

Palo Alto Networks

Proč je úspěšné v boji proti útočníkům

Palo Alto Networks & Nir Zuk

- Check Point engineer
- Netscreen Principal Developer (first stateful inspection firewall, first intrusion prevention system)
 - Akvizice Juniper
- 2005 založeno Palo Alto Networks
- 2007 první firewall podle kterého Gartner definoval „next-generation firewall“
- 2011 poprvé leader v Gartner MQ enterprise firewall
- 2012 NYSE 4. největší IPO v roce 2012
- 2014 zakládající člen Cyber Threat Alliance
- 2018 Global Cyber Range Initiative
- 2021 NASDAQ

Acquisition

- Morta Security was acquired for an undisclosed sum in January 2014.[\[34\]](#)[\[35\]](#)
- Cyvera was acquired for approximately \$200 million in April 2014.[\[36\]](#)[\[37\]](#)
- CirroSecure was acquired for an undisclosed sum in May 2015.[\[38\]](#)
- LightCyber was acquired for approximately \$100 million in March 2017.[\[39\]](#)
- Cloud Security company Evident.io was acquired for \$300 million in cash in March 2018, creating the Prisma Cloud division.[\[40\]](#)
- Secdo was acquired for an undisclosed sum in April 2018.[\[41\]](#)
- Cloud security company RedLock was acquired for \$173 million in October 2018.[\[42\]](#)
- In February 2019, Palo Alto Networks acquired security orchestration company Demisto for \$560 million.[\[43\]](#)

Acquisition

- In May 2019, Palo Alto Networks acquired container security startup Twistlock for \$410 million.[\[44\]](#)
- In June 2019, Palo Alto Networks acquired serverless security startup PureSec for \$47 million.[\[45\]](#)[\[46\]](#)
- In September 2019, Palo Alto Networks announced its intent to acquire IoT startup Zingbox for \$75 million.[\[47\]](#)
- In November 2019, Palo Alto Networks announced its intent to acquire machine identity-based micro-segmentation company Aporeto, Inc. for \$150 million [\[48\]](#)
- In March 2020, Palo Alto Networks announced its intent to acquire [SD-WAN](#) company CloudGenix, Inc. for \$420 million. This acquisition was completed in April 2020.[\[49\]](#)[\[50\]](#)
- In August 2020, Palo Alto Networks announced its intent to acquire Crypsis Group for \$265 million.[\[51\]](#)
- In November 2020, Palo Alto Networks announced its intent to acquire Expanse for \$800 million.[\[52\]](#)
- In February 2021, Palo Alto Networks announced it acquired Bridgecrew for around \$156 million.[\[53\]](#)
- In November 2022, Palo Alto Networks announced its intent to acquire Cider Security for an enterprise value of around \$300 million.[\[54\]](#)

A Ten-Time Leader in Gartner Network Firewall Magic Quadrant

- **Positioned as a LEADER** in the 2021 Gartner® Magic Quadrant™ Network Firewalls for the eleven consecutive year.
- Achieved the **highest position** for ability to execute and **furthest position** for completeness of vision.
- Powered by over a decade of industry-first innovations, our **ML-Powered NGFWs** provide critical protection from the threats of today and tomorrow, while extending security to all users and all applications throughout the enterprise.



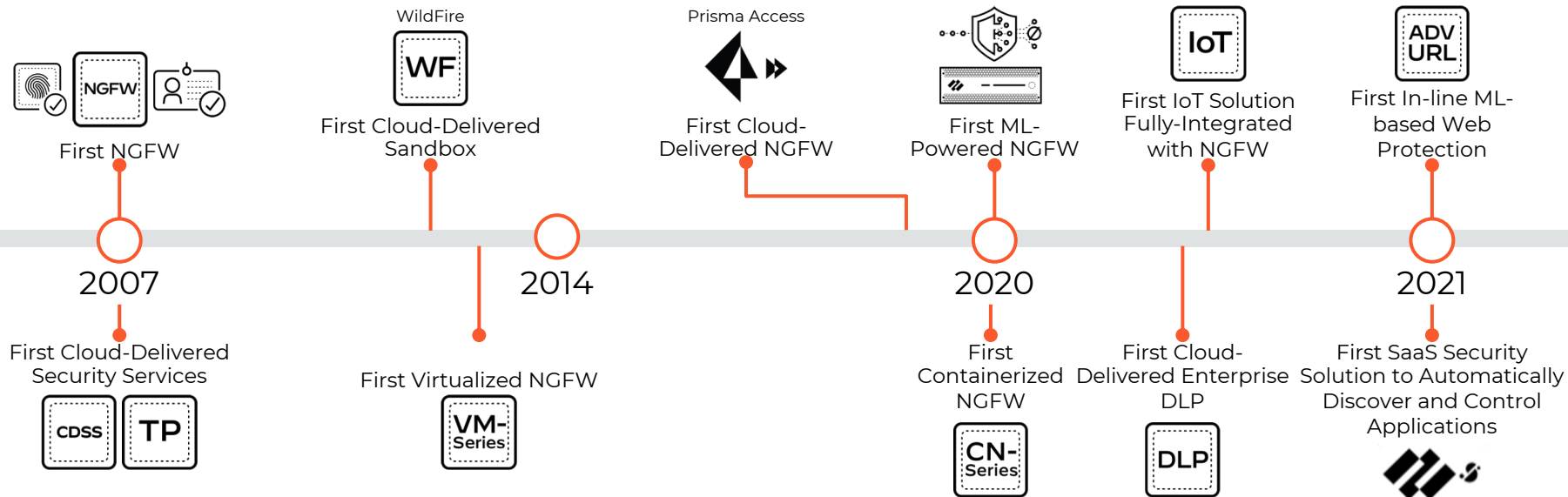
Gartner does not endorse any vendor, product or service depicted in its research publications and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should 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.

Gartner and Magic Quadrant are registered trademarks of Gartner, Inc and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.
Gartner, Magic Quadrant for Network Firewalls, Rajpreet Kaur | Adam Hills | Jeremy D'Hoine | Nat Smith | Aaron McQuaid, 1 November 2021.

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.

14 Years of Industry Firsts

Selected List



Powered by PAN-OS

Pokračování

- 4.4. Snídaně s Palo Alto Networks: Jak Palo Alto Networks chrání koncové body
 - <https://nextgenfw.cz/skoleni/snidane-s-palo-alto-networks-jak-palo-alto-networks-chrani-koncove-body/>
- 25.4. Snídaně s Palo Alto Networks: Pokročilé funkce NGFW Palo Alto Networks a co vám přináší
 - <https://nextgenfw.cz/skoleni/snidane-s-palo-alto-networks-pokrocile-funkce-ngfw-palo-alto-networks-a-co-vam-prinasi/>

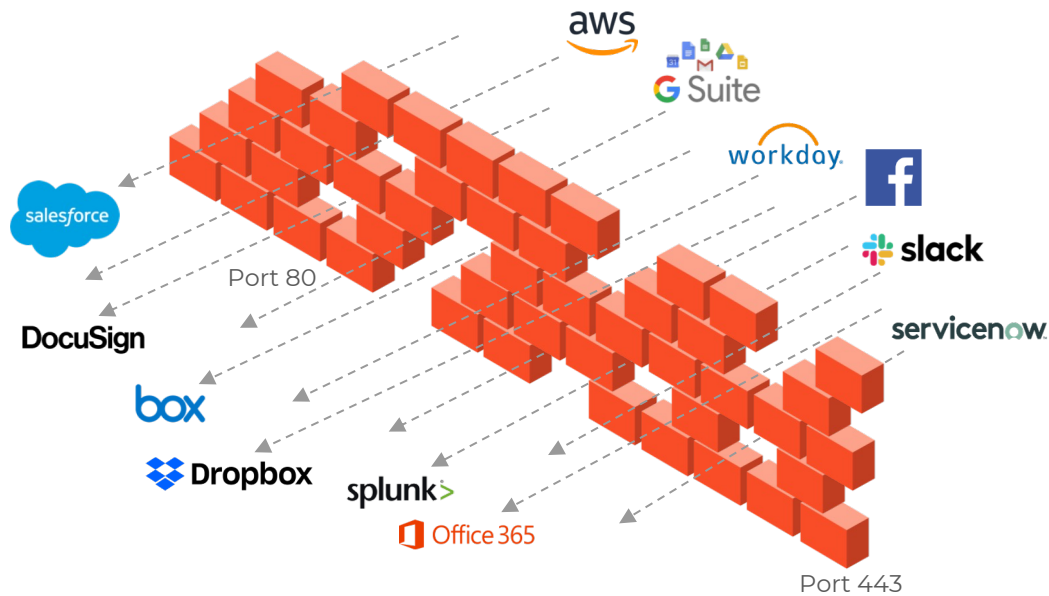
The Network Security Challenge

Applications have changed

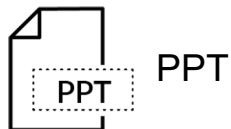
- Ports \neq Applications
- IP Addresses \neq Users
- Packets \neq Content
- IP Addresses \neq Trusted Devices

A new approach is required

- Visibility on all ports/protocols
- All security features enabled all the time
- Application, user, content and device identification
- Inline prevention of known and unknown threats
- Threat Intelligence sharing between all components



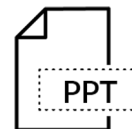
Complete Visibility for Better Security Outcomes



PPT



Slideshare-
Uploading



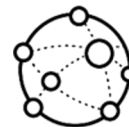
Marked "Private
and Confidential"



