EXCLUSIVE NETWORKS

paloalto NETWORKS

WACHSEN SIE

mit der NGFW der Serie PA-400 von Palo Alto Networks

Enter

Inhaltsverzeichnis

Einführung

NICHT ALLE NGFW SIND GLEICH

Palo Alto Networks entwickelte 2007 die erste Next-Generation Firewall (NGFW) überhaupt. Eine NGFW ist eine erweiterte Version einer herkömmlichen Firewall, die kontextbezogen Authentifizierungsentscheidungen unter Berücksichtigung der Benutzer, des Inhalts und der Anwendung trifft. NGFWs sind ein entscheidender Baustein der Sicherheitsinfrastruktur moderner Unternehmen und haben sich zum Standard für die Netzwerksicherheit entwickelt. **Aber nicht alle NGFWs sind gleich.**

Während sich ein Großteil der Sicherheitsbranche darauf konzentrierte, die Reaktionszeit auf Cyberangriffe zu verkürzen, setzte Palo Alto Networks darauf, die Firewall von einem reaktiven zu einem proaktiven Sicherheitskontrollpunkt zu verwandeln.

Was die Palo Alto Networks NGFW von anderen unterscheidet, ist ihre Technologie. Die **einzigartige Single-Pass-Architektur,** die eingebettete **ML-Technologie,** das **Betriebssystem PAN-OS** als Kernstück und der **Plattformansatz** sind die Gründe dafür, dass inzwischen mehr als 85.000 Kunden Palo Alto Networks vertrauen, wovon über 62.000 NGFWs einsetzen. Durch die Zusammenarbeit mit uns haben auch Sie die Möglichkeit, Ihr Cybersecurity-Angebot für Ihre Kunden zu differenzieren und Ihre Umsätze ANZUKURBELN!

Wir erklären Ihnen unsere 4 wichtigsten technologischen Unterscheidungsmerkmale

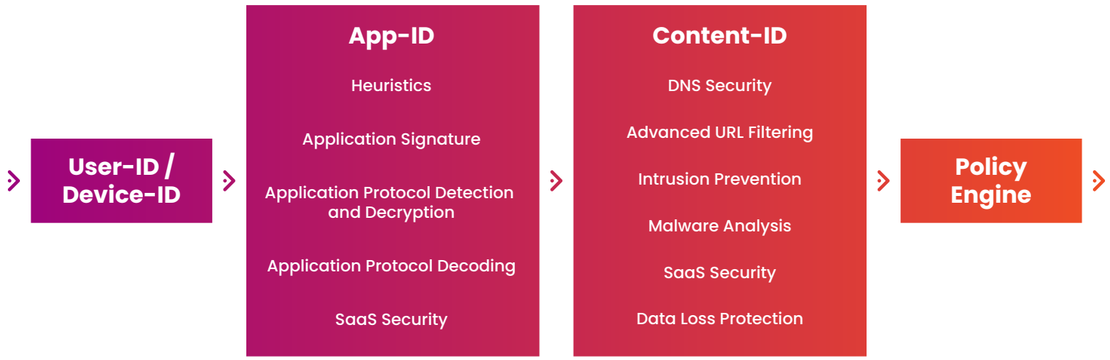
Lesen Sie weiter, um die 4 wichtigsten technologischen Unterscheidungsmerkmale der NGFW-Technologie von Palo Alto Networks besser zu verstehen

1) EINZIGARTIGE SINGLE-PASS-ARCHITEKTUR

Jahrelang haben Sicherheitsunternehmen versucht, Dienste zur Abwehr von Bedrohungen wie Intrusion Prevention Systems (IPS), Netzwerk-Antivirus, Analyse des Benutzerverhaltens, Data Loss Prevention (DLP) und Geräteklassifizierung in die Firewall zu integrieren, um den Einsatz mehrerer Geräte gleichzeitig zu vermeiden. Die Integration macht durchaus Sinn, denn die Firewall ist sozusagen das Herzstück einer Sicherheitsinfrastruktur. Dieser Ansatz birgt jedoch ein weit verbreitetes Problem: ein Mangel an kohärenter und vorhersehbarer Leistung, wenn die Sicherheitsdienste aktiviert sind.

