungslage eine völlig andere war. Der Datenverkehr wird nur an bestimmten Ports überprüft. Das Hinzufügen von Geräten mit einer einzigen Funktion zum Verteidigungsarsenal kann bestimmte Probleme lindern. Allerdings leidet darunter auch die Leistung und die allgemeine Transparenz. Darüber hinaus führt eine Vernachlässigung der Grundlagen häufig zu starken Belastungen für ein Sicherheitsteam, das nicht angemessen ausgestattet ist, um Sicherheitslücken zu beheben und Datenlecks zuverlässig zu schließen. In einer Ponemon-Umfrage von 2019 äußerten 67 % der Befragten, sie hätten zu wenig Zeit und Ressourcen, um alle Sicherheitslücken zum Schutz vor Datenlecks zu schließen.[1]

Schützen Sie Ihr Netzwerk vor Comprehensive Exploit, Malware und Command and Control

Der Bedrohungsschutz von Palo Alto Networks Threat Prevention legt mehrere Schutzschichten um ihr Netzwerk, sodass auf Bedrohungen in jeder Phase eines Angriffs reagiert werden kann. Zusätzlich zu den traditionellen IPS-Fähigkeiten ist nur Threat Prevention in der Lage, Bedrohungen an sämtlichen Ports zu entdecken und zu blockieren, anstatt nur Signaturen anhand einer Liste mit einer begrenzten Anzahl vorher festgelegter Ports aufzurufen.

Unsere Kunden auf der ganzen Welt teilen Informationen über Bedrohungen. So gelingt es, die Erfolgsquote moderner Angriffe stark zu reduzieren, da diese bereits kurz nach ihrer ersten Entdeckung gestoppt werden. Threat Prevention profitiert von unseren anderen cloudbasierten Sicherheitsabonnements, deren tägliche Aktualisierungen es ermöglichen, Exploits, Malware, schädliche URLs, Command and Control (C2), Spyware usw. abzuwehren. Als unverzichtbarer Bestandteil jeder Palo Alto Networks NGFW kann Threat Prevention im Verbund mit anderen Abonnements von Palo Alto Networks den Schutz vor neuen, bisher unbekannten Bedrohungen nahezu in Echtzeit gewährleisten. Zu diesen Abonnements zählen der WildFire®-Malwareschutz gegen unbekannte dateibasierte Bedrohungen, das URL-Filtering gegen Attacken aus dem Web, DNS-Sicherheit gegen Attacken, bei denen der Domain Name Service verwendet wird, sowie IoT-Sicherheit für mehr Transparenz und Kontext auf privaten Geräten.

Wichtige Funktionen

Anwendung aktivieren, Bedrohung abwenden

Anwendungen spielen eine zentrale Rolle, wie Unternehmen ihre Geschäfte abwickeln. Daher wurde ihre Verfügbarkeit für die Benutzer mithilfe von Netzwerken erhöht, wobei verschlüsselte Kanäle über nicht standardmäßige Ports verwendet (häufig mit der Absicht, eine Überprüfung durch eine Firewall zu vermeiden) und die Ports häufig gewechselt wurden, damit die Benutzer stets Zugriff hatten.

Leider wird bei modernen Angriffen genau dieses Vorgehen ausgenutzt, um unerkannt in Netzwerke einzudringen. Die Angreifer gelangen über Tunnel in Anwendungen, verstecken sich in verschlüsseltem Datenverkehr und greifen ungeschützte Ziele an, um sich in einem Netzwerk festzusetzen und bösartige Aktivitäten zu starten.

Wir schützen Ihr Netzwerk vor solchen Bedrohungen, indem wir mehrere Schutzschichten bereitstellen, mit denen wir die Bedrohung in jeder Phase des Angriffs abwehren. Zusätzlich zu den traditionellen IPS-Fähigkeiten ist Threat Prevention in der Lage, Bedrohungen an sämtlichen Ports zu entdecken und zu blockieren, anstatt Signaturen anhand einer Liste mit einer begrenzten Anzahl vorher festgelegter Ports aufzurufen. Mithilfe der Technologien User-ID™ und App-ID™ stellen unsere ML-gestützten NGFWs zu jedem Datenverkehr über sämtliche Ports einen Kontext her. So gerät niemals eine Bedrohung aus dem Blickfeld der Threat Prevention-Engine, und zwar unabhängig von der eingesetzten Umgehungsmethode.

