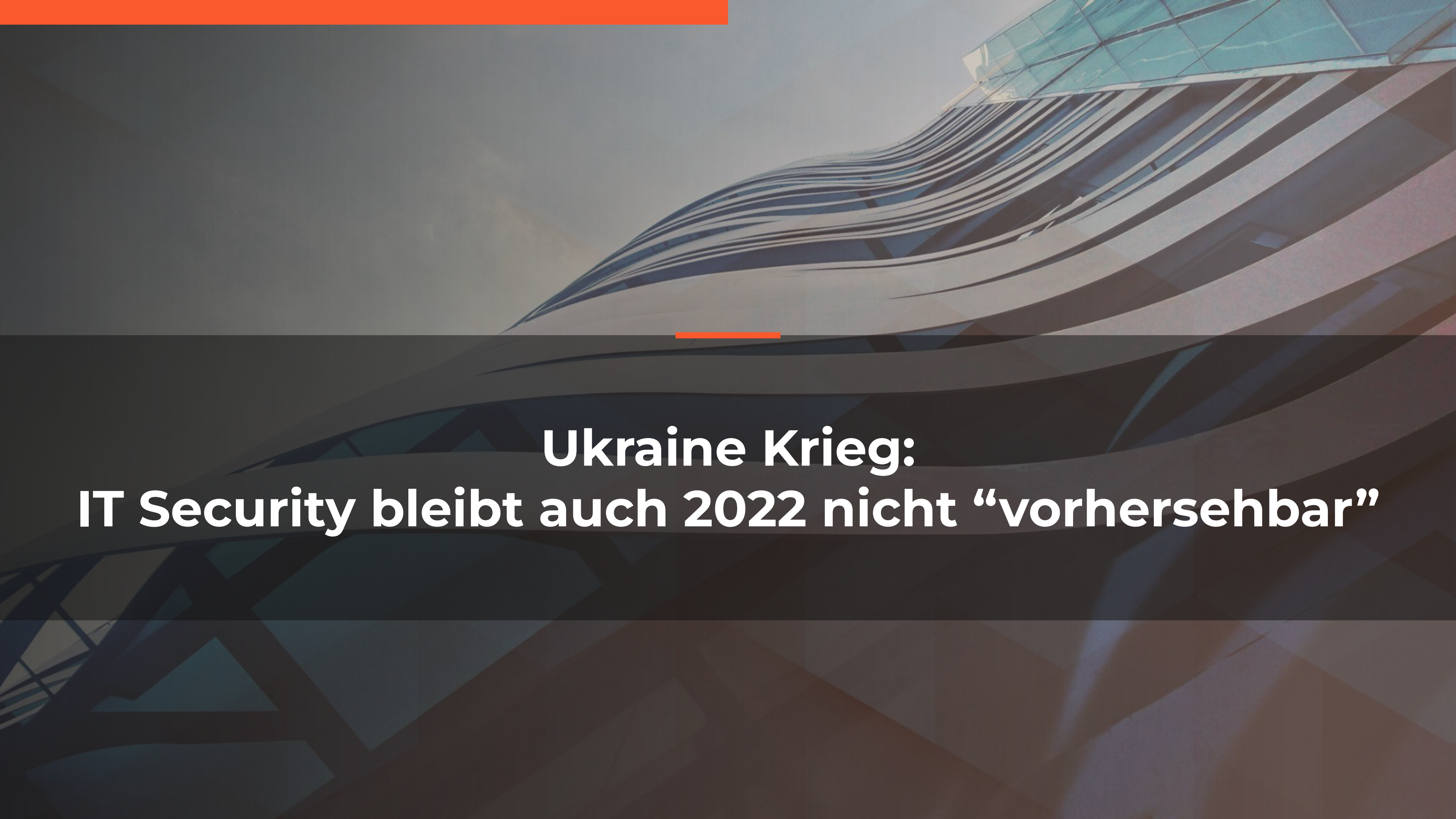
What’s next?

Neuigkeiten in Palo Alto Networks Strata

Christian Kurta | System Engineer - Palo Alto Networks
Manuel Lecher-Peham | System Engineer - KBC Group

paloalto® NETWORKS | Cybersecurity Partner of Choice

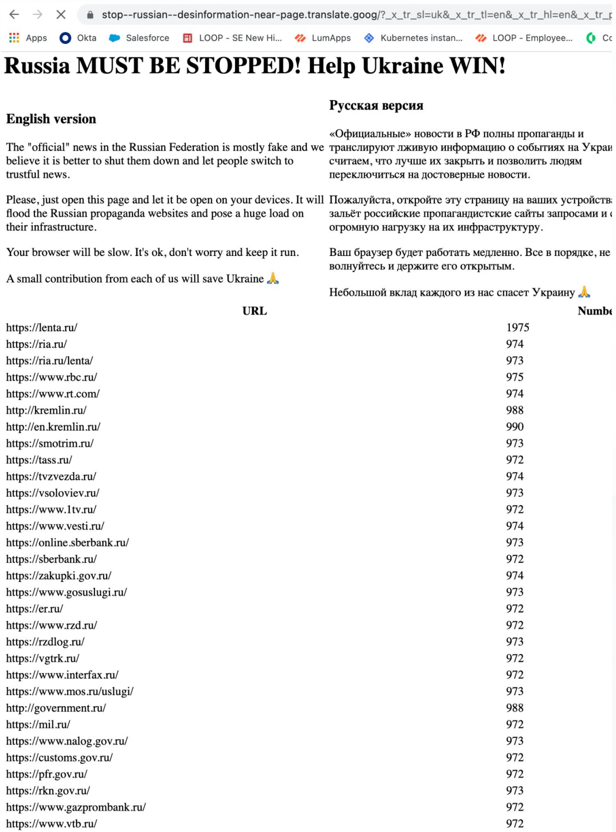


Ukraine Krieg:
IT Security bleibt auch 2022 nicht “vorhersehbar”

Aktuelle Sicherheitsbedrohungen

1. Cyberkrieg ist realität geworden: Cyber Pearl Harbor
2. Malware wird kommerziell / Entwicklung auf Staatskosten
3. Das Internet ist nicht mehr “frei” / Krieg im BGP
4. Die Cloud wird einfach besetzt (Co-Locations) / Lumen bzw Cogent
5. Ransomware-as-a-Service Gruppen gehen aufeinander los

1 Cyberkrieg ist realität geworden: Cyber Pearl Harbor



stop--russian--desinformation-near-page.translate.goog/?_x_tr_sl=uk&_x_tr_tl=en&_x_tr_hl=en&_x_tr_p

Russia MUST BE STOPPED! Help Ukraine WIN!

English version

The "official" news in the Russian Federation is mostly fake and we believe it is better to shut them down and let people switch to trustful news.

Please, just open this page and let it be open on your devices. It will flood the Russian propaganda websites and pose a huge load on their infrastructure.

Your browser will be slow. It's ok, don't worry and keep it run.

A small contribution from each of us will save Ukraine 🙏

Русская версия

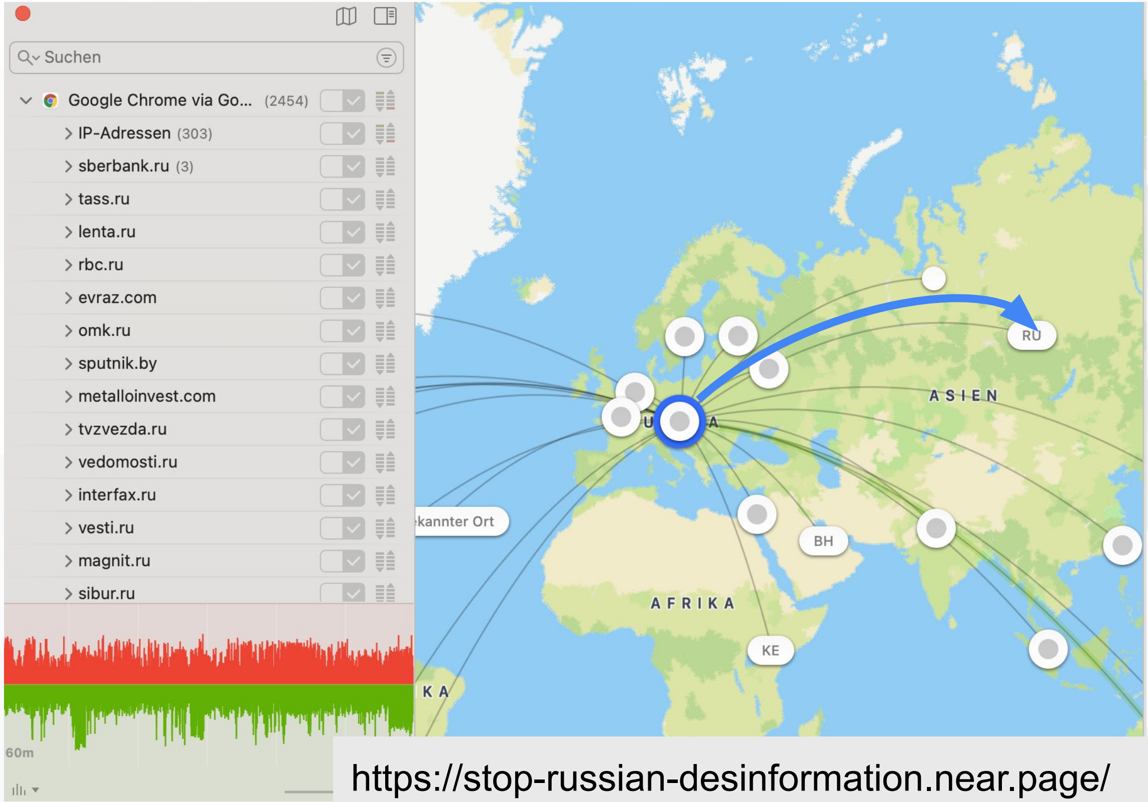
«Официальные» новости в РФ полны пропаганды и транслируют лживую информацию о событиях на Украи считаем, что лучше их закрыть и позволить людям переключиться на достоверные новости.