Denn während die Basis-Firewall bei hohem Durchsatz und geringer Latenz sehr gut funktioniert, nimmt die Leistung der Firewall bei zunehmender Latenz ab, wenn zusätzliche Sicherheitsfunktionen aktiviert werden. Noch wichtiger ist, dass die Sicherheitsfunktionen **eingeschränkt** werden, da ein Ansatz, bei dem eine Abfolge von Funktionen verwendet wird, viel weniger flexibel ist als einer, bei dem alle Funktionen dieselben Informations- und Durchsetzungsmechanismen nutzen.

Palo Alto Networks wählte bei der Entwicklung seiner NGFW einen ganz anderen Ansatz: Die Firewall basiert ausschließlich auf einer **Single-Pass-Architektur**. Die Lösung für diese Leistungs- und Flexibilitätsherausforderungen ist ein einzigartiger Single-Pass-Ansatz für die Paketverarbeitung, der in einem einzigen Durchgang – für alle Bedrohungen und Inhalte – die Vernetzung, die Policy-Suche, die Anwendungsdekodierung und den Signaturabgleich durchführt. Vom Prinzip her bedeutet das: „Alles auf einmal scannen". Dieser Ansatz ermöglicht es, den Verarbeitungsaufwand, der für die Ausführung mehrerer Funktionen in einem einzigen Sicherheitsgerät erforderlich ist, massiv zu reduzieren und eine konsistente, vorhersehbare Leistung zu garantieren, wenn zusätzliche Sicherheitsdienste aktiviert werden.



Die wichtigsten Vorteile einer Single-Pass-Architektur:

- keine zusätzlichen Leistungsoverheads bei der Aktivierung zusätzlicher Funktionen
- einfache Handhabung aller Aspekte der Bedrohungsabwehr in der Sicherheitsrichtlinie
- vereinfachte Handhabung durch weniger Konsolen und Funktionslücken für eine effektivere Sicherheitsabdeckung
- signifikant niedrigere Gesamtbetriebskosten

Wir erklären Ihnen unsere 4 wichtigsten technologischen Unterscheidungsmerkmale

2) ML-GESTÜTZTE TECHNOLOGIE

Die Technologie des maschinellen Lernens (ML) unterstützt jetzt die NGFWs von Palo Alto Networks und setzt damit einen neuen Standard in Sachen proaktive Sicherheit. Die Technologie ermöglicht es NGFWs, kontinuierlich aus riesigen Datenmengen zu lernen, um Bedrohungen an mehreren Fronten zu erkennen. Sie hilft Sicherheitsteams, viel effektiver zu arbeiten und dient als erste Verteidigungslinie einer jeden modernen, effektiven Sicherheitsplattform.

Die Schlüsselkomponenten einer ML-gestützten NGFW von Palo Alto Networks sind die folgenden:

1) Inline-ML

Die ML-Algorithmen sind in den Firewall-Code eingebettet, sodass die Firewall eine Datei während des Herunterladens analysieren und sie sofort blockieren kann, wenn sie bösartig ist, ohne auf Offline-Tools zugreifen zu müssen. Die Zeit von der Sichtbarkeit bis zur Prävention geht gegen Null.

2) Verzögerungsfreie Signaturen

Eine ML-gestützte NGFW zeichnet sich durch eine völlige neue Art der Bereitstellung von Signaturen aus. Anstatt mindestens fünf Minuten auf einen geplanten Push zu warten, werden Signatur-Updates innerhalb von Sekunden nach der ML-Analyse durchgeführt und an die Firewall gestreamt, so dass eine neue Bedrohung bereits beim ersten Benutzer gestoppt wird und zukünftige Mutationen automatisch blockiert werden.