Der Datenverkehr von Unternehmen wird immer häufiger durch TLS-/SSL-Verschlüsselung unsichtbar gemacht. Das verringert die Transparenz, was wiederum Angreifer nutzen, um Attacken durchzuführen – dies bedeutet ein erhöhtes Risiko für Ihr Unternehmen. Unsere ML-basierten NGFWs bieten native Entschlüsselung. So ist es möglich, mithilfe von Richtlinien den TLS-/SSL-Datenverkehr selektiv zu entschlüsseln und zu kontrollieren, um eine angemessene Balance zwischen Sicherheit und Leistung zu erhalten.[2]

Bedrohungen in jeder Phase abwenden

Im Lauf der Jahre konnten sehr viele Angriffe darauf zurückgeführt werden, dass Abwehrtools mit nur einem spezifischen Zweck von den Angreifern überwunden wurden. Das Threat Prevention-Abonnement garantiert umfassenden Schutz, da es eng mit unseren ML-basierten NGFWs integriert ist und so verschiedene Abwehrmechanismen zusammenführt:

- **Die heuristische Analyse** deckt ungewöhnliche Paket- und Datenverkehrsmuster auf, wie etwa Port-Scans, Host-Sweeps und Denial-of-Service-Attacken (Nichtverfügbarkeit des Dienstes, DoS).
- **Einfach konfigurierbare, anpassbare Signaturen für Sicherheitslücken** versetzen Sie in die Lage, maßgeschneiderte Abwehrmittel für Ihr Netzwerk mit seinen speziellen Bedürfnissen zu entwickeln. Sie können sogar Regeln aus bekannten Open-Source-Formaten wie Snort und Suricata® importieren.
- **Weitere Möglichkeiten, sich vor Angriffen zu schützen**, wie etwa das Blockieren ungültiger oder nicht korrekt geformter Pakete, GP-Defragmentierung sowie TCP-Reassembly, schützen vor Umgehung und Verschleierung.

Palo Alto Networks verwendet nativ integrierte Abwehrtechnologien, damit Bedrohungen, die eine Technologie umgehen, durch eine andere abgewehrt werden können. Für einen effektiven Schutz sind Sicherheitsfunktionen notwendig, die eigens entwickelt wurden, um Informationen zu teilen und Kontext sowohl zum überprüften Datenverkehr als auch zu den identifizierten und blockierten Bedrohungen zu liefern.

In einem Durchgang auf alle Bedrohungen hin überprüfen

Die Threat Prevention-Engine setzt Standards, indem sie den Datenverkehr überprüft und einordnet sowie Malware und das Ausnutzen von Sicherheitslücken in einem einzigen Durchgang entdeckt und blockiert. Herkömmliche Bedrohungsschutztechnologien benötigen zwei oder mehr Überwachungsengines und mehrere Regelwerke, die jeweils einzeln verwaltet werden müssen. Dies führt zu größeren Verzögerungen und einem höheren Verwaltungsaufwand, während zugleich die Leistung enorm verringert wird. Wir verwenden ein einheitliches Signaturformat für alle Bedrohungen. Dies ermöglicht eine schnelle Verarbeitung, da sämtliche Analysen in einem einzigen, integrierten Scan stattfinden. So werden redundante Prozesse, die bei herkömmlichen Lösungen an der Tagesordnung sind, überflüssig.

1. „Gaps in Resources, Risk and Visibility Weaken Cybersecurity Posture“, Ponemon Institute, Februar 2019: https://www.balbix.com/app/uploads/Ponemon-Survey-Vuln-Management-.pdf.
2. Zum Durchsatz mit aktivierter Threat Prevention für eine bestimmte Palo Alto Networks-Firewall: paloaltonetworks.com/resources/datasheets/product-summary-specsheet.

