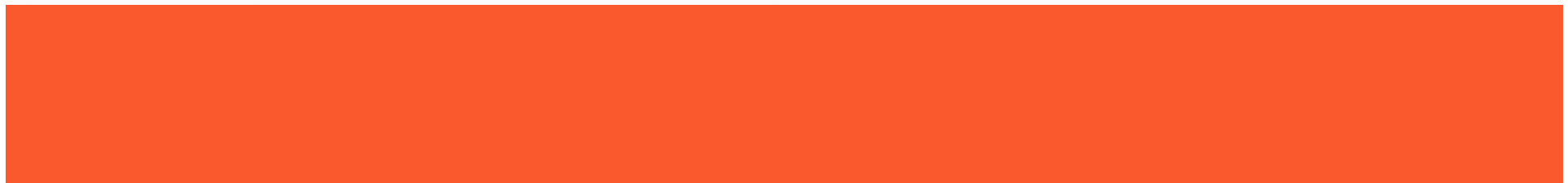




# Palo Alto Networks PAN-OS 10.0

*Presenter : Dnyaneshwar Narale  
Co-Host: Rupesh Sharma  
Network Techlab India Pvt.Ltd.*



# Agenda

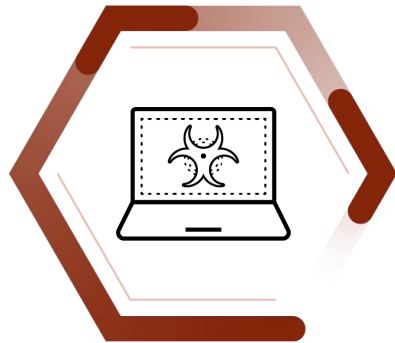
1. **Sapporo Launch News** | 10 min
2. **New Capabilities in PAN-OS 10.0** | 15 min
  - a. TLS 1.3 Decryption
  - b. HA Clustering
  - c. Data Processing Card
  - d. GlobalProtect
  - e. SD-WAN Enhancement
3. **Security Subscription Updates** | 20 min
  - a. In-Line ML
  - b. Threat Prevention
  - c. DNS
4. **Summary** | 5 mins



# Introducing The World's First ML-Powered NGFW

PAN-OS 10.0

## Typical Industry Response Is Manual



### React to New Attacks

Result: First victim gets compromised before protection is delivered

*Mean Time To Identify: 206 Days*



### React to New Devices

Result: Unidentified, unsecured devices pose massive risk to the network

*Casino breached through fish tank*



### React to Environment Changes

Result: Breaches due to human errors and misconfigurations

*99% of firewall breaches due to misconfig. Gartner*

## Introducing The World's First ML-Powered NGFW



### **Proactively Stop New Threats**

*For the first time ever, in-line ML-based malware and phishing prevention. And zero-delay signature updates.*



### **Proactively Secure IoT Devices**

*For the first time ever, integrated IoT Security based on ML to detect and protect IoT devices*



### **Proactively Make Policy and Config Changes**

*For the first time ever, a firewall that collects telemetry data for ML-based security policy optimization. Eliminate breaches due to misconfiguration.*

Attend the June 17 Virtual Event To Learn

*What's changing in our customers' worlds*

*How the security industry typically responds to these changes, and why that is no longer productive*

*How we are disrupting the industry once again, this time with a radically new ML-powered approach*

# Let's Dive Into PAN-OS 10.0

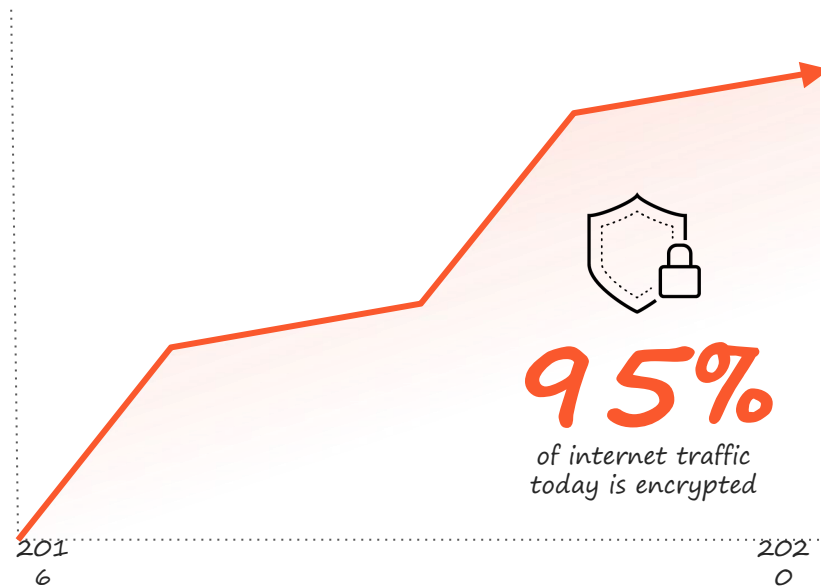
# TLS 1.3 Decryption

Never been more easy to decrypt

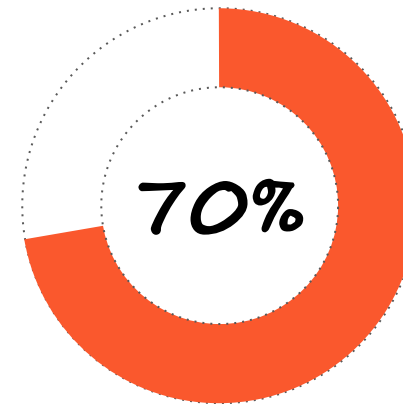


## Massive Risks Within Encrypted Traffic

Encrypted traffic is now the norm



And attackers are taking advantage



More than 70% of malware campaigns in 2020 will use some type of encryption to conceal malicious activity, says Gartner

Source: [Encrypted Traffic \(2016\)](#) | [Encrypted Traffic \(2020\)](#) | [Encrypted Walwave \(Gartner\)](#)

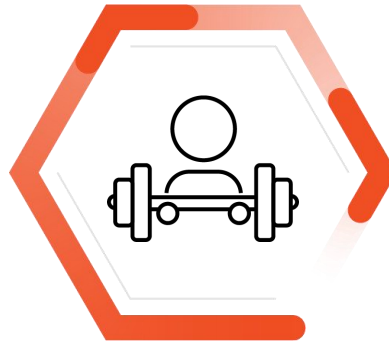
\* | © 2020 Palo Alto Networks. All rights reserved. Internal Use Only. Do Not Share Externally.

## Decryption Is Necessary For Protection



*Protection requires decryption*

*Without decryption, security tools cannot effectively stop malware*



*Deploying decryption is usually hard*

*Lack of expertise, fear of business disruption, troubleshooting complexity*



*Cloud apps making the need to decrypt more urgent*

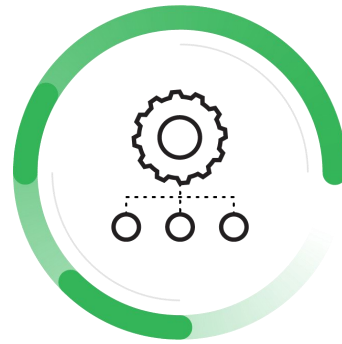
*Increasing adoption of HTTP/2 and encryption with modern protocols like TLS 1.3*

## Deploying Decryption Is Now Easier Than Ever



### *Mitigate security risks*

*Control use of legacy TLS protocols, insecure ciphers & incorrectly configured certs*



### *Deploy decryption, worry-free*

*Easily deploy and maintain decryption using purpose-built troubleshooting & visibility*



### *Secure cloud apps, quickly*

*Secure traffic that uses protocols like TLS 1.3 and HTTP/2. Now with up to 2X performance boost*

# HA Clustering

## Challenges with Horizontal Scaling and Multi-Data Center



**Lack of Scalability**

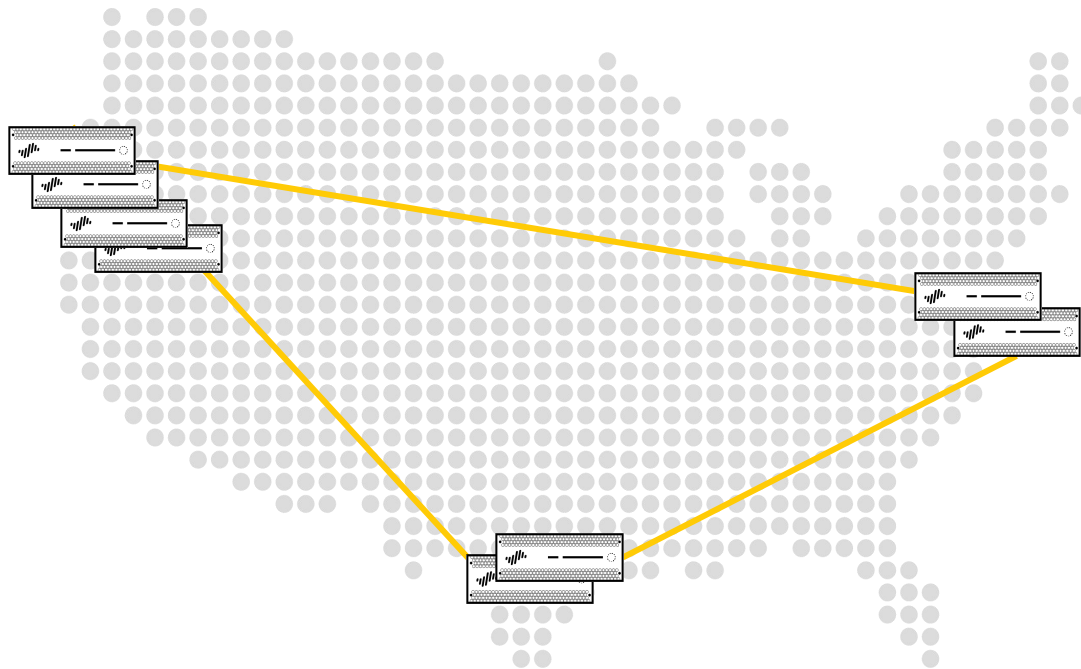
*Need a simple and cost effective way to add firewalls*