3) ML-gestützte Sichtbarkeit aller IoT-Geräte

Ältere IoT-Sicherheitslösungen hängen von bestehenden Definitionen von Geräten ab und sind nicht in der Lage ein unerwartetes oder gefährliches Verhalten zu erkennen. ML-gestützte NGFWs gruppieren dagegen ähnliche Geräte automatisch, wie z. B. Kameras und Tablets, anhand ML-basierter Klassifizierungen, um ungewöhnliche und schädliche Aktivitäten zu verfolgen und zu verhindern.

4) Automatisierte, intelligente Richtlinienempfehlungen

Anstatt permissive Richtlinien zu verwenden, die das Netzwerk unbekannten Bedrohungen aussetzen, vergleicht die ML-gestützte NGFW die Metadaten von Millionen von IoT-Geräten mit denen des Netzwerks, um normale Verhaltensmuster zu ermitteln. Für jedes IoT-Gerät und jede Kategorie empfiehlt die ML-gestützte NGFW dann eine Richtlinie für zulässiges Verhalten, was Netzwerkadministratoren unzählige Stunden manueller Updates erspart.

Die wichtigsten Vorteile einer ML-gestützten Technologie:

- Die ML-gestützte NGFW verändert die Art und Weise, wie Sicherheit bisher eingesetzt und durchgesetzt wurde.
- Tests haben ergeben, dass sie proaktiv bis zu 95 % der neuen Bedrohungen sofort verhindert.
- Sie stoppt bösartige Scripts und Dateien, ohne die Benutzerfreundlichkeit zu beeinträchtigen.
- Sie erweitert die Sichtbarkeit und den Schutz für IoT-Geräte ohne zusätzliche Hardware. Basierend auf Kundendaten steigt die Anzahl der erkannten IoT-Geräte um das Dreifache.
- Sie reduziert menschliche Fehler und automatisiert die Aktualisierung von Sicherheitsrichtlinien, um die fortschrittlichsten Angriffe zu verhindern.

Wir erklären Ihnen unsere 4 wichtigsten technologischen Unterscheidungsmerkmale

3) PAN-OS-BETRIEBSSYSTEM

PAN-OS ist das Betriebssystem hinter der Palo Alto Networks NGFW. Es ist das Gehirn der Maschine und trägt dazu bei, die Kernelemente eines Unternehmens – Benutzer, Anwendungen, Geräte und Inhalte – zu festen Bestandteilen der Sicherheitspolitik eines Unternehmens zu machen.

Durch die neueste Version von PAN-OS, 11.0 Nova, werden die branchenführenden Inline Deep Learning-Funktionen von Palo Alto Networks erweitert, um noch mehr hochgradig ausweichende Zero-Day-Angriffe zu stoppen. Das Betriebssystem enthält viele Innovationen, darunter eine stärkere Sicherheitsvorkehrung mit AIOps, um Fehlkonfigurationen zu reduzieren, die zu Sicherheitsverletzungen führen können.

Nova legt die Messlatte dafür hoch, wie Unternehmen proaktiv die Cyberhygiene verbessern und Sicherheitsarchitekturen vereinfachen können.

Sehen Sie sich die Veranstaltung zur Einführung von PAN-OS 11.0 Nova on demand an

HIER ANSCHAUEN

Wir erklären Ihnen unsere 4 wichtigsten technologischen Unterscheidungsmerkmale

4) PLATTFORM-ANSATZ

Inmitten der makroökonomischen Herausforderungen unterstützt Palo Alto Networks seine Kunden bei der Konsolidierung ihrer Sicherheitsarchitekturen durch seinen integrierten Plattformansatz. Die Plattform ermöglicht die gemeinsame Nutzung von Endpunkt-, Netzwerk- und Cloud-Daten für eine effektivere Analyse und trägt dazu bei, das Risiko einer Sicherheitsverletzung zu senken und vor den neuesten Bedrohungen zu schützen, während sie gleichzeitig die volle Produktivität der Mitarbeiter und die Nutzung der Cloud ermöglicht. Die NGFWs gehören zum Strata-Teil der Palo Alto Networks-Plattform. Wenn Sie in die Palo Alto Networks NGFW investieren, investieren Sie in einen Weg in eine sichere Zukunft.