Пожалуйста, откройте эту страницу на ваших устройства зальёт российские пропагандистские сайты запросами и огромную нагрузку на их инфраструктуру.

Ваш браузер будет работать медленно. Все в порядке, не волнуйтесь и держите его открытым.

Небольшой вклад каждого из нас спасет Украину 🙏

URL	Numbe
https://lenta.ru/	1975
https://ria.ru/	974
https://ria.ru/lenta/	973
https://www.rbc.ru/	975
https://www.rt.com/	974
http://kremlin.ru/	988
http://en.kremlin.ru/	990
https://smotrim.ru/	973
https://tass.ru/	972
https://tvzvezda.ru/	974
https://vsoloviev.ru/	973
https://www.1tv.ru/	972
https://www.vesti.ru/	974
https://online.sberbank.ru/	973
https://sberbank.ru/	972
https://zakupki.gov.ru/	974
https://www.gosuslugi.ru/	973
https://er.ru/	972
https://www.rzd.ru/	972
https://rzdlog.ru/	973
https://vgtrk.ru/	972
https://www.interfax.ru/	972
https://www.mos.ru/uslugi/	973
http://government.ru/	988
https://mil.ru/	972
https://www.nalog.gov.ru/	973
https://customs.gov.ru/	972
https://pfr.gov.ru/	972
https://rkn.gov.ru/	973
https://www.gazprombank.ru/	972
https://www.vtb.ru/	972



Google Chrome via Go... (2454)
- IP-Adressen (303)
- sberbank.ru (3)
- tass.ru
- lenta.ru
- rbc.ru
- evraz.com
- omk.ru
- sputnik.by
- metalloinvest.com
- tvzvezda.ru
- vedomosti.ru
- interfax.ru
- vesti.ru
- magnit.ru
- sibur.ru

https://stop-russian-desinformation.near.page/

2 Malware wird kommerziell / Entwicklung auf Staatskosten

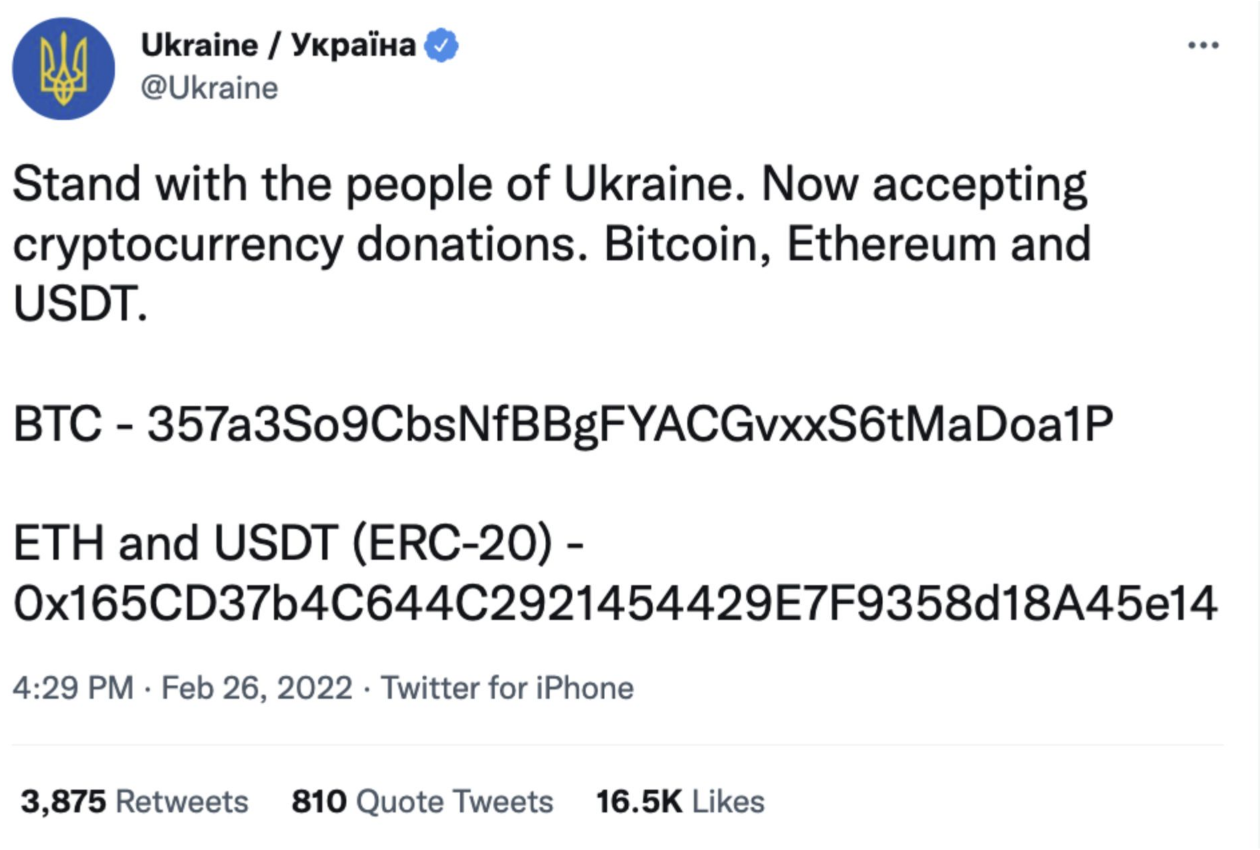
```
                                                                                     -58,-1,-43,-21,
12,91,49,-46,82,104,0,2,64,-124,82,82,82,83,82,80,104,-21,85,46,59,-1,-43,-119,
58,-125,-61,80,49,-1,87,87,106,-1,83,86,

                                                                                     104,45,6,24,123
-1,-43,-123,-64,15,-124,-61,1,0,0,49,-1,-123,-10,116,4,-119,-7,-21,9,104,-86,-5
,-30,93,-1,-43,-119,-63,104,69,33,94,49,-1,

                                                                                     -43,49,-1,87,16
,7,81,86,80,104,-73,87,-32,11,-1,-43,-65,0,47,0,0,57,-57,116,-73,49,-1,-23,-111
1,0,0,-23,-55,1,0,0,-24,-117,-1,

                                                                                     -1,-1,47,80,75,
6,117,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
```

Anonyme Kriegsfinanzierung



Ukraine / Україна
@Ukraine

Stand with the people of Ukraine. Now accepting cryptocurrency donations. Bitcoin, Ethereum and USDT.

BTC - 357a3So9CbsNfBBgFYACGvxxS6tMaDoa1P

ETH and USDT (ERC-20) - 0x165CD37b4C644C2921454429E7F9358d18A45e14

4:29 PM · Feb 26, 2022 · Twitter for iPhone

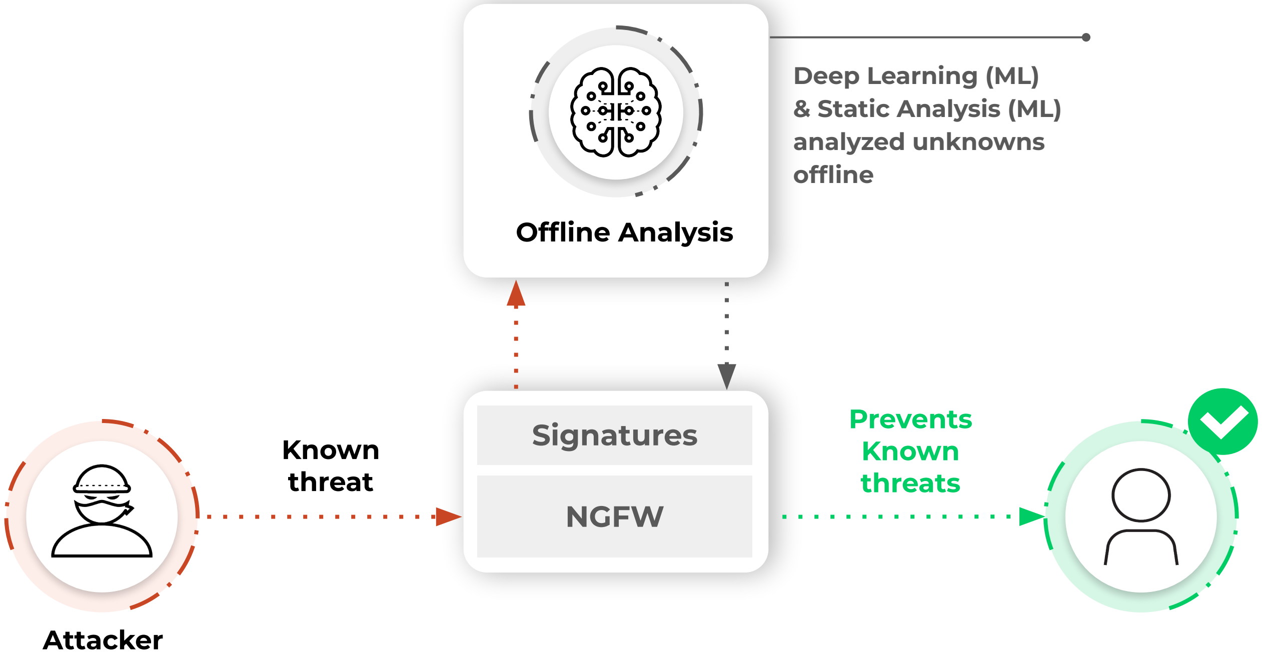
3,875 Retweets **810** Quote Tweets **16.5K** Likes paloalto

