Why Choose NGFW PA Series
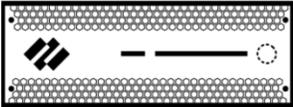
External Facing for Customers

paloalto®
NETWORKS

Why Choose NGFW - PA Series

paloalto
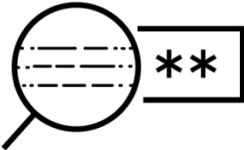NETWORKS

Best-of-Breed Across the Board
Leading the Way in Network Security Innovation

NGFW

A **Leader** in Gartner Magic Quadrant Network Firewalls 11-Time Leader
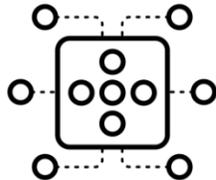
Gartner

Zero Trust

A **Leader** in Forrester Zero Trust eXtended Ecosystem Platform Providers Wave

FORRESTER®

SD-WAN

A **Leader** in Gartner Magic Quadrant WAN Edge Infrastructure

Gartner

ZTNA

A **Leader** in Forrester Zero Trust Network Access New Wave

FORRESTER®

SASE

Frost & Sullivan's Global **Company of the Year** Award for SASE

FROST & SULLIVAN

SASE

Gartner Single Vendor **Leader** in SASE Magic Quadrant (Aug 16, 2023)

Gartner

Leadership In Critical Third-Party Assessments

paloalto NETWORKS

THE MOVEMENT TO A BEST-OF-BREED PLATFORM IS REAL

"Since the end of 2019, Palo Alto Networks has been able to grow their overall NGFW market share from ~20% to **~30%**, more than any of their major competitors. This growth matches a trend where **customers are seeing the value of broader, integrated offerings** from strategic vendors in critical areas of security."

Fernando Montenegro
Senior Principal Analyst, Cybersecurity
Omdia

Building Modern Solutions to Modern Problems is in our DNA

Network Security Management

PN

WF

Advanced Malware Analysis

WF

DNS | **SD-WAN**

ADV URL | **ADV TP**

CN-Series
Containerized Firewall

2007

2009

2010

2011

2013

2014

2018

2019

2020

2021

2022

TP

First NGFW shipped with App-ID

UF | **GP**

VM-Series
Virtualized Firewalls

Cloud Delivered Firewall Service

IoT | **DLP** | **CASB**

Industry's First ML-NGFW

AIOps | **ADV WF**

paloalto NETWORKS

Best-In-Class Network Security Platform
For Any User Accessing Any Application

Internet

Private Cloud / DC

Public Cloud

SaaS Applications

Network Security Platform

UNIFIED MANAGEMENT AND OPERATIONS
with Strata Cloud Manager | Panorama and AIOps

Cloud-Delivered Security Services

| ADV TP | ADV URL | ADV WF | DNS | SaaS | DLP | IoT | SD-WAN | GP |

PA-Series **Hardware Firewalls**

Software Firewalls Cloud NGFW VM-Series CN-Series

SASE

HQ

Branch Office

Mobile

Home

BENEFITS

Safer
48%
more zero-day attacks stopped in real-time with inline deep learning, compared to legacy vendors

—

Intelligent
189K
new malicious websites detected using AI every day

—

Faster
<10 seconds
from threat detection to threat prevention. 180x faster than competing products

paloalto NETWORKS

Hardware Firewalls
World's First Machine Learning-Powered Next Generation Firewall

PA-400 Series

PA-460
4.4 Gbps App-ID

PA-450
3.0 Gbps App-ID

PA-445
2.2 Gbps App-ID

PA-440
2.2 Gbps App-ID

PA-415
1.2 Gbps App-ID

PA-410
1.2 Gbps App-ID

PA-1400 Series

PA-1420
9.5 Gbps App-ID

PA-1410
6.8 Gbps App-ID

PA-3400 Series

PA-3440
24 Gbps App-ID

PA-3430
20.5 Gbps App-ID

PA-3420
16.9 Gbps App-ID

PA-3410
11 Gbps App-ID

VM-Series

VM-Series
VM-Series   VM-Series
VM-Series   VM-Series
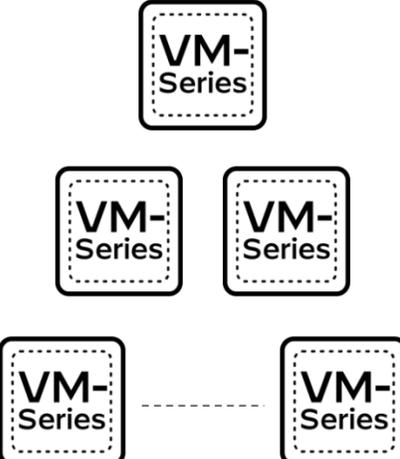
VM-Series
Ranging from xxx
Mbps to zzz Gbps
App-ID

