Net++ TECHNOLOGY

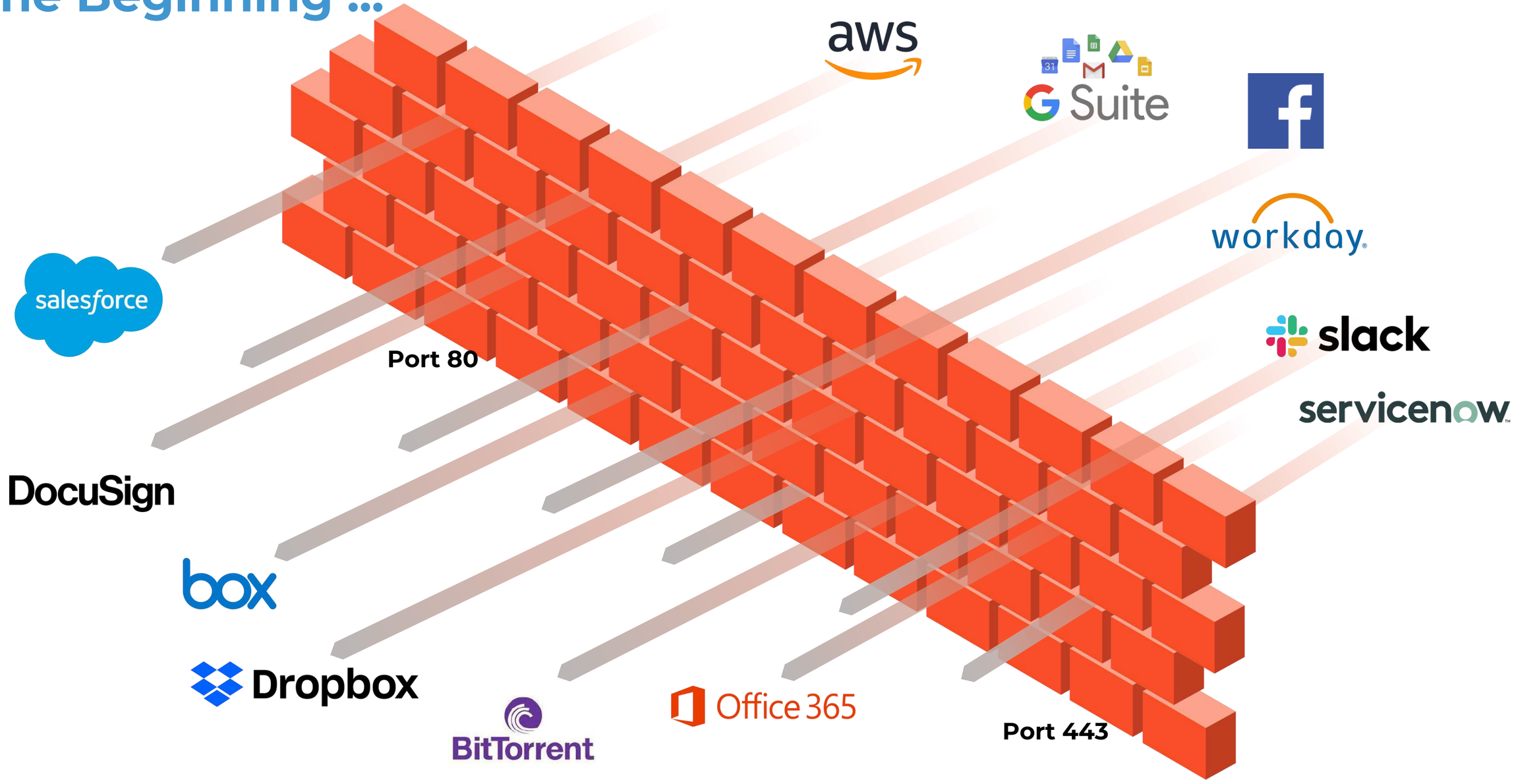
Trust no network traffic

Dimitrije Veličanin

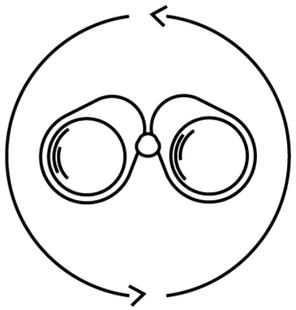
Palo Alto Networks NGFW (Hi)story

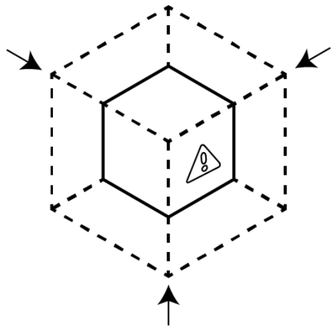
Global Cybersecurity Leader

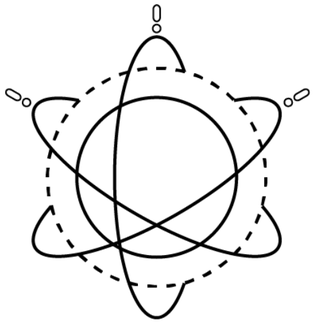
In the Beginning …



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

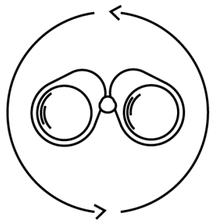
Public Cloud

SaaS

Mobile Users

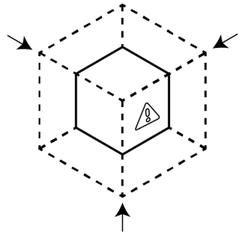
IoT

Prevention Capabilities



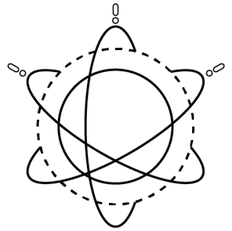
Gain Complete Visibility

- 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

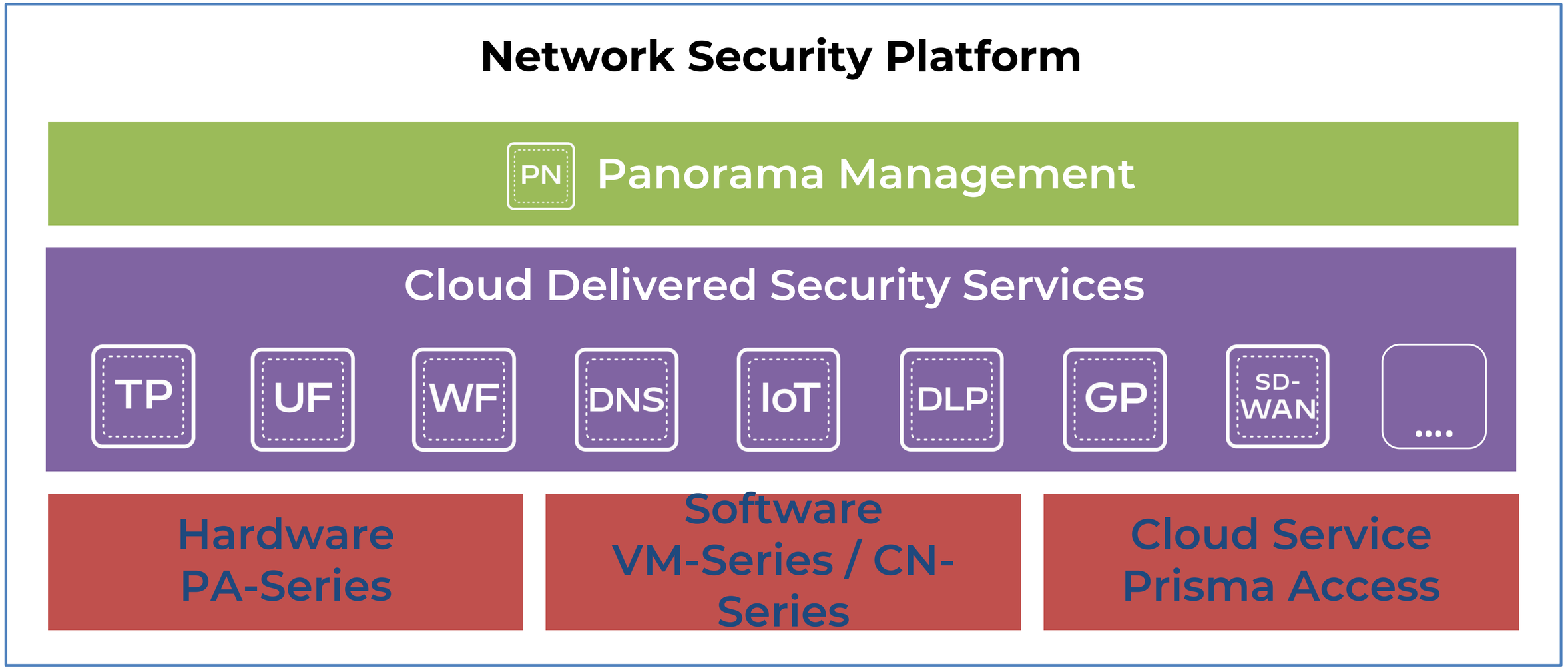
- Exploits
- Malware
- Command & Control
- Malicious Websites
- Bad Domains
- Stolen Credentials