**Need Always-On Availability**

*Need the ability to redirect and load share traffic to multiple locations, including when a data center goes down*

## Simply Scale with High Availability Clustering



Simply add new appliances to scale performance and capacity



Enable always-on availability for exceptional user experience



Gain consistent security that seamlessly scales with your applications



Supported on: PA-3200, PA-5200, and PA-7000 VM-300, 500, 700

# New Hardware

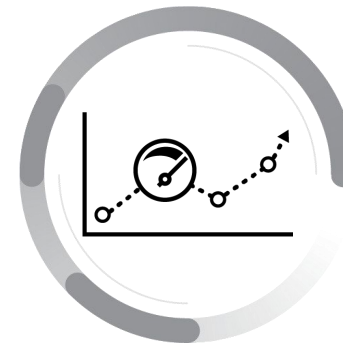
## Trends Driving New Hardware Requirements



*Increased utilization of security features*



*Increased encrypted traffic*



*Increased performance needs*



## Introducing the New Data Processing Card



*700+ Gbps App-ID throughput\*:  
2x Nearest Competitor*



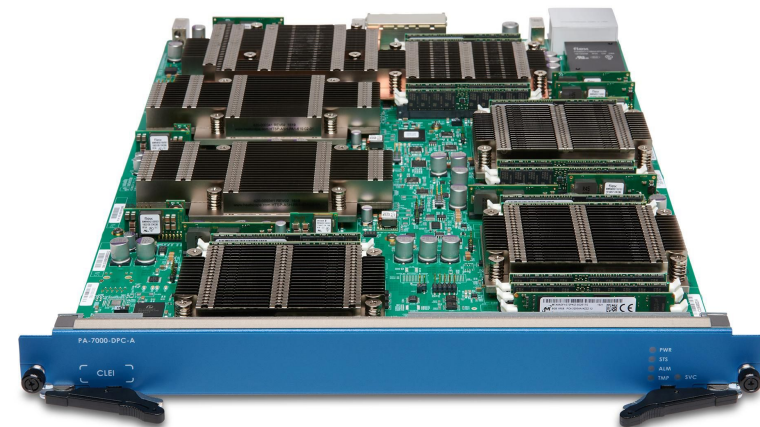
*33% decryption performance increase*



*Flexible options to scale security  
and performance*



*Investment protection: new card  
is backwards compatible*



*Performance without compromising security*

\*PA-7080 with 8x100G NPCS + 2xDPCs

\* | © 2020 Palo Alto Networks Confidential. Internal Use Only. Do Not Share Externally.

## Data Processing Card Pricing

*N America*

*\$189,900*

*International*

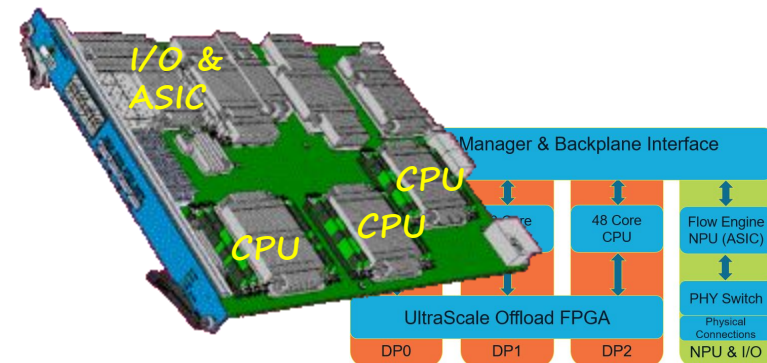
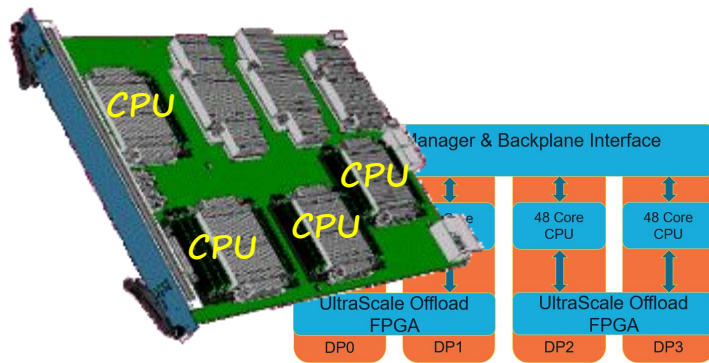
*\$217,400*

