EXCLUSIVE NETWORKS

paloalto NETWORKS

GROW

Your Business with Palo Alto Networks PA-400 Series NGFW

Enter

Table of Contents

Introduction

NOT ALL NGFW'S ARE CREATED EQUAL

Palo Alto Networks created the industry's first Next-Generation Firewall (NGFW) back in 2007. A NGFW is an advanced version of the traditional firewall that makes authentication decisions based on the context of the user, content, and application. Critical to any modern organisation's security infrastructure, NGFWs have become the standard for network security. **But not all NGFWs are created equal.**

While much of the security industry was focused on reducing the time it takes to react to cyberattacks, Palo Alto Networks has been leading a mission to turn the firewall from a reactive security control point to a proactive one.

What sets the Palo Alto Networks NGFW apart is its technology. With a **unique, Single-Pass Architecture,** embedded **ML-powered technology,** the **PAN-OS operating system** at its core and a **platform approach,** it's easy to see why over 85,000 customers trust Palo Alto Networks, over 62,000 of which have NGFWs deployed in the field. In partnering with us, you too share the opportunity to differentiate your cybersecurity offering to your customers and watch your business GROW!

Top 4 Technology Differentiators Explained

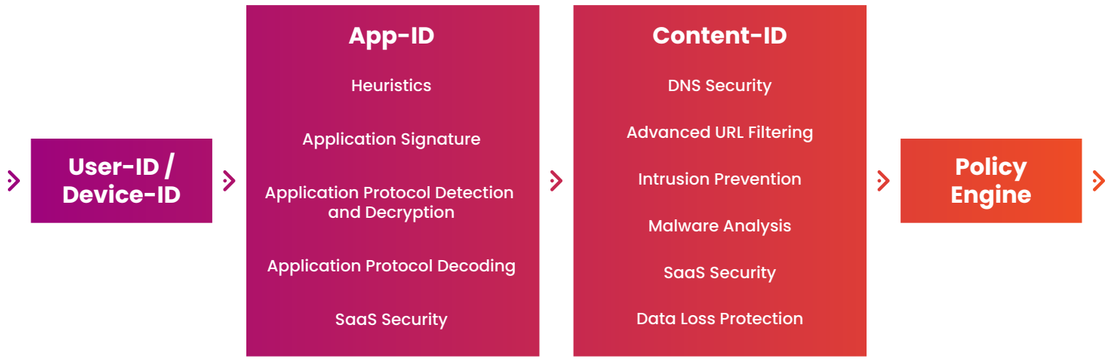
Read on to understand the top 4 Palo Alto Networks NGFW technology differentiators in more detail

1) UNIQUE, SINGLE-PASS ARCHITECTURE

For years, security companies have tried to integrate threat prevention services, such as intrusion prevention systems (IPS), network antivirus, user behaviour analysis, data loss prevention (DLP), and device classification, into the firewall to avoid the need for multiple devices. Integration makes perfect sense because the firewall sits at the heart of a security infrastructure. But the approach presents a common problem: a lack of consistent and predictable performance when security services are enabled.

That's because, while the base firewall may function very well at high throughput and low latency, when added security functions are enabled, firewall performance decreases while latency increases. More importantly, security capabilities become more **limited** because a 'sequence of functions' approach is much less flexible than one where all functions share the same information and enforcement mechanisms.

Palo Alto Networks took a very different approach when they designed their NGFW, which is 'built from the ground up' using a **Single-Pass Architecture.** It addresses these performance and flexibility challenges with a unique single-pass approach to packet processing, performing networking, policy lookup, application decoding, and signature matching – for all threats and content – in one single pass. Think of it as 'scan it all, scan it once.' This approach massively reduces the processing overhead required to perform multiple functions in one single security device, and it enables consistent, predictable performance when extra security services are activated.



Key benefits to remember about a Single-Pass Architecture:

- No additional performance overhead when enabling additional features.
- Easy management of all threat prevention aspects of security policy.
- Simplified management through fewer consoles and functional gaps for more effective security coverage.
- Significantly lower total cost of ownership.

Top 4 Technology Differentiators Explained

2) ML-POWERED TECHNOLOGY

Machine Learning (ML) technology now powers Palo Alto Networks' NGFWs, setting a new standard in proactive security. The technology enables NGFWs to learn continuously from vast amounts of data to detect threats across multiple fronts, helps security teams to work much more effectively, and serves as the first line of defence in any modern, effective security platform.