✓ **Network Perimeter** ✓ **WFH** ✓ **Small Branches** ✓ **Private/Public Clouds**

Single Pass Architecture

Delivering Predictable Performance with Services Enabled

1. Scan all Security Functions in a Single Pass
2. Add Services (CDSS) with no additional performance impact
3. No Trade off between Performance and Security
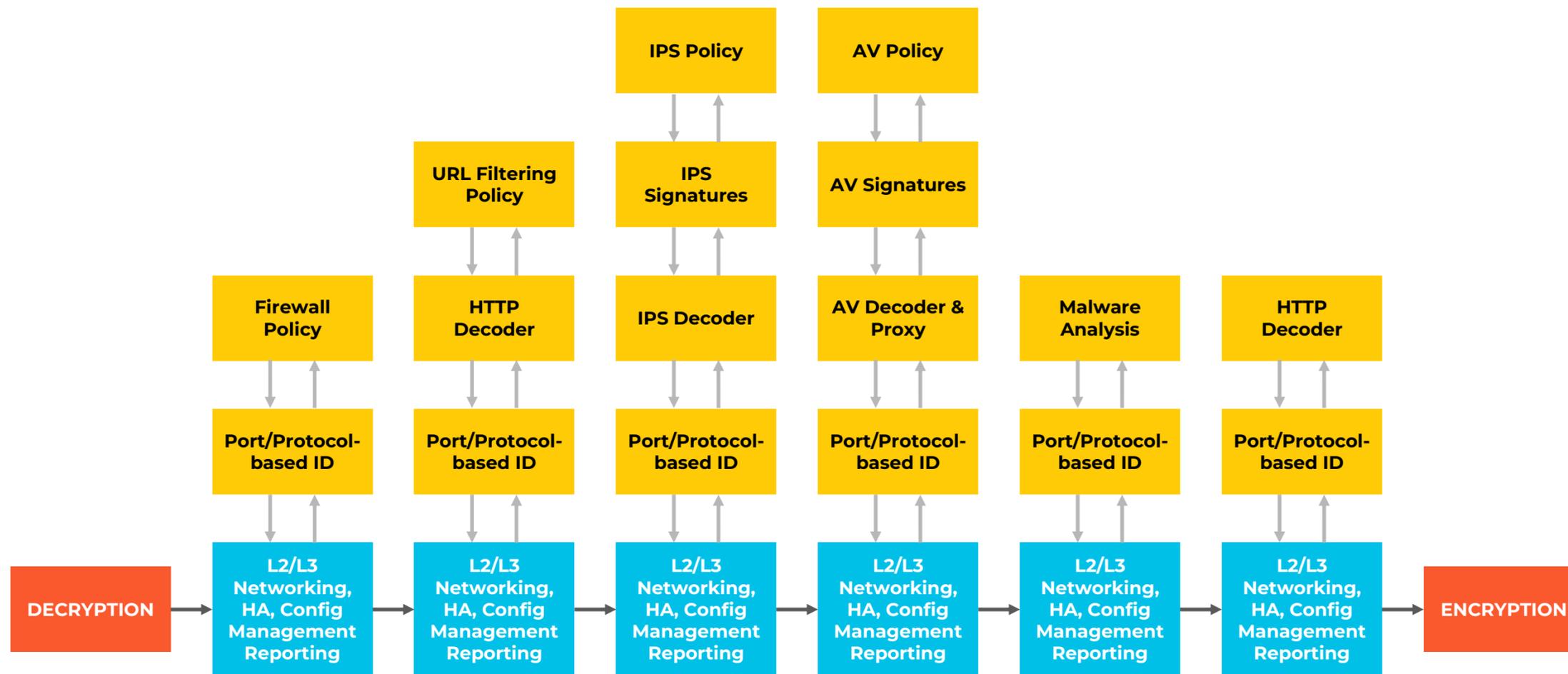
Multi-Pass Approach: Multiple Passes Degrade Performance

Single Pass Architecture

Maximize Performance with Services (subs) Enabled

*PA-400 Series is built with **Single Pass Architecture***

1. Scan all Security Functions in a 'Single Pass'
2. Add Services with no additional performance impact
3. Predictable performance when using individual services, or multi-service bundles
4. Datasheet Performance metrics maintained with services enabled