Palo Alto Networks Plattform-Komponenten:

Netzwerk-Sicherheit
STRATA | PRISMA SASE

Erstklassige Sicherheit für Hardware, Software und SASE

Cloud-Sicherheit
PRISMA-CLOUD

Umfassende Plattform zur Sicherung aller in der Cloud ausgeführten Anwendungen

Sicherheitsmaßnahmen
CORTEX

Ein neuer Ansatz für SOC mit vollständig integrierten Daten, Analysen und Automatisierung

Die ML-gestützte NGFW der Serie PA-400 von Palo Alto Networks

Unternehmen jeder Größe benötigen hohe Netzwerkgeschwindigkeiten, um wettbewerbsfähig zu bleiben. Langsame Verbindungen und Netzwerkausfälle können die Produktivität, den Umsatz und das Kundenerlebnis beeinträchtigen. Zum Glück müssen IT-Teams die Sicherheitsfunktionen der Firewall nicht abschalten, um eine optimale Leistung zu erzielen.

Die Einstiegsserie PA-400 von Palo Alto Networks mit den Modellen PA-410, PA-415, PA-440, PA-445, PA-450 und PA-460 bietet ML-gestützte NGFW-Funktionen für dezentralisierte Unternehmensniederlassungen, Einzelhandelsstandorte sowie kleine und mittlere Unternehmen.

Die PA-400 Serie bietet kompromisslose Sicherheit und hohen Durchsatz, selbst bei verschlüsseltem Datenverkehr, und ist die perfekte Plattform für das Wachstum, das Ihr Unternehmen in die Zukunft zu führen wird!

Mit einem kompakten Design, das einfach zu implementieren ist und niedrige Gesamtbetriebskosten bietet, können Kunden proaktive Netzwerksicherheit auf jeden Winkel ihres Unternehmens ausdehnen.

Vorteile der PA-400 Serie:

- 10x mehr Leistung bei der Erkennung von Bedrohungen und der SSL-Entschlüsselung im Vergleich zur letzten Generation der PA-220
- <10 s für die Erkennung und Verbreitung neuer Bedrohungssignaturen, was das Risiko einer Systeminfektion um 99,5 % reduziert
- Einfach zu bedienen, schnell, belastbar und erschwinglich

Hier finden Sie das Datenblatt der PA-400 Serie für weitere Details:

DOWNLOAD

CLOUD-GESTÜTZTE SICHERHEITSDIENSTE

Die ML-gestützte NGFW der Serie PA-400 kann mit Cloud-Delivered Security Services (CDSS) kombiniert werden, sodass Kunden mit einem einzigen Kauf mehrere Services für umfassende Sicherheit an jedem Standort erhalten. Die Bündelung von Sicherheitsdienstleistungen verbessert die Sicherheit und vereinfacht gleichzeitig die Beschaffungsprozesse.

Weitere Firewall-Anleitungen finden Sie hier:

GUIDES

Wer sind unsere größten Konkurrenten?

Heute wurde Palo Alto Networks im Gartner® Magic Quadrant™ 2022 zum Leader für Netzwerk-Firewalls gekürt, eine Position, die das Unternehmen im 11. Jahr in Folge einnimmt.

Figure 1: Magic Quadrant for Network Firewalls

Source: Gartner (December 2022)

Zu den herausragenden Vorteilen gegenüber der Konkurrenz gehören laut Gartner ein starkes Produktportfolio, mehrere Bereitstellungsmodi – es gibt auch eine Software-NGFW der VM-Serie – , fortschrittliche Sicherheitsfunktionen und die Fähigkeit, die Netzwerksicherheit für Kunden durch einen konsolidierten Plattformansatz zu vereinfachen.