These four features are key components of a Palo Alto Networks ML-Powered NGFW:

1) Inline Machine Learning

ML algorithms are embedded in the firewall code so the firewall can inspect a file while it's being downloaded and block it instantly if it's malicious, without having to access offline tools. The time from visibility to prevention is close to zero.

2) Zero-Delay Signatures

An ML-Powered NGFW rearchitects the way signatures are delivered. Instead of waiting at least five minutes for a scheduled push, signature updates are performed and streamed to the firewall within seconds after ML analysis is done so a new threat will be stopped at the first user, and future mutations will be automatically blocked.

3) ML-Powered Visibility Across IoT Devices

Older IoT security solutions depend on existing definitions of devices and can't track unexpected or dangerous behaviour. The ML-Powered NGFW automatically groups similar devices, such as cameras and tablets, using ML-based classifications so it can track and prevent unusual and harmful activity.

4) Automated, Intelligent Policy Recommendations

Rather than using permissive policies, which expose the network to unknown threats, the ML-Powered NGFW compares metadata from millions of IoT devices to that of the network to establish normal behaviour patterns. For each IoT device and category, the ML-Powered NGFW then recommends a policy of allowable behaviours, saving network administrators countless hours of manual updates.

Key benefits to remember about ML-Powered Technology:

- The ML-Powered NGFW disrupts the way security has been deployed and enforced.
- Based on testing, it proactively prevents up to 95% of new threats instantly.
- It stops malicious scripts and files without sacrificing the user experience.
- It extends visibility and protection to IoT devices without additional hardware. Based on customer data, the number of detected IoT devices increases by a factor of three.
- It reduces human error and automates security policy updates to prevent the most advanced attacks.

Top 4 Technology Differentiators Explained

3) PAN-OS OPERATING SYSTEM

PAN-OS is the operating system behind the Palo Alto Networks NGFW. It's the brain of the machine and helps to make the core elements that run a business – users, applications, devices, and content – integral components of an organisation's security policy.

The newest version of PAN-OS, 11.0 Nova, extends Palo Alto Networks' industry-leading inline deep learning capabilities to stop even more highly evasive, zero-day threats. It includes many innovations, including stronger security posture with AIOps to reduce misconfigurations that can lead to security breaches.

Nova raises the bar for how organisations can proactively improve cyber hygiene and simplify security architectures.

Watch the PAN-OS 11.0 Nova launch event on demand

WATCH HERE

Top 4 Technology Differentiators Explained

4) PLATFORM APPROACH

Amid macroeconomic challenges, Palo Alto Networks is helping customers to consolidate their security architectures through their integrated platform approach. The platform allows the sharing of endpoint, network, and cloud data for more effective analysis, helping to lower the risk of a breach and protect against the latest threats while enabling full employee productivity and cloud adoption. NGFWs sit in the Strata part of the Palo Alto Networks platform. When you invest in the Palo Alto Networks NGFW, you're investing in a path to a more secure future.

Palo Alto Networks platform components:

Network Security
STRATA | PRISMA SASE

Best-in-class security delivered across hardware, software and SASE

Cloud Security
PRISMA CLOUD

Comprehensive platform to secure everything that runs in the cloud

Security Operations
CORTEX

A new approach to SOC with fully integrated data, analytics and automation

The Palo Alto Networks PA-400 Series ML-Powered NGFW

Organisations of all sizes need high network speeds to stay competitive. Slow connections and network outages can reduce productivity, sales, and customer experience. Fortunately, IT teams don't need to turn off firewall security features to get top performance.

The entry-level Palo Alto Networks PA-400 Series, comprising the PA-410, PA-415, PA-440, PA-445, PA-450, and PA-460, brings ML-Powered NGFW capabilities to distributed enterprise branch offices, retail locations, and small and medium businesses.

The PA-400 Series offers no-compromise security and high throughput, even when securing encrypted traffic, and is the perfect growth platform to accelerate your business into the future!

Customers can extend proactive network security to every corner of their business with a compact design that's easy to deploy and offers low TCO.