SAY HELLO TO PAN-OS NEBULA

Now, you can stop zero-day threats in zero time

SEE HOW IT WORKS TODAY ▶

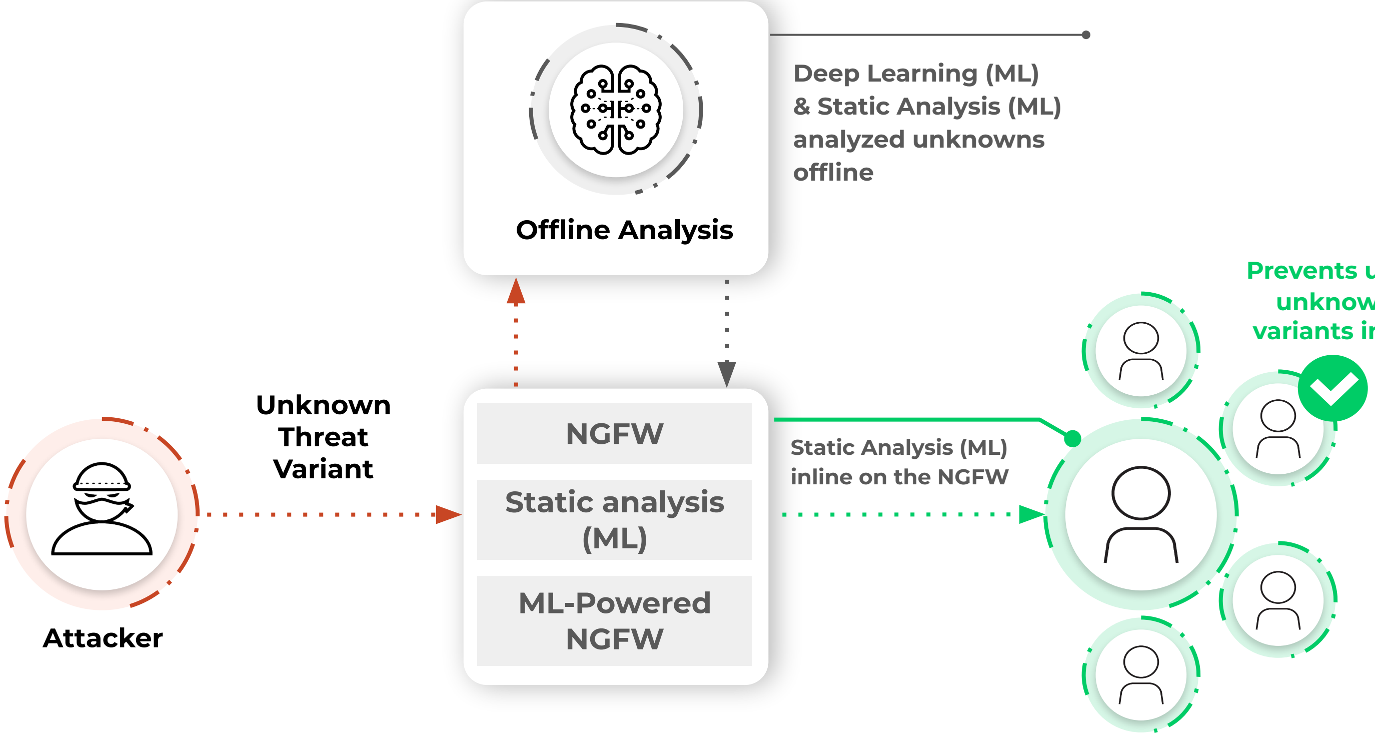
Traditional Network Security Stops Known Attacks with Signatures



Offline Analysis

Deep Learning (ML) & Static Analysis (ML) analyzed unknowns offline

ML-Powered NGFW was a Huge Step in Defending Unknown Attacks



Offline Analysis

Deep Learning (ML) & Static Analysis (ML) analyzed unknowns offline

Attacker

Unknown Threat Variant

NGFW

Static analysis (ML)

ML-Powered NGFW

Static Analysis (ML) inline on the NGFW

Prevents up to 95% unknown threat variants in real time

Organizations Must Assume Nation State-Level Attack Sophistication

Rise in malware using Cobalt Strike

73%

YoY*

Sophisticated **Red Team tools** now empower attackers of **all skill levels** to evade detection

Phishing services with built-in detection evasions

90%

Successful phishing attacks have increased with hybrid work and evasive **phishing-as-a-service**

Stealthy data exfil attacks per month

>20M

Widely available **hack tools** are bringing sophisticated **data exfiltration techniques** to all

Modern Network Security Requires a Fundamentally New Approach to Stop Zero-day Threats

Harness the power of Deep Learning

Powerful detection for today's most evasive and targeted attacks

Analyze real traffic as attacks unfold

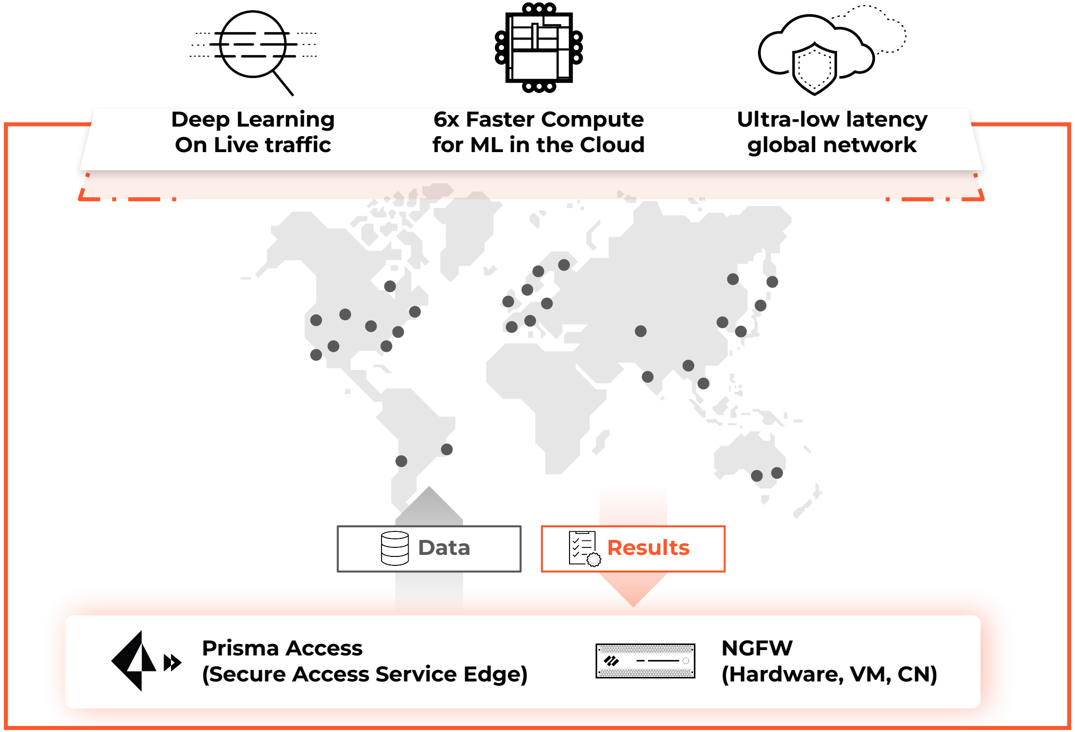
Detects targeted attacks that evade offline simulations and web crawlers

Run inline by being blazingly fast

Prevents an attack by stopping the 0-day and saving the initial victim

Introducing 'Inline Deep Learning'