*Investment protection*

*Use with existing PA-7000 Series chassis  
Use along with existing NPCs*

*Orderability expected July 2020*

## DPC (New) And 100G-NPC (Existing)



**DPC**

- 4 PAN-OS Data Plane CPUs
- No ASIC or TCAM
- No Physical Ports

**100G-NPC**

- 3 PAN-OS Data Plane CPUs
- ASIC with TCAM
- 4x100G + 8x10G Ports

# Quarantine Compromised Devices

# Current Approach is Not Enough for Today's Mobile Workforce

Hostname: win721-host  
Username: domain\jdoe



User's endpoint gets compromised

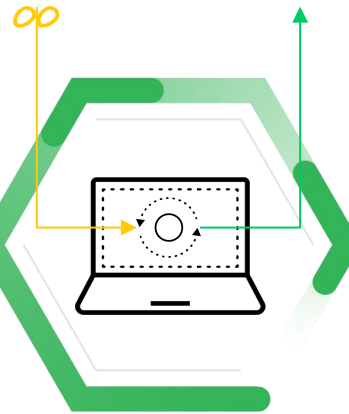
IP Address:  
10.72.99.100



NGFW sees malicious network activity and restricts endpoint's IP address

IP Address:  
10.72.99.1

IP Address:  
10.1.1.50



But endpoint's IP address changes and reconnects to the network

## GlobalProtect Device Quarantine



*Identify and quarantine  
infected devices*

*Leveraging immutable  
characteristics*



*Automatically  
apply restrictions*

*On external and  
internal network*

# SD-WAN Enhancements

# Forward Error Correction & Packet Duplication



*Improved User Experience*

*Reliable performance for highly sensitive, real-time applications*

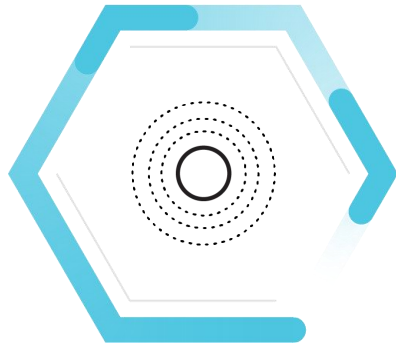


*Granular Control*

*Ability to finetune packet loss thresholds to preserve bandwidth*

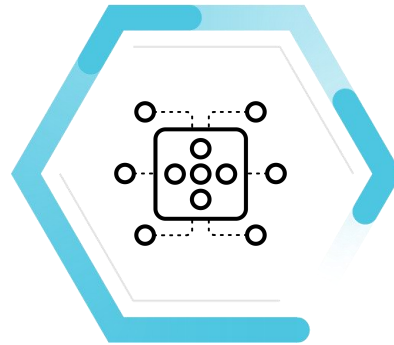


# Introducing End-to-End Monitoring of SaaS Application Health



## **Flexible Monitoring Options**

*Preserve bandwidth while ensuring great user experience*



## **Accurate Path Health Measurements**

*From the branch to the SaaS application server*

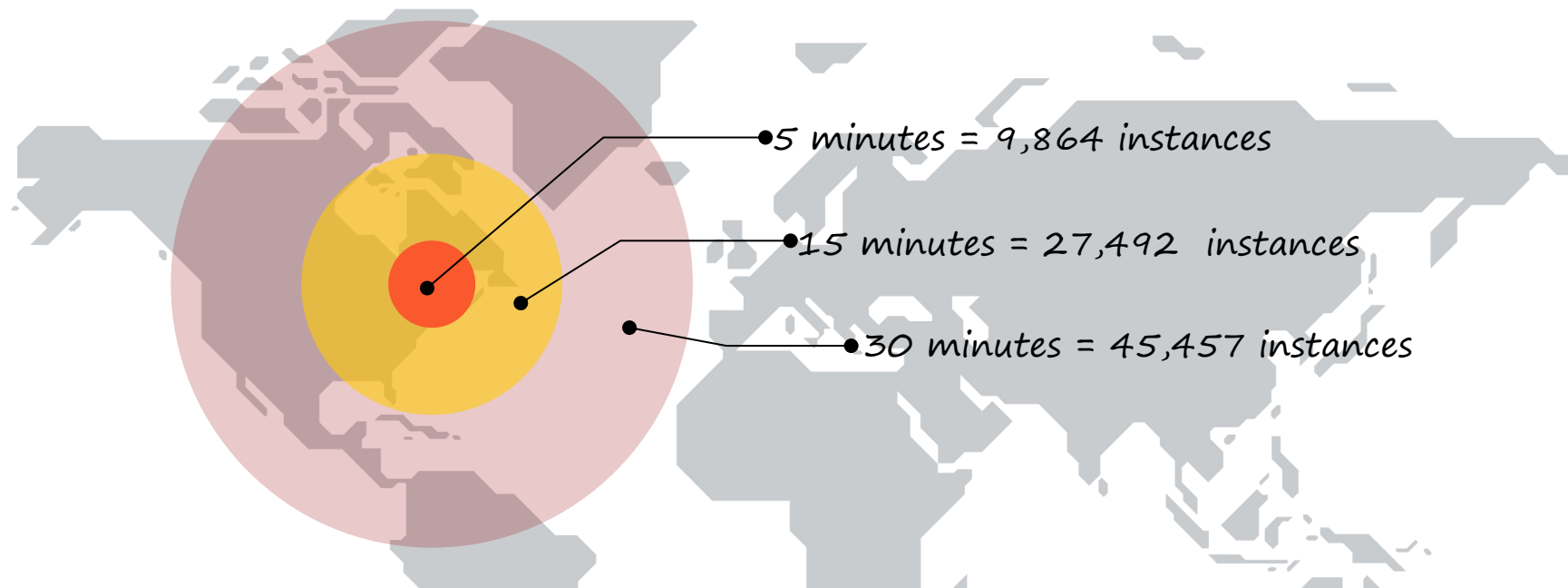


## **Exceptional User Experience**

*Determine optimal path with end-to-end path health measurements*

# Every Second Matters with ML-Based Inline Prevention

## Attackers Have 2 Critical Advantages...



*Speed of Proliferation and Polymorphism*

## Existing Solutions Struggle to Prevent Net-New Attacks in Time



**Siloed Approach**

*Can't keep up with the scale of new attacks*



**Require Compromise**

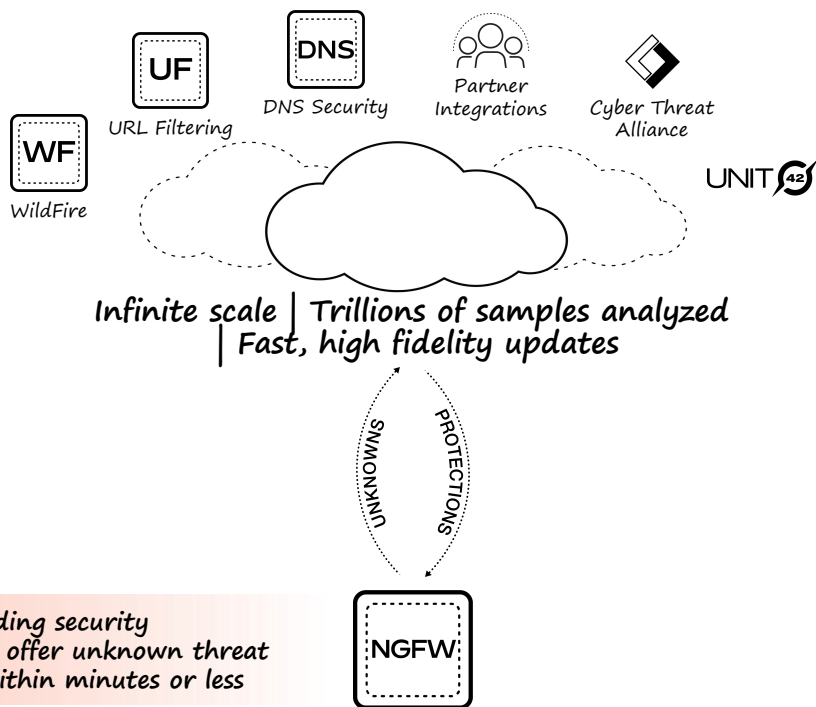
*Accurate prevention depends on on a first victim*



**Stop Business**


*Current hold-and-release approaches impact users and revenue*

## Today's Prevention of Unknown Threats Through Cloud Scale

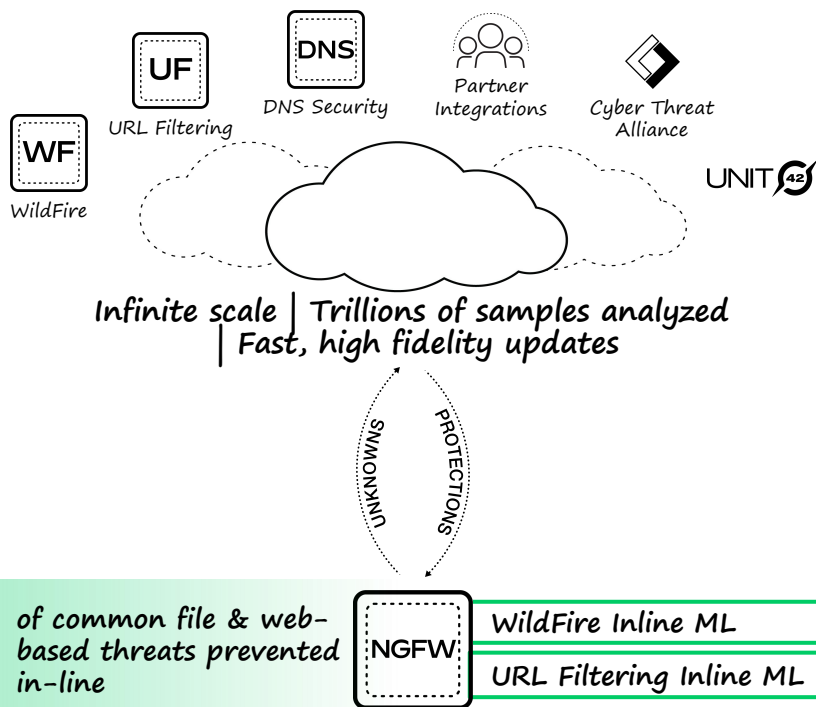


Cloud-delivered security services scale prevention capabilities

Shared intelligence allows the fastest distribution of protections

-  File Protections: **5 min**
-  URL Protections : **1 min**
-  DNS Protections: **Instant**

## Prevention of Unknown Threats with Inline Machine Learning



Up to **95%** of common file & web-based threats prevented in-line

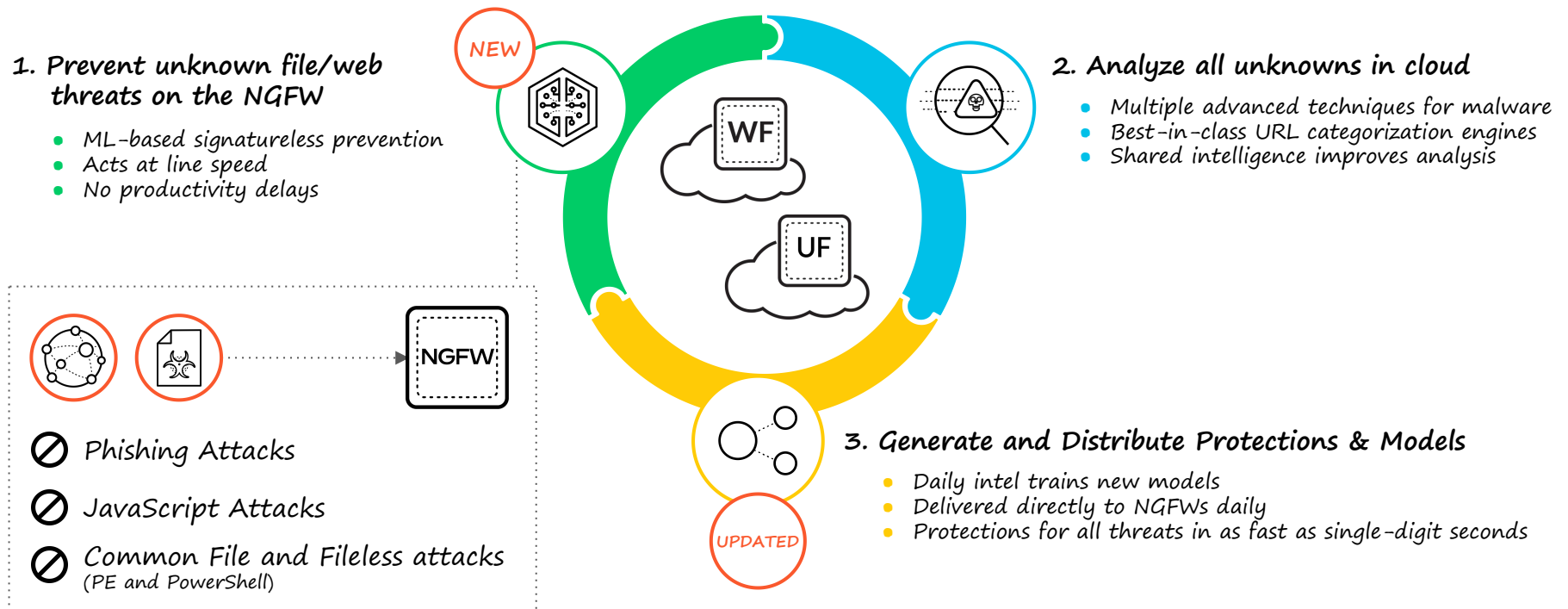
Cloud-delivered security services scale prevention capabilities

Shared intelligence allows the fastest distribution of protections

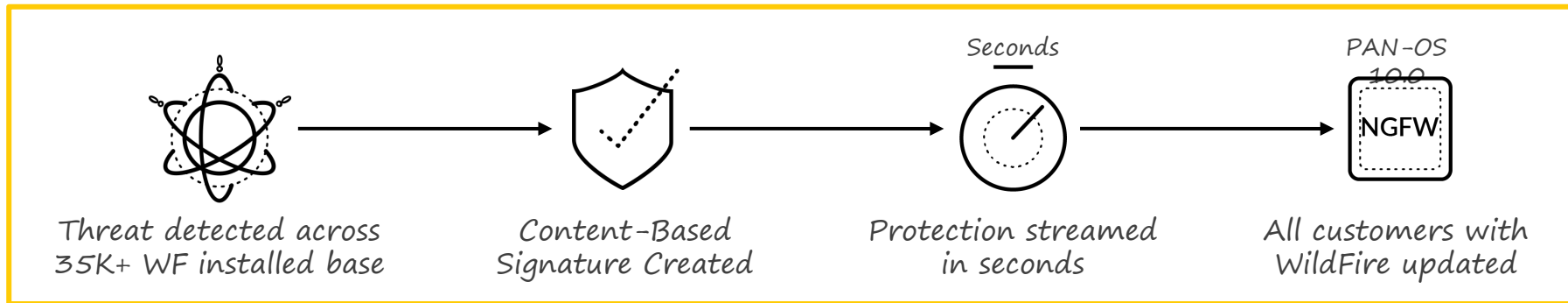
-  File Protections: **Instant**
-  URL Protections : **Instant**
-  DNS Protections: **Instant**

\* | © 2020 Palo Alto Networks Confidential. Internal Use Only. Do Not Share Externally.