Finance



Slideshare



Online Storage
& Backup



joe.davis



HTTP



SSL



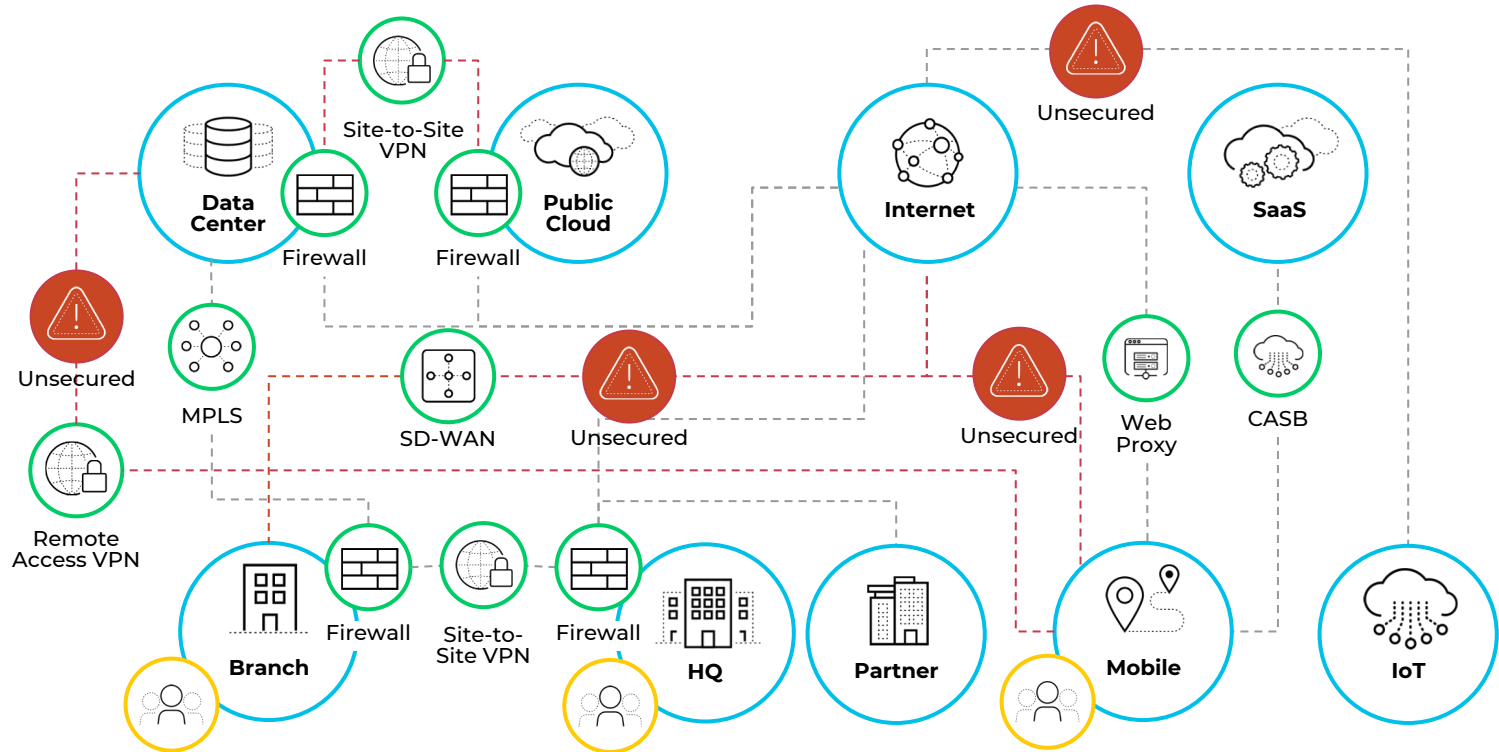
Canada

172.16.1.10
source IP

TCP/443
destination port

64.81.2.23
destination IP

Legacy Network Security Architecture

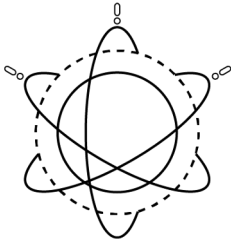
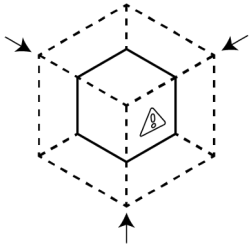
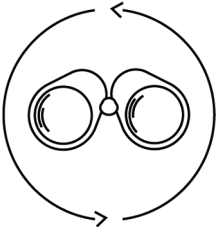


1 Complex

2 Security Gaps

3 Poor User Experience

Preventing Successful Attacks



**Complete
Visibility**

**Reduce Attack
Surface**

**Prevent
Known Threats**

**Prevent
Unknown Threats**

**Consistent Across
all Locations**



Headquarters



Branch
Offices



Data Center/
Private Cloud



Public Cloud



SaaS

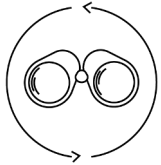


Mobile Users



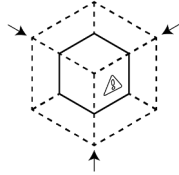
IoT

Prevention Capabilities



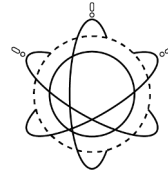
Gain Complete Visibility

- All Applications
- All Users
- All Content
- All Devices
- All Endpoints
- Encrypted Traffic
- SaaS & Cloud
- Mobile



Reduce Attack Surface Area

- Block "Bad" Apps
- Limit App Functions
- Limit File Types
- Block High-risk Websites
- Verify Users
- Limit Devices
- Control Sharing



Prevent All Known Threats

- Exploits
- Malware
- Command & Control
- Malicious Websites
- Bad Domains
- Stolen Credentials



Prevent and Detect Unknown Threats

- Dynamic Analysis
- Exploit Techniques
- Malware Techniques
- Machine Learning
- Static Analysis
- Anomaly Detection
- Analytics

Architectural Flexibility

**Hardware
PA-Series**



**High Performance
Physical Appliances
& Chassis**

**Software
VM-Series / CN-Series**



**Virtual Software
VM & CN Series**

**Cloud Service
Prisma Access**



**Cloud Delivered
Security**

Cloud Delivered Security Services



Scale

Thwart targeted attacks & coordinated campaigns



Leverage

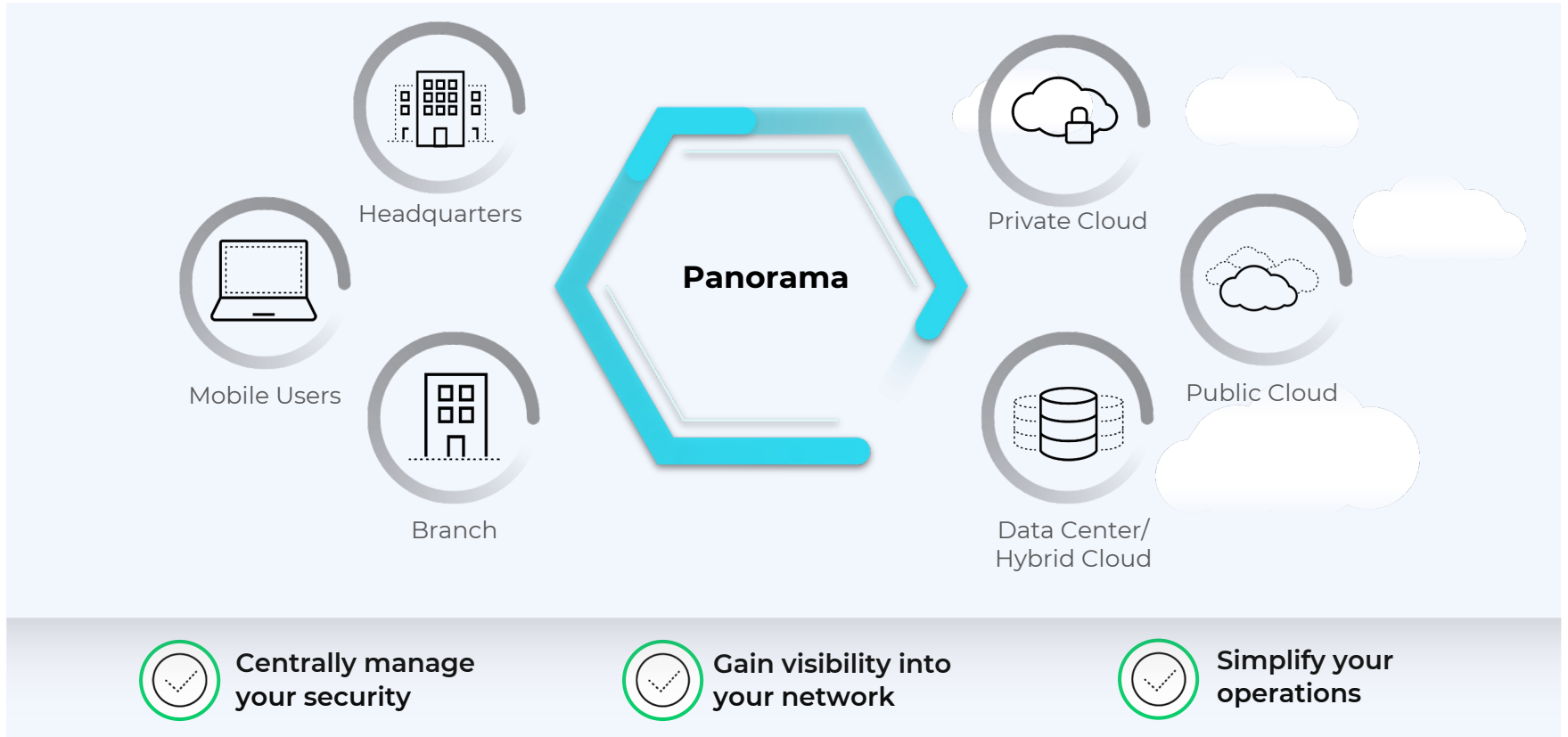
Learn once, apply everywhere



Agility

Quickly consume new security innovations


Centralized Visibility and Management




Simple Security Rules Safely Enable Your Business

NAME	TAGS	Source			Destination	APPLICATION	SERVICE	ACTION	PROFILE	Rule Usage	
		ZONE	USER	DEVICE	ZONE					RULE USAGE	APPS SEEN
Sanctioned SaaS App...	Allowed	Trust	acme\finance	any	Untrust	boxnet concur docusign ms-office365 slack	application-...	Allow	[Profile Icons]	-	0
Tolerated SaaS Appli...	Acceptable	Trust	acme\all_em...	any	Untrust	gmail-base gmail-downl... google-base linkedin-base twitter-base	application-...	Allow	[Profile Icons]	-	0
Access Points	wirelessinfra	Trust	any	Aruba_APs	any	any	application-...	Allow	[Profile Icons]	-	0
RaspberryPi	wirelessinfra	Trust	any	RaspberryPi	any	any	application-...	Allow	[Profile Icons]	-	0