PA-400 Series benefits:

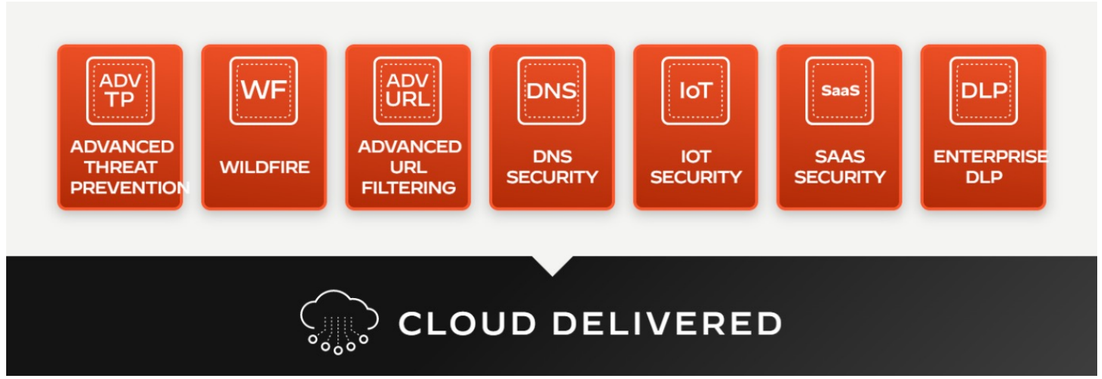
- 10x increase in threat detection and SSL decryption performance compared to the last generation PA-220
- <10 seconds to detect and push new threat signatures reducing system infections by 99.5%
- Easy to use, fast, resilient, and affordable

Get the PA-400 Series family datasheet here for extra detail

DATASHEET

CLOUD-DELIVERED SECURITY SERVICES

The PA-400 Series ML-Powered NGFW can be combined with Cloud-Delivered Security Services (CDSS), so that, with a single purchase, customers receive multiple services for comprehensive security at each location. Security services bundles improve security while simplifying procurement.



Get more firewall guides here:

GUIDES

Who's The Main Competition?

Today, Palo Alto Networks is positioned as a Leader in the 2022 Gartner® Magic Quadrant™ for Network Firewalls, a position it holds for an impressive 11th consecutive year.

Figure 1: Magic Quadrant for Network Firewalls

Source: Gartner (December 2022)

Standout advantages compared to the competition, according to Gartner, include a strong product portfolio, multiple deployment modes – a VM-Series software NGFW also exists - , advanced security features, and the ability to simplify network security for customers with a consolidated platform approach.

REPORT

PA-400 SERIES BEATS COMPETITION IN HEAD-TO-HEAD TESTING

So how good is the PA-400 Series in reality?
To give you an idea, Miercom, an independent network and security testing organisation, put the PA-400 Series and a similarly priced Fortinet firewall through rigorous testing, and concluded that the PA-400 series:

- Maintains predictable throughput, while Fortinet showed significant performance degradation
- Offers up to 6X better performance
- Provides up to 9X lower TCO

Read the report to find out what was tested and how.

REPORT

Why Choose Exclusive Networks To Help You Grow With Palo Alto Networks?

As a Palo Alto Networks Global Centre of Excellence, we bring opportunity, relevance, and value to our customers every day as we drive change across the Palo Alto Networks channel.

With each day, our 14-year Palo Alto Networks partnership grows from strength to strength, fuelled by our highly skilled, Palo Alto Networks accredited people, constant innovation around the Palo Alto Networks platform, our incredible customers and ecosystems, and our global services and scale.

THROUGH OUR SPECIALIST CYBERSECURITY FOCUS, WE DELIVER:

- End-to-end Palo Alto Networks services, managed through our Exclusive Global Deal Desk for GSIs, SPs, and global deployments, and co-ordinated locally for national needs
- Worldwide expertise through our Palo Alto Networks Authorised Support Centres (ASC), Network Operations Centre (NOC), Authorised Training Centres (ATC), and Certified Professional Services Partner (CPSP) accreditations
- Multiple Palo Alto Networks consumption choices, designed to best meet our customer needs, from CSP Marketplaces, stock availability, our Exclusive On Demand (X-OD) subscription platform, Financing and Leasing services, to Managed Security Service Distributor (MSSD)
- Trusted relationships as part of our local and global Palo Alto Networks and Exclusive Networks communities, partners, and technology ecosystems
- Advanced local knowledge, technical guidance, marketing and business development skills for faster Palo Alto Networks enablement and growth

Discover more and join our Exclusive Palo Alto Networks community today:

LEARN MORE

How Can We Help You Get Started With Palo Alto Networks PA-400 Series ML-Powered NGFW Sales?