As organizations consolidate and constantly increase their security postures, Single Pass Architecture ensures that threat performance remains predictable
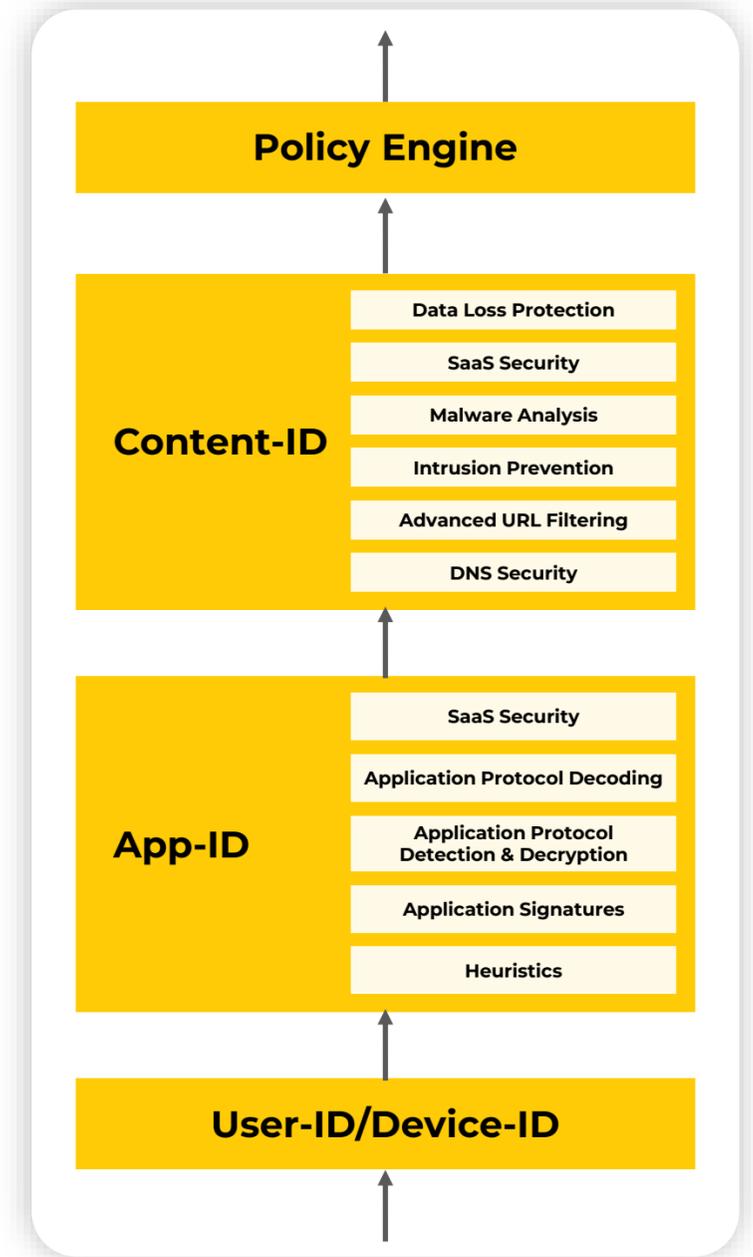
Our Single-Pass Architecture provides:

- 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.

Single-Pass Architecture

Integrated, Prevention-Oriented Security

For many years, security professionals have pursued the goal of integrating threat prevention services into the firewall to alleviate the need for additional devices for intrusion prevention systems (IPS), network antivirus, user behavior analysis, data loss prevention (DLP), device classification, and other functions. This integration makes perfect sense because the firewall is the cornerstone of security infrastructure.

Policy Engine

Content-ID
- Data Loss Protection
- SaaS Security
- Malware Analysis
- Intrusion Prevention
- Advanced URL Filtering
- DNS Security

App-ID
- SaaS Security
- Application Protocol Decoding
- Application Protocol Detection & Decryption
- Application Signatures
- Heuristics

User-ID/Device-ID

Scan it All, Scan it Once

paloalto NETWORKS

Miercom Report
Superior PA-400 Series performance with Services Enabled

Fortinet FG 201F	**1.8x Perf** → PA-460	2.1x Lower TCO
Fortinet FG 101F	**6.6x Perf** → PA-450	9.4x Lower TCO
Fortinet FG 81F	**3.4x Perf** → PA-440	5.9x Lower TCO
Fortinet FG 61F	**5.3x Perf** → PA-410	6.9x Lower TCO