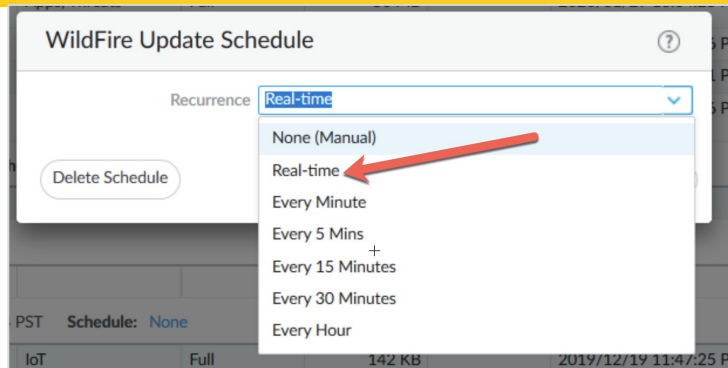
# How It Works: Inline ML-based Prevention for Files and Web-Based Attacks



## Slashing Our Industry-Leading Time for Distributed Protections



**BEFORE**  
Industry-leading 5-minute signature generation/distribution time

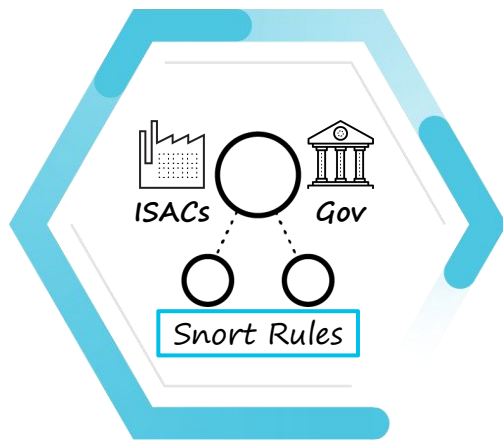


**With PAN-OS 10.0**  
Protection streams to NGFW in single-digit seconds



# Threat Prevention

## Critical Use Cases for Open Source Network IDPS Signatures



*Share & Consume  
Threat Definitions*



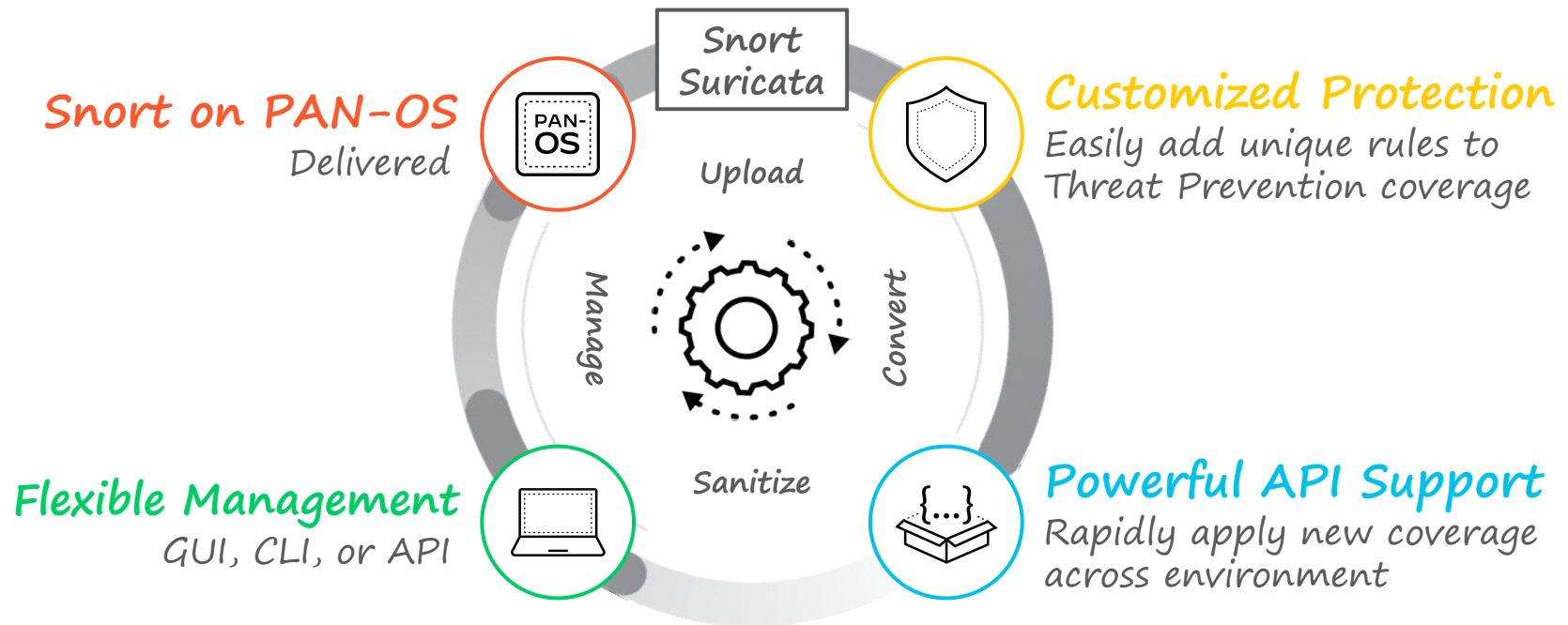
*Address Threats  
Unique to Environment*



*Integrate  
Coverage*

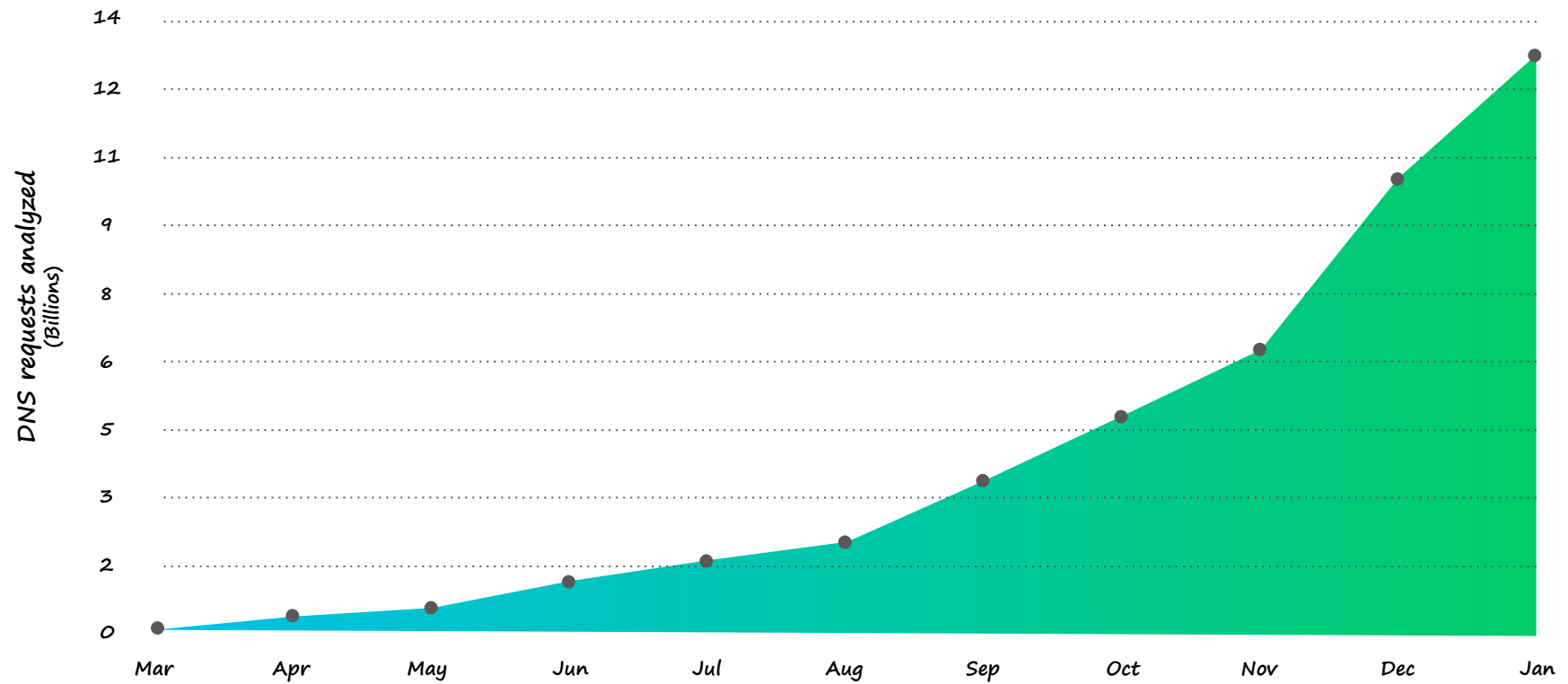
*Key Challenge: Automating ingestion and deployment of new signatures*