Rule usage to guide policy optimization



Users




Devices



Applications

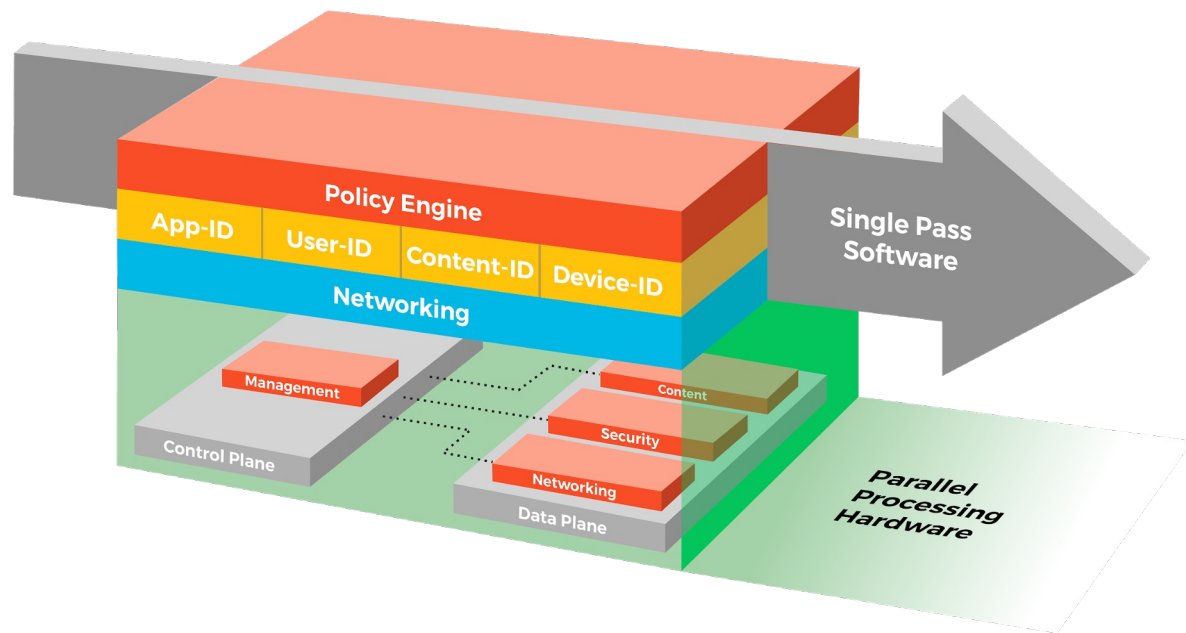
No need to specify ports



All Security Subscriptions

One Policy One Unified Console

Single Pass Parallel Processing (SP3) Architecture



Consistent Prevention Posture: Purpose-built HW, Virtual Software or Cloud Delivered Service

Legacy Multi-Vendor Approach vs. Platform Approach

Capability (examples)

Current State

Future State – Platform

Firewall



Intrusion Detection



URL Filtering



Sandbox Detection



Remote Access for Users



Endpoint + EDR Security



Public Cloud Security / Compliance



Secure Web Gateway



SaaS Security / SaaS Compliance



SD-WAN



Your World Is Changing



Attacks are constantly and automatically morphing



New devices are proliferating rapidly and silently



Surface areas of attack are increasing rapidly

But 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

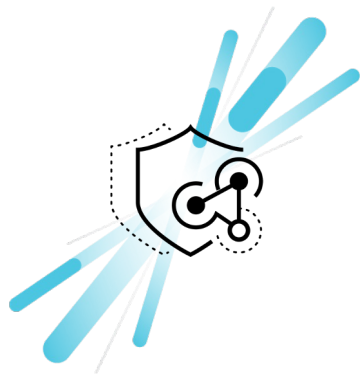
Result: Breaches due to human errors and misconfigurations

[99% of firewall breaches due to misconfig, Gartner](#)



**A New Disruptive Approach Is
Needed**

The World Needs A New Type of Firewall That uses ML to...



Prevent Never-before-seen Items

Identifies new variants of threats & new devices without relying on signatures



Recommend Policy & Config Changes

Analyzes device behavior to automatically create IoT Security policies, uses infrastructure changes for configuration changes



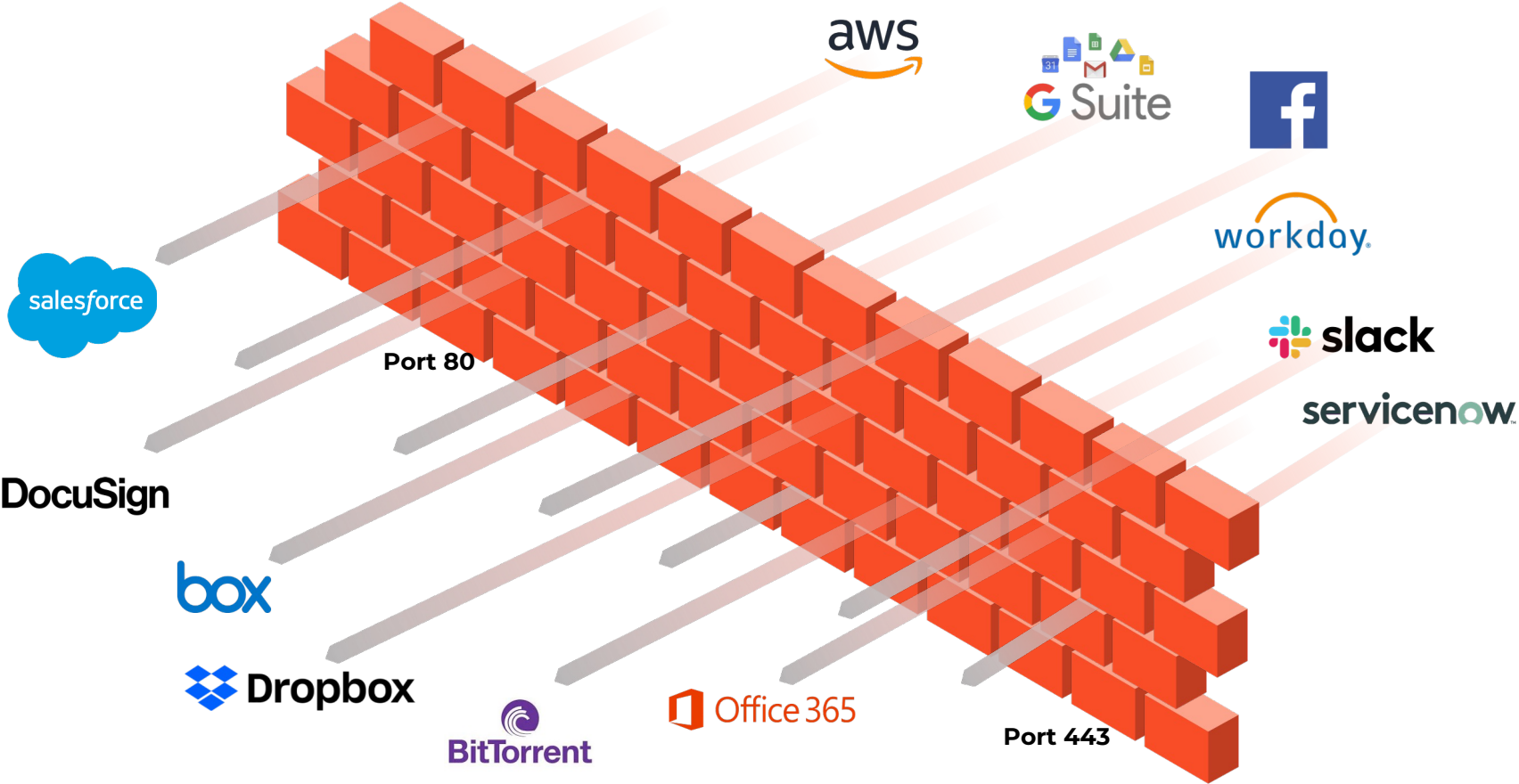
Detect Through Cloud-scale

Enables machine learning at cloud scale through continuous collection of data and telemetry

A PARADIGM SHIFT IN CYBERSECURITY... INTELLIGENT NETWORK SECURITY

Introducing The World's First ML-Powered NGFW

In the Beginning ...



But 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](#)

With Multiple Industry-Firsts...



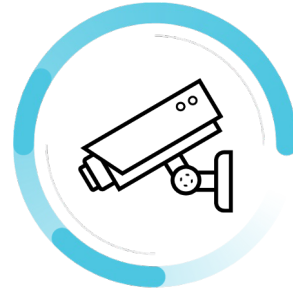
Instant protection from threats using ML

Up to 95% of unknown file- and web-based threats prevented inline



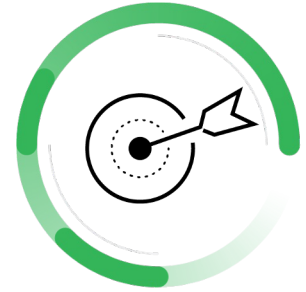
Near real-time protection via signatures

<10 second signature delivery, resulting in 99.5% reduction in systems infected



Complete, natively integrated IoT security

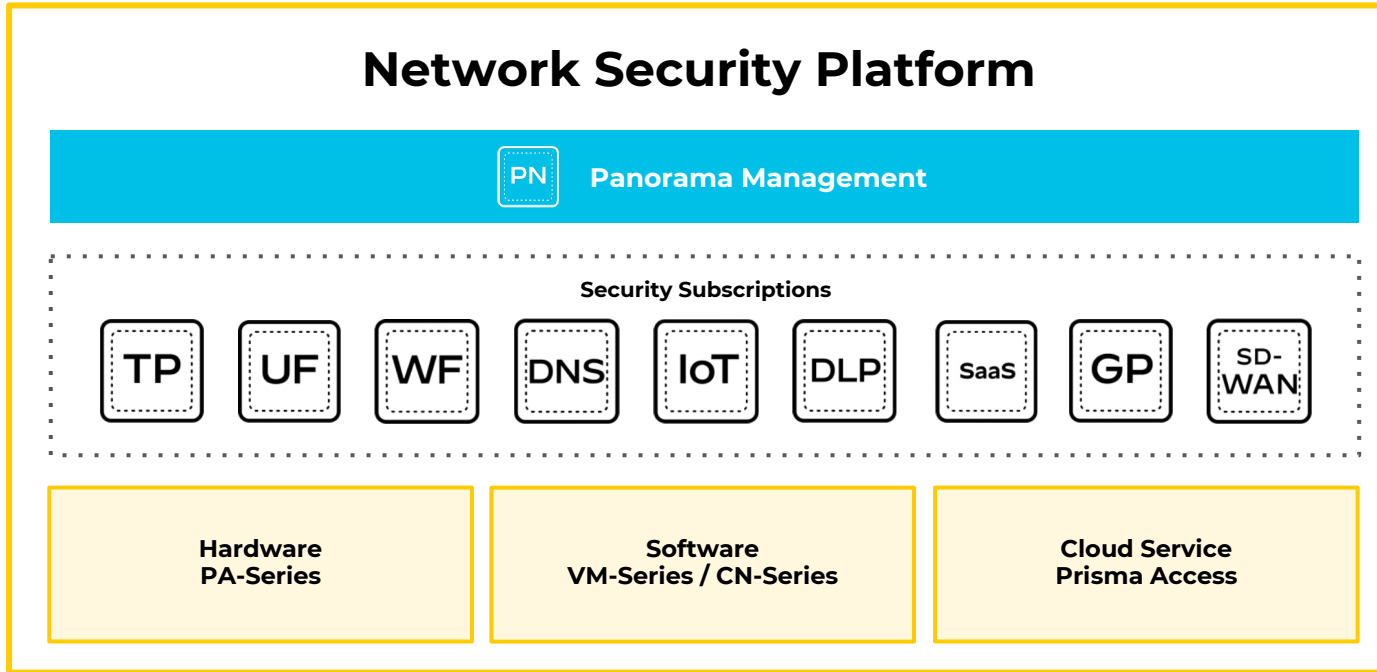
3x IoT devices detected (testing with beta customer)