Prevent and Detect Unknown Threats

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

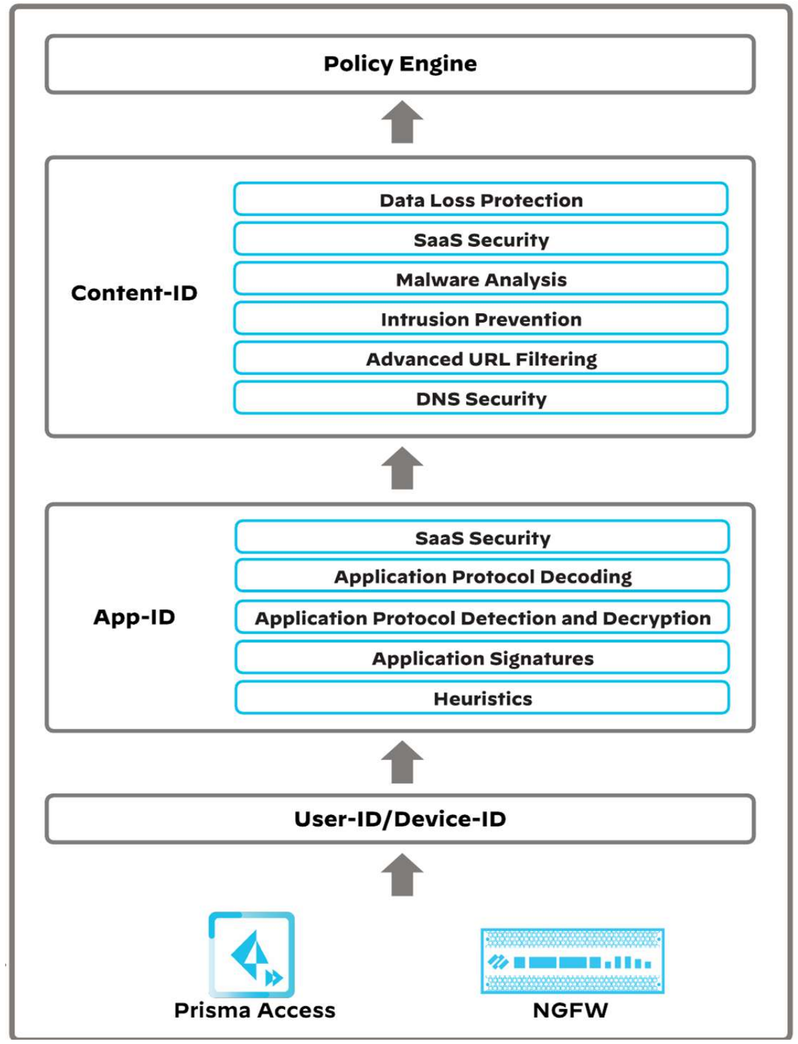
NetOne TECHNOLOGY

Palo Alto Networks Security Platform Components

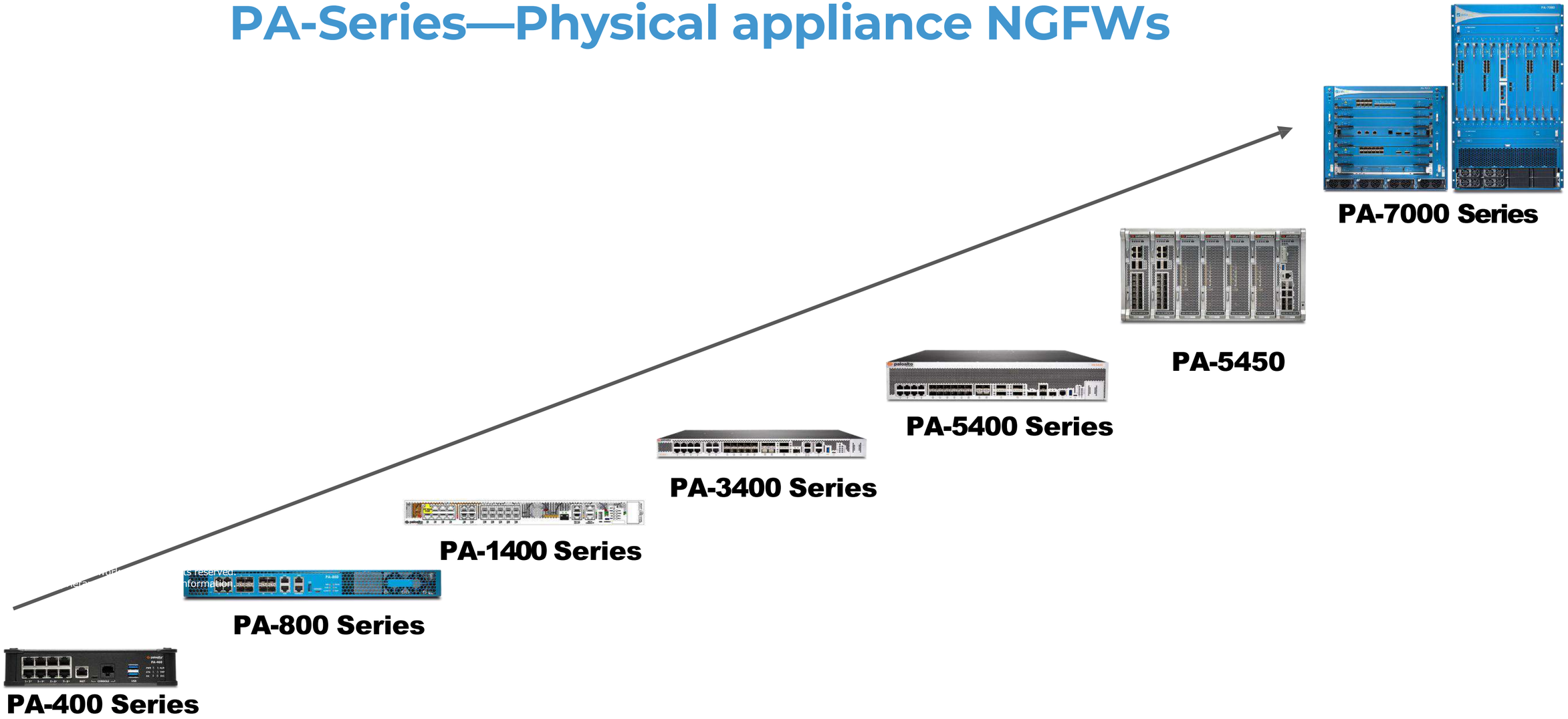


Palo Alto Networks NGFW

- PA-Series—Physical appliance NGFWs.
  - Internet perimeter
  - Data center perimeter
  - Campus and branch
- VM-Series—Virtualized form-factor NGFWs.
  - Public and private cloud
- CN-Series—Containerized NGFWs.
  - Kubernetes clusters
- NGFWs performs multiple security functions with a single-pass architecture, offering consistent performance.
- Legacy firewalls typically follow a sequence of separate functions in packet processing, suffering from deteriorated performance as features get enabled.



PA-Series—Physical appliance NGFWs

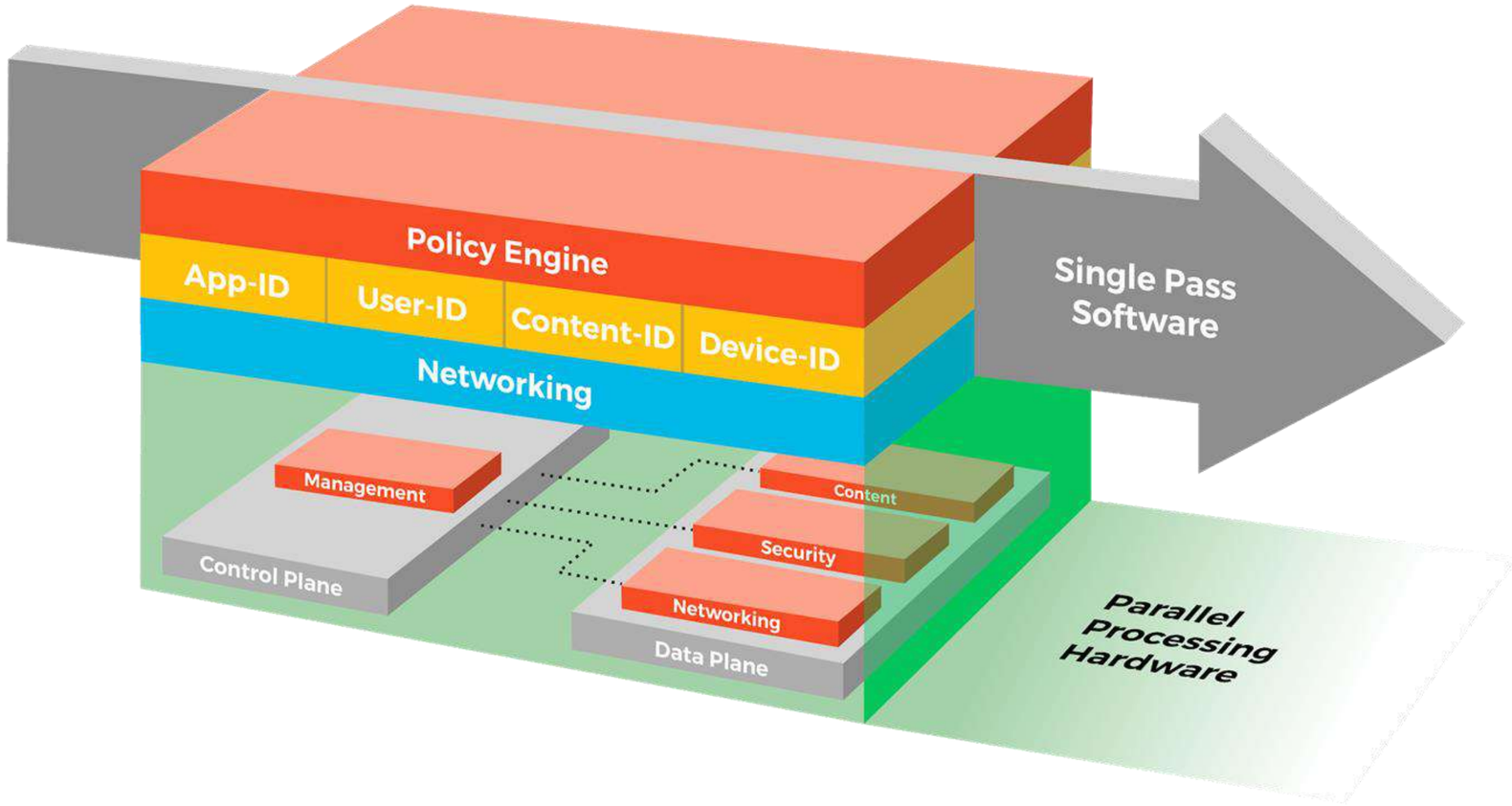


Small Branches & Remote Locations

Network Perimeter

Large Data Centers

Single Pass Parallel Processing (SP3) Architecture



Predictable Performance for All Features Turned On

Simple Security Rules Safely Enable Your Business

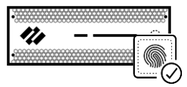
NAME	TAGS	Source			Destination	APPLICATION	SERVICE	ACTION	PROFILE	Rule Usage	
		ZONE	USER	DEVICE	ZONE					RULE USAGE	APPS SEEN
Sanctioned SaaS App...	Allowed	Trust	acme\finance	any	Untrust	boxnet concur docusign ms-office365 slack	application-...	Allow		-	0
Tolerated SaaS Appli...	Acceptable	Trust	acme\all_em...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