## Introducing Snort Support in Threat Prevention

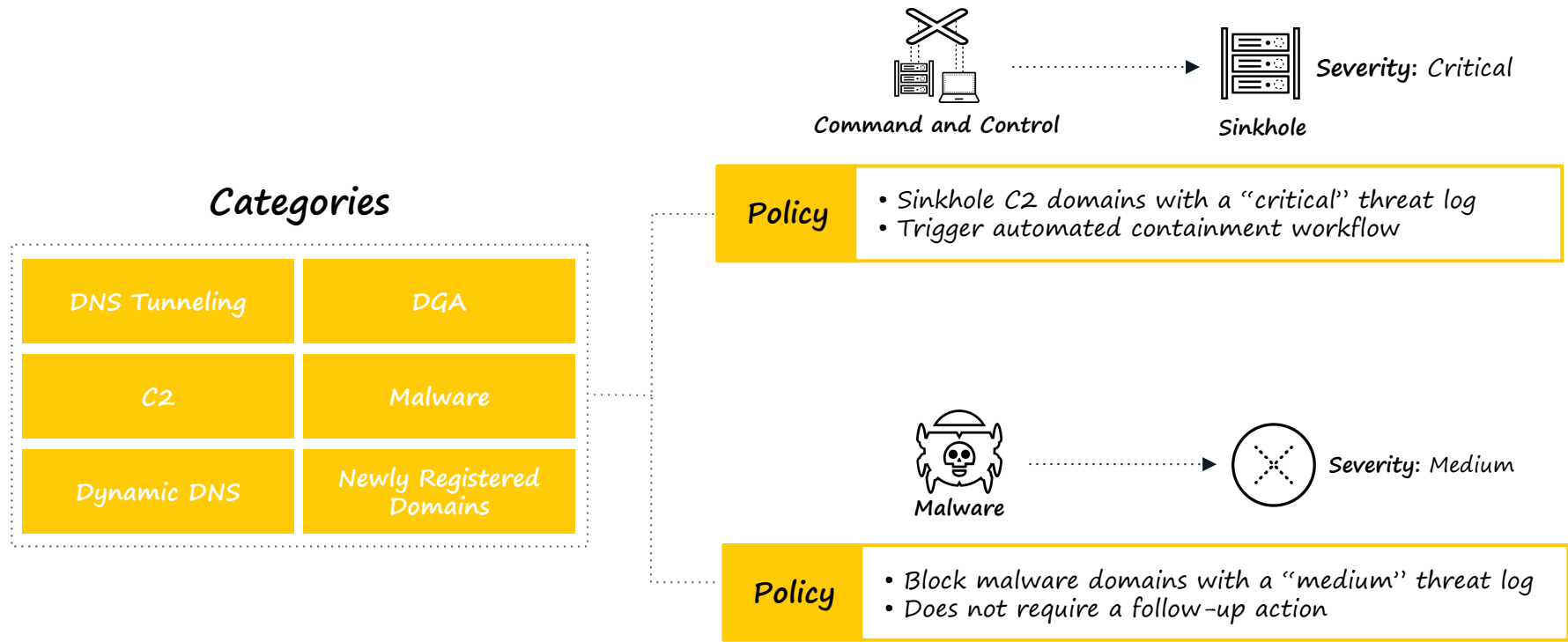


# DNS Security

## One Year in, Amazing Growth...



# Introducing Category-Based Visibility and Control for DNS Threats



## DNS Analytics

### DNS Visibility

- Complete visibility across all DNS traffic and trends
- Filter based on DNS categories and timeframes
- Abuse of DNS (malware, C2, tunneling, DGA)

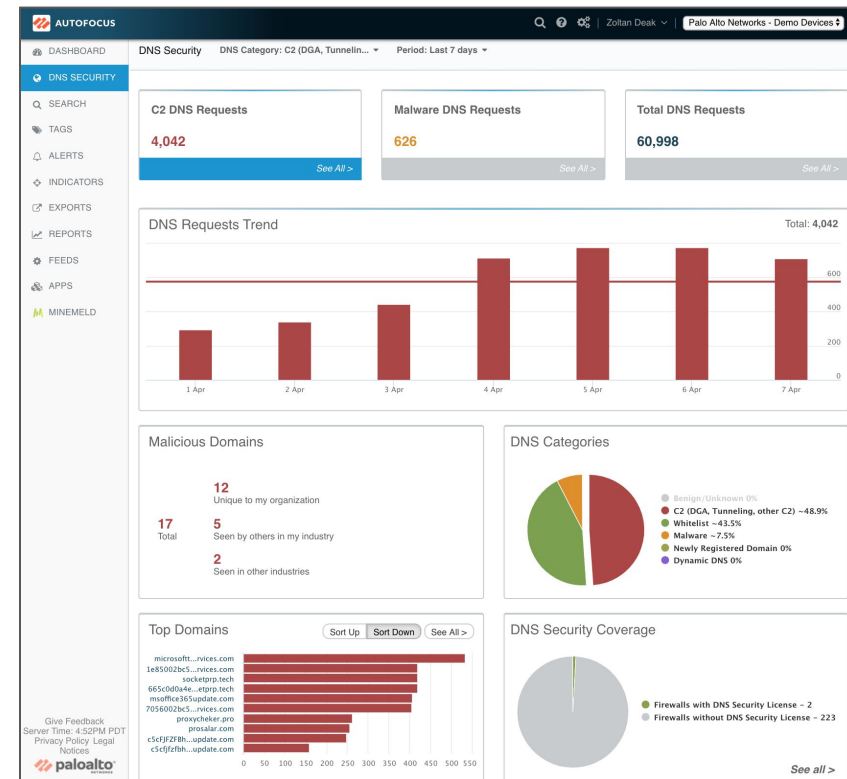
### DNS Intelligence Context

- Why a domain was blocked
- Pivot to related threat intel
- AutoFocus Tags
- Whois and passive DNS data

### DNS Hygiene

- Quickly view which firewalls in your estate are covered by DNS Security

Leverages AutoFocus UI - License Not Required



# IoT Security

Trust every device on your network



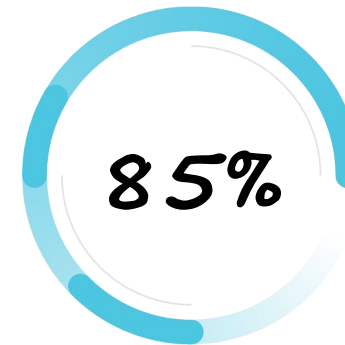
## Massive Increase in Connected Devices



*IoT devices  
market by 2026*



*Connected  
devices by 2025*



*Decision makers  
with IoT project  
budgets today*

## IoT is a Business Necessity that Introduces Risk



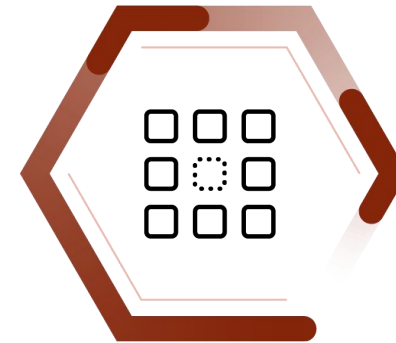
### *Massive Increase in Connected devices*

*30% of devices on enterprise networks today are IoT*



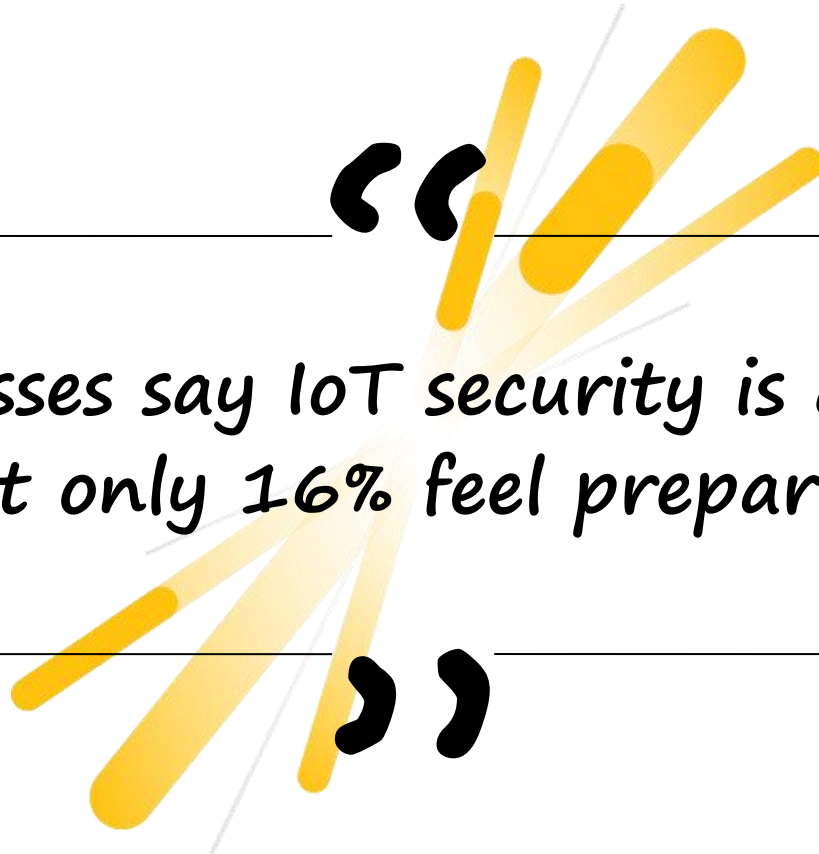
### *Pose a Huge Security Risk*

*Shipped with vulnerabilities and difficult to patch, yet have unfettered access*



### *Securing IoT Devices is Hard*

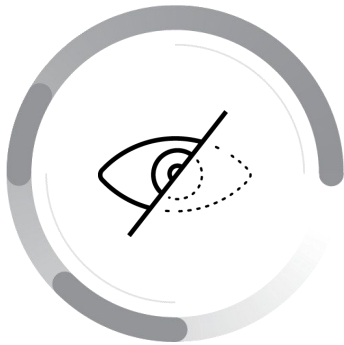
*Incredibly diverse devices; traditional IT security controls do not work*



75% of businesses say IoT security is a top priority,  
yet only 16% feel prepared

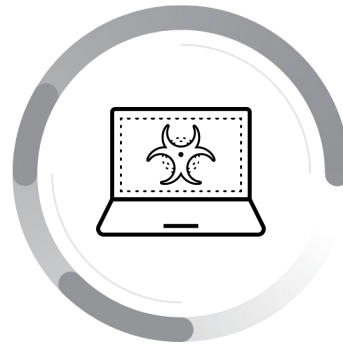
McKinsey

## Why Current Solutions Fail



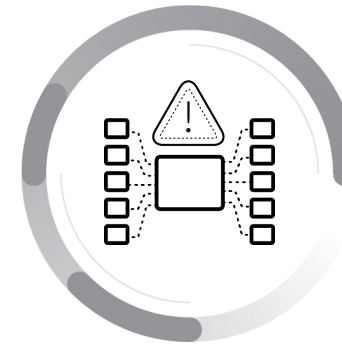
### Limited Visibility

*Cannot identify previously unseen IoT devices, accuracy requires constant effort*