Stop Zero-Day threats in Zero Time

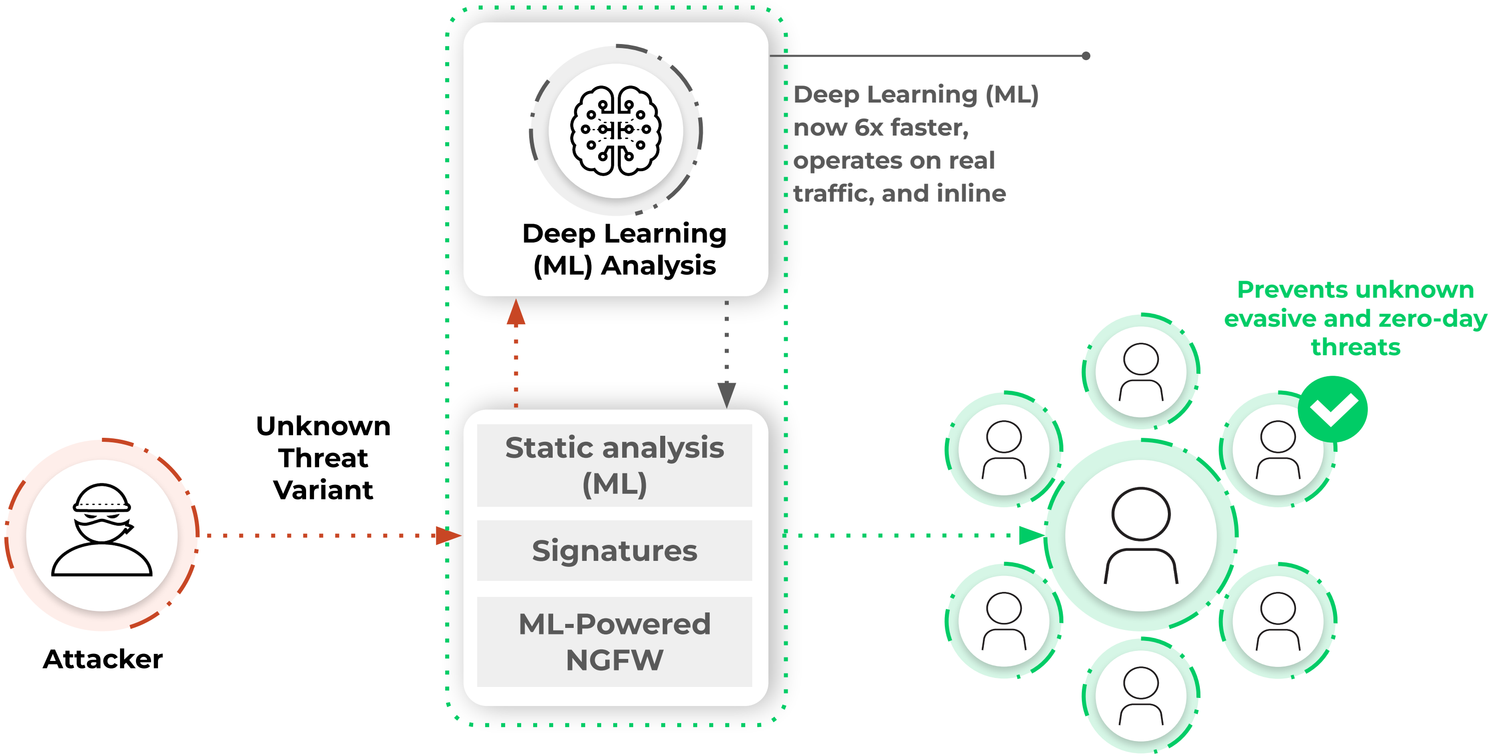


✓ All-new cloud-based **deep learning engine** detects today's most challenging **unknown attacks 6x faster**

✓ Brings **next-level prevention inline** to **defend the initial target**

✓ Ultra-low latency global network **streams real data** from **cloud-based** and **on-prem** network security deployments

PAN-OS Nebula is the Next Evolution in Network Security



Deep Learning (ML) now 6x faster, operates on real traffic, and inline

Prevents unknown evasive and zero-day threats

PAN-OS 10.2 Nebula

Stop Zero-Day threats in Zero Time with Nebula, the 10.2 release of our industry-leading PAN-OS

ADV TP

Advanced Threat Prevention
The only IPS to stop unknown C2 attacks in real-time, **48%** more than previously

ADV URL DNS

Adv URL and DNS Protection
Stops **40%** more phishing attacks, **40% greater** DNS threat coverage than any competitor

IoT

IoT Security 2.0
Safeguard every 'thing' with the industry's smartest security for IoT devices

AIOps

AIOps
Predictably better security and higher ROI with industry's **first AIOps for NGFWs**

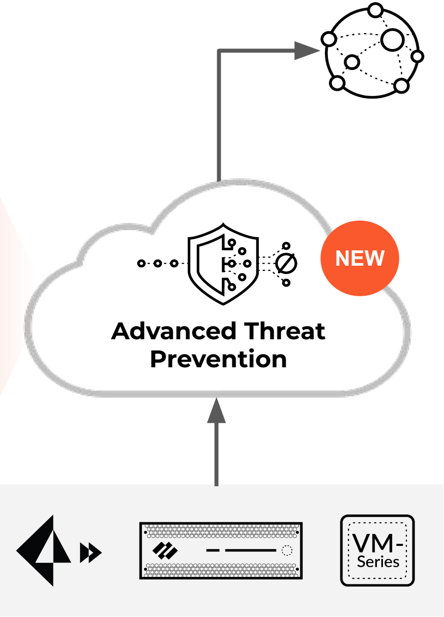
Advanced Threat Prevention

The industry's *only* IPS to stop unknown C2 in real-time

Unknown C2 Detection Engine

- Deep Learning models
- Encrypted Traffic Classifier
- Anomaly Detector
- Malware Family Classifier
- Continuous Model Validation/Training Pipeline
- Prevention against C2 derived from hack tools (Eg: Cobalt Strike)

+ all the leading capabilities from Threat Prevention



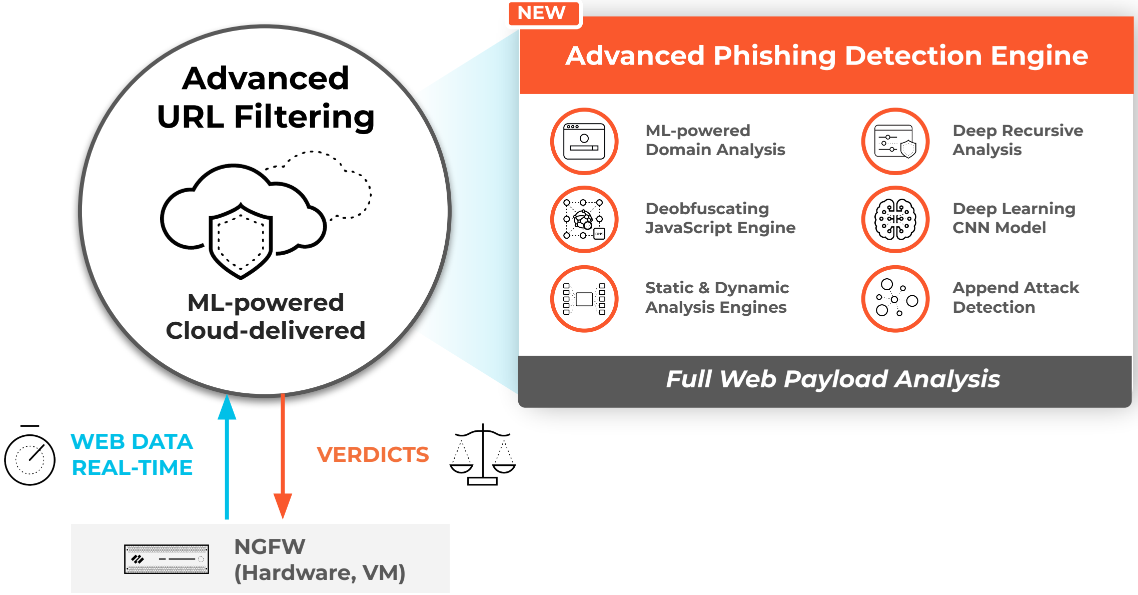
48%

Increase in C2 threat detection compared to industry's leading Threat Prevention solution

Previously unknown C2 communications **blocked inline**

Advanced URL Filtering

The Industry’s *First* Real-Time Prevention of New and Evasive Web-based Attacks



Advanced URL Filtering

ML-powered Cloud-delivered

NEW

Advanced Phishing Detection Engine

ML-powered Domain Analysis

Deep Recursive Analysis

Deobfuscating JavaScript Engine

Deep Learning CNN Model

Static & Dynamic Analysis Engines

Append Attack Detection

Full Web Payload Analysis

WEB DATA REAL-TIME

VERDICTS

NGFW (Hardware, VM)