REPORT

DIE PA-400 SERIE SCHLÄGT DIE KONKURRENZ IN HEAD-TO-HEAD-VERGLEICHEN

Wie gut ist die PA-400 Serie in Wirklichkeit? Um Ihnen einen Eindruck zu vermitteln, hat Miercom, ein unabhängiges Netzwerk- und Sicherheitstestunternehmen, die PA-400 Serie und eine Firewall von Fortinet einer ähnlichen Preisklasse strengen Tests unterzogen und kam zu dem Schluss, dass die PA-400 Serie:

- einen vorhersehbaren Durchsatz beibehält, während Fortinet eine deutliche Leistungsverschlechterung zeigte
- eine bis zu 6x bessere Leistung hat
- bis zu 9x niedrigere Gesamtbetriebskosten hat

Lesen Sie den Bericht, um zu erfahren, was getestet wurde und wie.

REPORT

Warum Sie sich für Exclusive Networks entscheiden sollten, wenn Sie zusammen mit Palo Alto Networks Ihre Geschäfte ankurbeln möchten

Als globales Kompetenzzentrum von Palo Alto Networks bieten wir unseren Kunden Tag für Tag neue Chancen, Relevanz und Mehrwert, indem wir den Wandel im gesamten Palo Alto Networks Channel vorantreiben.

Mit jedem Tag wächst unsere 14-jährige Partnerschaft mit Palo Alto Networks weiter an, angetrieben von unseren hochqualifizierten, von Palo Alto Networks akkreditierten Mitarbeitern, der kontinuierlichen Innovation rund um die Palo Alto Networks-Plattform, unseren unglaublichen Kunden und Ökosystemen sowie unseren globalen Services.

DURCH UNSERE SPEZIALISIERUNG AUF CYBERSICHERHEIT SIND WIR IN DER LAGE, FOLGENDES ANZUBIETEN:

- End-to-End-Services von Palo Alto Networks, die von unserem exklusiven Global Deal Desk für GSI, SP und globale Implementierungen verwaltet und für nationale Anforderungen lokal koordiniert werden
- Weltweite Expertise durch unsere von Palo Alto Networks autorisierten Support Centres (ASC), das Network Operations Centre (NOC), Autorisierte Training Centres (ATC) und die Akkreditierung als Certified Professional Services Partner (CPSP)
- Mehrere Palo Alto Networks-Konsumoptionen, die auf die Bedürfnisse unserer Kunden zugeschnitten sind, von CSP-Marktplätzen, Lagerverfügbarkeit, unserer Exclusive On Demand (X-OD) Abonnement-Plattform, Finanzierungs- und Leasing-Services bis hin zum Managed Security Service Distributor (MSSD)
- Vertrauensvolle Beziehungen als Teil unserer lokalen und globalen Palo Alto Networks und exklusiven Networks Communities, Partner und Technologie-Ökosysteme
- Fortgeschrittenes lokales Know-how, technische Beratung, Marketing- und Geschäftsentwicklungsfähigkeiten für eine schnellere Aktivierung und ein schnelleres Wachstum von Palo Alto Networks

Erfahren Sie mehr und werden Sie noch heute Mitglied unserer exklusiven Palo Alto Networks Community:

MEHR DAZU

Wie können wir Ihnen beim Einstieg in den Vertrieb von ML-gestützten NGFWs der Serie PA-400 von Palo Alto Networks helfen?

Unser Exclusive Networks Team von Palo Alto Networks-Spezialisten ist bereit, Ihnen bei der Einführung von Palo Alto Networks zu helfen und Sie auf den Verkauf vorzubereiten! Zusätzlich zu unserem neuen Onboarding- und Befähigungsprogramm für Partner werden wir Sie auf folgende Weise unterstützen.

IDENTIFIZIERUNG

Wir helfen Ihnen bei der Identifizierung der Endkunden, die am besten auf ein Gespräch mit Palo Alto Networks reagieren werden, basierend auf Ihren eigenen Daten und Ökosystemen und unserer Business Intelligence.