Our Exclusive Networks team of Palo Alto Networks specialists are ready to help you to onboard Palo Alto Networks and get ready to sell! In addition to following our new partner onboarding and enablement programme, here's how we'll support you.

IDENTIFY

We'll help you to identify the most likely end customer accounts that will respond to a Palo Alto Networks conversation, based on your own data, ecosystems, and our business intelligence.

We can also help you to determine which contacts in your database you can prioritise to demonstrate added value. Examples include:

- CISO - reduce risks from the weak points across the organisation
- Head of Infrastructure - protect the boundaries in a world with no perimeter while threats continue to diversify
- Network Security Engineer - Ensure there are no surprises when working with new solutions

How Can We Help You Get Started With Palo Alto Networks PA-400 Series ML-Powered NGFW Sales?

INTRODUCE

Along with marketing and business development support, these industry-leading sales tools will help accelerate your Palo Alto Networks pipeline and give you the best sales conversion rate.

SECURITY LIFECYCLE REVIEWS (SLRS)

Security Lifecycle Reviews (SLRs) provide reports that summarise the security and operational risks your customer's organisation faces. The reports break the data down so you can help your customer quickly and easily identify how they can reduce their attack surface.

Each section of the SLR report focuses on different types of network activity — application usage, web-browsing, data transfer, and threat prevalence — and surfaces the greatest risks in each area. SLR reports display your customer's organisation's statistics alongside the averages for their industry peers, so you can help them to best understand their results in context.

SLRs can be used as part of an initial NGFW evaluation, or during regular security check-ups to assess threat exposure. The average sales conversion rate from SLR to closed-won business is a huge 80%! Our team will share with you the tried and tested marketing and sales tools used to promote and run an SLR. Our SEs will be happy to run the first SLRs for you and train you to be self-sufficient in your own SLR delivery.

ULTIMATE TEST DRIVE WORKSHOPS (UTDS)

Ultimate Test Drives (UTDs) are another widely successful sales tool to help you educate prospective customers. Delivered in both face to face and virtual formats, these hands-on workshops let customer teams, and even your own SE team, experience Palo Alto Networks technology by focusing on the features they're most interested in, allowing them to ask questions of the experts, and providing them the chance to experiment without business disruption in isolated lab environments.

The latest ML-Powered NGFW UTD Workshop covers these topics:

- Learn to ensure application access is by User-IDs
- Configure Cloud Identity Engine for authentication and identity/User-ID
- Create an application-based policy with Policy Optimiser
- Set up granular control for Social Media and Sanctioned SaaS Applications
- Add new decryption policies to decrypt SSL (TLS 1.3) traffic
- Create a custom report in the Application Command Center
- Learn to use the new AIOps dashboard

Get started with a UTD for your own SE team!

How Can We Help You Get Started With Palo Alto Networks PA-400 Series ML-Powered NGFW Sales?

OPTIMISE

Once you've started to build your Palo Alto Networks NGFW pipeline, there are a number of sales incentives you can use to help maximise the deal. Current live incentives on the Palo Alto Networks partner portal include:

PARTNER PERKS SALES INCENTIVE

- NextWave partner sales representatives who close/win qualifying opportunities can earn up to 50,000 NextWave Rewards Points (equivalent to $5,000 USD).
- Points are based on eligible products and deal size opportunities, plus a new customer bonus! (Min deal value is $25K)

REFRESH+

- Earn extra discount offers for gen-4 hardware trade-ins, à la carte subscriptions, core security bundle subscriptions, and network management..
- Ends 31st July 2024

How Can We Help You Get Started With Palo Alto Networks PA-400 Series ML-Powered NGFW Sales?

DELIVER

When it comes to NGFW delivery, there are multiple ways we can help you to add value.

FLEXIBLE FINANCING OPTIONS

Our financing programme enables end customers to move to an OPEX model while partners maintain CAPEX, upfront payments. Partners select the payment plan – standardised, deferred, or ramped – that fits customer requirements and finance hardware, software, and services through us.