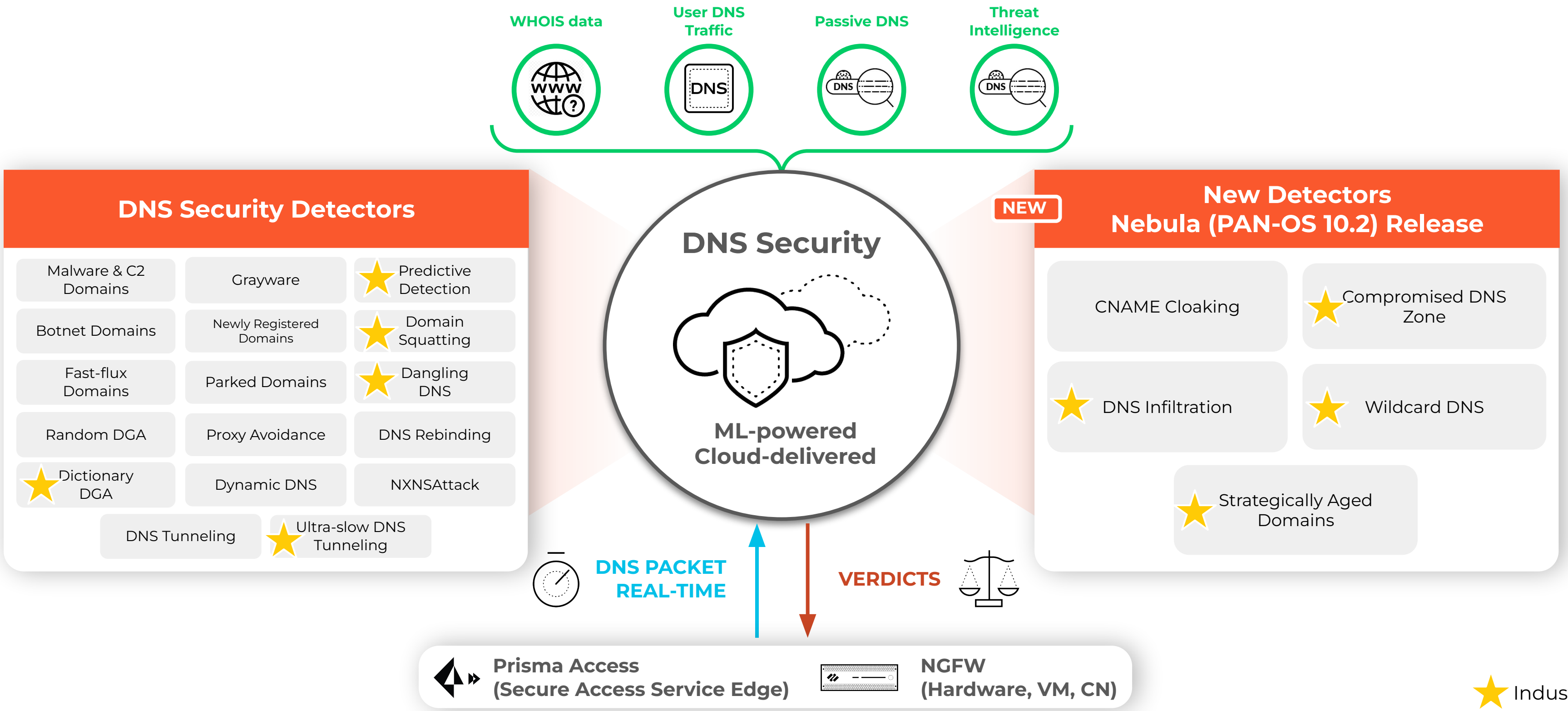
✓ **Prevents 40% more threats than traditional web filtering databases**

✓ **Powerful new detectors defeat evasive techniques used in 90% of modern phishing kits**

✓ **76% of malicious URLs discovered 24 hours before other vendors**

DNS Security

The industry's *leading* DNS Threat coverage, 40% More Than Any Other Vendor



WHOIS data

User DNS Traffic

Passive DNS

Threat Intelligence

DNS Security Detectors

- Malware & C2 Domains
- Grayware
- ★ Predictive Detection
- Botnet Domains
- Newly Registered Domains
- ★ Domain Squatting
- Fast-flux Domains
- Parked Domains
- ★ Dangling DNS
- Random DGA
- Proxy Avoidance
- DNS Rebinding
- ★ Dictionary DGA
- Dynamic DNS
- NXNSAttack
- DNS Tunneling
- ★ Ultra-slow DNS Tunneling

DNS Security

ML-powered Cloud-delivered

NEW

New Detectors Nebula (PAN-OS 10.2) Release

- CNAME Cloaking
- ★ Compromised DNS Zone
- ★ DNS Infiltration
- ★ Wildcard DNS
- ★ Strategically Aged Domains

DNS PACKET REAL-TIME

VERDICTS

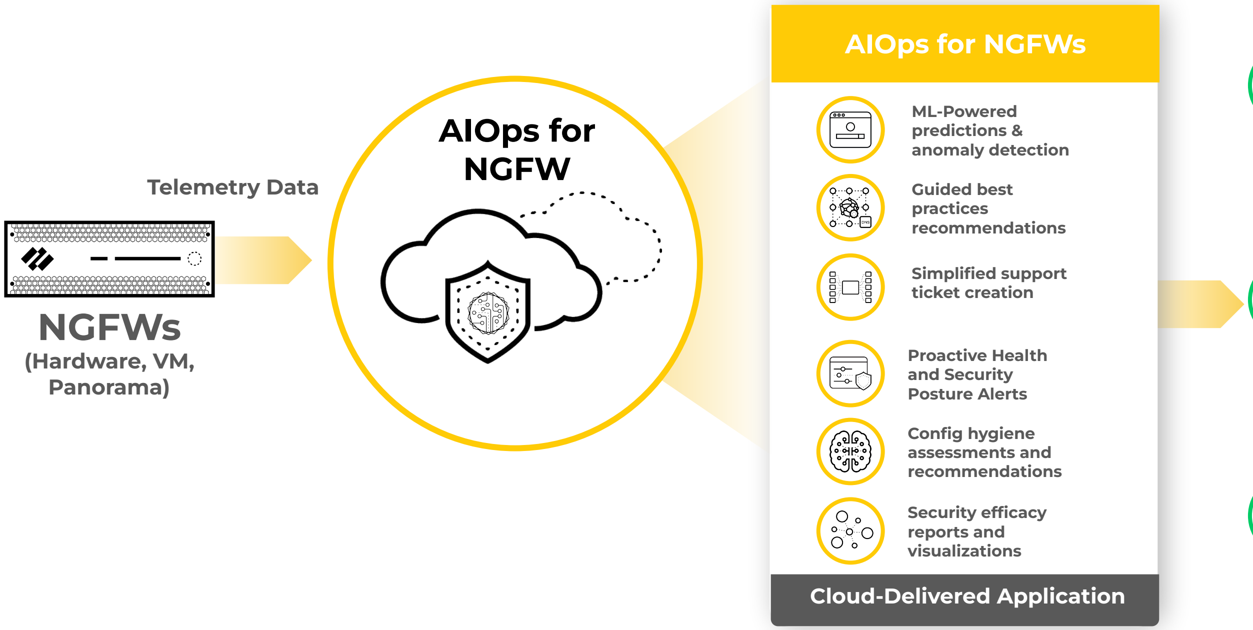
Prisma Access (Secure Access Service Edge)

NGFW (Hardware, VM, CN)

★ Industry First

Introducing Industry’s first AIOps for NGFWs

Revolutionize NGFW operations with ML-powered insights for the best security posture and optimal health



AIOps for NGFWs

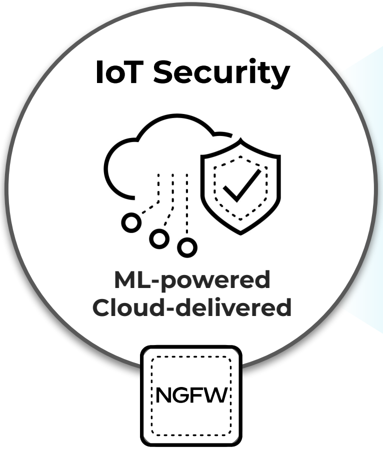
- ML-Powered predictions & anomaly detection
- Guided best practices recommendations
- Simplified support ticket creation
- Proactive Health and Security Posture Alerts
- Config hygiene assessments and recommendations
- Security efficacy reports and visualizations

Cloud-Delivered Application

- ✓ **Get best practices** recommendations that are easy to deploy
- ✓ **Gain insights** across your deployment to maximize return on investment
- ✓ **Predict** firewall health, performance and capacity disruptions

IoT Security 2.0

Safeguard every ‘thing’ with the industry’s smartest security for smart devices



IoT Security

ML-powered
Cloud-delivered

NGFW

IoT Security 2.0

Visibility

- **>90%** devices identified in less than 48 hours with ML
- NEW — Unified visibility for security analysts with XDR integration
- Enhanced — Built-in integrations eliminate IoT blindspots in existing security solutions

Prevention

- Built-in prevention for known and unknown IoT threats
- Enhanced — **20X** Faster Zero Trust security with automated policies
- NEW — **1-Click** Automated posture and compliance reporting

Deployment

- NEW — **70X time** saved in activating IoT Security on current NGFW without changing current topology