Unsere Threat Prevention-Technologie durchkämmt jedes Datenpaket auf seinem Weg durch die Plattform und untersucht die Bytesequenzen im Paketheader ebenso gründlich wie jene innerhalb der Datei. Daraus lassen sich wichtige Details zum Paket ableiten, zum Beispiel die genutzte Anwendung, die Quelle und das Ziel, ob das Protokoll RFC-konform ist und ob die Payload einen Exploit oder Schadcode enthält. Zusätzlich zu den einzelnen Paketen analysieren wir auch den Kontext, der sich aus der Eingangsreihenfolge und der Sequenz mehrerer Pakete ergibt, um Verschleierungstechniken zu erkennen und abzuwehren. Das alles geschieht in einem einzigen Scan, sodass der Netzwerkverkehr nicht beeinträchtigt wird.

Intrusion Prevention optimal nutzen

Bei bedrohungsbasierten Schutzmaßnahmen werden Eindringversuche und Vermeidungstechniken einschließlich Portscans, Pufferüberläufen, Remote-Code-Ausführungen, Protokollfragmentierung und Verschleierung sowohl im Netzwerk als auch auf den verschiedenen Anwendungsebenen aufgespürt und blockiert. Die Schutzmaßnahmen beruhen auf dem Vergleich von Signaturen und dem Auffinden von Anomalien, wobei Protokolle dekodiert und analysiert werden. Die so gewonnenen Informationen werden verwendet, um Warnungen zu senden und verdächtige Datenverkehrsmuster zu blockieren. Beim zustandsbehafteten Vergleich von Mustern werden mehrere Pakete überprüft. Hierbei werden die Reihenfolge des Eingangs und die Abfolge berücksichtigt, damit der gesamte zugelassene Datenverkehr gutartig und frei von Vermeidungstechniken ist. Das ist unsere Intrusion Prevention-Technologie:

- **Analyse auf der Grundlage der Protokolldekodierung:** Zustandsbehaftete Dekodierung des Protokolls und anschließende intelligente Anwendung von Signaturen, um Exploits im Netzwerk und in Anwendungen aufzudecken.
- **Schutz auf der Basis von Protokollanomalien:** Nicht RFC-konforme Protokollnutzung wird entdeckt, ebenso überlange RI- und FTP-Logins.
- **Leicht konfigurierbare, anpassbare Signaturen für Sicherheitslücken** ermöglichen die Anpassung der Intrusion Prevention-Fähigkeiten an die speziellen Bedürfnisse Ihres Netzwerks.

Es gibt viele Möglichkeiten, eine einzige Sicherheitslücke auszunutzen. Daher beruhen unsere Intrusion Prevention-Signaturen auf der Sicherheitslücke selbst, was einen stärkeren Schutz gegen eine Vielzahl von Exploits ermöglicht. So kann eine einzige Signatur eine Vielzahl von Versuchen stoppen, eine bekannte Sicherheitslücke im System oder in einer Anwendung auszunutzen.

Maßgeschneiderte Signaturen für neue Bedrohungen

Threat Prevention bietet auch flexiblen Support für die Anpassung von Snort- und Suricata-Regeln, wodurch schon nach kurzer Zeit ein Schutz bei neu entdeckten Sicherheitslücken möglich wird. Dieser Support entspricht in Verbindung mit der fortlaufenden Entwicklung individueller Signaturen einem der wichtigsten Anwendungsfälle, macht isolierte IPS- oder IDS-Lösungen vollkommen überflüssig und trägt dazu bei, dass ein implizites IPS-bezogenes Ziel angestrebt wird. Die Bereitstellung von Signaturen für unbestätigte oder in naher Zukunft absehbare Sicherheitslücken fungiert als Notbehelf, bis die gesamte Software und alle Anwendungen Ihrer Organisation ein verifiziertes Update erhalten können. Mit dem Konversionssupport können Sie Snort- und Suricata-Regeln automatisch konvertieren, bereinigen, hochladen und verwalten. Dies ermöglicht Ihnen die Nutzung von Intelligence-Feeds und spart im Vergleich zu herkömmlichen signaturbasierten IPS-Technologien Zeit und Arbeitsaufwand. Sie können mithilfe exponierter APIs die Anwendung neuer Snort-Regeln in Ihrer gesamten Umgebung automatisieren.