Miercom

Palo Alto Networks
Next Generation Firewall (NGFW)
Competitive Performance

Summary Report SR210617B
Performance Validation Testing
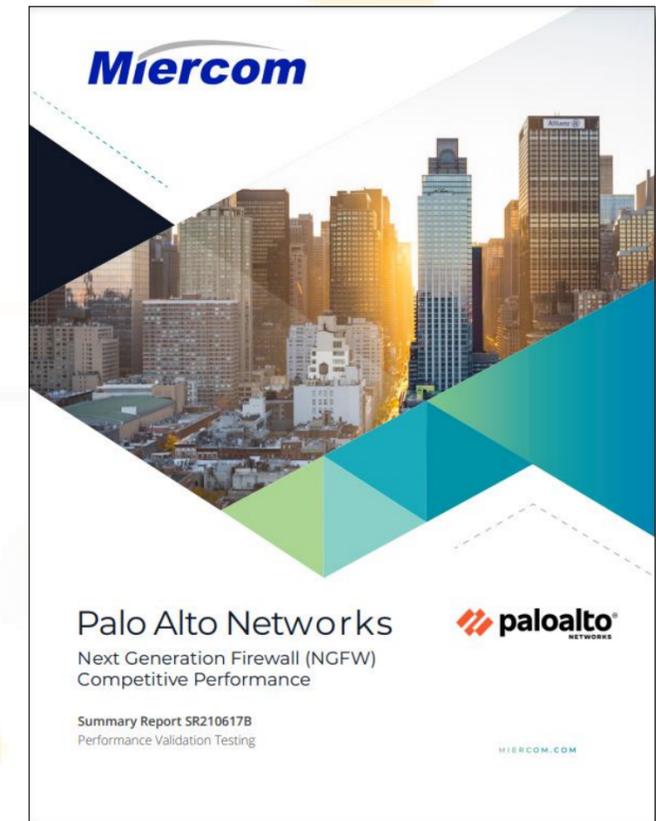
Comparing Throughput and TCO
with and without Services Enabled

PA-400 Series performance is **up to 6x** better than Fortinet with services enabled
PA-400 Series offers **up to 9x** lower Total Cost of Ownership per protected Mbps

Predictable Performance with Single Pass Architecture

1. Scan all Security Functions in a 'Single Pass'
2. Get Predictable Datasheet Performance with services enabled
3. Add Services (CDSS) with no additional performance impact

PA-3440

PA-3430

PA-3420

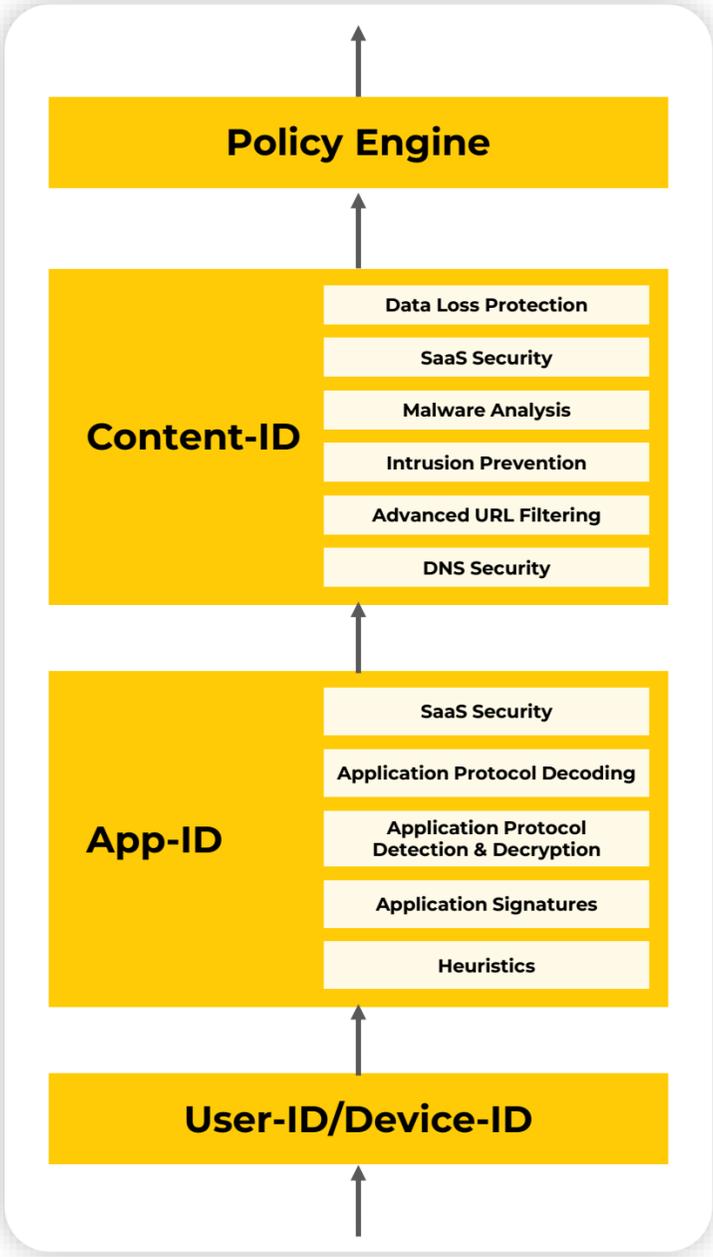PA-3410

paloalto

Single-Pass Architecture

Integrated, Prevention-Oriented Security

Our Single-Pass Architecture provides:

- 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.
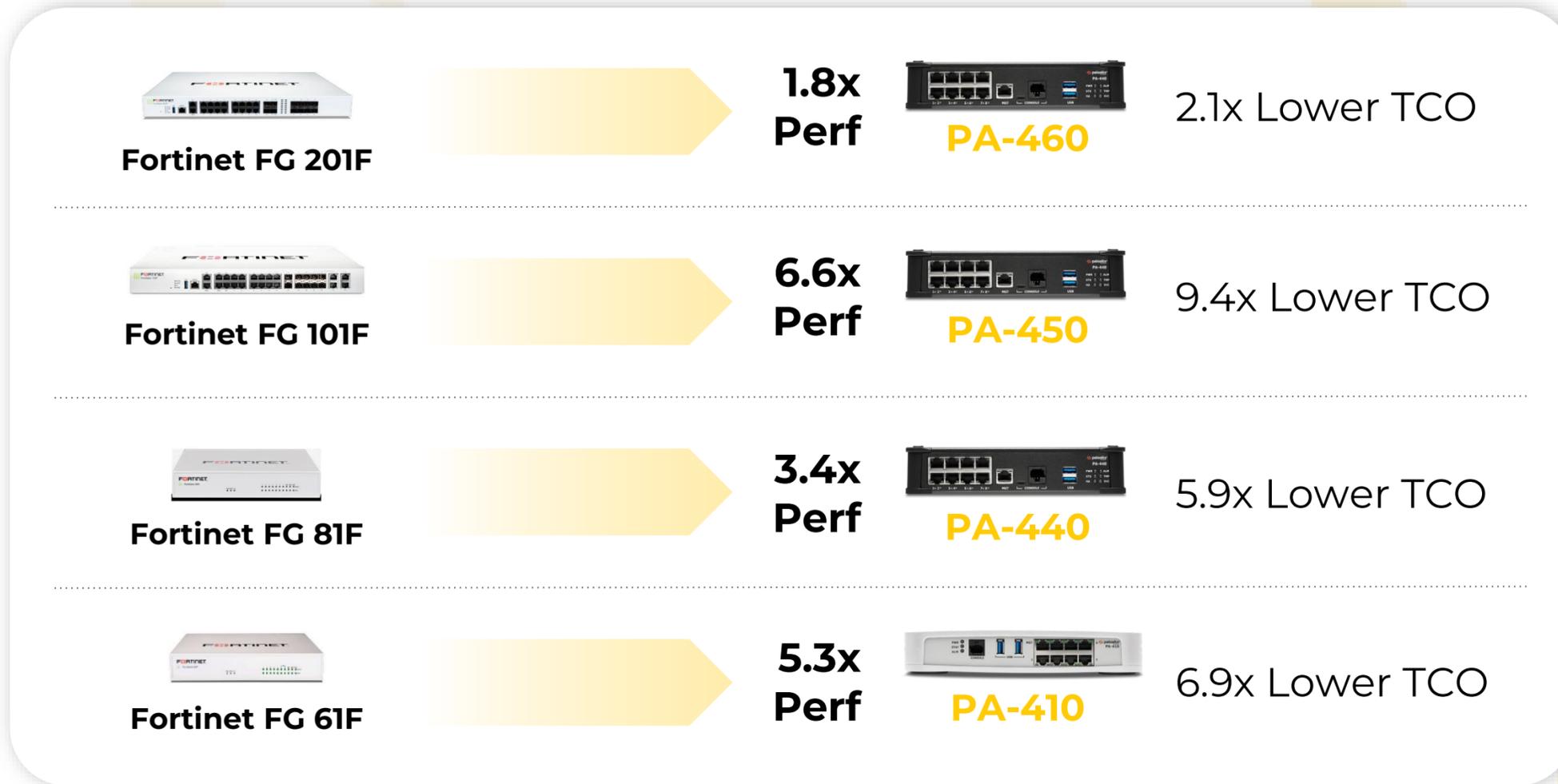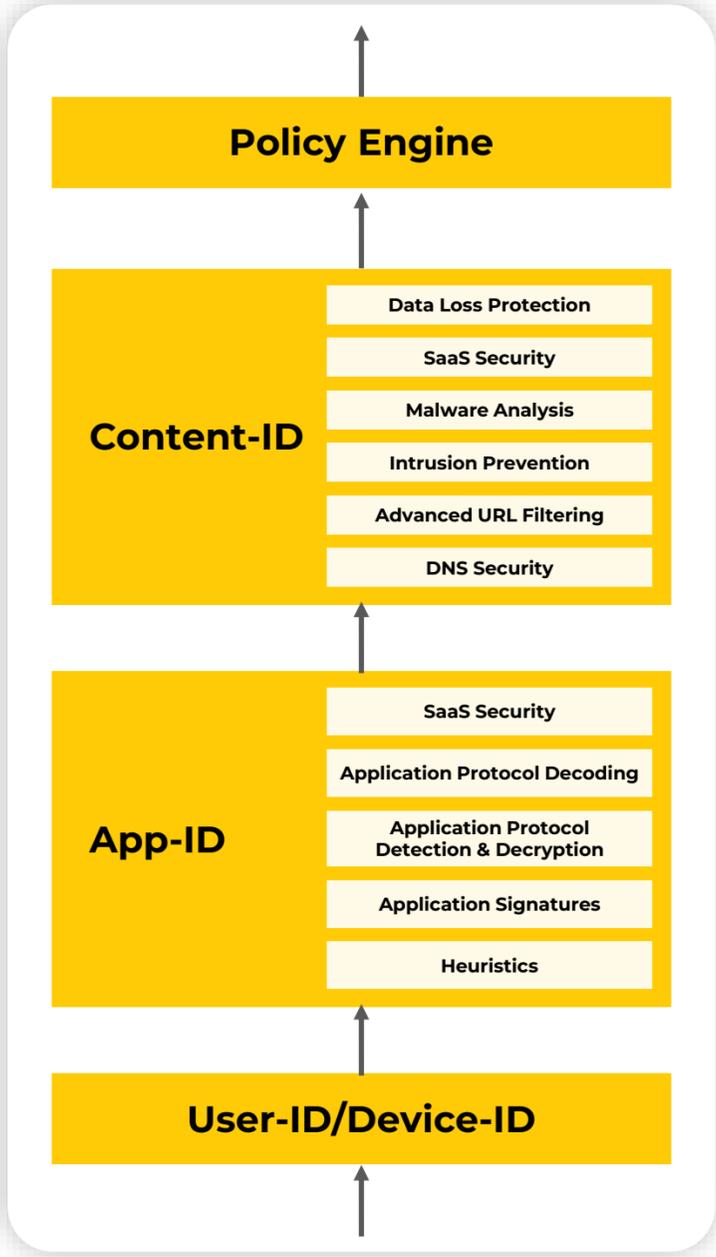- Significantly lower total cost of ownership.