✓ **Quick & accurate discovery**

✓ **Best-in-class protection**

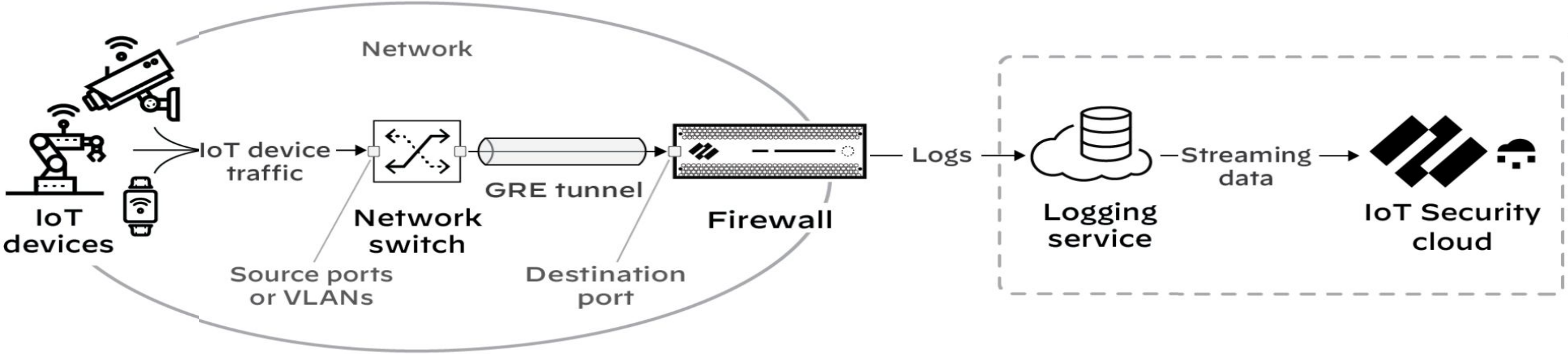
✓ **Automated Zero Trust Security**

✓ **Integrated workflows**

ERSPAN (Encapsulated remote SPAN)

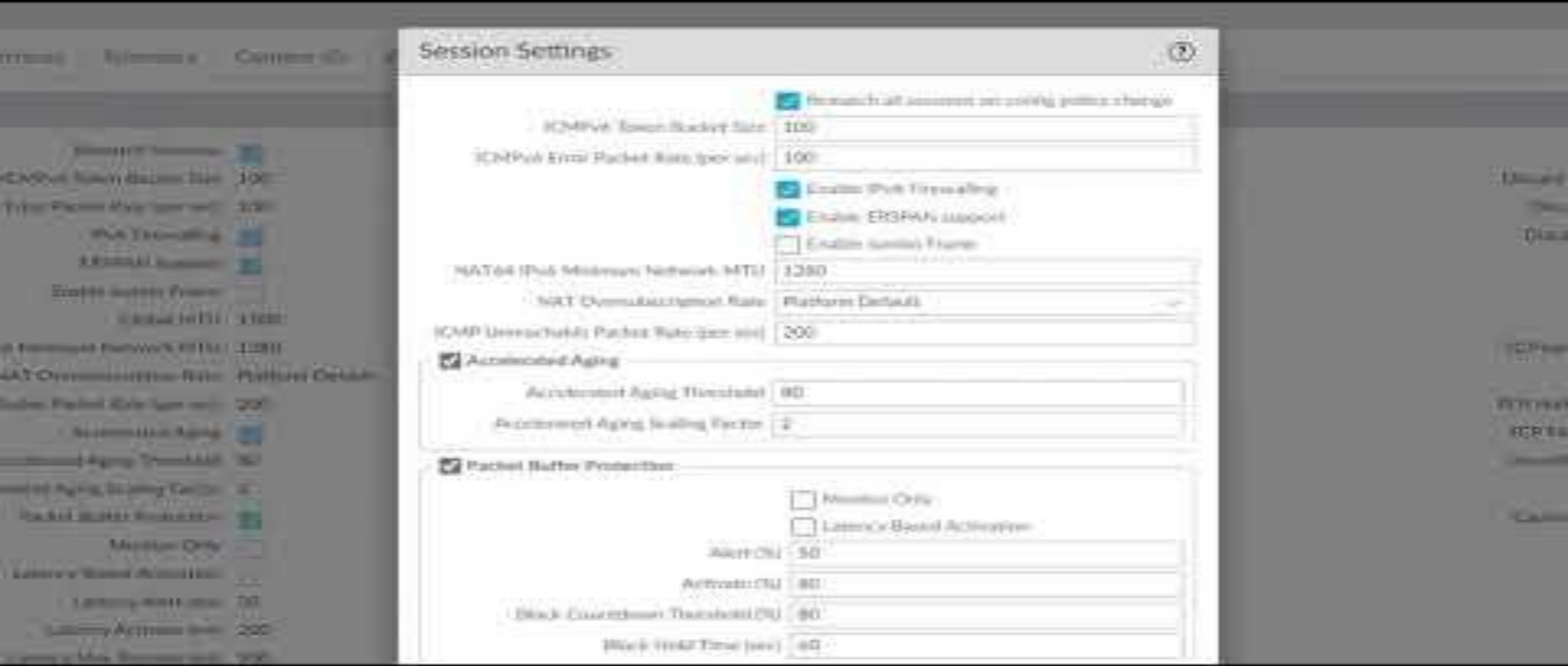
Einfaches IoT Onboarding

ERSPAN Setup for IoT



Supported Devices: Catalyst 9600,9500,9400,9300. Not Supported: Catalyst 9200

Older HW: Catalyst 6500, 7600, 4500, Nexus, ASR 1000



Session Settings

☑ Rematch all sessions on config policy change

ICMPv6 Token Bucket Size: 100

ICMPv6 Error Packet Rate (per sec): 100

☑ Enable IPv6 Firewalling

☑ Enable ERSPAN support

□ Enable Jumbo Frame

NAT64 IPv6 Minimum Network MTU: 1280

NAT Oversubscription Rate: Platform Default

ICMP Unreachable Packet Rate (per sec): 200

☑ Accelerated Aging

Accelerated Aging Threshold: 80

Accelerated Aging Scaling Factor: 2

☑ Packet Buffer Protection

□ Monitor Only

□ Latency Based Activation

Alert (%): 50

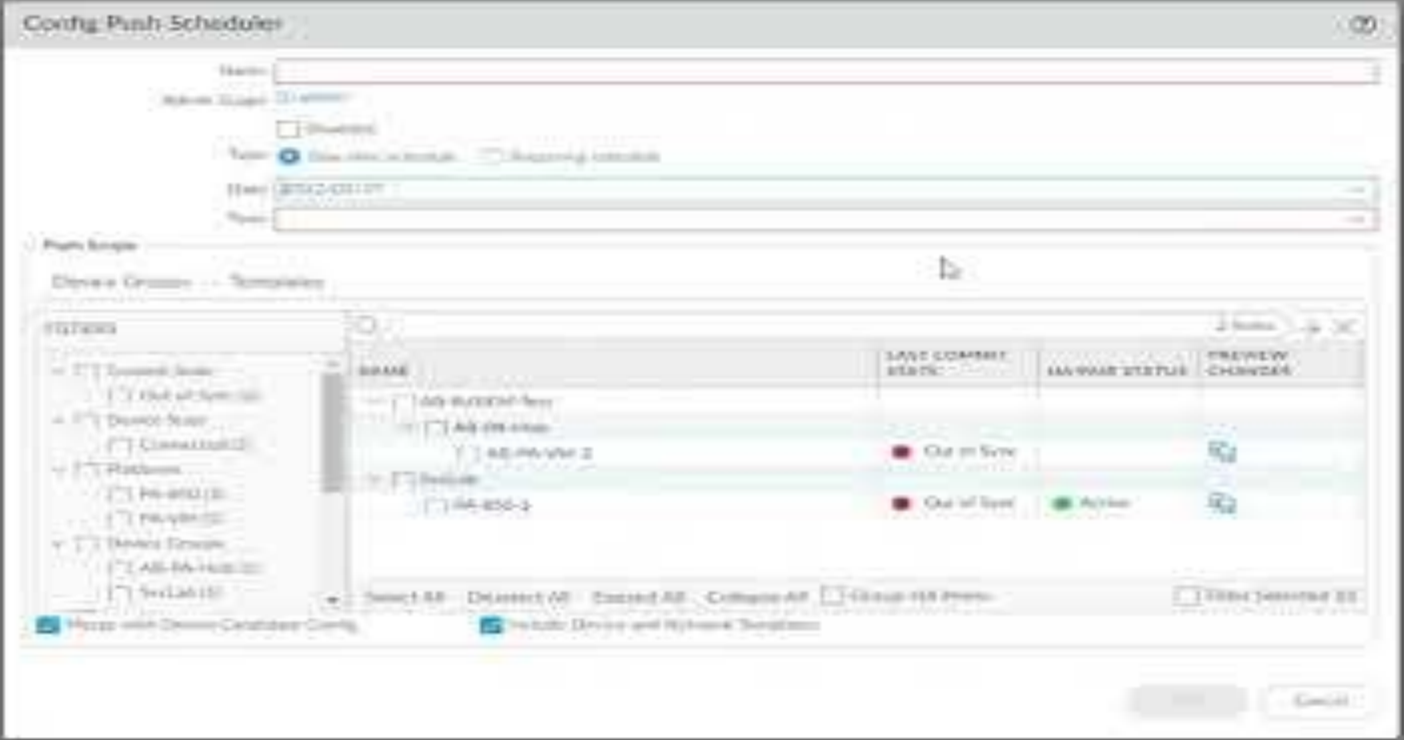
Activate (%): 80

Block Countdown Threshold (%): 80

Block Hold Time (sec): 60

Panorama Features

Scheduled Commit



Config Push Scheduler

Name:

Admin Scope: admin

□ Disabled

Type: ● One-time schedule ○ Recurring schedule

Date: 2022-03-17

Time:

Push Scope

Device Groups | Templates

FILTERS
- □ Commit State
  - □ Out of Sync (2)
- □ Device State
  - □ Connected (2)
- □ Platform
  - □ PA-850 (1)
  - □ PA-VM (1)
- □ Device Groups
  - □ AB-PA-Hub (1)
  - □ SvLab (1)

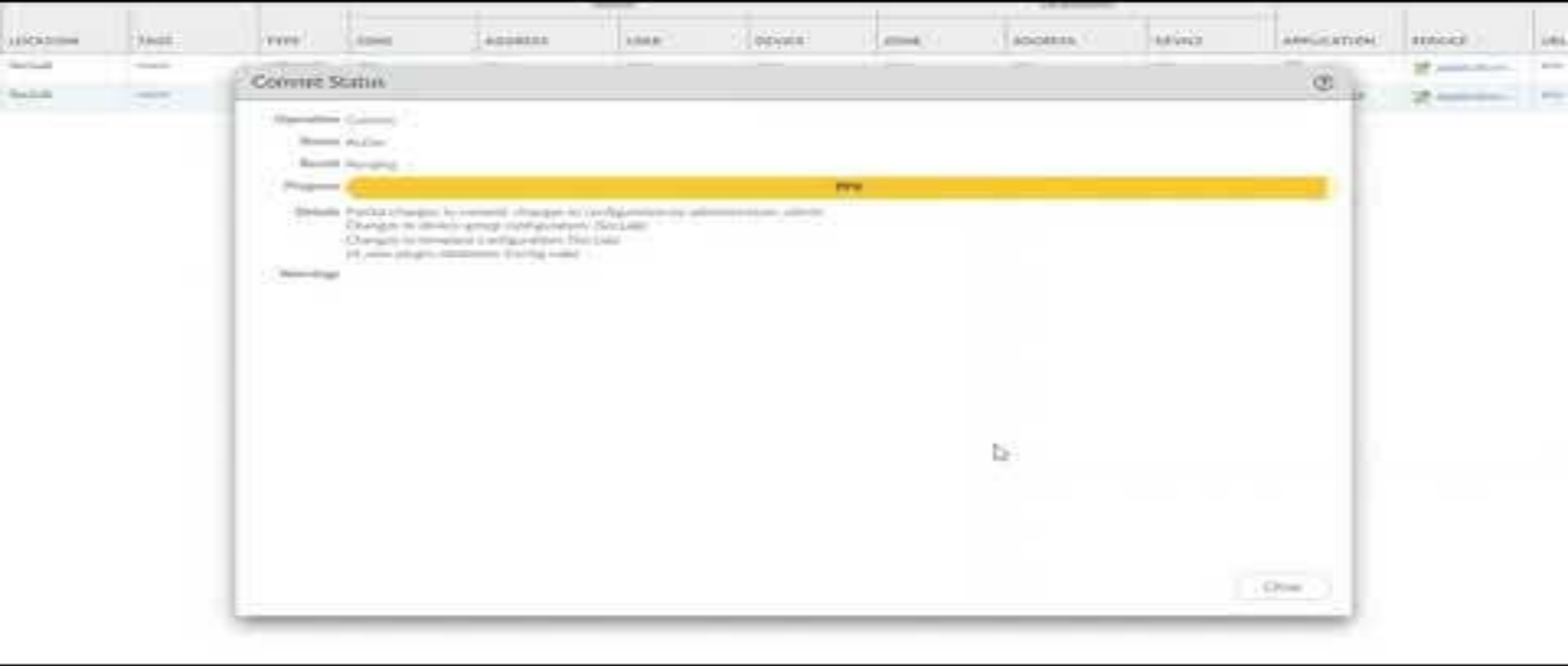
NAME	LAST COMMIT STATE	HA PAIR STATUS	PREVIEW CHANGES
□ AB-BRANCH-Test			
□ AB-PA-Hub			
□ AB-PA-VM-2	● Out of Sync		⧉
□ SvLab			
□ PA-850-1	● Out of Sync	● Active	⧉

Select All Deselect All Expand All Collapse All □ Group HA Peers □ Filter Selected (0)

☑ Merge with Device Candidate Config ☑ Include Device and Network Templates

Panorama Features

Partial Commit



Commit Status

Operation Commit

Status Active

Result Pending

Progress [illegible]

Details Partial changes to commit: changes to configuration by administrators: admin
Changes to device group configuration: (SecLab)
Changes to template configuration: (SecLab)
[illegible]

Warnings

Global Protect 6.0

Endpoint Traffic Policy Enforcement

Prevents traffic bypassing the tunnel, either through malicious inbound access or applications binding to the physical adapter, or end-user tampering with the routing table.

Redesigned GlobalProtect App User Interface for Windows and macOS

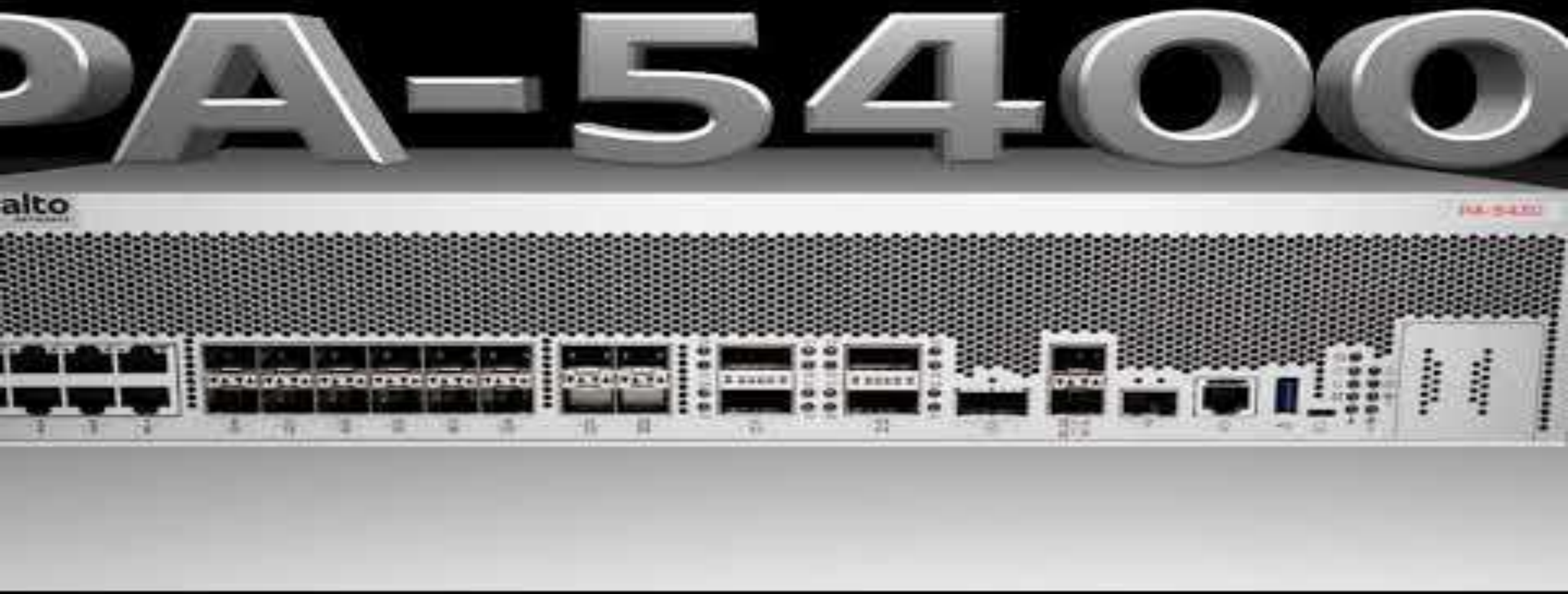
A new, streamlined user interface for macOS and Windows endpoints provides improved workflows for quickly understanding connectivity and access issues.

SAML Authentication with Cloud Authentication Service

SAML Authentication is now integrated with Cloud Authentication Service, enabling authentication using cloud identity providers (IdPs) such as Onelogin or Okta.