Automatic policy recommendations

99% of breaches are caused by misconfiguration, according to Gartner

Delivered As Part Of a Platform



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



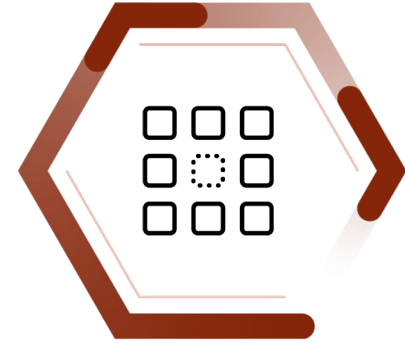
Massive Increase in Connected devices

30% of devices on enterprise networks today are IoT



Pose a Huge Security Risk

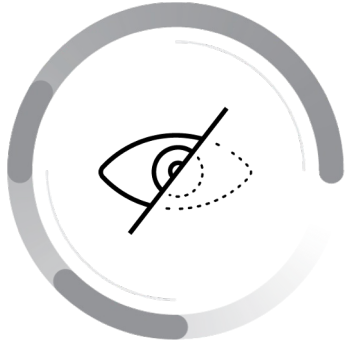
Shipped with vulnerabilities and difficult to patch, yet have unfettered access



Securing IoT Devices is Hard

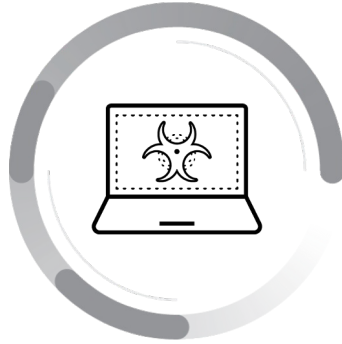
Incredibly diverse devices; traditional IT security controls do not work

Why Current Solutions Fail



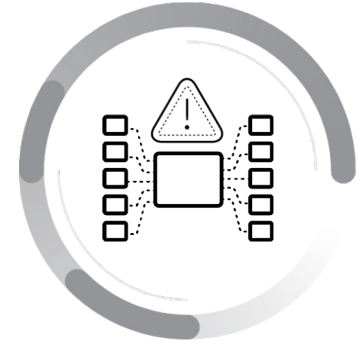
Limited Visibility

Cannot identify previously unseen IoT devices, accuracy requires constant effort



No Protection

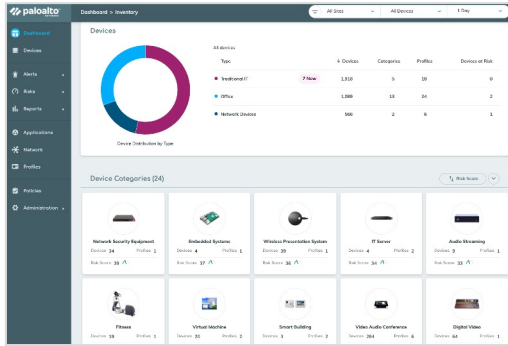
Existing visibility-centric solutions do not offer native prevention or enforcement



Hard to Implement

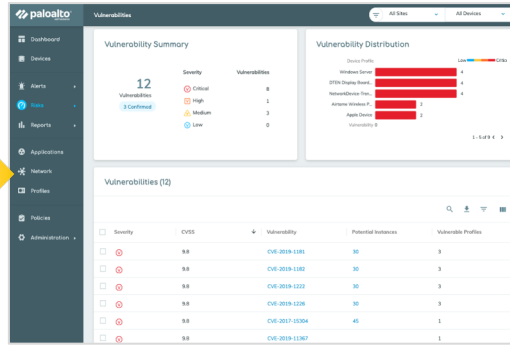
Require changes to network infrastructure, security team workflows and integrations

Introducing IoT Security



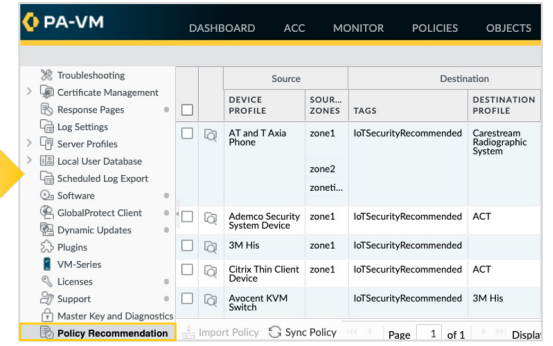
Complete Visibility

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



In-depth Risk Analysis

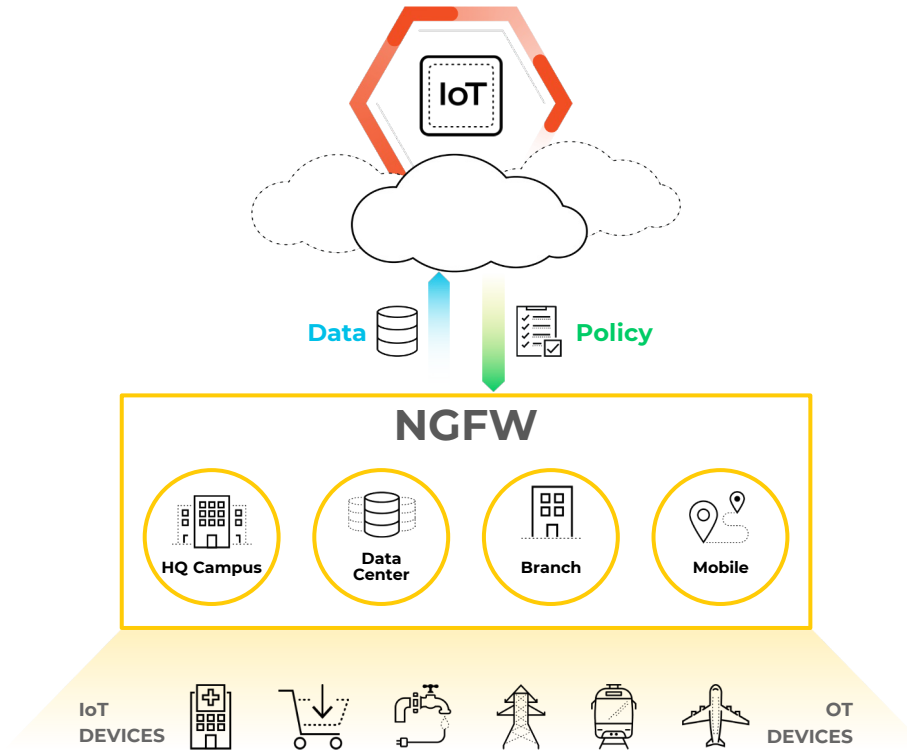
Quickly understand anomalies, vulnerabilities and severity to make confident decisions