For many years, security professionals have pursued the goal of integrating threat prevention services into the firewall to alleviate the need for additional devices for intrusion prevention systems (IPS), network antivirus, user behavior analysis, data loss prevention (DLP), device classification, and other functions. This integration makes perfect sense because the firewall is the cornerstone of security infrastructure.

Policy Engine

Content-ID
- Data Loss Protection
- SaaS Security
- Malware Analysis
- Intrusion Prevention
- Advanced URL Filtering
- DNS Security

App-ID
- SaaS Security
- Application Protocol Decoding
- Application Protocol Detection & Decryption
- Application Signatures
- Heuristics

User-ID/Device-ID

Scan it All, Scan it Once

paloalto NETWORKS

Miercom Competitive Report Available

Include head to head comparisons

PA-5430 VS **FG-4201**

PA-3440 VS **FG-2601F**

PA-3420 VS **FG-1801F**

PA-3400 series/PA-5400 series ML-Powered NGFWs

- Offer **up to 1.3X higher** throughput with security services enabled.

- Bring **superior real-world application** traffic performance.

- Provide a **lower Total Cost of Ownership per MB** secured.

Palo Alto Networks
Next Generation Firewall (NGFW)
Competitive Performance for Enterprise HQ
and Data Center Edge Use Cases

8 July 2022
Detailed Report DR220527D
Performance Validation Testing

[Download Report](#)

Third Party Testing Demonstrates Competitive Strength of PA-3400 series/PA-5400 series

|

Industry Validations

Inline Machine Learning

Our Solution:
ML-Powered NGFW with Inline deep learning provides real time protection against zero day threats.

Our Proof Points

Real-time security updates

99%

of CobaltStrike command and control traffic prevented compared to 20% (FTNT) and 13% (CSCO)
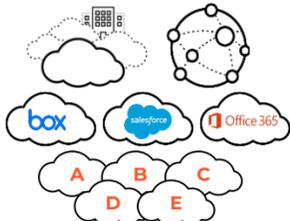
2022 SecureIQlab CobaltStrike report

True Zero Trust

Our Solution:
Natively integrated User-ID, App-ID, Device-ID — that enable policies of least privilege — and continuously assess trust.