STOCK DELIVERY IN DAYS

Exclusive Networks is part of the Palo Alto Networks Global Stocking Programme to accelerate customer lead times, deliver quicker access to superior levels of security, and support you with a predictable platform for growth.

Stock for the Palo Alto Networks PA-400, PA-1400 and PA-3400 Series ML-Powered NGFWs ships daily across EMEA and APAC from three Exclusive Networks central stock hubs in the UK, Netherlands, and Singapore.

Read more about the programme here

To take quick advantage of our stock availability and deliver to your customers in days, please request that your order is taken from stock via the Exclusive Networks team.

SIMPLE-TO-SELL SERVICES

Our services help you to scale through local and global delivery. Some examples of extra value services we can help you to bring your customers include:

Deployment as a Service

Our Palo Alto Networks Deployment Services allow you to rapidly scale your own services, covering end-to-end steps of the deployment lifecycle through an experienced team across over 150 countries.

Read more

Engineer as a Service

Engineer as a Service provides our Palo Alto Networks customers with experienced engineering resource, to physically attend sites and carry out Palo Alto Networks ‘smart hands’ activities within an SLA.

Read more

How Can We Help You Get Started With Palo Alto Networks PA-400 Series ML-Powered NGFW Sales?

SUPPORT

PALO ALTO NETWORKS AUTHORISED SUPPORT CENTRE (ASC)

Our Palo Alto Networks Authorised Support Centres (ASCs) across EMEA, DACH, and APAC, provide a 1st and 2nd line support offering for Palo Alto Networks: Exclusive Networks Premium Support. This gives your customers peace of mind for their Palo Alto Networks investment as it's delivered to the same SLAs, but at a more affordable cost with faster response times than direct from the vendor.

Find out more here

STORIES OF SUCCESS

Many partners begin their Palo Alto Networks partnership the 'classic' way with NGFWs, expand across the platform and go on to enjoy long success and business growth.

In this example, SCALTEL Group evolved from traditional networking partner to security partner and Managed Service Provider with Palo Alto Networks and Exclusive Networks.

In 2022, they achieved Palo Alto Networks Diamond Innovator Partner status, the highest level available in the Palo Alto Networks NextWave Partner Programme.

Read more about their growth journey here: How SCALTEL Grew Its Business with Palo Alto Networks

ENABLE

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

Exclusive Networks is a Palo Alto Networks Authorised Training Partner (ATP) and Authorised Training Centre (ATC). In partnering with us, you and your customers can access Palo Alto Networks accredited training courses that are delivered in multiple languages to a frequent timetable by our experts across the globe.

Our specialist in-house accredited trainers run our Palo Alto Networks courses both virtually, and onsite at our Exclusive Training Centres (ETCs), for added flexibility and choice of format that best suits a busy schedule. Here are the latest courses:

- Firewall 11.0 Essentials: Configuration and Management (EDU-210)
- Panorama 11.0: Managing Firewalls at Scale (EDU-220)
- Firewall 11.0: Troubleshooting (EDU-330)

READ MORE

In Summary

IN PARTNERING WITH EXCLUSIVE NETWORKS TO GROW YOUR BUSINESS WITH PALO ALTO NETWORKS, HERE'S WHAT YOU'LL BENEFIT FROM.

TECHNOLOGY POWERED BY OVER A DECADE OF INDUSTRY-FIRST INNOVATIONS:

- Positioned as a LEADER in the 2022 Gartner Magic Quadrant For Network Firewalls for the eleventh consecutive year
- Provides critical protection from the threats of today and tomorrow
- Packs a powerful security punch

SUPERIOR FEATURES YOUR CUSTOMERS WILL THANK YOU FOR:

- Better throughput performance
- Simple licensing
- Breadth of security features
- Integrated platform
- It just works

SUPPORTED BY THE SKILLS AND SCALE AND OF A GLOBAL CYBERSECURITY SPECIALIST:

- Proven marketing and sales tools and enablement
- Easy-to-sell deployment services
- Best-in-class support
- Top-rated training

AVAILABLE NOW TO SHIP:

- Meet your customers' urgent timescales
- No production delays
- No more waiting around to give your customers the best security, now and for the future

EXCLUSIVE NETWORKS

paloalto NETWORKS

Ready to Grow?

Contact our Palo Alto Networks specialists to start a conversation today.

CONTACT