Wir können Ihnen auch dabei helfen, herauszufinden, welchen Kontakten in Ihrer Datenbank Sie Priorität einräumen können, um einen Mehrwert zu schaffen. Beispiele hierfür sind:

- CISO - Reduzieren der Risiken, die von den Schwachstellen im Unternehmen ausgehen
- Infrastrukturverantwortliche - Schutz der Grenzen in einer Welt ohne Grenzen, während die Bedrohungen immer vielfältiger werden
- Network Security Engineer - Dafür sorgen, dass es bei der Arbeit mit neuen Lösungen keine Überraschungen gibt

Wie können wir Ihnen beim Einstieg in den Vertrieb von ML-gestützten NGFWs der Serie PA-400 von Palo Alto Networks helfen?

EINFÜHRUNG

Zusammen mit Marketing- und Geschäftsentwicklungsunterstützung werden diese branchenführenden Vertriebstools dazu beitragen, Ihre Palo Alto Networks-Pipeline zu beschleunigen und Ihnen die beste Conversion Rate im Vertrieb zu ermöglichen.

SECURITY LIFECYCLE REVIEWS (SLR)

Im Rahmen von Security Lifecycle Reviews (SLR) werden Berichte erstellt, die die Sicherheits- und Betriebsrisiken zusammenfassen, denen das Unternehmen Ihres Kunden ausgesetzt ist. In den Berichten werden die Daten aufgeschlüsselt, sodass Sie Ihren Kunden helfen können, auf schnelle und einfache Weise zu erkennen, wie sie ihre Angriffsfläche reduzieren können.

Jeder Abschnitt des SLR-Berichts konzentriert sich auf verschiedene Arten von Netzwerkaktivitäten — Anwendungsnutzung, Web-Browsing, Datenübertragung und Verbreitung von Bedrohungen — und zeigt die größten Risiken in jedem Bereich auf. In den SLR-Berichten werden die Statistiken Ihres Kunden zusammen mit den Durchschnittswerten anderer Unternehmen im selben Sektor angezeigt, so dass Sie ihm helfen können, seine Ergebnisse in den Kontext zu stellen.

SLR-Berichte können als Teil einer anfänglichen NGFW-Bewertung aber auch während regelmäßiger Sicherheitsüberprüfungen zur Bewertung der Bedrohungslage eingesetzt werden. Die durchschnittliche Conversion Rate vom SLR-Bericht zum Verkaufsabschluss liegt bei satten 80 %! Unser Team teilt mit Ihnen die bewährten Marketing- und Verkaufsinstrumente, die zur Förderung und zum Betrieb von SLR-Berichten eingesetzt werden. Unsere Vertriebskräfte werden gerne die ersten SLR-Berichte für Sie selbst durchführen und Sie darin schulen, Ihre eigenen SLR-Berichte eigenständig durchzuführen.

ULTIMATE TEST DRIVE WORKSHOPS

Ultimate Test Drives (UTDs) sind ein weiteres sehr erfolgreiches Verkaufsinstrument, das Ihnen hilft, potenzielle Kunden zu informieren. Diese praktischen Workshops, die sowohl als Präsenzveranstaltungen als auch virtuell angeboten werden, ermöglichen es Kundenteams und sogar Ihrem eigenen Vertriebsteam, die Technologie von Palo Alto Networks kennenzulernen. Sie konzentrieren sich auf die Funktionen, die die Teilnehmer am meisten interessieren, ermöglichen es ihnen, Experten Fragen zu stellen und bieten ihnen die Möglichkeit, in isolierten Laborumgebungen ohne Betriebsunterbrechung zu experimentieren.

Im Fokus des jüngsten ML-gestützten NGFW UTD Workshops stehen die folgenden Fragen:

- Wie stellt man sicher, dass der Zugriff auf die Anwendungen über Benutzer-IDs erfolgt?
- Wie konfiguriert man die Cloud Identity Engine für die Authentifizierung und die Prüfung der Identität/Benutzer-ID?
- Wie erstellt man eine anwendungsbasierte Richtlinie mit Policy Optimiser?
- Wie richtet man eine granulare Kontrolle für soziale Medien und sanktionierte SaaS-Anwendungen ein?
- Wie fügt man neue Entschlüsselungsrichtlinien zur Entschlüsselung des SSL-Verkehrs (TLS 1.3) hinzu?
- Wie erstellt man einen benutzerdefinierten Bericht im Application Command Center?
- Wie verwendet man das neue AIOps-Dashboard?