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

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**

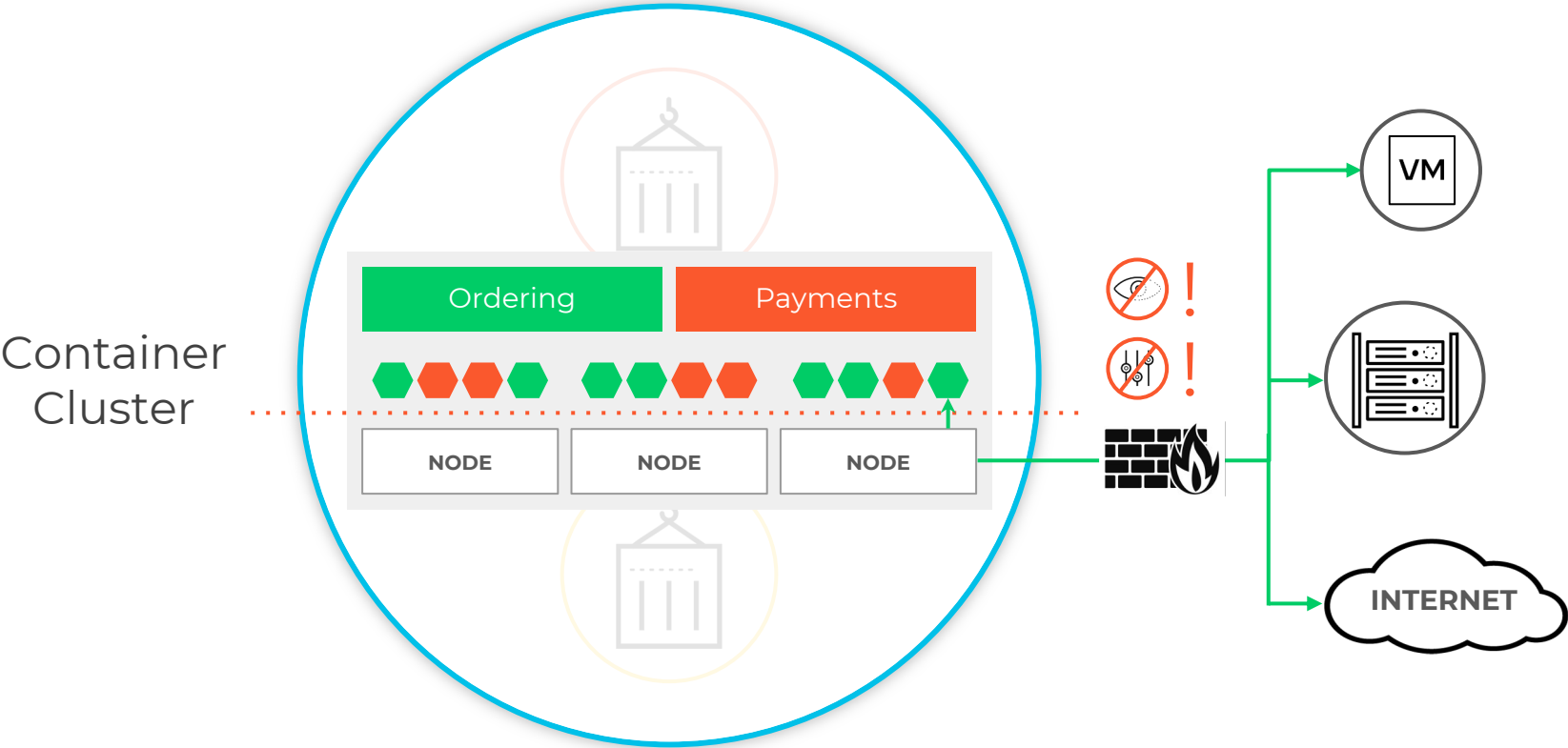


**Inconsistent tools
and management**



**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

Supported Cloud Native Infrastructures

Self-Managed



On-premises

Public Cloud

Cloud-Managed

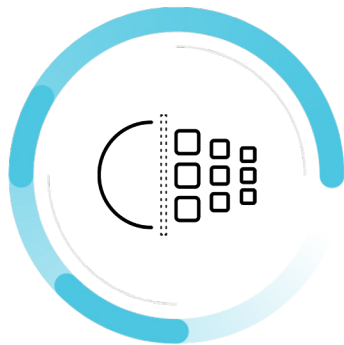


CN-Series Container Firewall Use Cases



East-West Layer 7 Traffic Protection

Enforce trust boundaries between namespaces and other workload types



Outbound Traffic Protection

URL filtering and content inspection

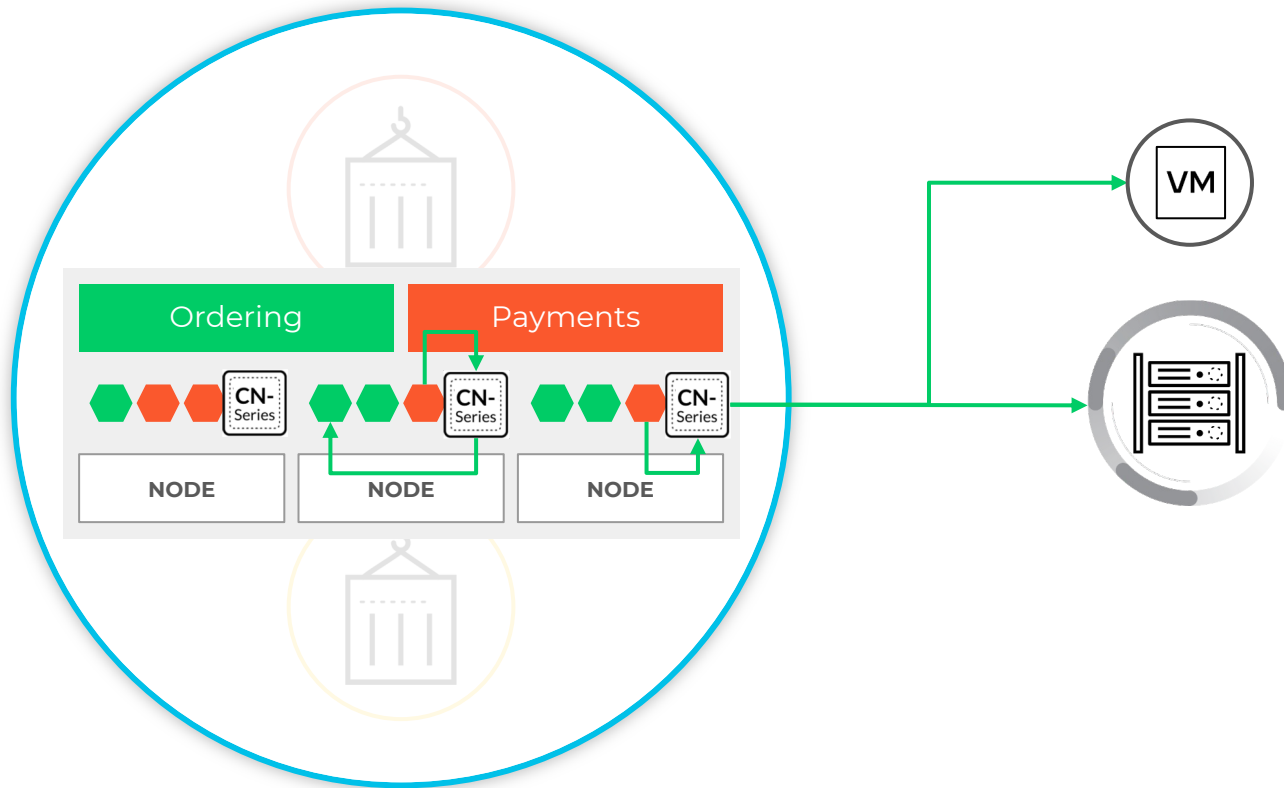


Inbound Threat Prevention

Stop known and unknown threats

Use Case 1: East-West Layer 7 Traffic Protection

Shared Container Cluster



CN-Series Container Firewall Differentiated Capabilities



**Centralized
Management**



**DevOps-Ready
Orchestration**



**Kubernetes Visibility
& Context**

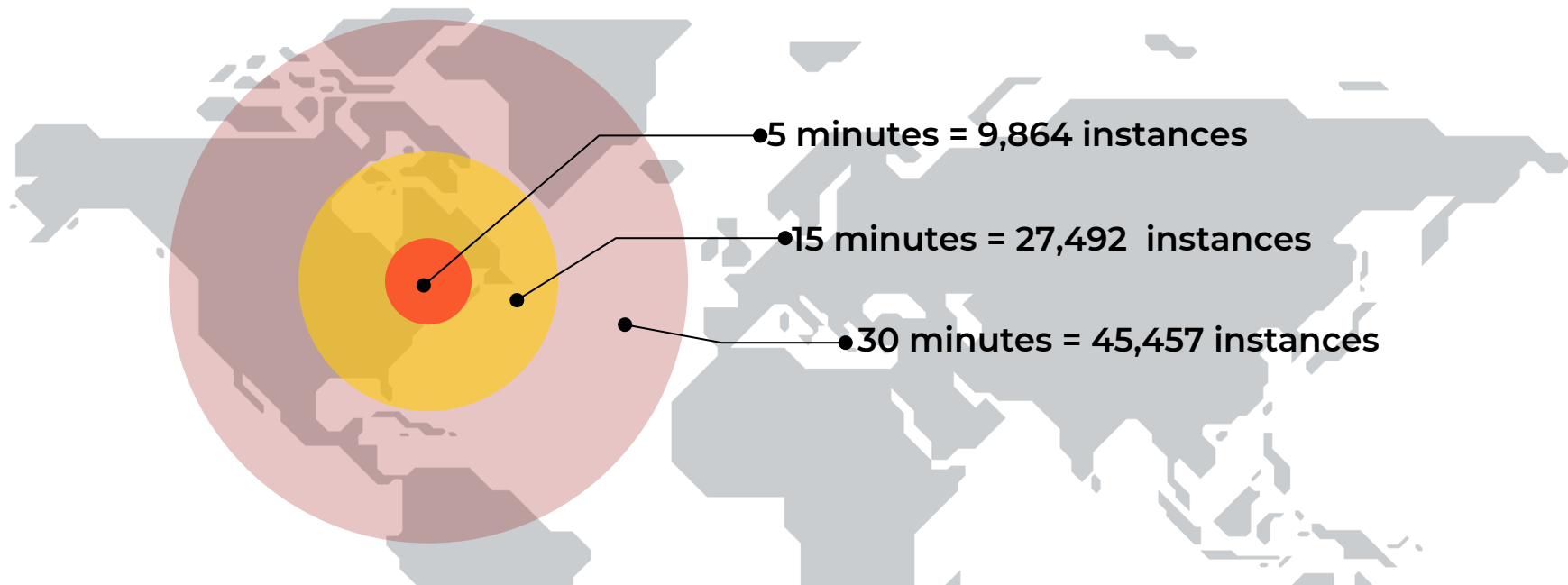


**Best-in-Class
Security**

ML-Based Inline Prevention

Every Second Matters

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

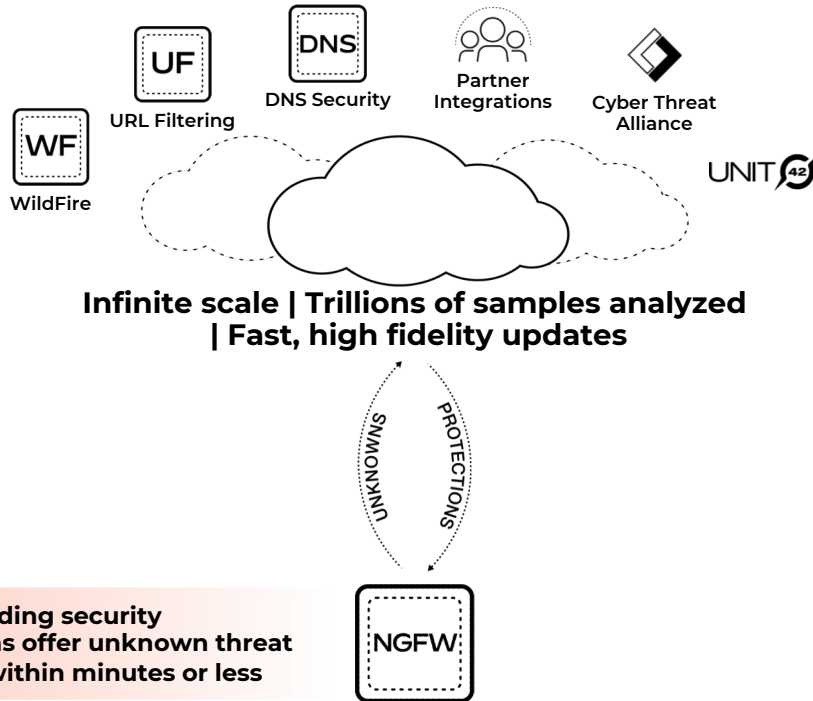
Accurate prevention depends on on a first victim