Schutz gegen Malware

Der integrierte Malwareschutz nutzt durchsatzbasierte Signaturen anstelle von Hashblocks und blockiert Malware, ehe sie dem Zielhost gefährlich werden kann. Dies funktioniert sowohl mit bekannter Malware als auch mit künftigen Varianten, selbst wenn diese bisher nirgendwo gesichtet wurden. Unsere streambasierte Scanengines schützt Ihr Netzwerk, ohne die signifikante Latenz zu verursachen, die zu den größten Nachteilen von Antivirussystemen für Netzwerke auf Basis proxybasierter Scanengines zählt. Beim streambasierten Scannen wird der Datenverkehr überprüft, sobald die ersten Pakete einer Datei empfangen werden, womit sowohl Bedrohungen als auch Leistungseinbrüche, wie sie bei herkömmlichen isolierten Lösungen vorkommen, abgewendet werden. Einige der wichtigsten Antimalwarefunktionen:

- **Integrierte, streambasierte Erkennung und Abwehr** von Malware, die in komprimierten Dateien und Webinhalten verborgen ist.
- **Schutz gegen Durchsatz,** der in gängigen Dateitypen versteckt ist, wie etwa Office/Microsoft 365™-Dokumenten und PDFs.
- **Aktualisierungen von WildFire** garantieren den Schutz gegen Zero-Day-Malware.

Signaturen gegen Malware jeder Art werden direkt aus Milliarden von Mustern generiert, die Palo Alto Networks sammelt, einschließlich bisher unbekannter Malware, die an WildFire, unser Forschungsteam für Bedrohungen (Unit 42) sowie an forschende Drittanbieter und Technologiepartner weltweit gesendet wird.

Vergleich zwischen durchsatz- und hashbasierten Signaturen

Durchsatzbasierte Signaturen finden im Body von Dateien Muster, die verwendet werden können, in Zukunft Veränderungen dieser Datei zu identifizieren, und zwar auch, wenn der Inhalt nur leicht modifiziert worden ist. So können wir polymorphe Malware, die ansonsten als neue, unbekannte Datei behandelt würde, sofort identifizieren und blockieren.

Hashbasierte Signaturen passen zu einer festen Kodierung, die bei jeder einzelnen Datei unverwechselbar ist. Da ein Dateihash sehr einfach zu ändern ist, wirken hashbasierte Signaturen nicht gegen polymorphe Malware oder Varianten derselben Datei.

Integration mit WildFire

Erweitern Sie Ihren Schutz auf Zero-Day-Malware und C2-Angriffe: Nutzen Sie WildFire, die fortschrittlichste Analyse- und Präventionsengine für hoch evasive Zero-Day-Malware

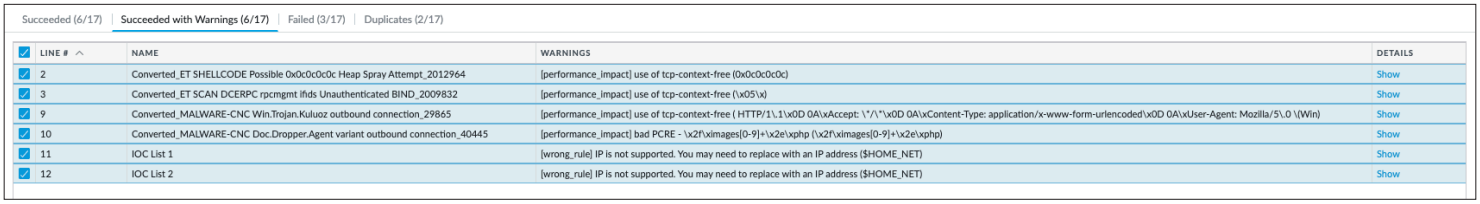

Abbildung 1: Snort-Support auf PAN-OS®

und Exploits. Dieser cloudbasierte Dienst kombiniert mehrere Techniken, zu denen die dynamische und statische Analyse, innovatives Maschinenlernen und Bare-Metal-Analysen zählen, um selbst die evasivsten Bedrohungen zu entdecken und abzuwenden. Sobald eine Bedrohung identifiziert wurde, beurteilt Threat Prevention in Echtzeit sämtliche ML-basierten NGFW-Formfaktoren und stoppt so die weitere Verbreitung der Bedrohung in Ihrem Unternehmen sofort.