Starten Sie mit einem UTD-Workshop für Ihr eigenes Vertriebsteam!

Wie können wir Ihnen beim Einstieg in den Vertrieb von ML-gestützten NGFWs der Serie PA-400 von Palo Alto Networks helfen?

LIEFERUNG

Wenn es um die Bereitstellung von NGFWs geht, gibt es mehrere Möglichkeiten, wie wir Ihnen dabei helfen können, Mehrwert zu schaffen.

FLEXIBLE FINANZIERUNGSMÖGLICHKEITEN

Unser Finanzierungsprogramm ermöglicht es den Endkunden, zu einem Betriebskostenmodell überzugehen, während die Partner ihre Investitionskostenstruktur mit Vorauszahlungen beibehalten. Partner wählen den Zahlungsplan (Standard, mit späterem Zahlungstermin oder mit Ratenzahlungen), der den Kundenanforderungen entspricht und finanzieren Hardware, Software und Dienstleistungen über uns.

AB LAGER IN WENIGEN TAGEN LIEFERBAR

Exclusive Networks ist Teil des globalen Lagerprogramms von Palo Alto Networks, um die Vorlaufzeiten für Kunden zu verkürzen, einen schnelleren Zugang zu einem überragenden Sicherheitsniveau zu ermöglichen und Sie mit einer berechenbaren Plattform bei Ihrem Wachstum zu unterstützen.

Die Lagerbestände der ML-gestützten NGFWs von Palo Alto Networks PA-400, PA-1400 und PA-3400 Serie werden täglich in EMEA und APAC von drei Exclusive Networks-Zentrallagern in Großbritannien, den Niederlanden und Singapur ausgeliefert.

Lesen Sie hier mehr über das Programm

Um die Vorteile unserer Lagerverfügbarkeit zu nutzen und Ihre Kunden innerhalb weniger Tage zu beliefern, bitten Sie das Team von Exclusive Networks, Ihre Bestellung aus dem Lager zu nehmen.

EINFACH ZU VERKAUFENDE DIENSTLEISTUNGEN

Unsere Dienstleistungen helfen Ihnen bei der Skalierung durch lokale und globale Lieferung.
Hier finden Sie Beispiele für Mehrwertdienste, die wir Ihren Kunden anbieten können:

Deployment as a Service

Unsere Palo Alto Networks Deployment Services ermöglichen es Ihnen, Ihre eigenen Dienstleistungen schnell zu skalieren. Ein erfahrenes Team in über 150 Ländern deckt alle Schritte des Deployment-Lebenszyklus ab.

Mehr dazu

Engineer as a Service

Engineer as a Service stellt unseren Kunden von Palo Alto Networks erfahrene technische Ressourcen zur Verfügung, die vor Ort einsetzbar sind und im Rahmen eine SLAs Palo Alto Networks 'Smart Hands'-Aktivitäten durchführen.

Mehr dazu

Wie können wir Ihnen beim Einstieg in den Vertrieb von ML-gestützten NGFWs der Serie PA-400 von Palo Alto Networks helfen?

UNTERSTÜTZUNG

PALO ALTO NETWORKS AUTHORISED CENTRE (ASC)

Unsere von Palo Alto Networks autorisierten Support-Zentren (ASC) in den Regionen EMEA, DACH und APAC bieten einen 1st- und 2nd-Line Support und für Palo Alto Networks: den Premium Support für Exklusive Networks. So können Ihre Kunden beruhigt sein, dass ihre Investition in Palo Alto Networks zu den gleichen SLA geliefert wird, aber zu einem günstigeren Preis und mit schnelleren Reaktionszeiten als direkt vom Hersteller.