Rule usage to guide policy optimization

One Policy One Unified Console

NetOne TECHNOLOGY

Modern Problems Require Modern Solutions



First NGFW shipped with App-ID

2007

2009

PN

Network Security Management

VM-Series

Virtualized Firewalls

2013

2014

WF

Advanced Malware Analysis

Cloud Delivered Firewall Service

2018

2019

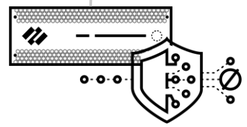
Secure SD-WAN

CN-Series

Containerized Firewall

2020

2020



Industry's First ML-NGFW

Powered by PAN-OS

Industry’s first ML-Powered NGFW

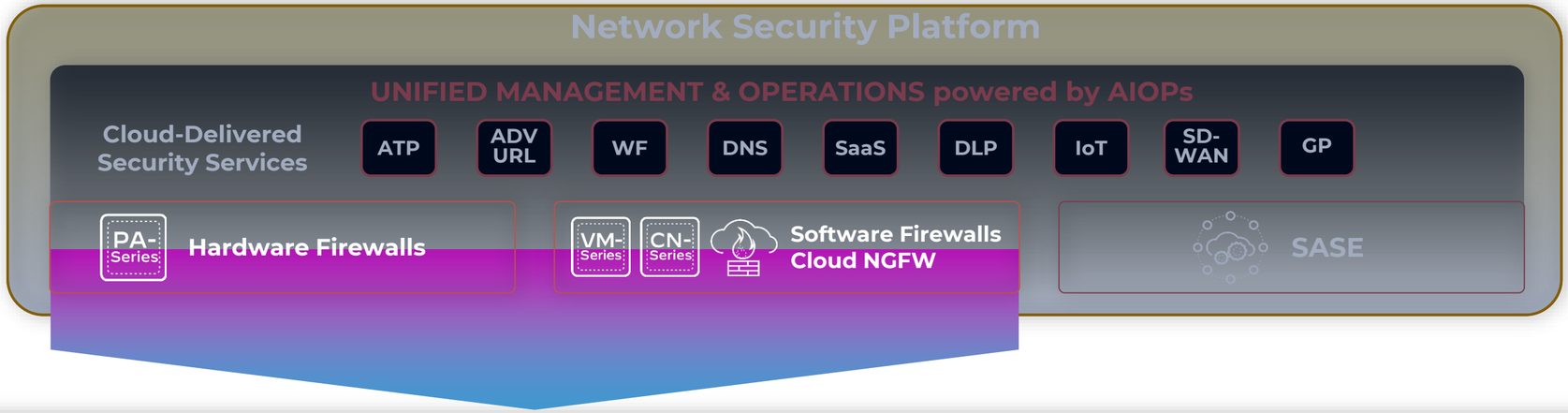
File Protections: **Instant**

URL Protections: **Instant**

DNS Protections: **Instant**

Protect up to 95% of unknown threats instantly

NEXT-GEN FIREWALLS: LEADING WITH CONTINUOUS INNOVATION



Proven innovation & execution

- 11-time leader in Gartner Magic Quadrant
- Leader in Forrester Wave™: Enterprise Firewalls
- CyberRatings.org Top AAA rating for Enterprise Firewall

Hardware & software form factors

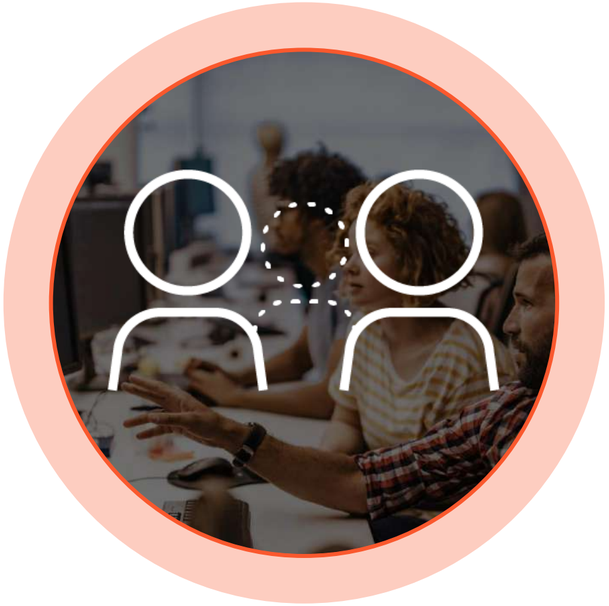
- 4th gen hardware for every location with up to 10x higher performance
- Software NGFWs to secure all networks and any cloud
- Security for IoT/OT and 5G environments

Unified management & operations

- Manage network security policies for your entire organization in one place
- One dashboard view for all on-prem and cloud implementations
- Revolutionize firewall operations and strengthen security posture with AIOps

KEY TRENDS IMPACTING NETWORK SECURITY

The shift to the cloud has gone mainstream



The nature of work has changed fundamentally

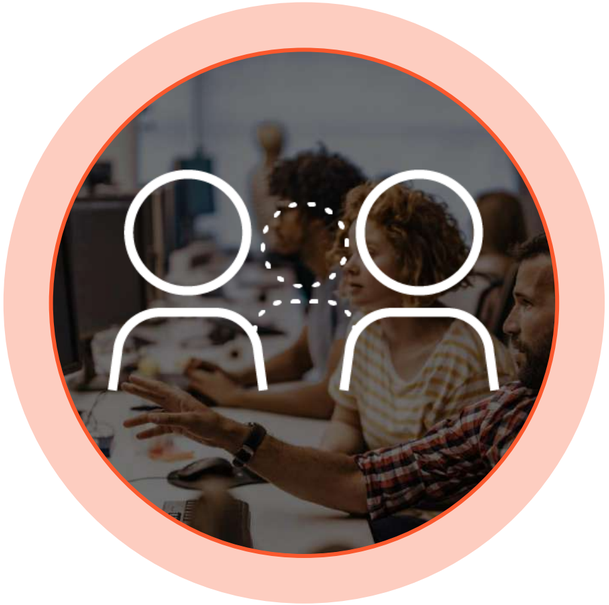
The threat landscape continues to escalate

KEY TRENDS IMPACTING NETWORK SECURITY

The shift to the cloud has gone mainstream

188%

YoY increase in Cloud incidents



The nature of work has changed fundamentally

61%

of organizations say they are struggling to secure the hybrid workforce

The threat landscape continues to escalate

53%

of organizations turn to AI for more effective threat detection

NetOne TECHNOLOGY

Transforming network security is critical to ensure a zero trust enterprise

data. Zero Trust is data-centric: Sensitive data is protected by microperimeters of control, security professionals have full visibility into these assets, and there is an in-depth understanding of how the business uses the data.[12]

Next-Generation Firewalls Are The Cornerstone Of Zero Trust

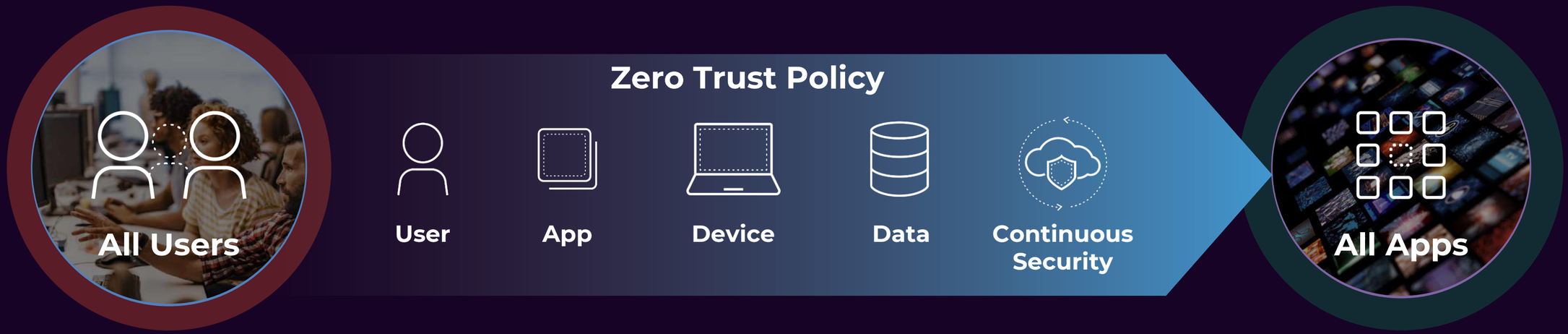
Advances in firewalls make the Zero Trust infrastructure possible. In a Zero Trust network, next-generation firewalls act as "segmentation gateways," taking security controls found in individual point products (firewalls, intrusion prevention systems, web application firewalls, content-filtering gateways, network access controls, VPN gateways, and other encryption products) and embedding them in a single solution.[13] Unlike traditional firewalls, these powerful technology considerations, have in-depth insight into your current environment, and fully evaluate and test vendor solutions. Forrester's study identified the following best practices:

- **Get a clear understanding of the implications of implementing a NGFW on both your infrastructure and staffing and budgetary resources.** It may seem like a no-brainer, but it is important to not only evaluate the technical aspects of a NGFW implementation, but the impact on resources as well. Technical factors, such as performance, security effectiveness, compatibility, and flexibility of the platform, were top of mind among survey respondents when evaluating NGFWs, but they also factored in cost, implementation time, and the IT resources needed to manage the solution (see Figure 4).