Schutz vor Command and Control

Es gibt kein Allheilmittel, mit dem sämtliche Bedrohungen von ihrem Netzwerk ferngehalten werden können. Nach einer Erstinfektion kommunizieren Angreifer mit der Hostmaschine über einen C2-Kanal, den sie verwenden, um zusätzliche Malware einzuspeisen, weitere Anweisungen zu geben und Daten zu stehlen. Unser C2-Schutz setzt genau bei diesen nicht autorisierten Kommunikationskanälen an. Diese werden abgeschnitten, indem Anfragen, die sich an bösartige Dokumente richten, oder Anfragen von bekannten C2-Toolkits auf infizierten Geräten blockiert werden.

Palo Alto Networks geht dabei über die Standardutomatisierung von C2-Signaturen auf der Basis von URLs und Domains hinaus. Wir generieren und liefern vollautomatisch nach wissenschaftlichen Kriterien erstellte C2-Signaturen, die auf bösartigem Datenverkehr basieren, der von WildFire anhand der Geschwindigkeit und Datenrate beobachtet wurde. Diese Signaturen sind durchsatzbasiert und können C2-Datenverkehr selbst dann identifizieren, wenn der C2-Host unbekannt ist oder sich rasch verändert. Sie können den allgemeinen C2-Schutz weiter ausbauen, indem Sie ein DNS Security-Abonnement abschließen. Dieses liefert Ihnen die Mittel, Angreifer davon abzuhalten, C2-Kanäle mithilfe von DNS-Tunneltaktiken zu verbergen.

Reduzierung der Angriffsfläche

Threat Prevention und die erweiterten Funktionen der aus der Cloud bereitgestellten Palo Alto Networks-Abonnements helfen Ihrer Organisation, deutlich weniger Angriffsfläche zu bieten und die entsprechenden geschäftlichen Risiken zu minimieren. In diesem Abschnitt nennen wir Ihnen einige Beispiele für die zusätzlichen Technologien.

SSL-Entschlüsselung

Der Datenverkehr von Unternehmen ist größtenteils verschlüsselt. Dies ist eine gravierende Schwachstelle bei der Abwehr von Gefahren für ein Netzwerk, sofern der Datenverkehr nicht entschlüsselt und auf Bedrohungen überprüft wird. Unsere plattformeigene SSL-Entschlüsselung kann eingehenden und ausgehenden SSL-Datenverkehr selektiv entschlüsseln. Nach der Entschlüsselung wird der gesamte Datenverkehr vollständig überprüft. Wenn sich bestätigt, dass dieser unproblematisch ist, wird er erneut verschlüsselt und dann an sein Ziel weitergeleitet.

Dateiblockade

Bei einem sehr großen Teil der „Spear-Phishing“-Angriffe werden schädliche Dateien eingesetzt. Die Nachlässigkeit von Mitarbeitern wird als großes Sicherheitsrisiko betrachtet, da viele Mitarbeiter gar nicht wissen, was sicher ist und was nicht. Sie können die Gefahr einer Malwareinfektion verringern, indem Sie gefährliche Dateitypen daran hindern, Malware zu verbergen, wie etwa ausführbare Dateien, damit diese nicht in Ihr Netzwerk gelangen können. Das Blockieren von Dateien kann mit User-ID kombiniert werden, um aus der Sicht der beruflichen Rolle des Benutzers unnötige Dateien zu blockieren. So ist dennoch gewährleistet, dass alle Benutzer auf die Dateien zugreifen können, die sie auch benötigen, und Sie können den Zugriff im Detail regeln, damit Ihr Unternehmen weniger gefährdet ist. Sie können die Angriffsfläche weiter verringern, indem Sie sämtliche zugelassenen Dateien zur Analyse an WildFire senden. Dann kann festgestellt werden, ob diese Zero-Day-Malware enthalten.

Schutz vor unbeabsichtigtem Herunterladen

Nichts ahnende Benutzer können unabsichtlich Malware herunterladen, indem sie zum Beispiel ihre bevorzugte Website besuchen. Selbst der Betreiber dieser Website weiß nicht unbedingt, ob seine Seite kompromittiert ist. Unsere Threat Prevention-Techologie identifiziert potenziell gefährliche Downloads und sendet dem Benutzer eine Warnung, um sicherzustellen, dass dieser Download beabsichtigt ist. Die Entdeckung solcher „Phishing-Kit“-Landingpages und Web-Shell-Dateien (die den Fernzugriff auf Web-Server aktivieren wollen, um weitere interne Systeme angreifen zu können) ist in Threat Prevention in Form von Spywaresignaturen gepackt und ausgeliefert. Diese Funktionen können Sie erweitern, indem diese Funktion mit den Richtlinien für URL-Filtering und die Blockierung von Dateien verknüpft wird, damit auch Angriffe neuer, sich schnell verändernder Domains abgewendet werden.