Mehr dazu hier

ERFOLGSGESCHICHTEN

Viele Partner beginnen ihre Partnerschaft mit Palo Alto Networks auf die „klassische“ Weise mit NGFWs, erweitern ihr Angebot dann über die ganze Plattform hinweg und freuen sich über einen nachhaltigen Erfolg und eine positive Geschäftsentwicklung.

In diesem Beispiel entwickelte sich die SCALTEL-Gruppe vom traditionellen Netzwerkpartner zum Sicherheitspartner und Managed Service Provider für Palo Alto Networks und Exclusive Networks.

Im Jahr 2022 erhielt das Unternehmen den Status des „Palo Alto Networks Diamond Innovator Partners“, die höchste Stufe des Palo Alto Networks NextWave-Partnerprogramms.

Erfahren Sie hier mehr über diese Erfolgsgeschichte: Wie SCALTEL sein Geschäft mit Palo Alto Networks ausbauen konnte

ERMÖGLICHEN

AUTHORISED TRAINING PARTNER (ATP) & AUTHORISED TRAINING CENTRE (ATC)

Exclusive Networks ist ein autorisierter Schulungspartner (ATP) und ein autorisiertes Schulungszentrum (ATC) von Palo Alto Networks. Wenn Sie mit uns zusammenarbeiten, haben Sie und Ihre Kunden Zugang zu Palo Alto Networks akkreditierten Schulungskursen, die von unseren Experten mit hoher Frequenz weltweit in mehreren Sprachen durchgeführt werden.

Unsere spezialisierten und akkreditierten Ausbilder führen unsere Palo Alto Networks-Kurse sowohl virtuell als auch vor Ort in unseren Exclusive Training Centres (ETC) durch, um mehr Flexibilität und die Wahl des Formats zu ermöglichen, das am besten zu einem vollen Terminkalender passt. Hier ein Überblick über unsere neuesten Kurse:

- Grundlagen der Firewall 11.0: Konfiguration und Verwaltung (EDU-210)
- Panorama 11.0: Verwaltung von Firewalls in großem Maßstab (EDU-220)
- Firewall 11.0: Fehlersuche (EDU-330)

MEHR DAZU

Zusammenfassung

WENN SIE MIT EXCLUSIVE NETWORKS ZUSAMMENARBEITEN, UM IHR GESCHÄFT MIT PALO ALTO NETWORKS ZU ERWEITERN, ERWARTEN SIE DIE FOLGENDEN VORTEILE:

EINE TECHNOLOGIE, DIE AUF MEHR ALS EINEM JAHRZEHNT BRANCHENWEIT FÜHRENDER INNOVATIONEN BERUHT:

- die sich im 11. Jahr in Folge im Gartner Magic Quadrant 2022 zum Leader für Netzwerk-Firewalls gekürt wurde
- die kritischen Schutz vor den Bedrohungen von heute und morgen bietet
- die leistungsstarke Sicherheitspakete schnürt

UNTERSTÜTZT DURCH DIE KOMPETENZEN UND DIE MARKTGRÖßE EINES GLOBALEN CYBERSICHERHEITSSPEZIALISTEN,

- der bewährte Marketing- und Vertriebstools und Enablement ermöglicht
- der über einfach zu verkaufende Bereitstellungsdienste verfügt
- der einen erstklassigen Support bietet
- der sich durch erstklassige Schulung auszeichnet

TOP-FUNKTIONEN, FÜR DIE IHNEN IHRE KUNDEN DANKEN WERDEN:

- Bessere Durchsatzleistung
- Einfache Lizenzierung
- Breite Palette an Sicherheitsfunktionen
- Integrierte Plattform
- Es funktioniert einfach

SOFORT VERSANDBEREIT:

- Erfüllen Sie die dringenden Zeitvorgaben Ihrer Kunden
- Keine Produktionsverzögerungen
- Kein Warten mehr, um Ihren Kunden die beste Sicherheit zu bieten, jetzt und in Zukunft

Bereit für Ihre eigene Erfolgsgeschichte?

Kontaktieren Sie unsere Palo Alto Networks-Spezialisten, um noch heute das Gespräch mit uns aufzunehmen.

KONTAKT