Stop Business

Current hold, trickle and modify approaches impact users and revenue




Today's Prevention of Unknown Threats Through Cloud Scale



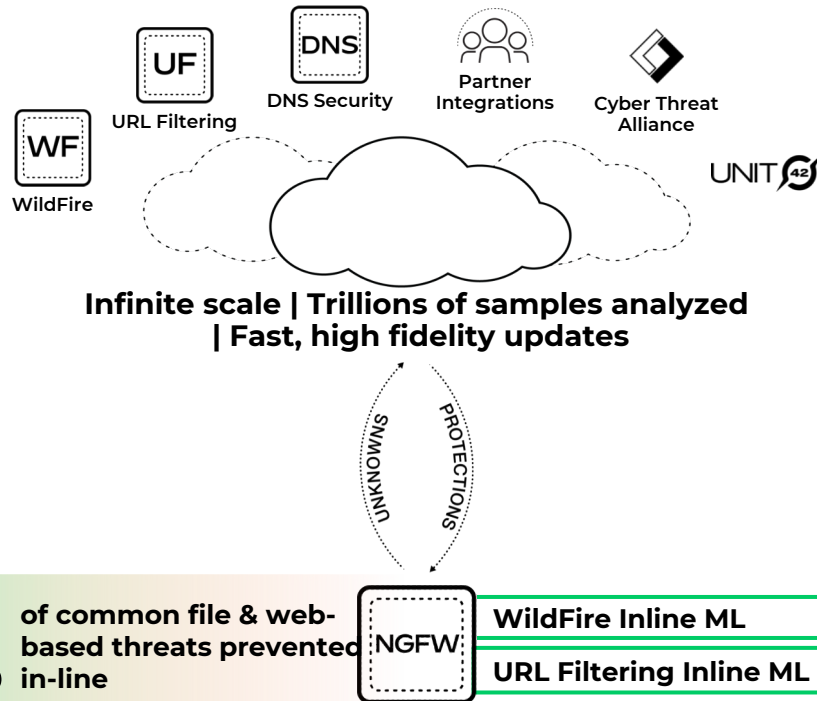
Industry-leading security subscriptions offer unknown threat protection within minutes or less

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**




Today's Prevention of Unknown Threats Through Cloud Scale



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**

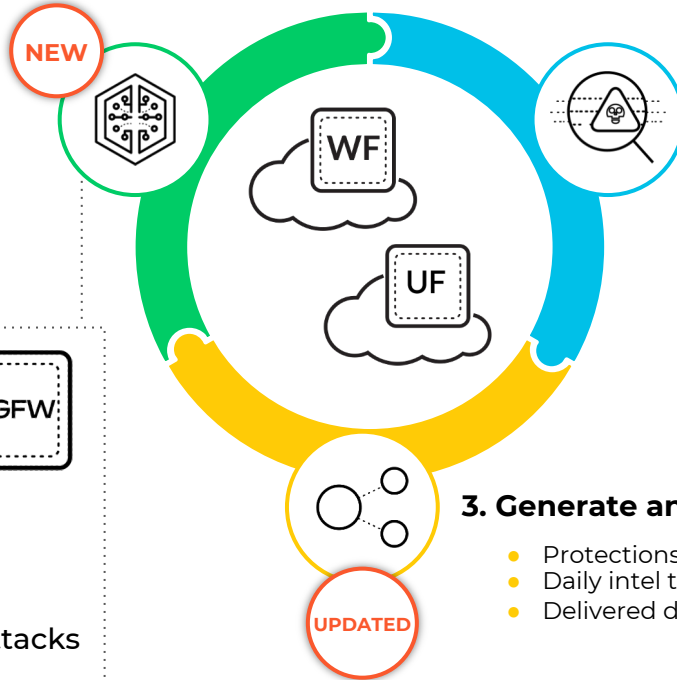
How It Works: Inline ML-based Prevention for Files and Web-Based Attacks

1. Prevent unknown file/web threats on the NGFW

- ML-based signatureless prevention
- Acts at line speed
- No productivity delays



- ⊘ Phishing Attacks
- ⊘ JavaScript Attacks
- ⊘ Common File and Fileless attacks (PE and PowerShell)



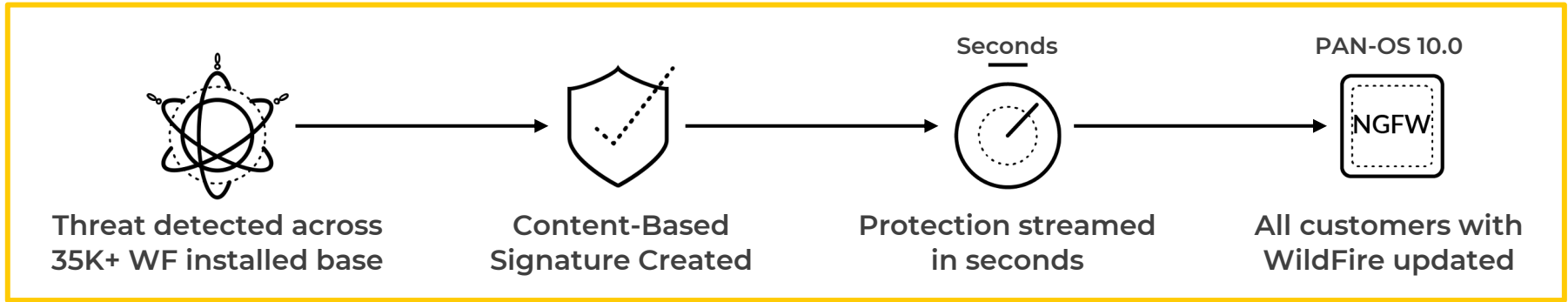
2. Analyze all unknowns in cloud

- Multiple advanced techniques for malware
- Best-in-class URL categorization engines
- Shared intelligence improves analysis

3. Generate and Distribute Protections & Models

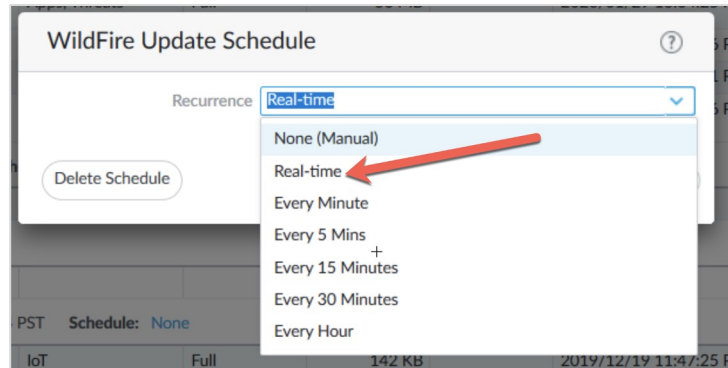
- Protections for all threats in as fast as single-digit seconds
- Daily intel trains new models
- Delivered directly to NGFWs daily

Slashing Our Industry-Leading Time for Distributed Protections



BEFORE

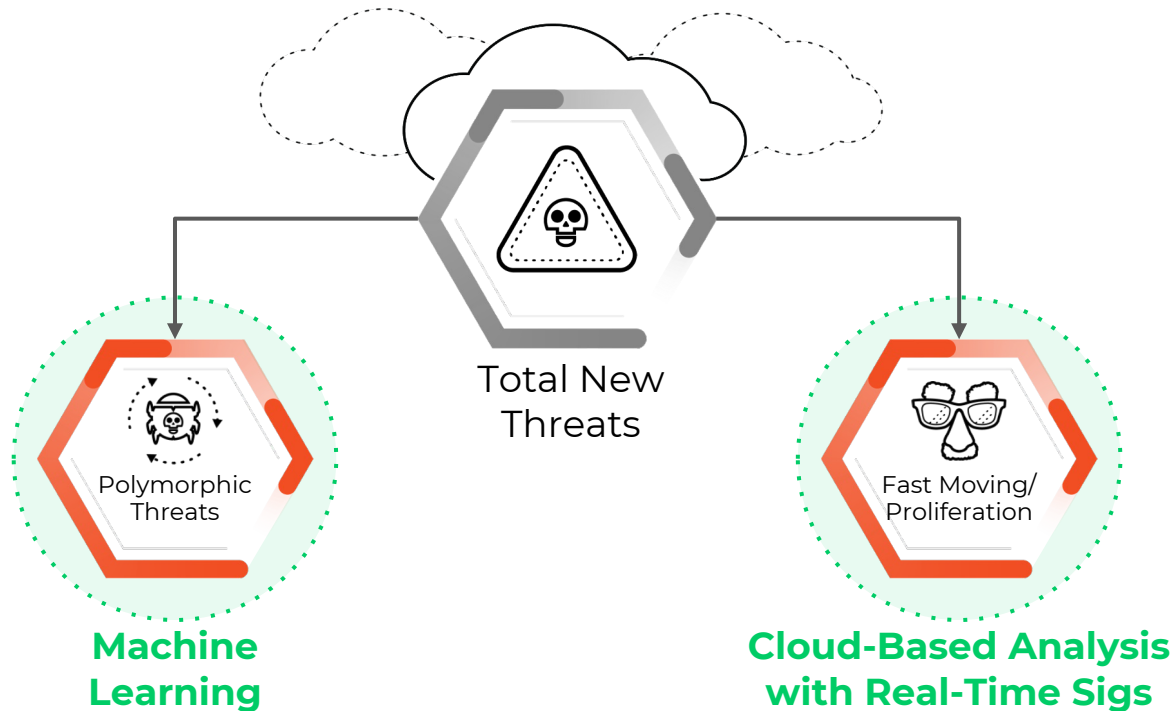
Industry-leading
5-minute signature
generation/
distribution time