Bedrohungen einfach und zielsicher verringern

DNS Sinkhole

Im Rahmen eines typischen Einsatzes, bei dem die Firewall sich nördlich vom lokalen DNS-Server befindet, identifiziert das Bedrohungsprotokoll den lokalen DNS-Resolver eher als Quelle des Datenverkehrs als den eigentlich infizierten Host. Im Ergebnis kann die Firewall die DNS-Query des infizierten Clients (also die Quelle der DNS-Query) nicht wahrnehmen. Die DNS Sinkhole-Funktion in Threat Prevention löst dieses Transparenzproblem, indem die Exfiltration verhindert und der Opferclient genau identifiziert wird. Die Sinkhole-Funktion ist so konfigurierbar, dass jede Anfrage an externe bösartige Domains oder IP-Adressen an eine interne IP-Adresse Ihres Netzwerks weitergeleitet wird. So wird jegliche C2-Kommunikation effektiv blockiert, in dem Anfragen dieser Art daran gehindert werden, das Netzwerk überhaupt zu verlassen.

Automatisierte Korrelationsobjekte

Unsere Threat Prevention-Technologie und unsere Protokolle beliefern die automatisierte Korrelationsengine, eine leistungsfähige Zusatzfunktion, mit der die Alarmfähigkeit der Palo Alto Networks-Firewalls und von Panorama zusätzlich gestärkt wird. Die Engine prüft, ob ähnliche Bedrohungsereignisse (etwa aus den Protokollen von Threat Prevention) miteinander zusammenhängen, was für eine höhere Wahrscheinlichkeit eines Angriffs auf Ihr Netzwerk sprechen würde. So können besonders gefährdete Stellen markiert werden, wie etwa kompromittierte Hosts im Netzwerk. Das versetzt Sie in die Lage, sich auf wenige konkrete Warnungen zu konzentrieren, das Risiko zu bewerten und Gefahren für ihre Netzwerkressourcen abzuwenden. Die Korrelationsobjekte profitieren von der Bedrohungsforschung in Unit 42 und der Analyse bisher unbekannter Bedrohungen aus WildFire und User-ID. So wird es möglich, Anomalien im Datenverkehr und Gefahrenindikatoren (Indicators of Compromise, IOCs) auszumachen, sodass Sie infizierte Geräte in Ihrem Netzwerk schnell und präzise identifizieren können.

Die Effizienz der Palo Alto Networks-Sicherheitsabonnements

In letzter Zeit haben Cyberangriffe an Umfang und Komplexität zugenommen, wobei fortschrittliche Methoden zur Umgehung von Netzwerksicherheitsgeräten und -tools verwendet werden. Dies stellt Unternehmen vor die Herausforderung, ihre Netzwerke zu schützen, ohne die Arbeitslast der Sicherheitsteams zu erhöhen oder die Produktivität des Unternehmens zu verringern. Unsere cloudbasierten Sicherheitsabonnements, die nahtlos mit der ersten ML-basierten NGFW-Plattform der Branche integriert sind, koordinieren die Informationen und bieten Schutz gegen alle Angriffsvektoren, verfügen über erstklassige Funktionalität

und eliminieren gleichzeitig die Lücken, die durch separate Netzwerksicherheitstools entstehen. Profitieren Sie von der stärksten Lösung, die derzeit auf dem Markt ist. Nutzen Sie unsere einheitliche Plattform und schützen Sie Ihre Organisation auch vor professionellen und schwer erkennbaren Angriffen. Threat Prevention und unsere Sicherheitsabonnements stehen für Sie bereit:

- **WildFire®:** Unbekannte Malware wird durch branchenführende, cloudbasierte Analysen automatisch erkannt und abgewehrt, um die Sicherheit von Dateien zu gewährleisten.
- **URL-Filtering:** Ermöglichen Sie die sichere Nutzung des Internets, indem Sie den Zugang zu bekannten und neuen schädlichen Websites verhindern, bevor sie von Benutzern aufgerufen werden können.
- **DNS-Sicherheit:** Unterbrechen Sie Angriffe, die DNS für C2-Aktivitäten und Datendiebstahl nutzen, ohne dass Änderungen an Ihrer Infrastruktur erforderlich sind.
- **IoT-Sicherheit:** Schützen Sie IoT-(Internet-of-things-) und OT-Devices in Ihren Unternehmen mit der ersten einsatzbereiten IoT-Sicherheitslösung der Branche.
- **GlobalProtect™-Netzwerksicherheit für Endpunkte:** Erweitern Sie die ML-basierten NGFW-Funktionen auf Ihre Remotebenutzer, um überall in Ihrer Umgebung einheitlich Sicherheit zu gewährleisten.

Unternehmensvorteile

Mit dem Threat Prevention-Abonnement haben Sie folgende Vorteile:

- **Umfassende Sicherheitsmaßnahmen schützen alle Daten, Anwendungen und Benutzer.** Der gesamte Datenverkehr wird überwacht; die Rolle von Anwendungen und Benutzern wird im Kontext vollständig erfasst und berücksichtigt.
- **Automatisierte Sicherheitsmaßnahmen reduzieren den manuellen Arbeitsaufwand.** Automatische Updates zu Bedrohungen halten Sie auf dem neuesten Stand.
- **Einsatz von Snort-Signaturen.** Sie können Snort- und Suricata-Regeln automatisch konvertieren, bereinigen, hochladen und verwalten, damit neue Bedrohungen entdeckt und wichtige Informationen vorteilhaft genutzt werden.
- **Detaillierte, richtlinienbasierte Kontrollen garantieren die Sicherheit Ihres Netzwerks.** Anstatt nur schädliche Inhalte zu blockieren, werden spezifische Dateiarten kontrolliert, wodurch Gefahren von Ihrer gesamten Organisation abgewendet werden.
- **Schaffen Sie das C2-Risiko aus der Welt.** Nutzen Sie automatisch generierte C2-Signaturen in angemessener Menge und Geschwindigkeit.

Tabelle 1: Threat Prevention-Durchsatz in der PA-Serie

Modell	Bedrohungsdurchsatz
PA-200	50 Mbit/s
PA-500	100 Mbit/s
PA-2020	200 Mbit/s
PA-2050	500 Mbit/s
PA-3020	1 Gbit/s
PA-3050	2 Gbit/s
PA-3060	2 Gbit/s
PA-5020	2 Gbit/s
PA-5050	5 Gbit/s
PA-5060	10 Gbit/s
PA-7050	100 Gbit/s
PA-7080	180 Gbit/s

Tabelle 2: Datenschutz und Lizenzierung – Zusammenfassung

Datenschutz beim Threat Prevention-Abonnement	
Vertraulichkeit und Datenschutz	Palo Alto Networks verfügt über strenge Datenschutz- und Sicherheitskontrollen, um unbefugten Zugriff auf sensible oder persönlich identifizierbare Informationen zu verhindern. Wir wenden branchenübliche Best Practices für Sicherheit und Vertraulichkeit an. Zusätzliche Informationen finden Sie in unseren Datenblättern zum Datenschutz.
Lizenzierung und Anforderungen	
Anforderungen	Für das Threat Prevention-Abonnement benötigen Sie die Palo Alto Networks Next-Generation Firewalls mit PAN-OS.
Empfohlene Umgebungen	Palo Alto Networks Next-Generation Firewalls sollten an allen Einsatzorten verwendet werden, da interne und externe Quellen netzwerkbasierte Bedrohungen über Exploits, Malware, Spyware, C2 oder URLs in Ihr Netzwerk einschleusen können.
Threat Prevention-Lizenz	Für Threat Prevention benötigen Sie eine separate Lizenz, die wir als integriertes, cloudbasiertes Abonnement der Palo Alto Networks Next-Generation Firewalls ausliefern. Sie ist auch im Rahmen der Palo Alto Networks Subscription ELA, der VM-Series ELA oder Prisma Access erhältlich.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Zentrale: +1 408 75 34 000
Vertrieb: +1 866 32 04 788
Support: +1 866 898 9087

www.paloaltonetworks.com