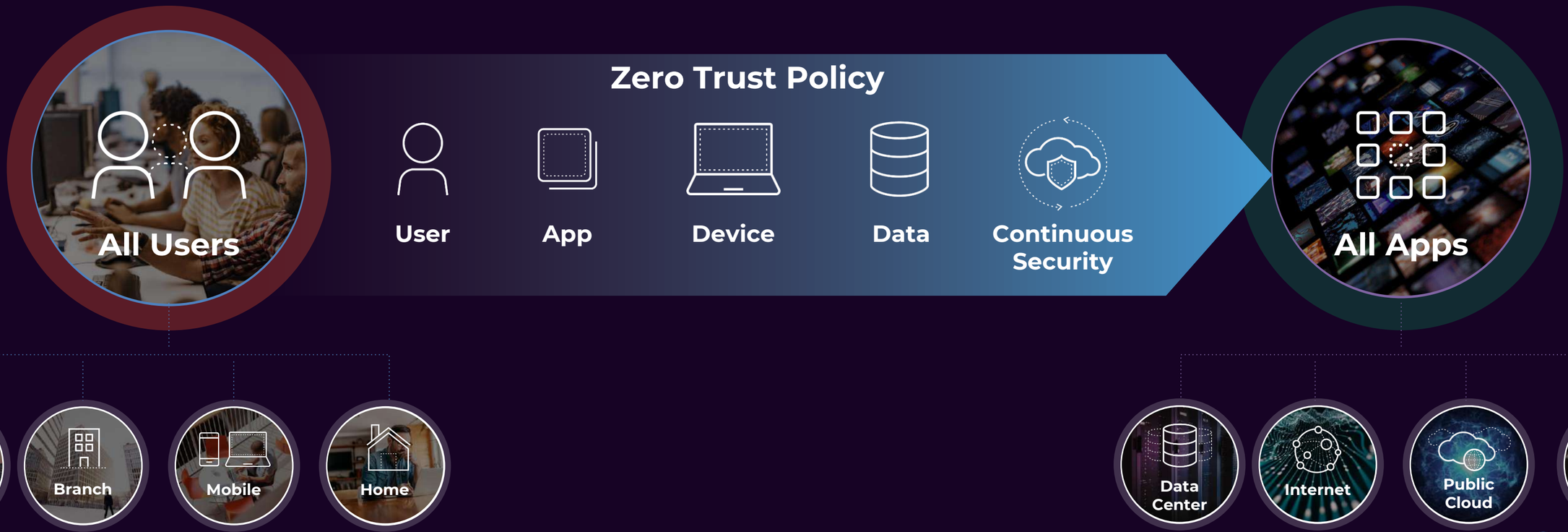
FORRESTER®

Zero Trust concept

Conceptually, Zero Trust Is Very Simple



But Zero Trust Must Apply to the Entire Enterprise



Enterprise Zero Trust Is Impossible with Point Products

Hardware Security Stack

Software Security Stack

SASE Security Stack

All Users

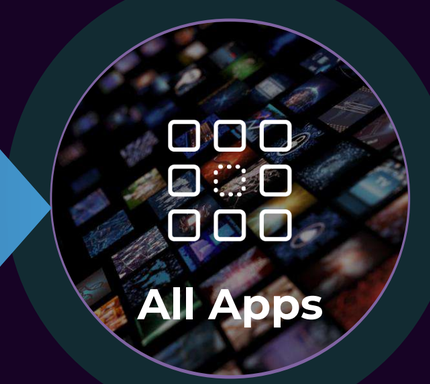
User

App

Device

Data

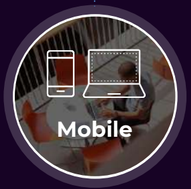
Continuous Security



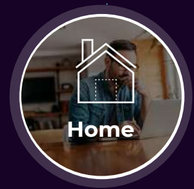
All Apps

Campus

Branch



Mobile

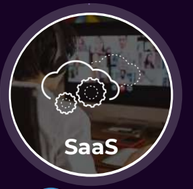


Home

Data Center

Internet

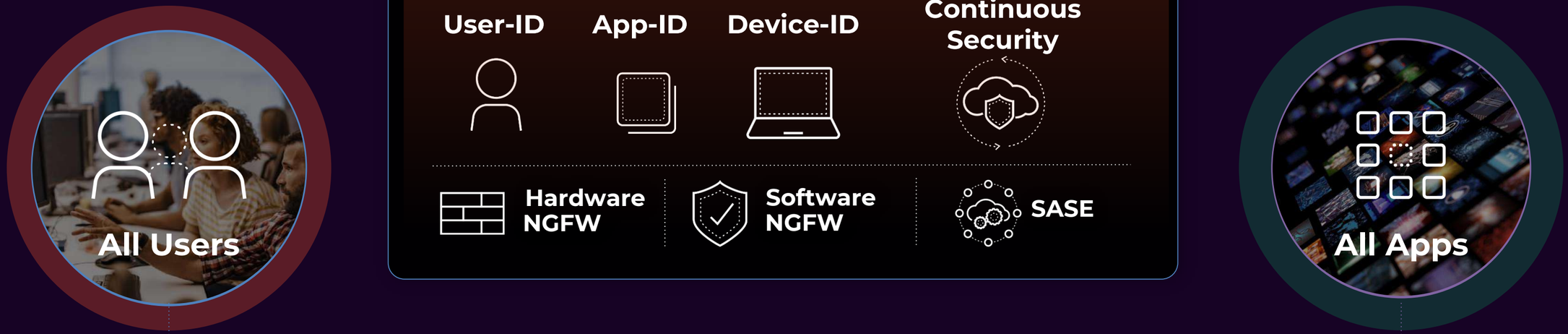
Public Cloud



SaaS

NetOne TECHNOLOGY

Enterprise Zero Trust Is Only Possible With A Platform



NetOne TECHNOLOGY

Best of Breed ~~or~~ and Platform Approach

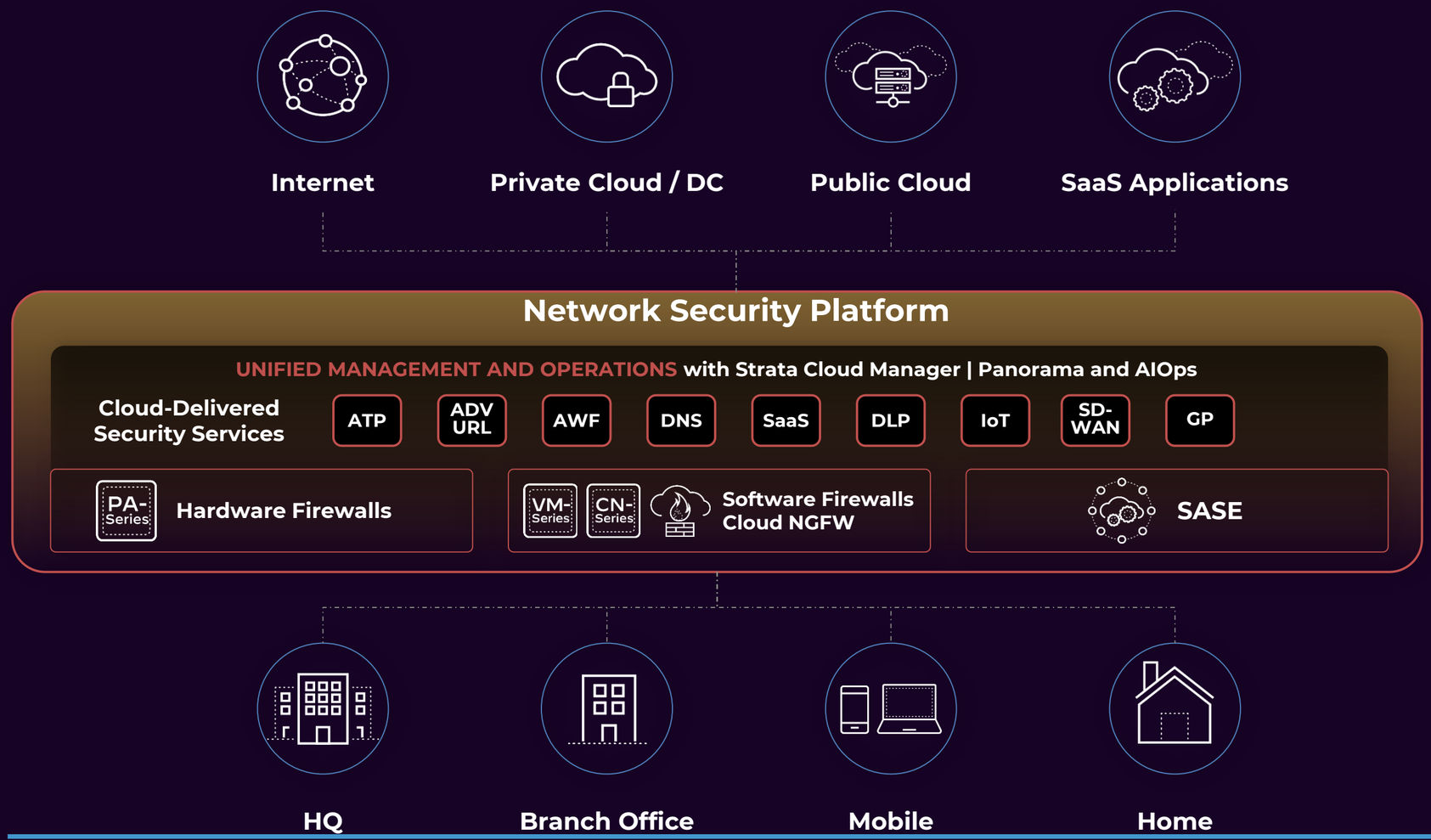
It’s not just our view...

77%

Of security executives think it is critical to reduce the number of security solutions and services they use

Source: Palo Alto Networks *What’s Next in Cyber* survey

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



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

NetOne TECHNOLOGY

Never Trust, Always Verify

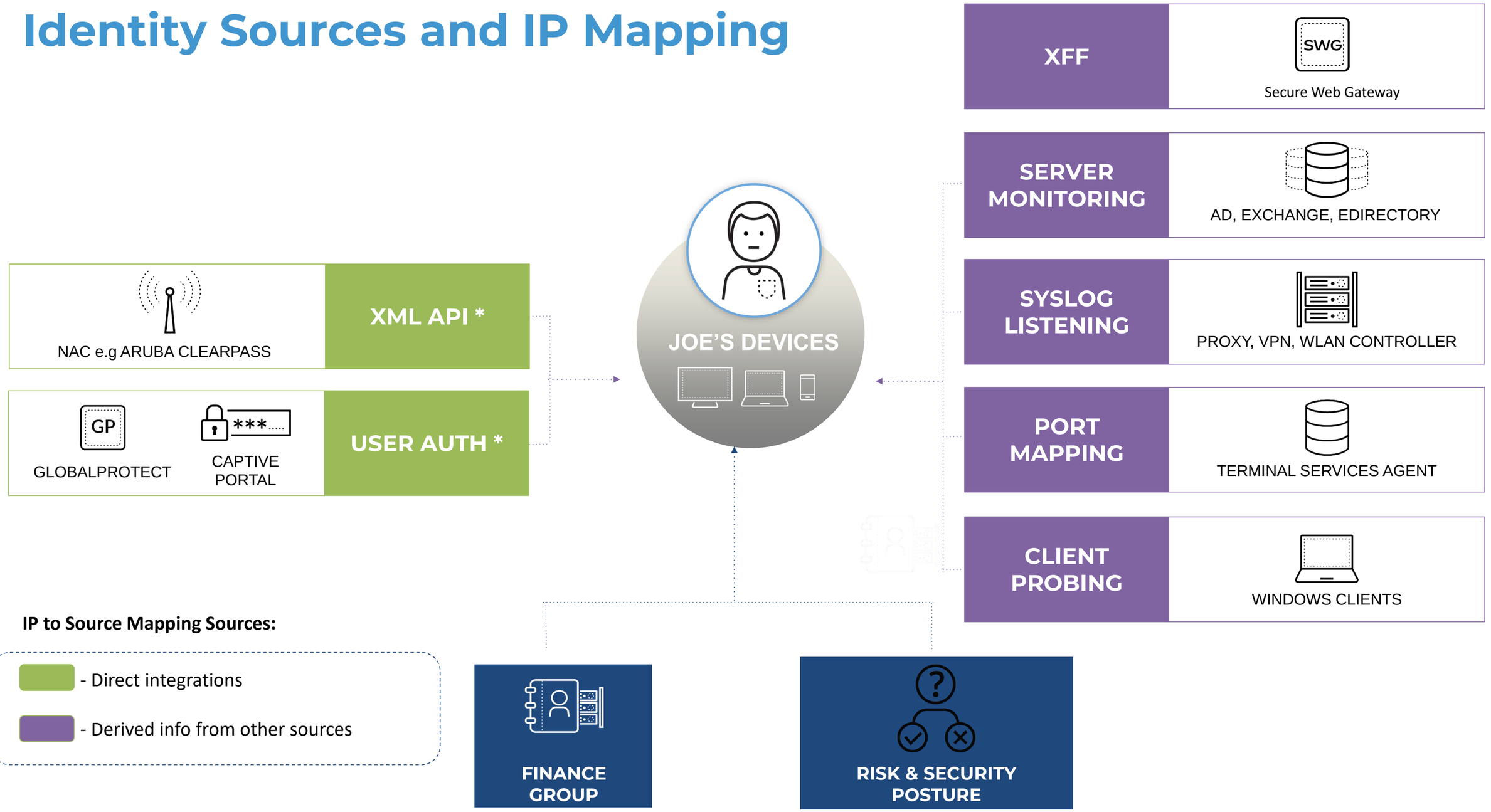
- Using strong authentication methods
- Leveraging network segmentation
- Preventing lateral movement
- Simplifying granular “least access” policies
- Providing Layer 7 Threat Prevention