With PAN-OS 10.0

Protection streams
to NGFW in
single-digit seconds

Stopping Attacker Advantage



Enabled by the Platform scale



Prevents initial infection



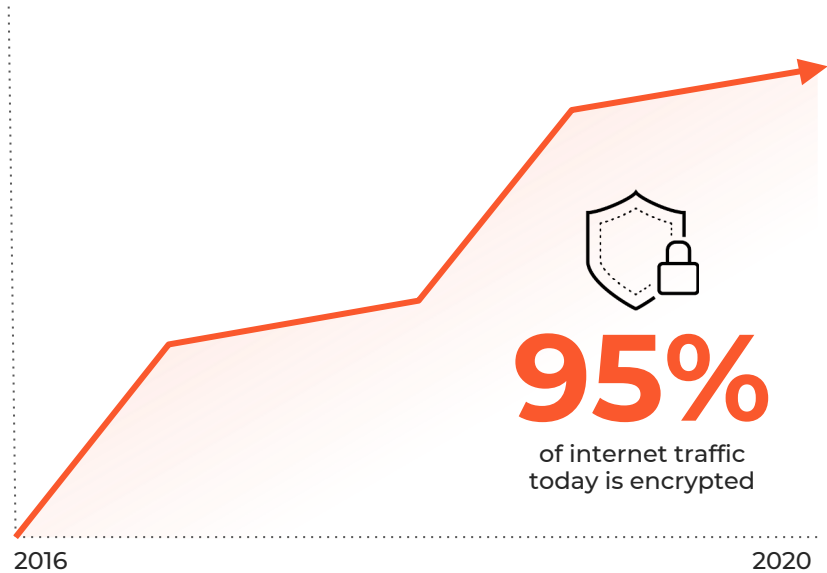
No Business Disruption

TLS Decryption

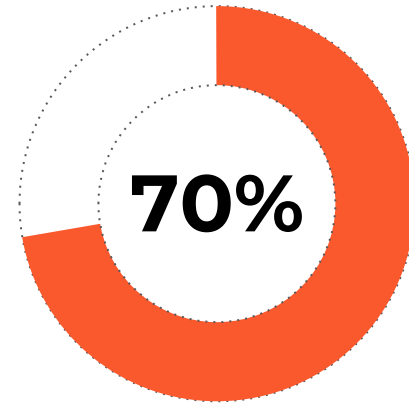
Never been more essential to decrypt

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)

Decryption is Necessary for Protection



Protection requires decryption

Without decryption, security tools cannot effectively stop malware



Deploying decryption is usually hard

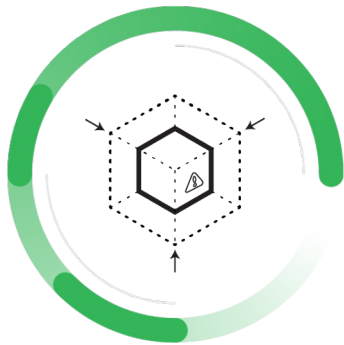
Lack of expertise, fear of business disruption, troubleshooting complexity



Cloud apps making the need to decrypt more urgent

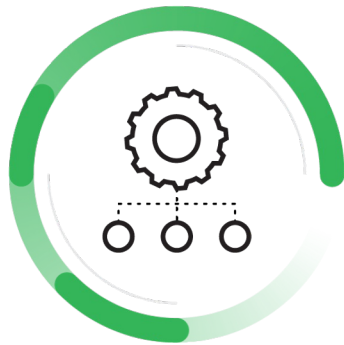
Increasing adoption of HTTP/2 and encryption with modern protocols like TLS 1.3

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

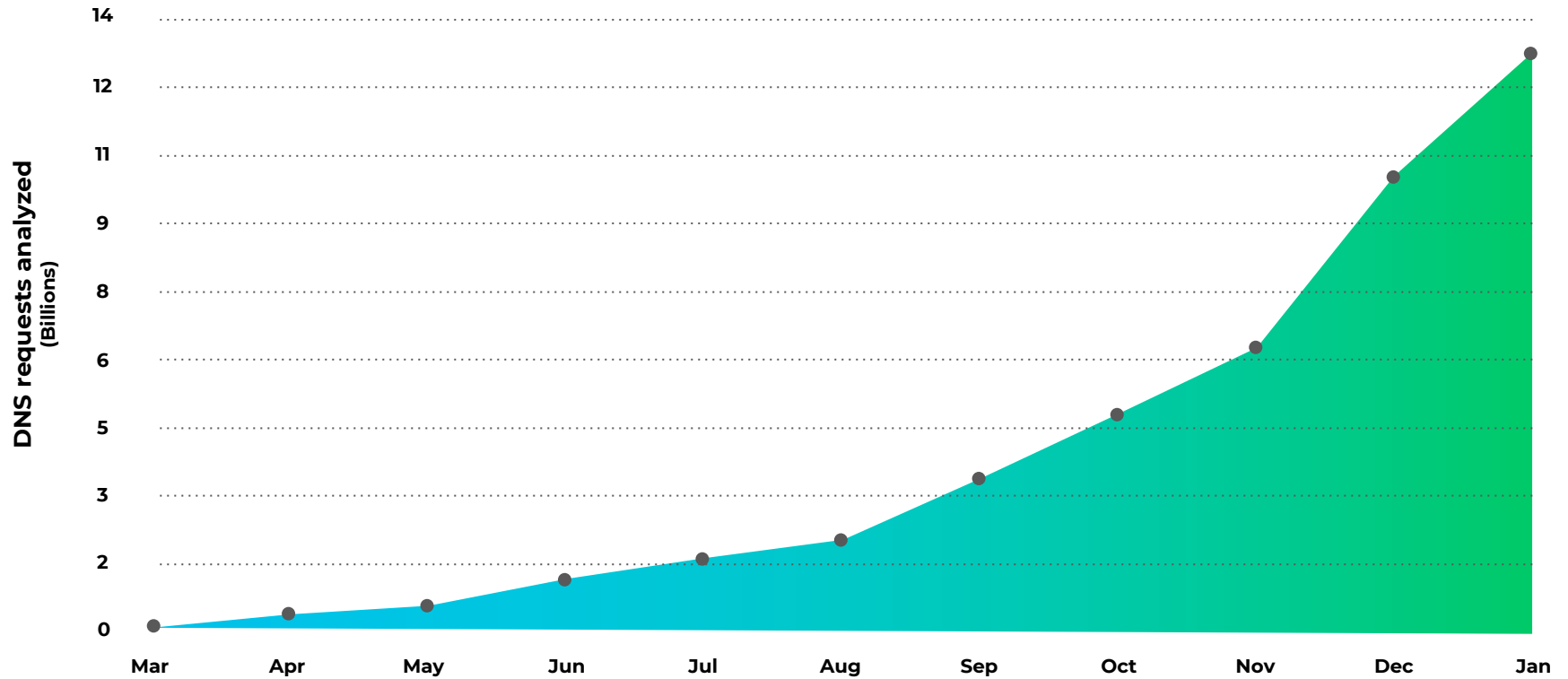


Secure cloud apps quickly

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

DNS Security

One Year in, Amazing Growth...



Modern Risks Presented by the DNS Protocol



**80% of
Malware**

DNS is abused for
command and control
and data theft



**Rate of New
Domains**

Malware using domain
generation algorithms evade
detection



**Data
Exfiltration**

Modern adversaries
using DNS tunneling

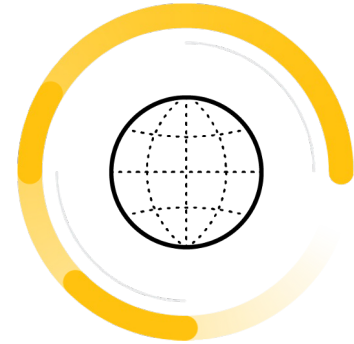
DNS Security



**Blocks known
bad domains**



**Stops malicious DNS
traffic with ML and
predictive analytics**

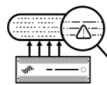


**Integration with
NGFW means it
cannot be bypassed**

Data



WildFire Analysis



Passive DNS



URL Filtering



Honeynets



Unit 42



Whois

Introducing Category-Based Visibility and Control for DNS



Categories

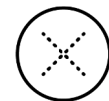
DNS Tunneling	DGA
C2	Malware
Dynamic DNS	Newly Registered Domains

Policy

- Sinkhole C2 domains with a “critical” threat log
- Trigger automated containment workflow



Malware



Severity: Medium

Policy

- Block malware domains with a “medium” threat log
- Does not require a follow-up action

DNS Analytics

DNS Visibility

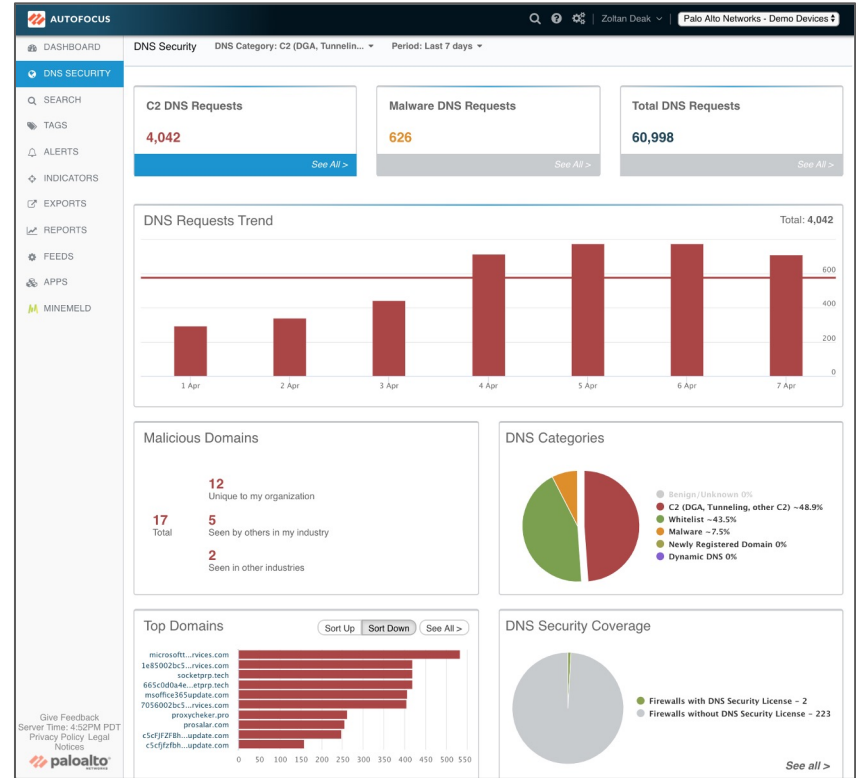
- Complete visibility across all DNS traffic and trends
- Filter based on DNS categories and timeframes
- Abuse of DNS (malware, C2, tunneling, DGA)