Our Proof Points

Cloud Identity Engine

Automatically detects and secures new SaaS apps (60000+ and more App-IDs), in real time with SaaS Security with Machine Learning

Unify all identity across on-prem and cloud with Cloud Identity Engine.

Single Pass Architecture

Our Solution:
Enable continuous trust verification (always-on App-ID, User-ID and Device-ID) and security inspection without compromising performance.

Our Proof Points

30%

Higher performance compared to our competitors when security services are turned on

Miercom Reports
400 | 3400/5400 | 5450 | VM

Operational Simplicity

Our Solution:
Feature parity across all form factors. Local and central management offer identical UX.

Our Proof Points

45%

Easy to use with a single secure mode of operation

Reduction of risk of a breach thanks to consistent policies (Forrester TEI Report)

Key Differentiators
Delivering industry-leading security built on Zero Trust innovation

Palo Alto Networks	Fortinet
Prevents highly evasive threats and patient zero in real time ML-Powered NGFW with Inline deep learning stops more threats than traditional solutions, providing real time protection against zero day threats	**Cannot prevent the most advanced zero-day threats** Traditional security only. Legacy IPS, database-driven URL and DNS services, and basic DLP (only available in the CLI)
Delivers foundational Zero Trust components Natively integrated User-ID, App-ID, Device-ID — foundational Zero Trust components that enable policies of least privilege — applied to all traffic. Continuously assess trust based on changes in device posture, user behavior, and app function.	**Lacks foundational Zero Trust components** Trust services not natively integrated and enabled by default, leading to poor security outcomes. Lacks new SaaS apps detection and unified identity.
Perfectly balances security and performance 30% higher performance compared to Fortinet when security services are turned on — a critical requirement to deliver zero trust with continuous security inspection	**Forces a trade off between security and performance** Loses over 74% of advertised datasheet performance when security services are enabled
Simplifies operations and reduces risk Simplified management and feature parity across all form-factors that reduces opex and risk of a breach by 45%	**Operationally complex which increases risk** Lacks feature parity and consistency across platforms (FortiManager, FortiOS and CLI), decreasing productivity and increasing opportunities for error
Maximizes return on your investment (a) Built-in AIOps to proactively improve security posture and health. (b) Continuous security improvement with SLR, Policy Optimizer, BPA and more. (c) 7 time winner of exceptional customer success. Result: 247% ROI and 30% lesser time to achieve proper security posture	**Not designed to optimize ROI** Inadequate tools to improve security posture. Fortinet has never won an industry award for their support in 22 years

paloalto
NETWORKS

The largest organizations in the world trust Palo Alto Networks - Network Security Platform

paloalto NETWORKS

We are leaders with Retailers

Security Challenges in the Retail Industry

The rapid digital transformation has increased retailers' attack surface and driven the demand for cybersecurity to keep their businesses safe from threats and bad actors.

70%
increase in phishing attacks since the start of the COVID-19

64%
Point of Sale (PoS) attacks accounted for 64% of data breaches

43%
online and web attacks doubled to 43% during the pandemic

57%
IoT devices are vulnerable to medium or high severity cyber attacks[1]

Vulnerable WiFi networks make retailers targets for e-commerce scalping and mobile ad hijacking

$1.6M
Initial average ransomware demanded

Yesterday's security was not built with digital innovations in mind

42 of the Top 50 Retailers Choose Palo Alto Networks

See what our retail customers are saying about Palo Alto Networks on Gartner Peer Insights:

5.0 ★★★★★ Dec 15, 2020
I have experience with several platforms, and Palo Alto Networks firewalls are head and shoulders above the rest.
Read Full Review

5.0 ★★★★★ Dec 16, 2020
The Palo Alto Networks NGFWs are great for small layer 4 deployments to complex layer 7 deployments.
Read Full Review

5.0 ★★★★★ May 29, 2021
BEST NGFW in the market!
Read Full Review

5.0 ★★★★★ May 28, 2021
It's the smart next-generation firewall.
Read Full Review

5.0 ★★★★★ Oct 23, 2020
Palo Alto Networks is key to our security and risk management.
Read Full Review

5.0 ★★★★★ Dec 11, 2020
If you're looking for best of breed, you've come to the right place.
Read Full Review

---

paloalto NETWORKS

Why Retailers Trust Palo Alto Networks

The COVID-19 pandemic has accelerated digital transformation in the retail industry while creating new security challenges as retailers adapt to new operating models. Take a look at how Palo Alto Networks' industry-leading ML-Powered Next-Generation Firewalls can secure retail businesses of all sizes—without slowing down the speed of innovation.