Global Protect 6.0

What’s next: Neue Hardware

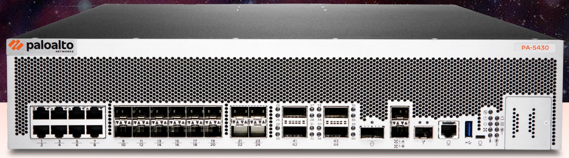


PA-5400
alto
PA-5400

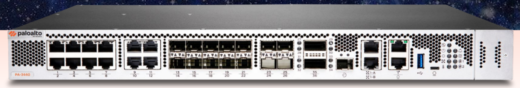
3x Faster Security

in a smaller package

PA-5400 Series



PA-3400 Series



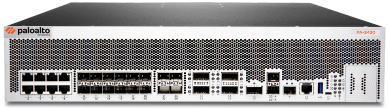
with new 4th Generation ML-Powered NGFWs

*Up to 3x performance compared to the PA-5200 Series and PA-3200 Series

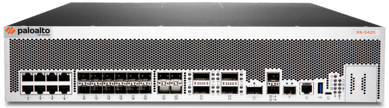
New ML-Powered PA-5400 and PA-3400 Series NGFW

3x security performance for Data Center, Internet Edge and Campus

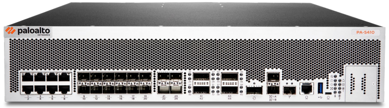
PA-5400 Series



PA-5430

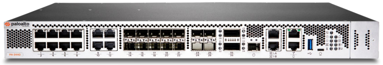


PA-5420

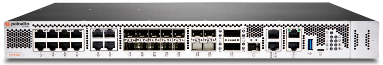


PA-5410

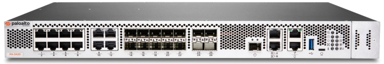
PA-3400 Series



PA-3440



PA-3430



PA-3420

PA-3410

	PA-5410	PA-5420	PA-5430
App-ID Performance	36.7 Gbps	47.5 Gbps	59.4 Gbps
Threat Performance	23.5 Gbps	30.5 Gbps	40.9 Gbps
Networking I/O	4x 40/100G; 4x 25G; 12x 10G; 8x mGig		
Size	2RU (30% Reduction)		

	PA-3410	PA-3420	PA-3430	PA-3440
App-ID Performance	11.3 Gbps	16.5 Gbps	19.6 Gbps	24 Gbps
Threat Performance	5.9 Gbps	8.8 Gbps	10.2 Gbps	12.7 Gbps
Networking I/O	4x 25G; 10x 10G; 12x mGig		2x 40/100G; 4x 25G; 10x 10G; 12x mGig	
Size	1RU (50% Reduction)			

50+ Features in PAN-OS 10.2 Nebula

Advanced Threat Prevention

- Advanced Threat Prevention subscription
- Inline Cloud Analysis/Deep learning Support
- Cloud-delivered ML-based C2 prevention

DNS Security

- 6 new attack techniques prevented

Advanced URL Filtering

- New anti-phishing capabilities
- Cloud Inline Categorization / Deep Learning Support
- HTTP Header Insertion Expansion

IoT Security

- ML-based automation of FW policy recommendations
- Simplification & automation for IoT data collection and traffic visibility
- Support for RSPAN & ERSPAN

AIOps

- Cloud-delivered application to strengthen security posture and maintain deployment health

Software Firewalls

- VM-Series Elastic Memory Profiles
- Auto-push content updates to software firewalls
- Support for 64 vCPUs on VM-Series; 47 vCPUs on CN-Series
- CN-Series Firewall as a Kubernetes CNF
- High Availability Support for CN-Series Firewall as a Kubernetes CNF
- Daemonset (vwire) IPv6 Support
- L3 IPv4 support for CN-Series
- IPv6 DAG Plugin Support
- DPDK support for CN-Series

Networking

- Advanced Routing Engine
- HA Cluster Behavior Change for Modular Systems

Decryption

- Multiple certificate support for inbound decryption

User-ID / CIE

- SCIM Support for CIE
- Extending visibility across additional platforms (SaaS Inline, Device Insights, ADEM, CDL, Explore, Visualization and Reporting)

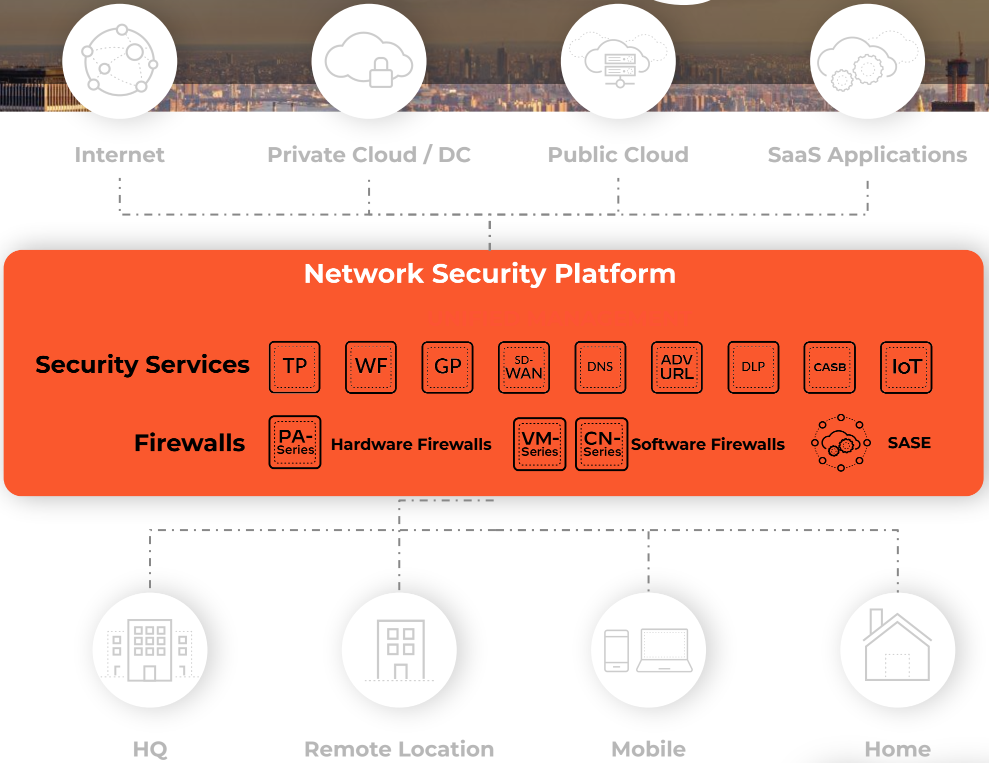
Management

- Simplified Software Upgrade
- Selective push to managed firewalls
- Auto content push for SW Firewalls
- Log Collector Health Monitoring on Panorama

5G Security

- New deployment option for 3G + 4G/ LTE networks
- Mobile Network Security Support on New Mid-Range and High-End Hardware Platforms

We've got next.



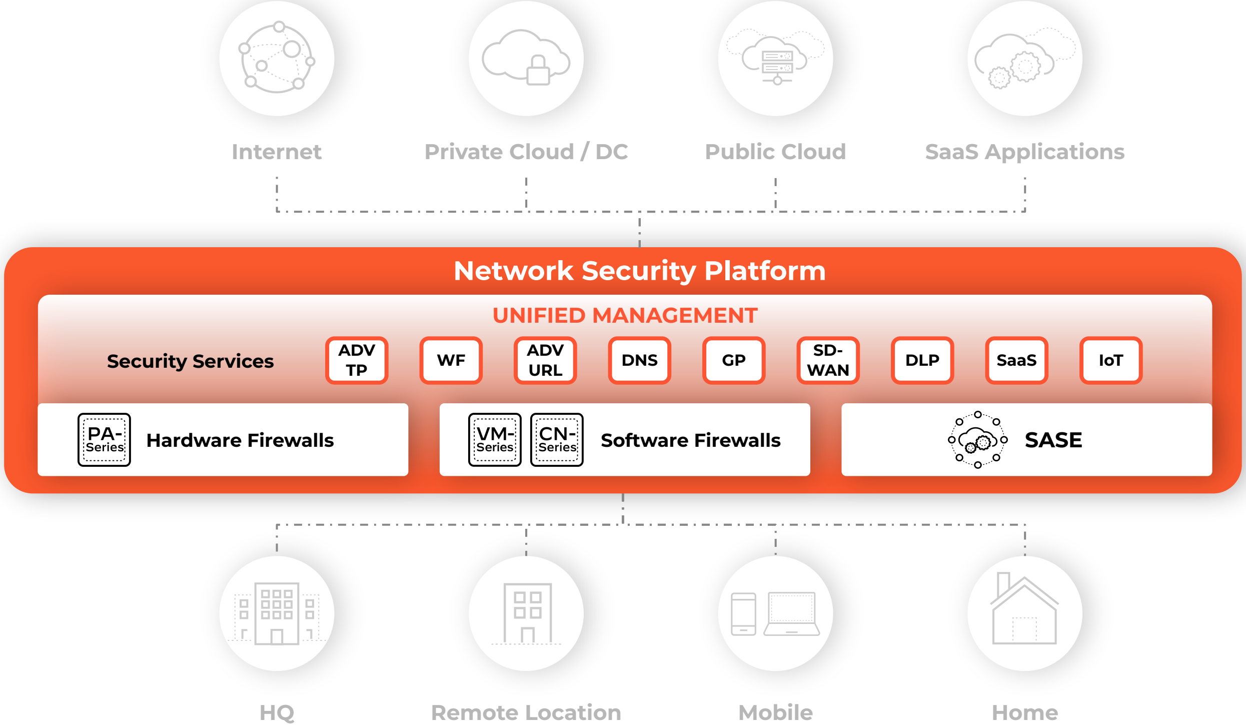
Best-in-class security for all users and applications

Integrated security services across hardware, software and SASE

Optimized end-user experience at all locations

Unified security operations

The Complete Network Security Platform



Best-in-class security for all users and applications

Integrated security services across hardware, software and SASE

Optimized end-user experience at all locations

Unified security operations

THANK YOU

paloalto® NETWORKS

Cybersecurity Partner of Choice