NetOO TECHNOLOGY

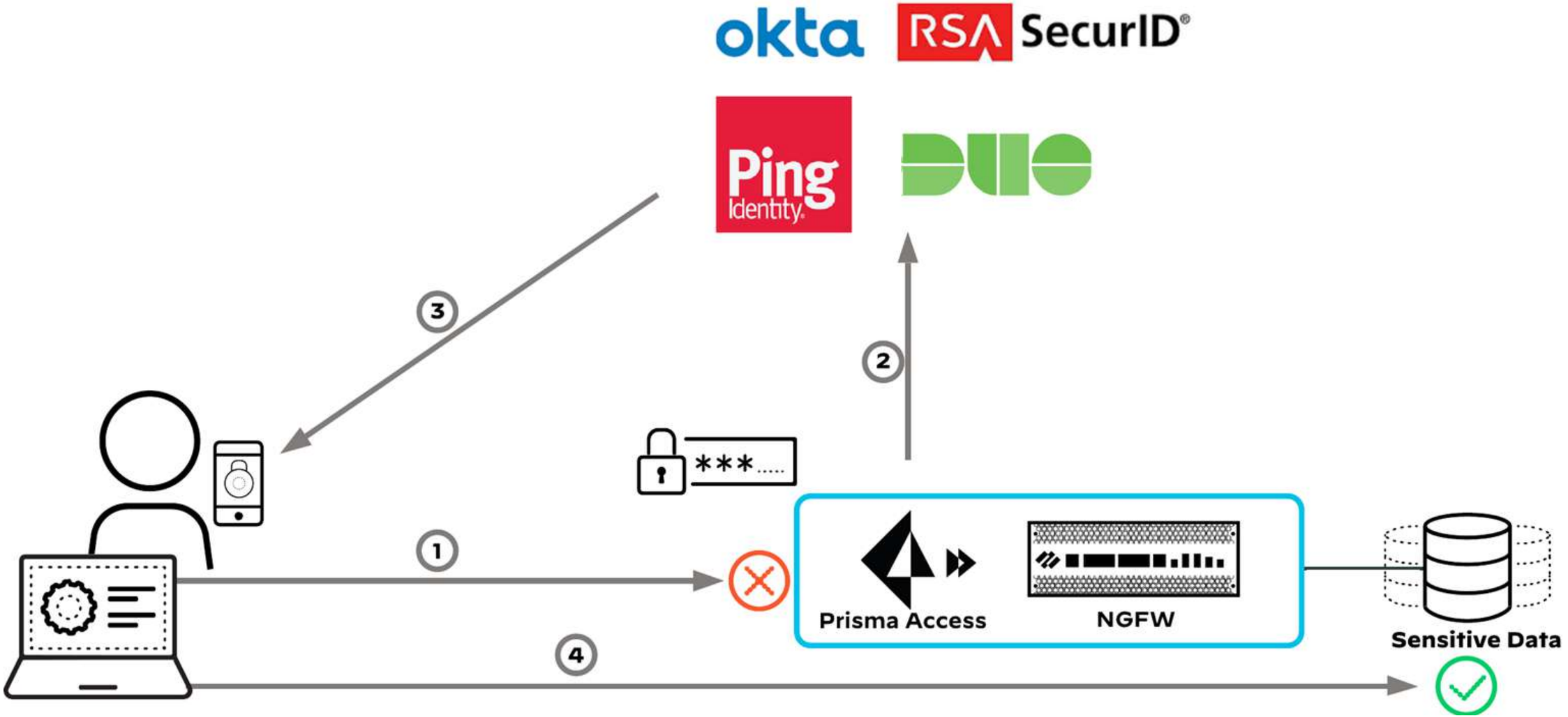
Using strong authentication methods

- Using strong authentication to verify user identity.
- Allow or block access to data and applications
- Multifactor authentication (MFA)
- Define policy rules on NGFWs
- Using IP address assignments to define static policies
- High-fidelity sources