### No Protection

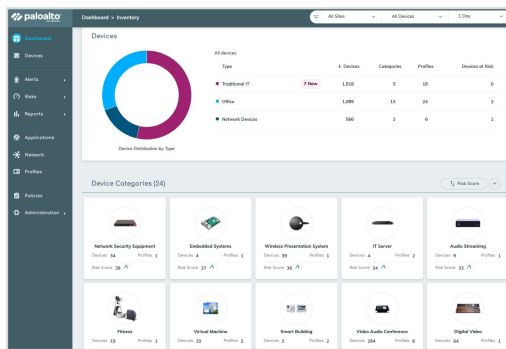
*Existing visibility-centric solutions do not offer native prevention or enforcement*



### Hard to Implement

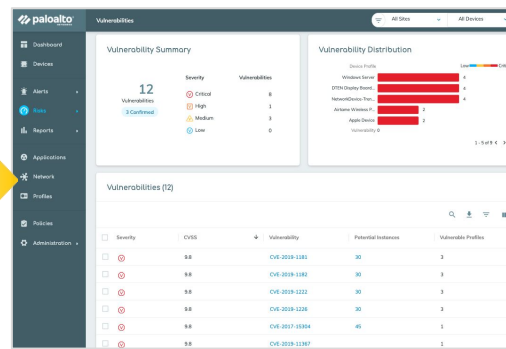
*Require changes to network infrastructure, security team workflows and integrations*

# Introducing IoT Security



## Complete Visibility

Accurately identify and classify all devices with ML, including those never seen before



## In-depth Risk Analysis

Quickly understand anomalies, vulnerabilities and severity to make confident decisions

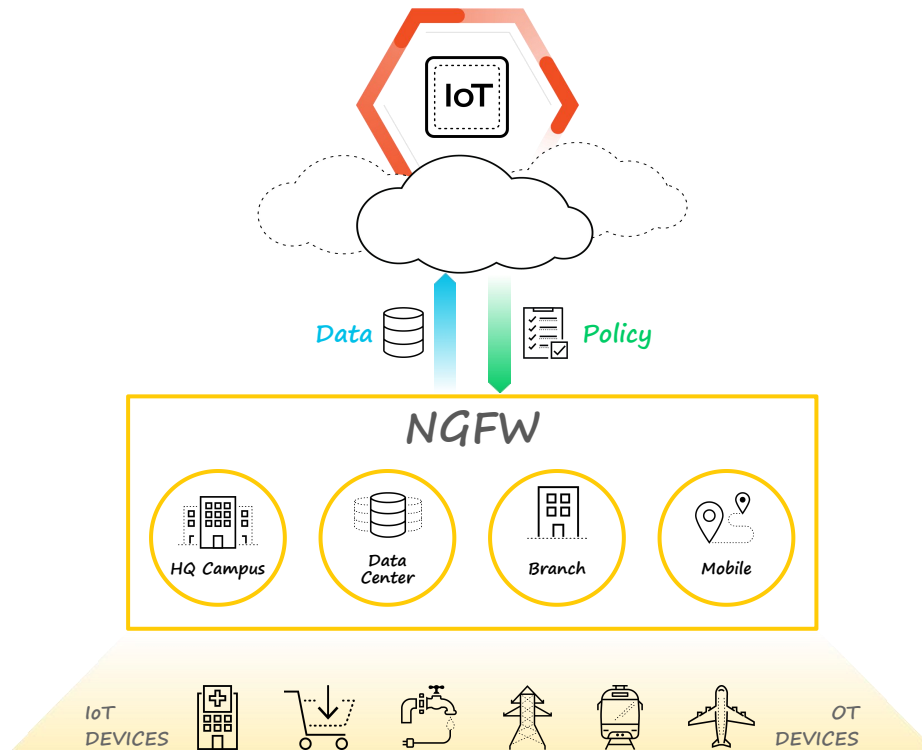
The screenshot shows the PA-VM dashboard with a table of policy recommendations. The table has columns for Source, Destination, and Destination Profile. A 'Policy Recommendation' button is visible at the bottom.

	Source	Destination
AT and T Axia Phone	zone1	Carestream Radiographic System
Ademco Security System Device	zone1	ACT
Citrix Thin Client Device	zone1	ACT
Avocent KVM Switch	zone1	3M His

## Built-in Enforcement

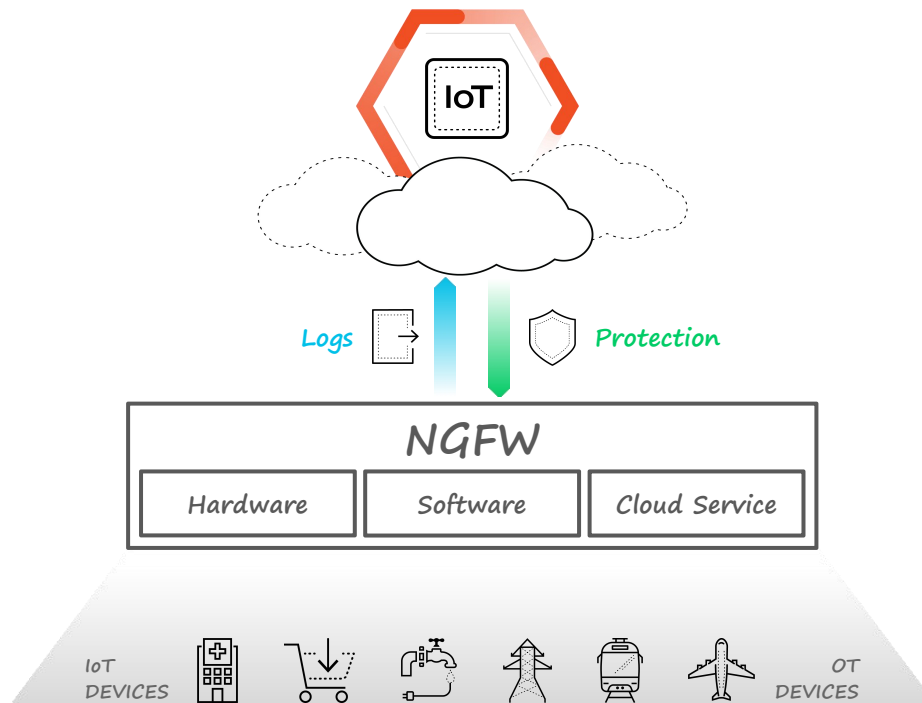
Safely automate enforcement on your next-gen firewall with a new Device-ID policy construct

## Best-in-Class Enterprise IoT Security Deployed Effortlessly



- ✓ Available on all NGFW form factors - Hardware, Software, Cloud Service
- ✓ Start with your existing firewall
- ✓ Scale linearly with multi-tenant cloud infrastructure
- ✓ Leverage prevention from existing subscriptions

## Best-in-Class Enterprise IoT Security Deployed Effortlessly



- ✓ Available across HQ campus, data center, branch and mobile
- ✓ Start with your existing firewall
- ✓ Leverage prevention from existing subscriptions
- ✓ Scale linearly with multi-tenant cloud infrastructure

# Trust Every Device On Your Network



## Use Your Infrastructure

*Deploy within minutes, no siloed sensors or enforcement products required*



## Leverage Existing Talent

*Maintain current operations and empower your existing Network Security team to protect IoT*



## Get Complete IoT Security

*Discover, secure and prevent threats on every IoT device in your network with one solution*



# CN-Series

Industry's First Containerized NGFW for Kubernetes

## Container Adoption is Increasing



*By 2023, more than 70% of global organizations will be running three or more containerized applications in production.*