Emerging Retail Trends

As consumers' shopping habits shift to the web, online sales and delivery continue to increase. During the COVID-19 pandemic, online retail sales increased over 32% in 2020[1]

Retailers are driving frictionless customer experiences through new channels like Buy Online Pick Up in Store (BOPUS) and Mobile Point-of-Sale (PoS)

Retailers are moving key business functions and applications in the cloud...

...as well as adopting automation and IoT devices in distribution centers

Retailers must also meet new compliance requirements to help ensure the security of credit card transactions (PCI DSS 4.0)

Why Palo Alto Networks for Retailers

Retailers need an end-to-end security platform uniquely positioned to help accelerate digital transformation initiatives and secure sensitive customer data.

Our ML-Powered Firewall platform

Protects frictionless customer experiences across all channels

NGFW — Next Generation Firewall

UF DNS — Advanced URL, DNS Security

SD-WAN — Next Generation SD-WAN

Empower store associates who use digital tools and technologies like smart devices for mobile point-of-sale, scanners for inventory management, and wearables for communications

NGFW — Next Generation Firewall

SD-WAN — Next Generation SD-WAN

DNS TP — Threat Prevention, DNS Security[1]

— Complete Zero Trust

Enables supply chain excellence by protecting automation systems and IoT devices

NGFW — Next Generation Firewall

— IoT Security

Supports regulatory compliance and data privacy requirements

NGFW — Next Generation Firewall

PN — Panorama Network Security Management

DLP — DLP Security

— Visibility, Network Segmentation and Policy Enforcement

paloalto NETWORKS

In A Volatile Industry, Palo Alto Networks Offers Stability & Growth

siliconANGLE
Dell sells RSA cybersecurity firm to private equity consortium for $2B+

Sophos acquisition bid presents potential growth, peril

Private equity firm Thoma Bravo made an offer to acquire Sophos for approximately $3.9 billion. Analysts discuss what the deal might mean for the endpoint security vendor.

Cybereason Lays Off 10% of Staff Months After Raising $325M

Forbes

CYBERSECURITY
The Demise Of Symantec
Richard Stiennon Former Contributor ⓘ
Industry analyst. Author.

Palo Alto Networks promoted to S&P 500, replacing Dish Network

Broadcom announces plans to buy VMware in $61 billion deal
PUBLISHED THU, MAY 26 2022 7:14 AM EDT

eking Alpha^α
ackBerry's Cylance: Anatomy f A Bad Acquisition

sdxcentral Will Citrix Share McAfee-FireEye's Fate?

paloalto
NETWORKS

Our Execution and Vision is Recognized by Analysts

CHALLENGERS | LEADERS

- Fortinet
- Cisco
- Palo Alto Networks
- Alibaba Cloud
- Juniper
- Check Point Software Technologies
- Huawei
- Microsoft
- Amazon Web Services
- SonicWall
- H3C
- Barracuda
- WatchGuard
- Hillstone Networks
- Sophos
- Sangfor Technologies
- Forcepoint

NICHE PLAYERS | VISIONARIES

ABILITY TO EXECUTE

COMPLETENESS OF VISION

As of September 2022   © Gartner, Inc

Gartner®

Gartner®

An 11-Time Leader
in 2022 Gartner® Magic Quadrant™ for Network Firewalls

11 Years of Delivering Network Innovation and Security

Gartner Magic Quadrant for Network Firewalls, Rajpreet Kaur, Jeremy D'Hoinne, Nat Smith, Adam Hils, 1st November 2021.

Gartner and Magic Quadrant are registered trademarks and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and are used herein with permission. All rights reserved.

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Palo Alto Networks.

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

paloalto
NETWORKS

We're a Leader in The Forrester Wave: Enterprise Firewalls, Q4 2024

THE FORRESTER WAVE™
Enterprise Firewall Solutions
Q4 2024

Top-ranked in Current Offering Category; Highest possible scores in Innovation, Vision, Roadmap Criteria

Report highlights:
- High scores possible in 18 criteria, including policy creation and management, automation efficacy, FW-as-a-Service, ZTE/SASE, SD-WAN, IoT/OT and more

- **Our platform approach** "provides feature-rich and fully-functional centralized management of PAN-OS firewalls – hardware and software – as well as Prisma SASE across a hybrid enterprise."

- "**Precision AI,** Palo Alto Networks' proprietary AI system, automates tasks with data from ML, deep learning, and AI models to enhance platform experience.

- "Its **ambitious roadmap, driven by customer feedback**, highlights capabilities that align with its vision for a secure future in the quantum and AI era."

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

The Forrester Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave™ are trademarks of Forrester Research, Inc. The Forrester Wave™ is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave™. Information is based on the best available resources. Opinions reflect judgment at the time and are subject to change.

Thank you