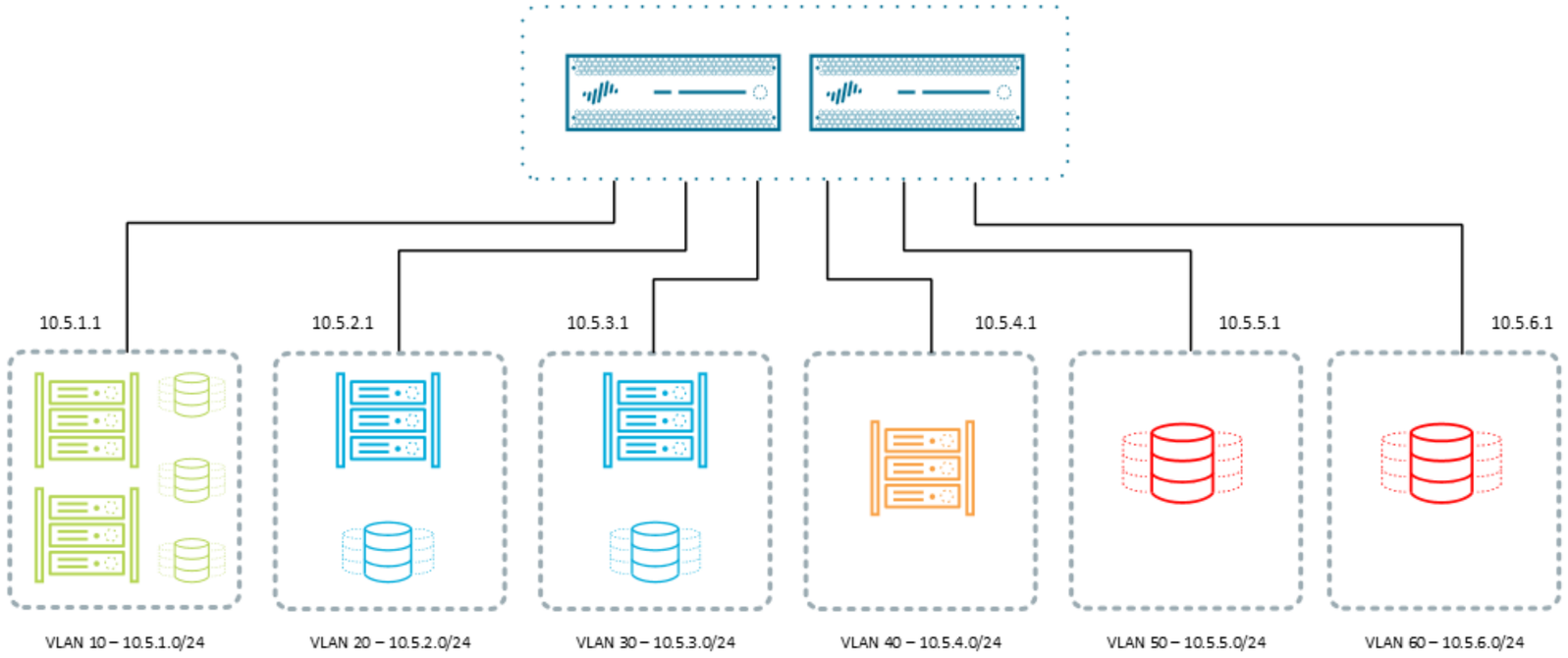
Identity Sources and IP Mapping



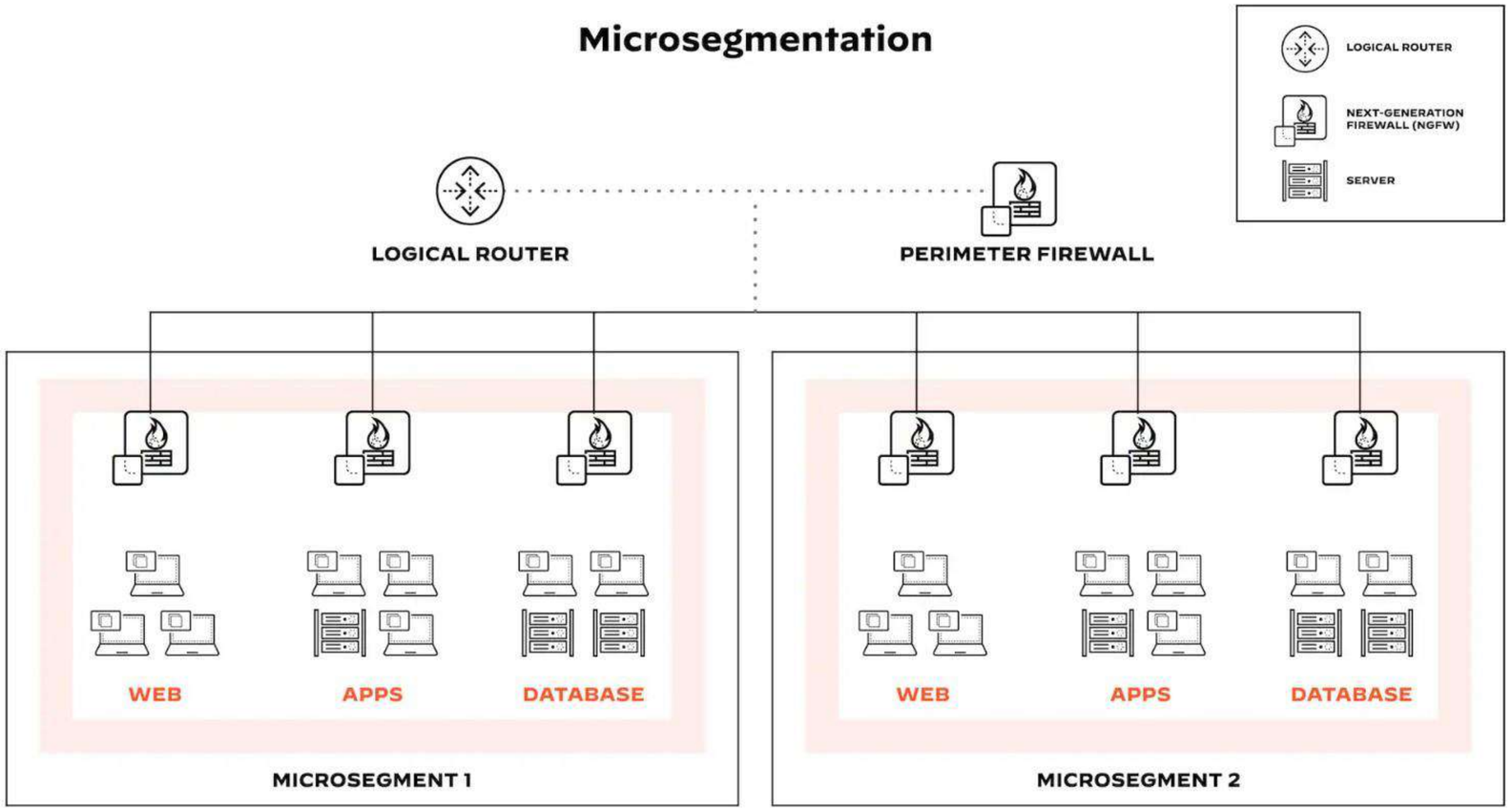
Multi-Factor Authentication



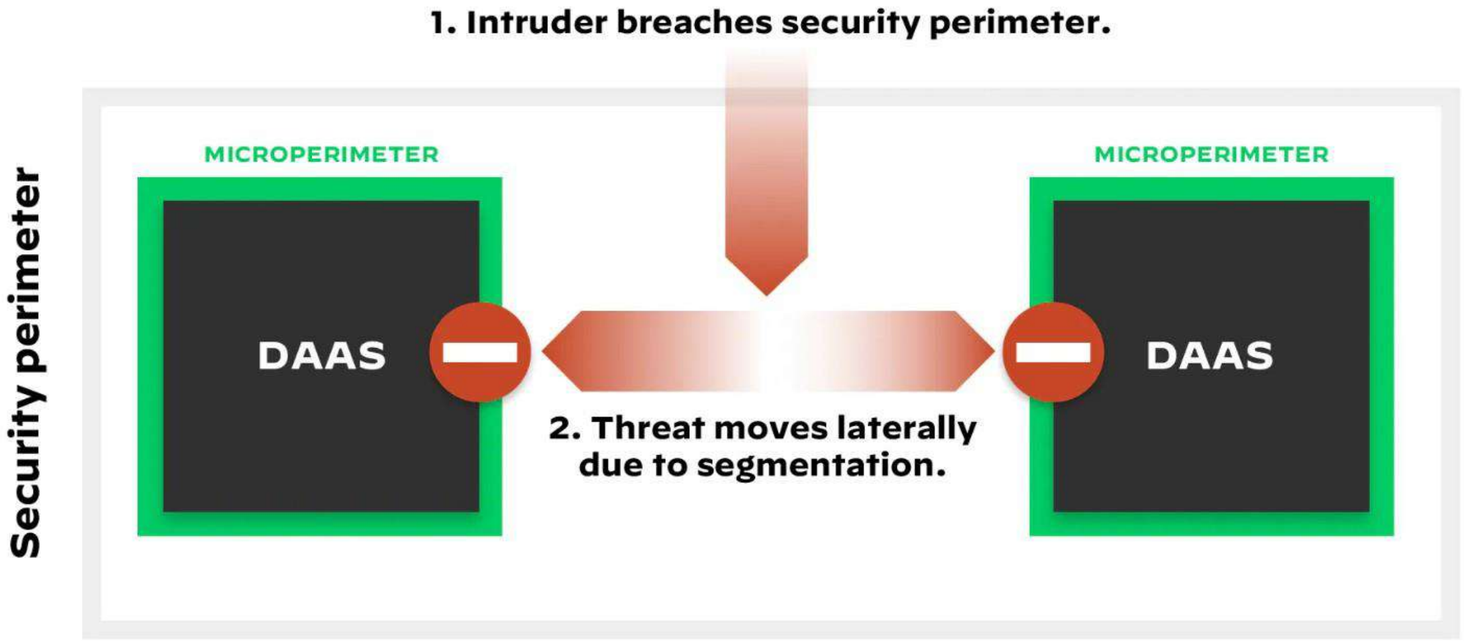
Network segmentation



Microsegmentation



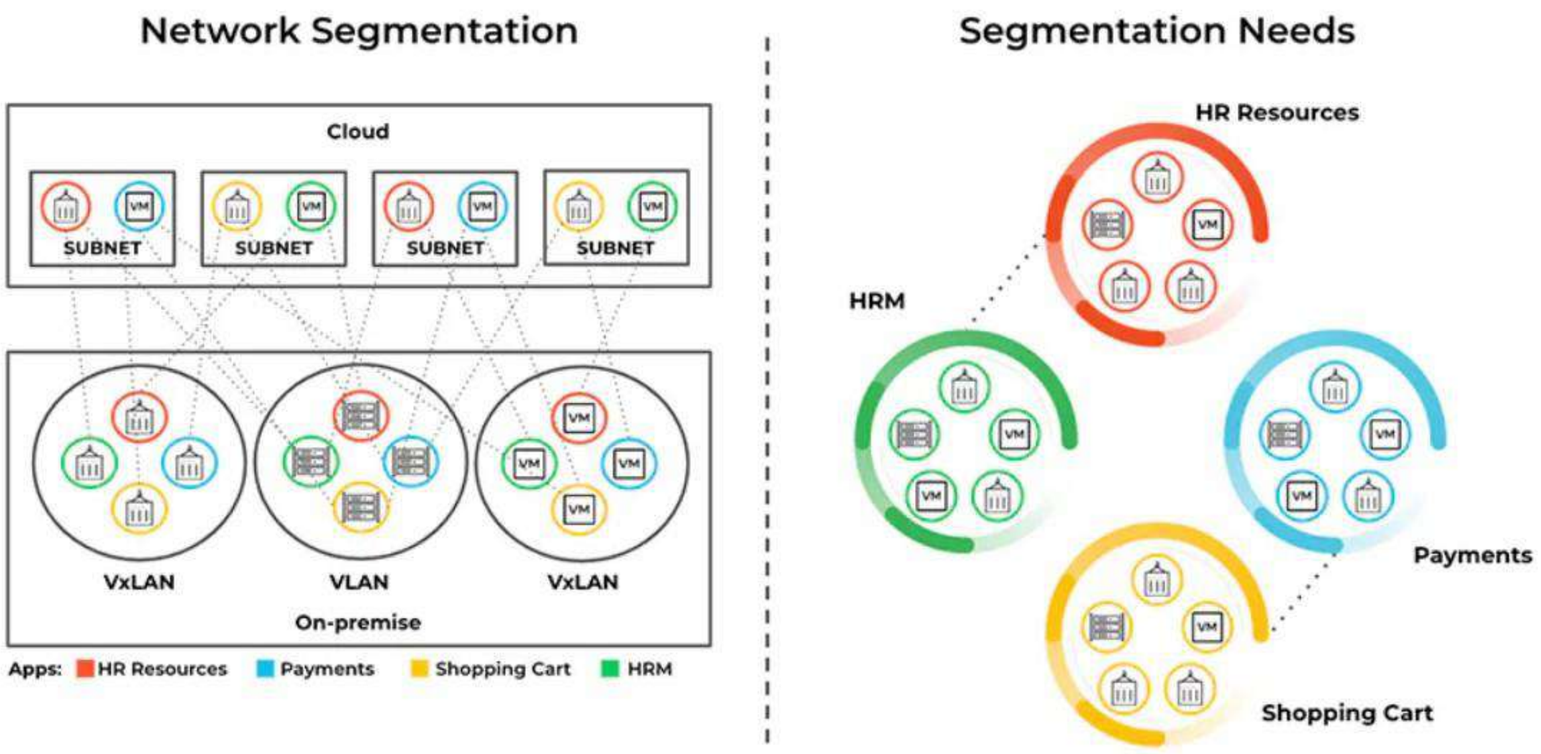
Microsegmentation stopping Lateral movement



Principle of Least Privilege (POLP)

- The principle of least privilege (PoLP) is an information security concept which maintains that a user or entity should only have access to the specific data, resources and applications needed to complete a required task
- The principle of least privilege is also a fundamental pillar of zero trust network access
- The principle of least privilege works by limiting the accessible data, resources, applications and application functions to only that which a user or entity requires to execute their specific task or workflow.
- Least privilege access is sometimes also referred to as minimum privilege access or least authority access.

Principle of Least Privilege (POLP)

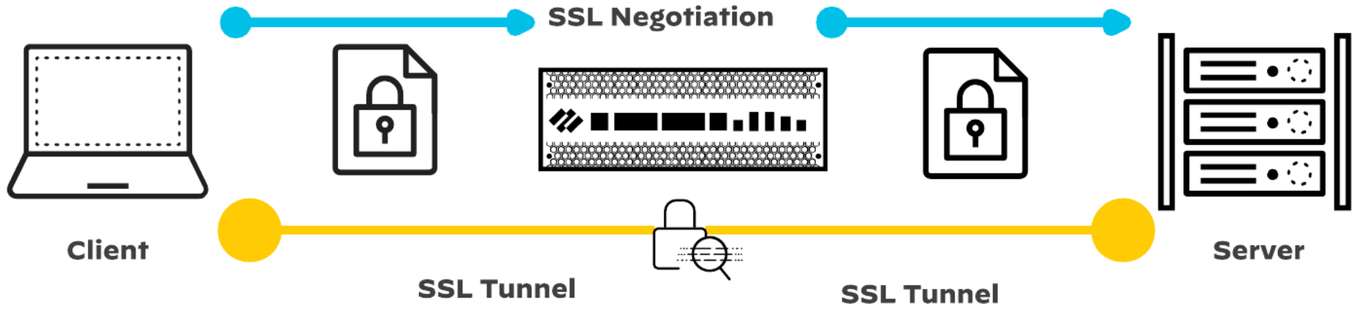


Benefits of the Principle of Least Privilege

- **Minimizes the attack surface**
- **Reduces malware propagation**
- **Improves operational performance**
- **Safeguards against human error**

Visibility into Encrypted Traffic

- To have granular visibility and control for the application, the NGFW must decrypt the traffic.
- Decryption is also required for security services in order to detect threats in encrypted traffic.
- NGFW and Prisma Access can decrypt and inspect both inbound and outbound SSL/Transport Layer Security (TLS) connections traversing the firewall.
- A decryption policy rule allows you to define traffic that you want the firewall to decrypt and to define traffic that is excluded from decryption.



Advanced Threats Require Advanced Network Security

Today's unknown and evasive attacks require deep analysis ...