*Gartner, 2019*

## Container Network Security Challenges for Network Security Teams



*Lack of visibility  
and control*

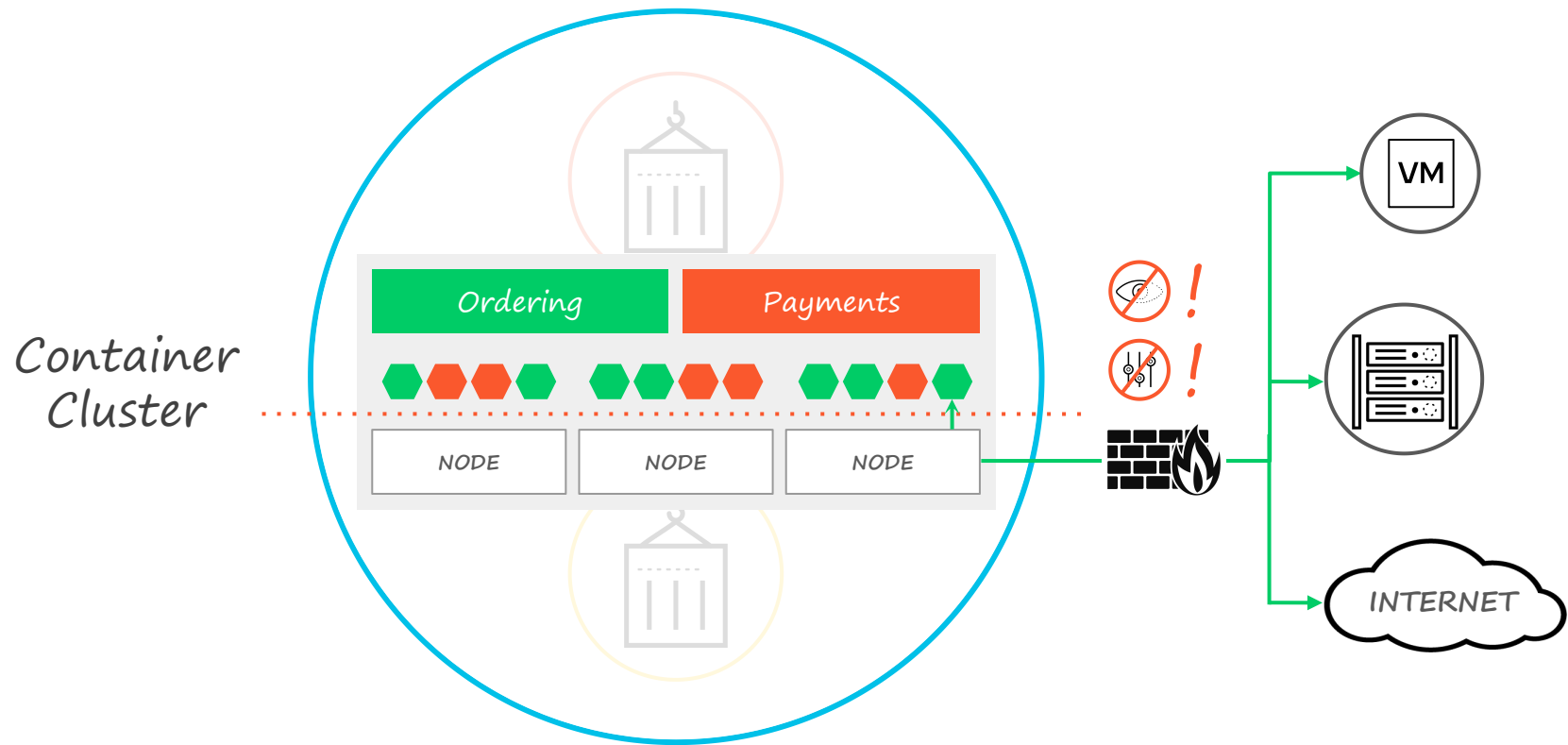


*Inconsistent tools  
and management*



*Lack of automation  
and scalability*

# Other FW Form Factors Lack Container Visibility and Context



# Introducing CN-Series Container Firewalls

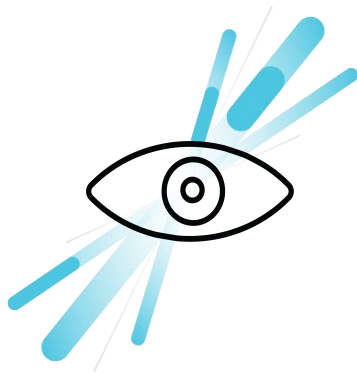
## NGFW for Kubernetes Environments

Containerized  
PAN-OS

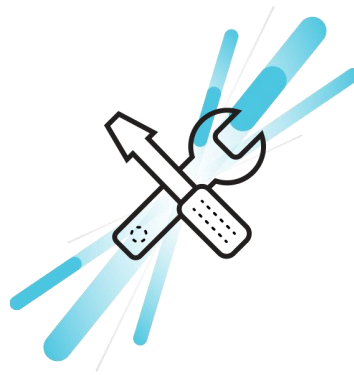
L7 Network Security &  
Threat Protection

Kubernetes  
Integrated

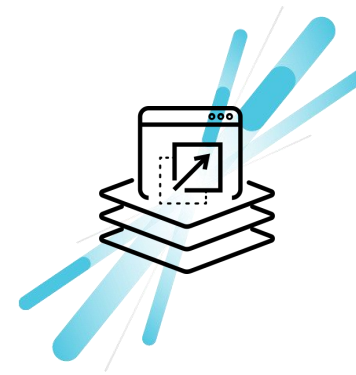
## Network Visibility and Threat Protection in Kubernetes



*Visibility into K8's  
constructs for  
context-based  
control*



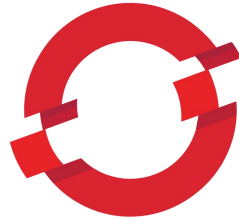
*Consistent policy  
creation and  
management with  
Panorama*



*Automate and  
scale with deep  
Kubernetes integration*

# Supported Cloud Native Infrastructures

*Self-Managed*



---

*On-premises*

*Public Cloud*

*Cloud-Managed*

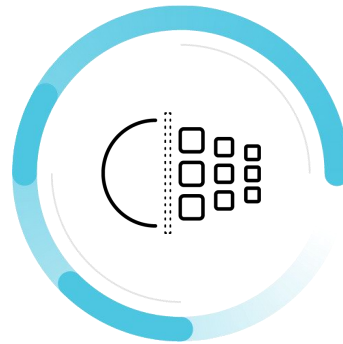


## CN-Series Container Firewall Use Cases



### East-West Layer 7 Traffic Protection

*Enforce trust boundaries  
between namespaces and other  
workload types*



### Outbound Traffic Protection

*URL filtering and  
content inspection*



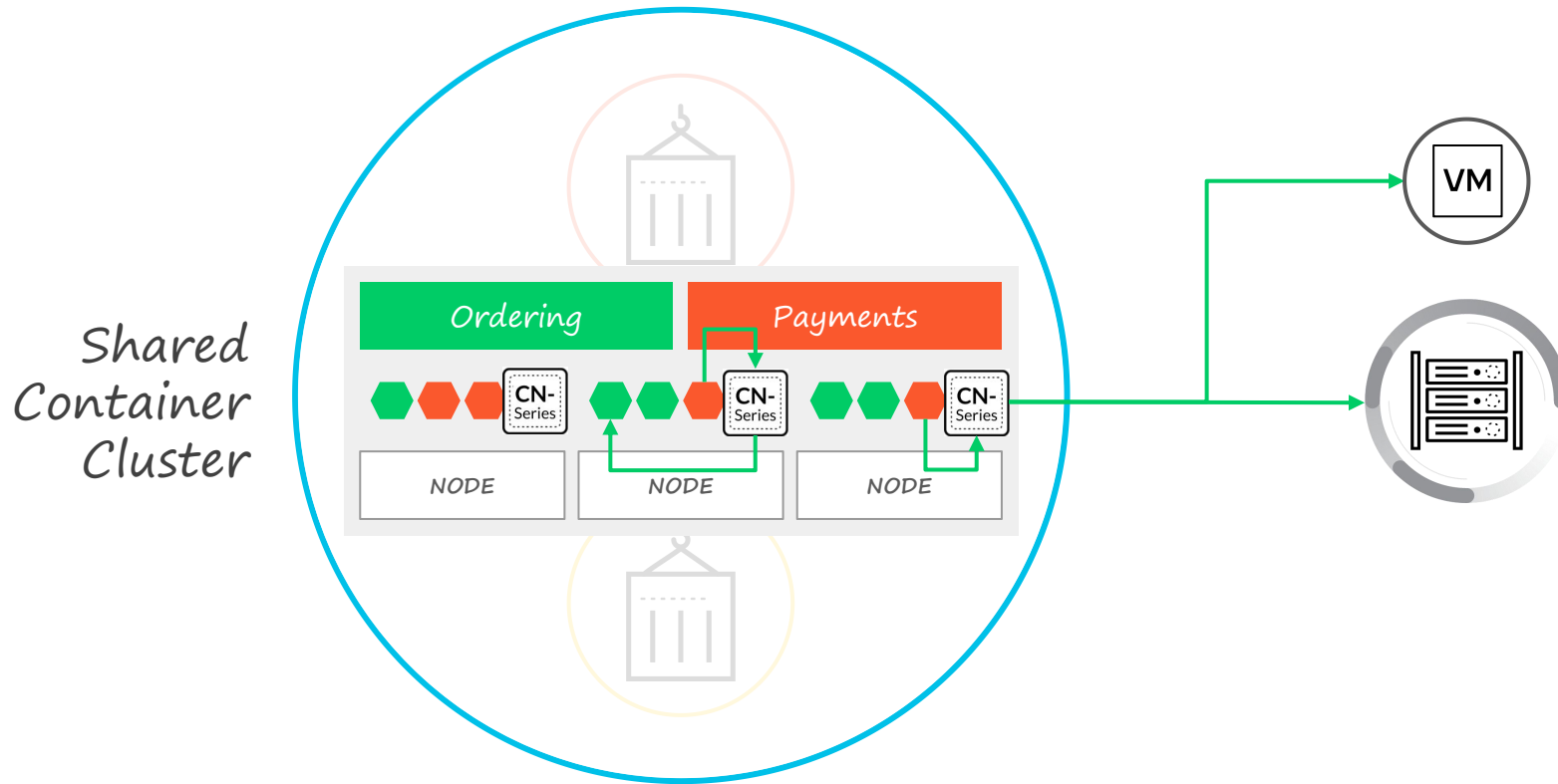
### Inbound Threat Prevention

*Stop known and  
unknown threats*



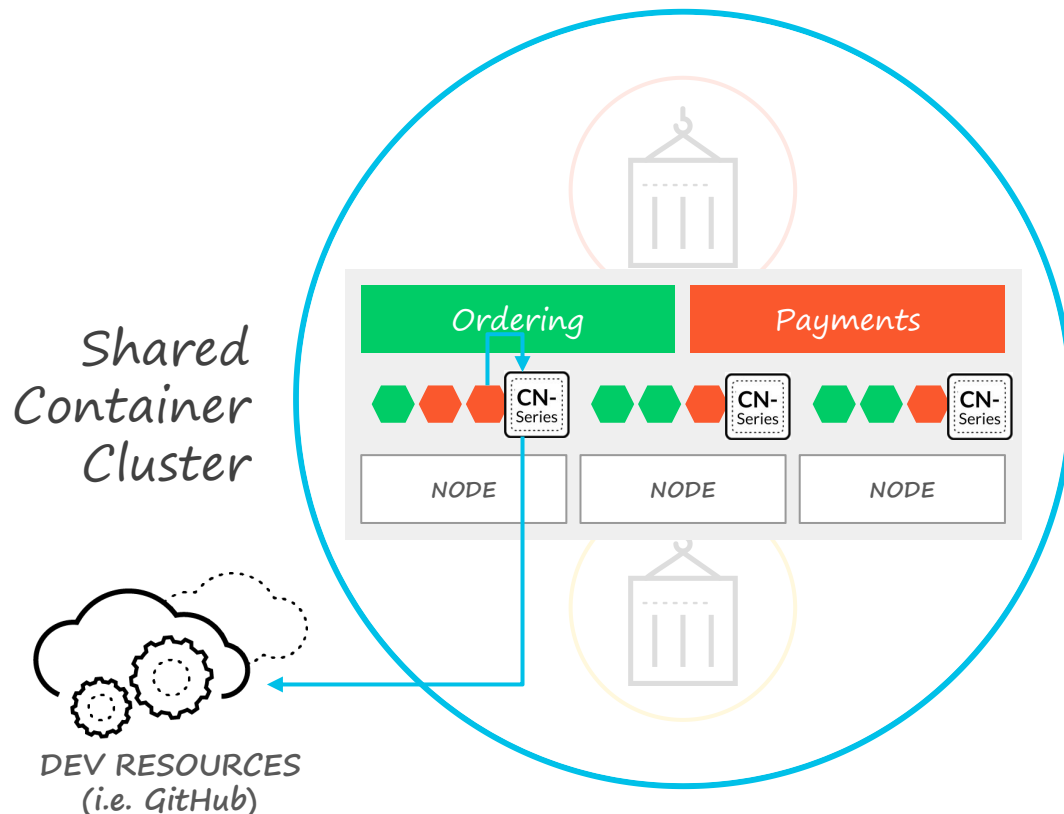
# Use Case 1: East-West Layer 7 Traffic Protection