DNS Intelligence Context

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

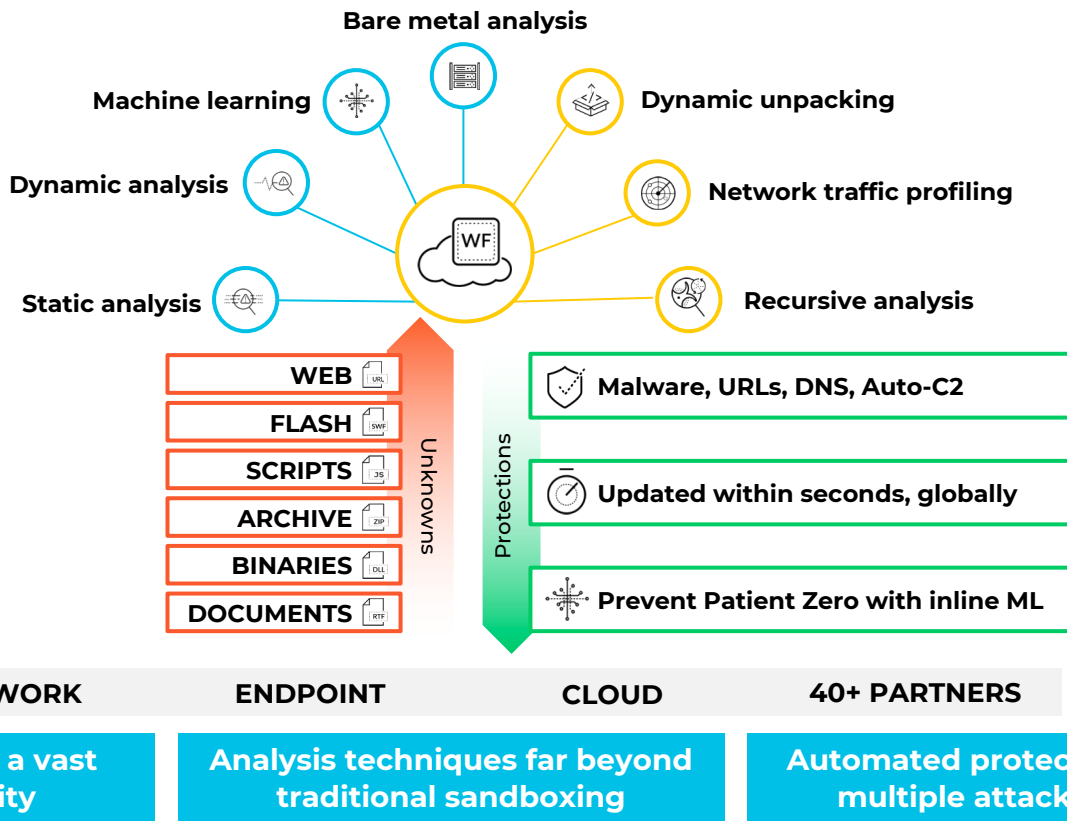
DNS Hygiene

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

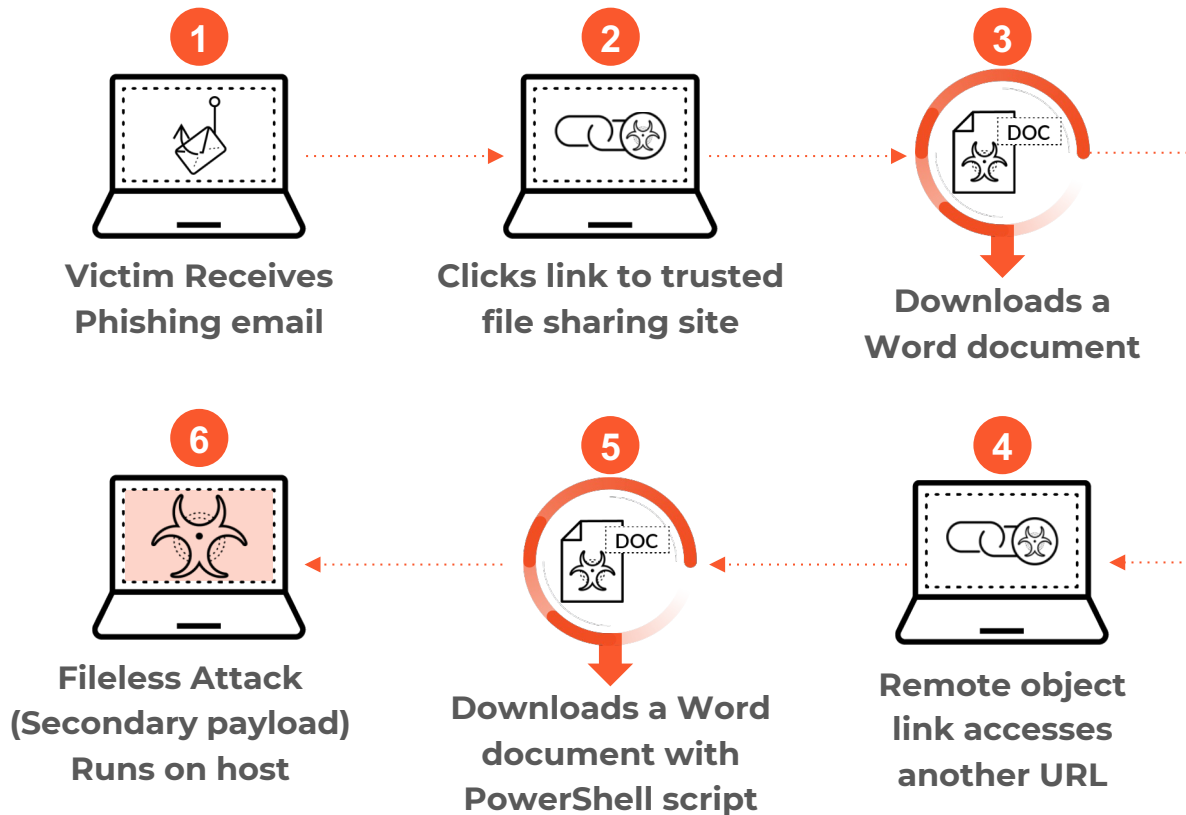


WildFire

Detect and Prevent New Threats with WildFire



Attackers Continue to Employ Sophisticated Multi-Vector Attacks



TACTICS

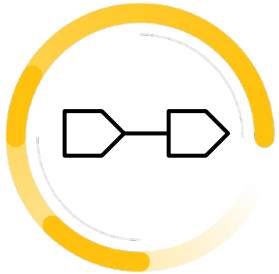
Break attack into smaller components

Deploy range of threats across stages

Use multiple points of entry (attack vectors)

Hide malicious content Behind benign URLs and legitimate cloud infrastructure

WildFire's Unique Multi-Vector Recursive Analysis



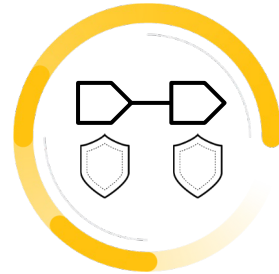
Crawl Each Stage Of Attack

Multiple vectors / file stages / network hops



Apply Cloud-Scale Recursive Analysis

Analyze each sample in net new environments



Generate Protections for Each Stage

Full attack + all other payloads



Share Protections & Visualize Campaign



Attackers Must Replace All Stages of Attack Workflow

The WildFire Advantage



Unbeatable Cloud Analysis Infrastructure



Best-in-Class File Analysis & URL Crawling



Unique view of entirety of attacker campaign

Supercharged Static Analysis Engine Delivers Quicker Detection



WildFire Static Analysis Engine

- Part of WildFire's multi-step malware analysis system
- Examines potentially malicious code without executing
- Critical to identifying variants of known malware
- Depends on timely and accurate threat models

What We Did



Incorporated best-in-class ML engine from XDR



Leveraged WildFire's infinite scale and compute

Results

14.5%

Improvement to
Static analysis model

What It Means



Improved final detection rates for malicious files



Faster determinations for immediate verdicts

Informace

- [Ransomware as a Service: Criminal “Entrepreneurs” Evolve Ransomware \(paloaltonetworks.com\)](#)
- https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/2022-unit42-ransomware-threat-report-final.pdf

Závěr?

- Zero Trust
- Měnicí prostředí musí mít možnost udržet úroveň bezpečnosti
- Prevence x Reakce
- Počet odborníků x počet incidentů
- Automatizace
- ML
- AI

Co si o tom myslí AI

- Automatizace:

- Mnoho úkolů v oblasti kybernetické bezpečnosti může být automatizováno pomocí AI a ML, což může uvolnit odborníky k řešení složitějších problémů. Například, může být automatizován proces detekce a reakce na útoky, což umožní rychlejší a účinnější reakci na kybernetické útoky.

- Detekce hrozeb:

- AI a ML mohou pomoci při detekci kybernetických hrozeb pomocí analýzy velkých objemů dat a identifikace anomálií v chování sítě. Tyto technologie mohou také pomoci v identifikaci hrozeb, které jsou založeny na nových neznámých taktikách a technikách.

- Prediktivní analýza:

- AI a ML mohou být použity k prediktivní analýze dat a trendů v oblasti kybernetické bezpečnosti, což umožní předvídat budoucí hrozby a přijmout preventivní opatření k jejich minimalizaci.

- Zlepšení obranyschopnosti:

- AI a ML mohou být také použity k vylepšení obranyschopnosti organizace. Například, mohou být použity k identifikaci a opravě zranitelností v systémech a aplikacích a k analýze bezpečnostních rizik v celé organizaci.

- Nicméně, je třeba poznamenat, že AI a ML nejsou náhradou za lidské odborníky v oblasti kybernetické bezpečnosti. Namísto toho, AI a ML mohou být použity k podpoře a doplnění lidských odborníků, kteří jsou stále potřební pro provádění složitých analýz a rozhodování v oblasti kybernetické bezpečnosti.

Thank you