Advanced deep learning techniques

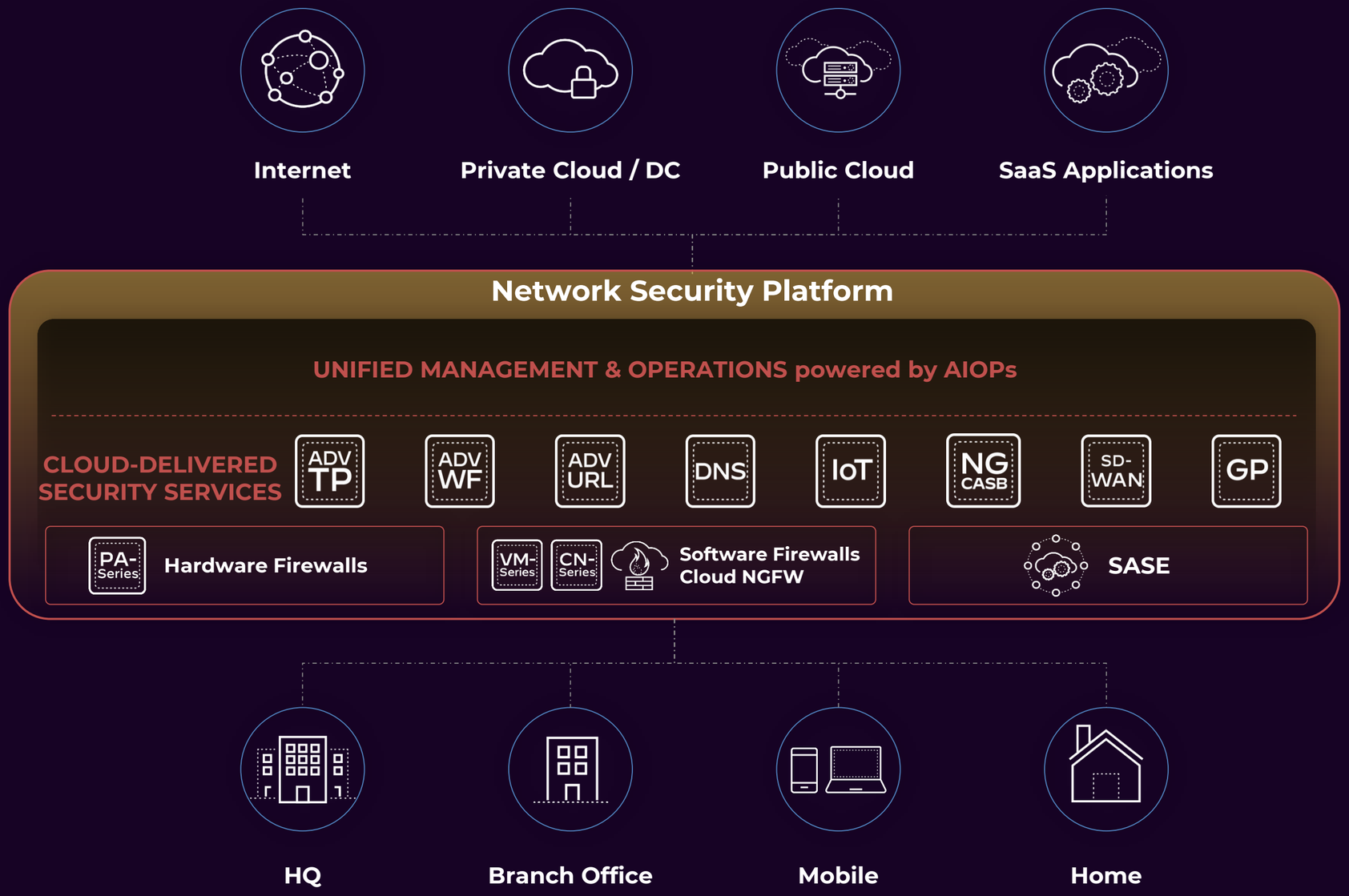
Inspection of real live traffic

... and protections must be real-time to prevent attacks

Cloud-scale ML & Crowdsourced Intel

At wire-speed, everywhere

BEST-IN-CLASS NETWORK SECURITY PLATFORM POWERED BY A BEST-IN-CLASS SECURITY ENGINE



ACHIEVE TRUE ZERO TRUST

5 BILLION
Events blocked per day with AI/ML-powered prevention of evasive threats in real time

30%
Higher performance than the next leading vendor

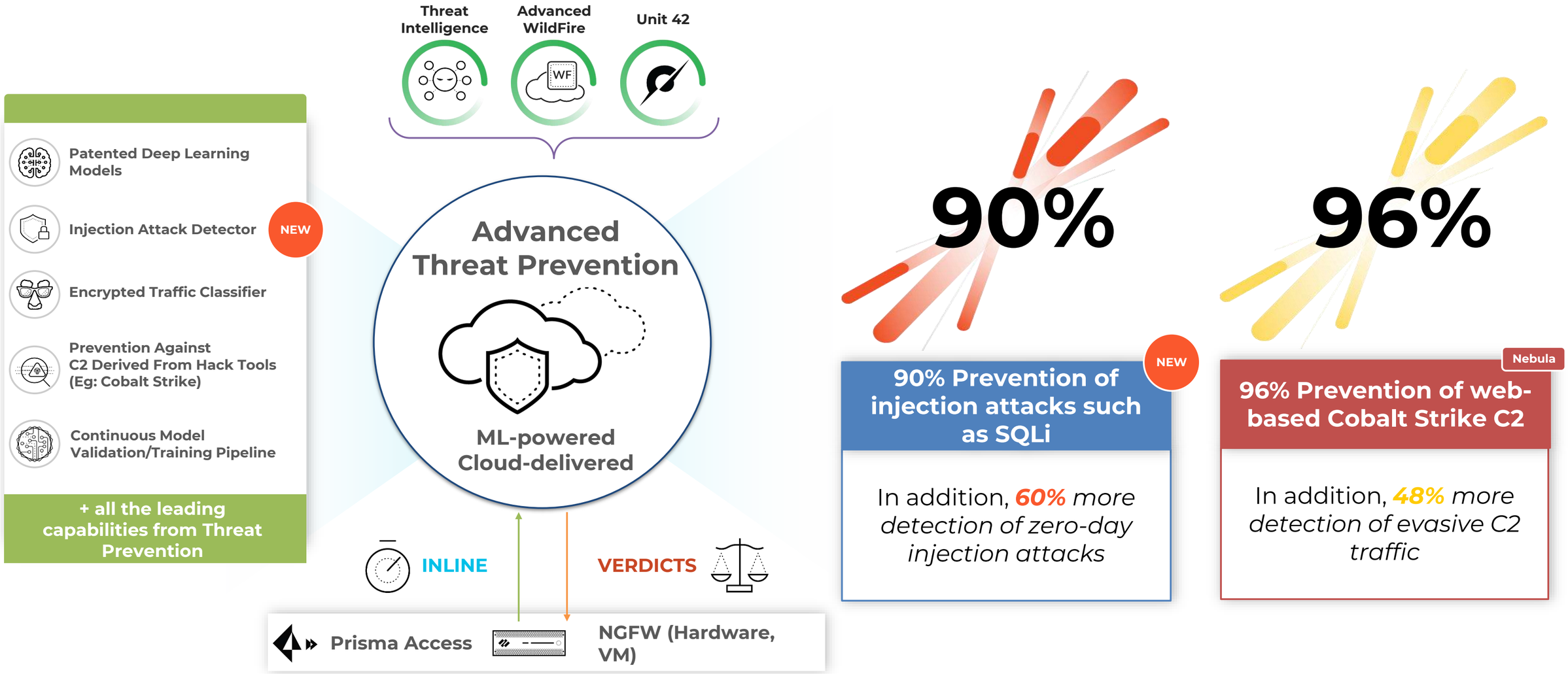
45%
Reduction of risk of a breach thanks to consistent policies

<6 MONTHS
See payback in less than 6 months

Net++ TECHNOLOGY

Reimagine IPS with Advanced Threat Prevention

Stop Zero-Day Attacks Inline



Details of Each Detection Methodology

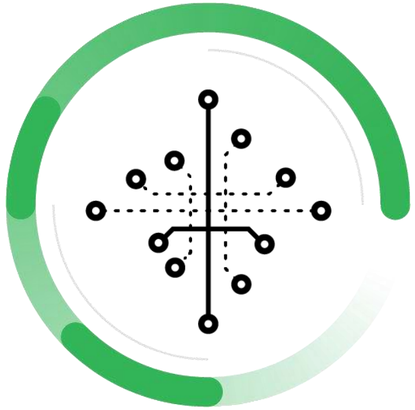
Signatures

Matching a set of **predetermined attributes**

Best for finding **known** malicious activity

Manual update is required to ensure the most up to date protection

Machine Learning



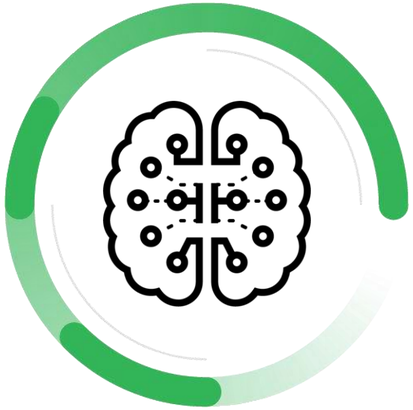
Examining large data sets to **find common features** and expose anomalies

Leverages **thousands** of data points

Best for finding **variants of known** malicious activity

Requires **human intervention** to manage and maintain

Deep Learning



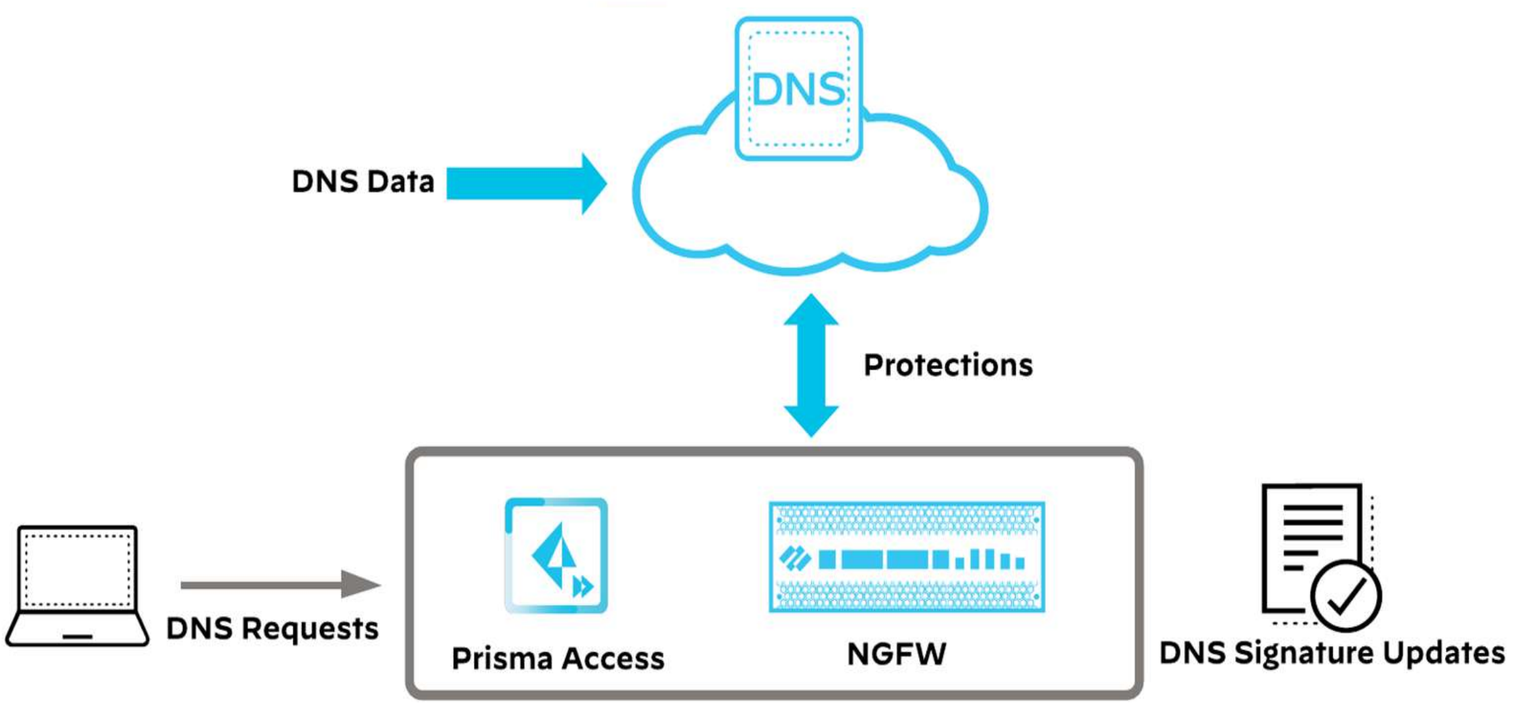
Uses an **artificial neural network** to pass data through several layers to interpret data features and relations