Recommended Subscriptions:



## Use Case 2: Outbound Traffic Protection

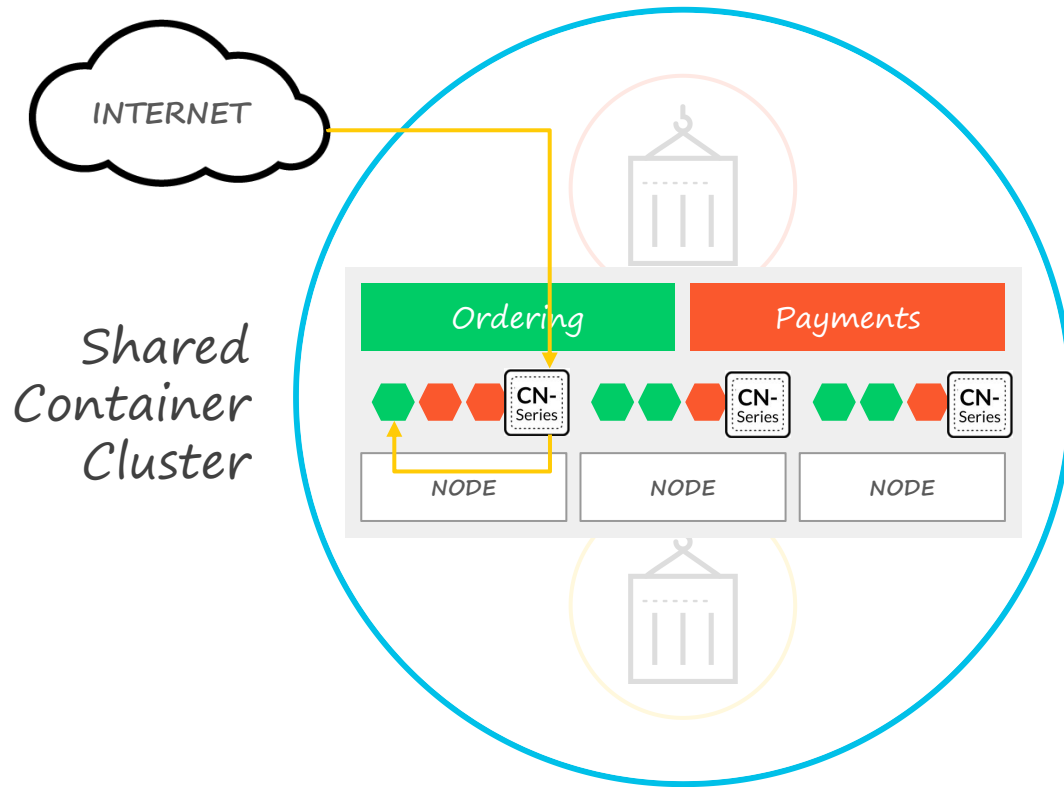
Recommended Subscriptions:



DEV RESOURCES  
(i.e. GitHub)

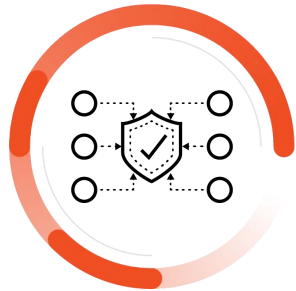
### Use Case 3: Inbound Traffic Protection

Recommended Subscriptions:



\* | © 2020 Palo Alto Networks Confidential. Internal Use Only. Do Not Share Externally.

## CN-Series Container Firewall Differentiated Capabilities



*Centralized Management*



*DevOps-Ready Orchestration*



*Kubernetes Visibility & Context*



*Best-in-Class Security*

# Summary Of Enhancements

## 70+ New Capabilities in PAN-OS 10.0

### IoT Security

- Visibility into IoT devices
- Behavioral anomaly detection
- Risk-based policy recommendations
- Native enforcement

### Prevention of Patient Zero

- Inline machine learning at the network level
- WildFire and URL Filtering prevent weaponized files, credential phishing, and malicious scripts
- Patented signatureless based approach

### CN-Series

- Containerized form factor of NGFW
- Native deployment within Kubernetes
- Centralized management with Panorama

### Decryption

- Support for TLS 1.3
- Better visibility
- Enhanced troubleshooting

### Networking

- HA clustering
- HA additional path monitoring groups
- Ethernet SGT protection

### GlobalProtect

- Identification and quarantine of compromised devices

### SD-WAN

- SaaS app path monitoring
- Forward error correction
- Packet duplication

### WildFire

- Multi-vector recursive analysis to prevent multi-stage, multi-hop, attacks
- Improvement to static analysis model delivering verdicts in seconds from over 90% of malicious PE samples

### Snort Support

- UI and API support of both SNORT and Suricata signatures
- Automatically convert, sanitize, upload, and manage IDPS signatures

### Data Processing Card

- New card for the PA-7000 Series: data processing card with 33% increase in throughput

### Policy Features

- X-Forwarded-For HTTP header data support in policy

### 5G Security

- 5G network slice security
- 5G and 4G equipment ID security
- 5G and 4G subscriber ID security

# Next-Gen Cybersecurity, Delivered Today

## World's First ML-Powered NGFW

A Virtual Event | Wednesday, June 17

[REGISTER NOW](#)

### Americas

Wednesday, June 17  
10 AM PDT  
90 min total



### Europe

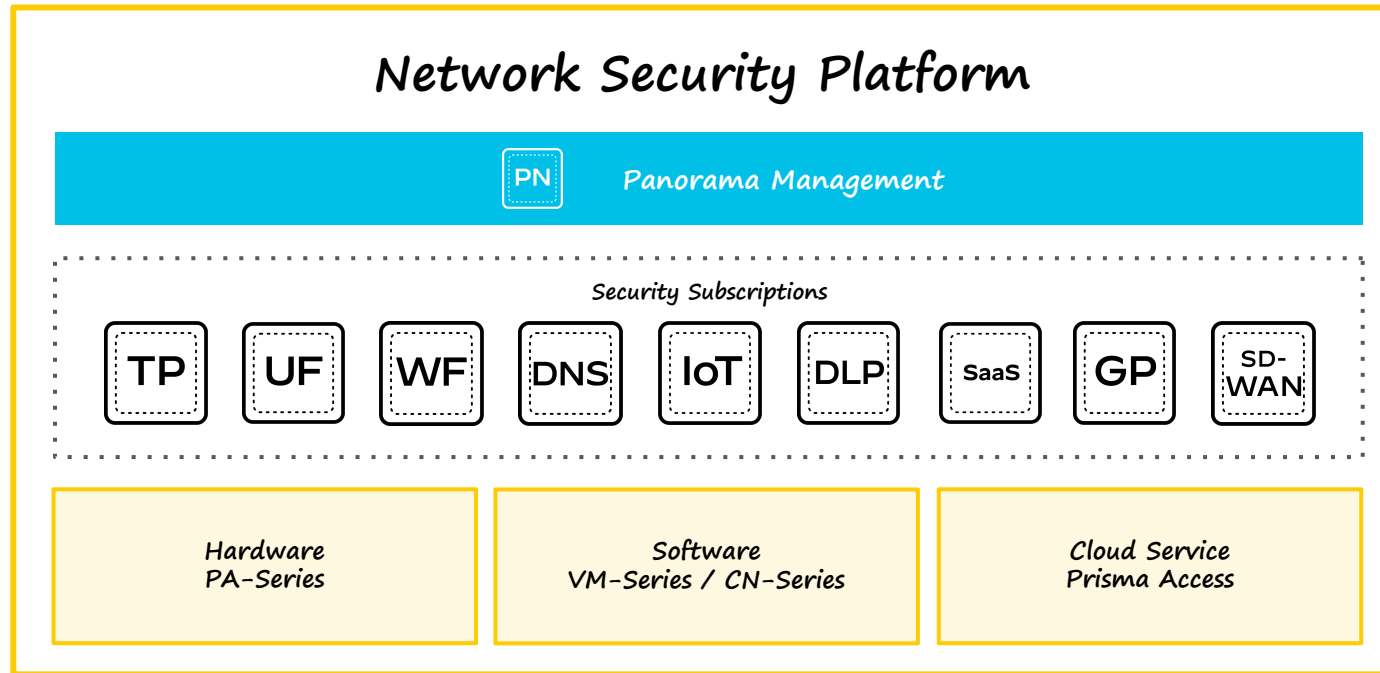
Thursday, 18 June  
12 PM BST  
90 min total



### Asia

Tuesday, 23 June  
11 AM SGT | 5 PM SGT  
90 min total

Delivered As Part Of a Platform



\* | © 2020 Palo Alto Networks Confidential. Internal Use Only. Do Not Share Externally.



# Demo Of ML-Powered NGFW



*Thank you*