Leverages **millions** of data points

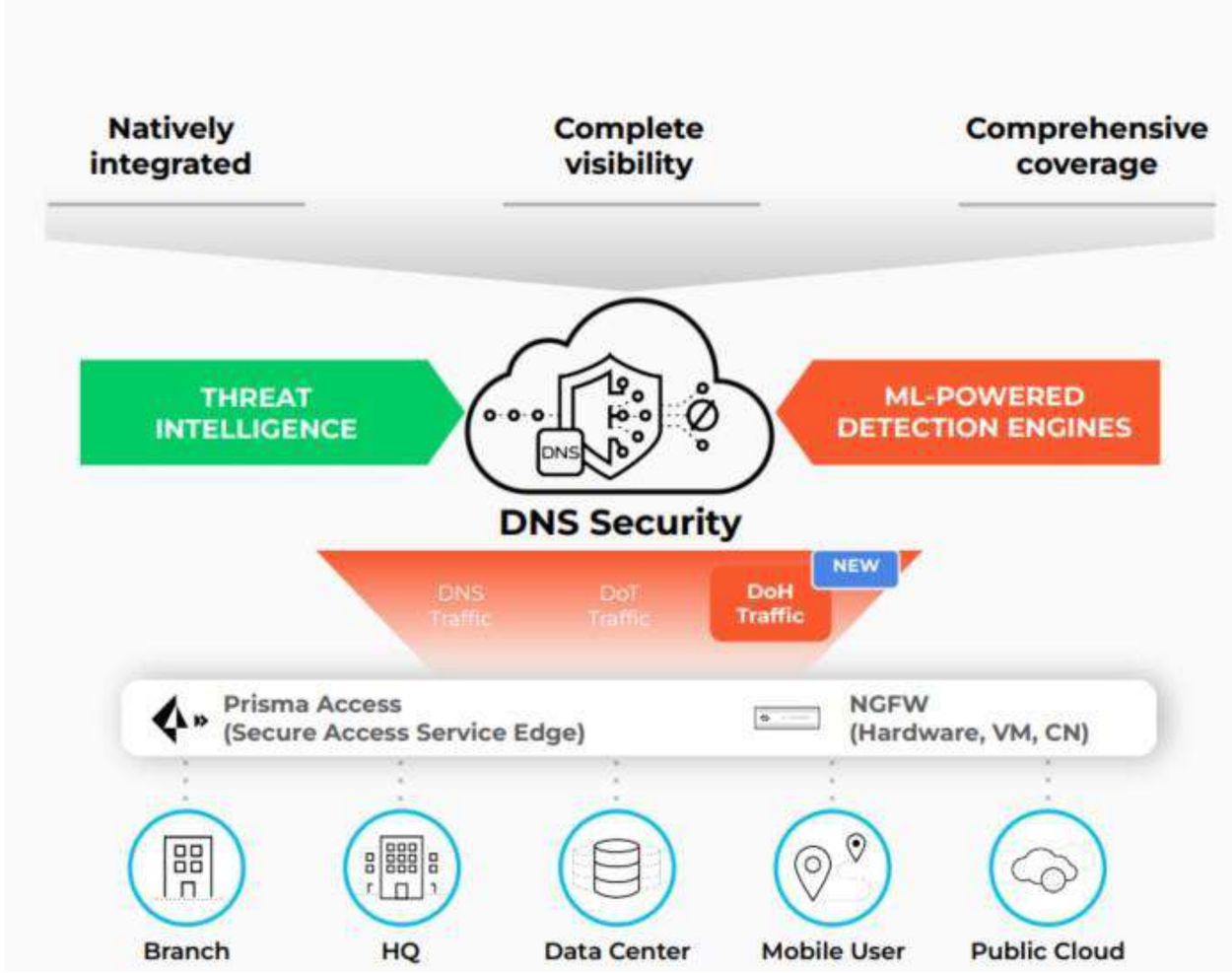
Best for finding **new/unknown** malicious activity

Algorithms **maintain themselves**

DNS is a critical point in most attacks



DNS Security: The Industry's Most Comprehensive Solution Against DNS-Layer Threats



40%

More threat coverage than any other vendor

ML-powered Industry-first detections

6X

Faster detection and prevention

Powered by Inline Deep Learning

- **ML-Powered Industry first detections**
- **Real-time protection against DNS-layer threats**
- **Infinitely scalable cloud-delivered**

NetOne TECHNOLOGY

Modern phishing attacks are highly evasive, making detection more difficult than ever

New, never-before-seen phishing URLs

Single-use and short-lived links

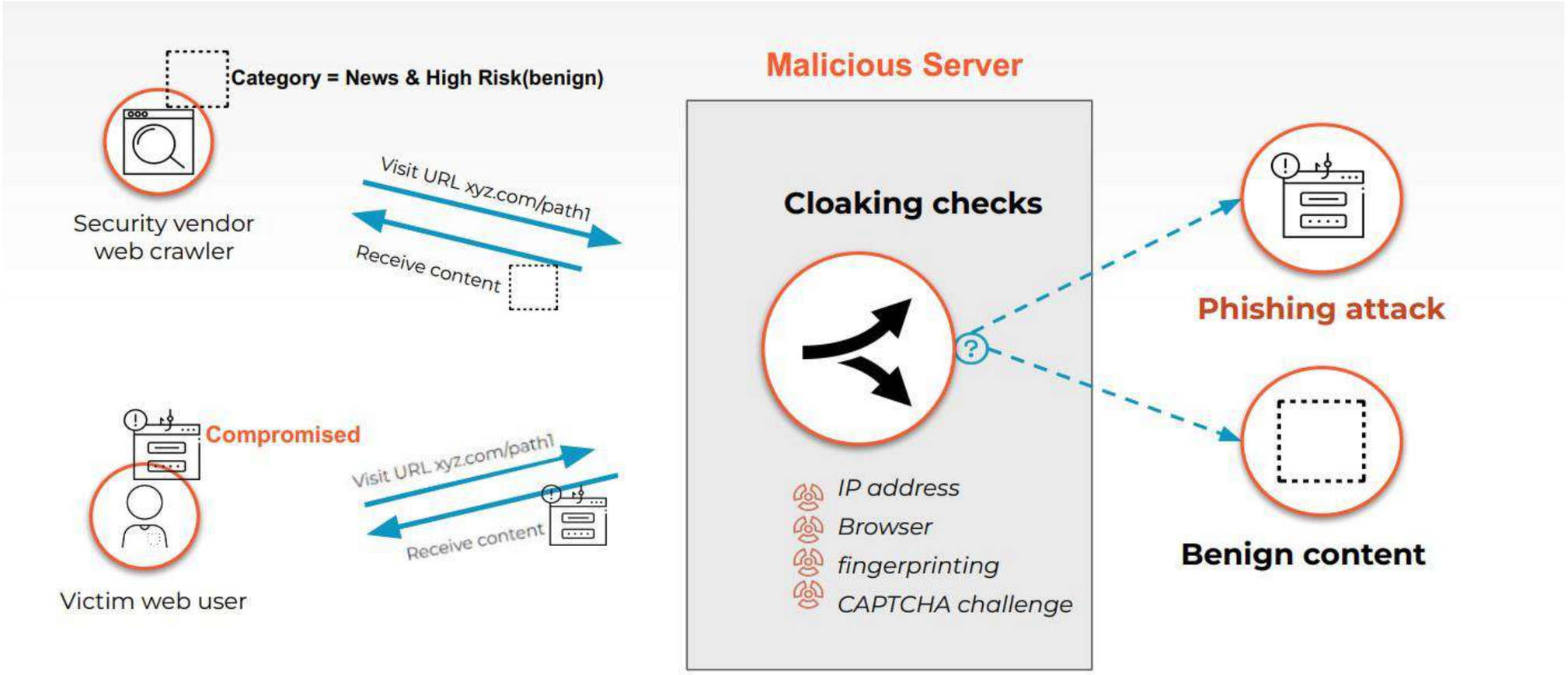
Hiding malicious content through cloaking

Attacks hiding within compromised websites

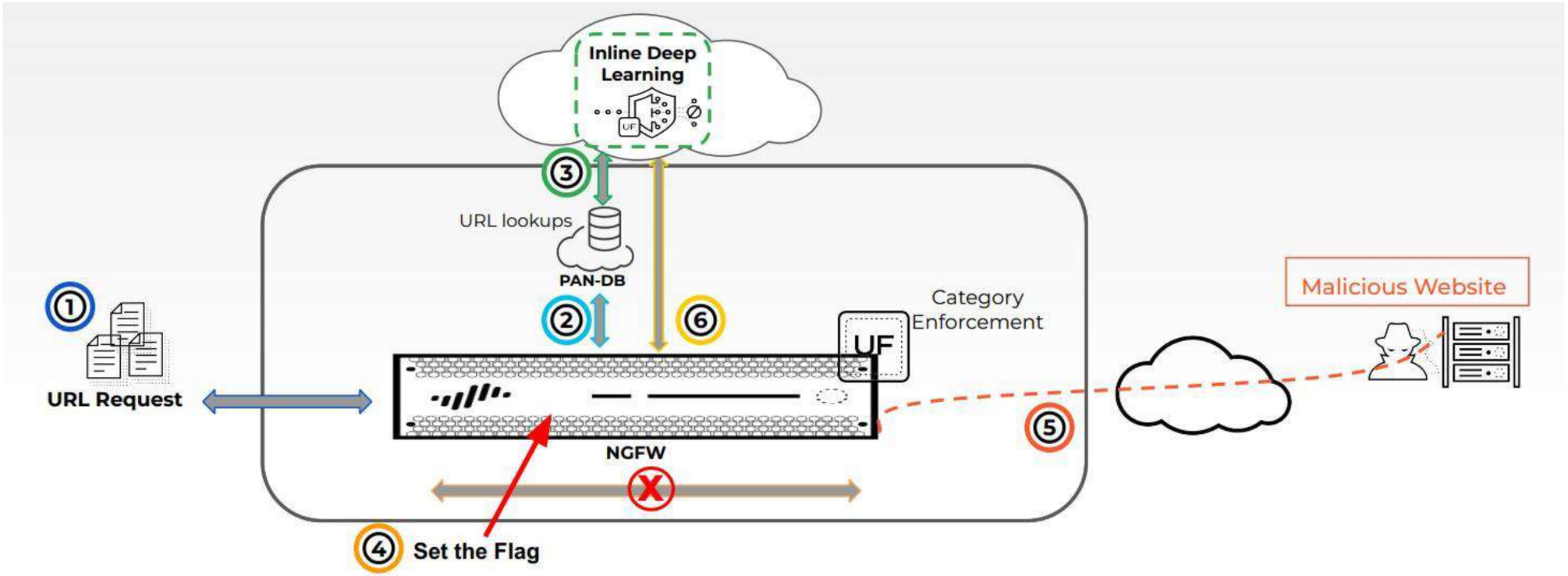
Multi-step attacks and CAPTCHA challenges

Modern attackers are innovating faster than traditional web security vendors to get through defenses and attack customers

Protection against Highly Evasive & Targeted Phishing attack



Protection against Highly Evasive & Targeted Phishing attack



① URL Request is made for a **xyz.com/path1/path2**

② URL Filtering checks PAN-DB and the site category is **high-risk & business-and-economy**

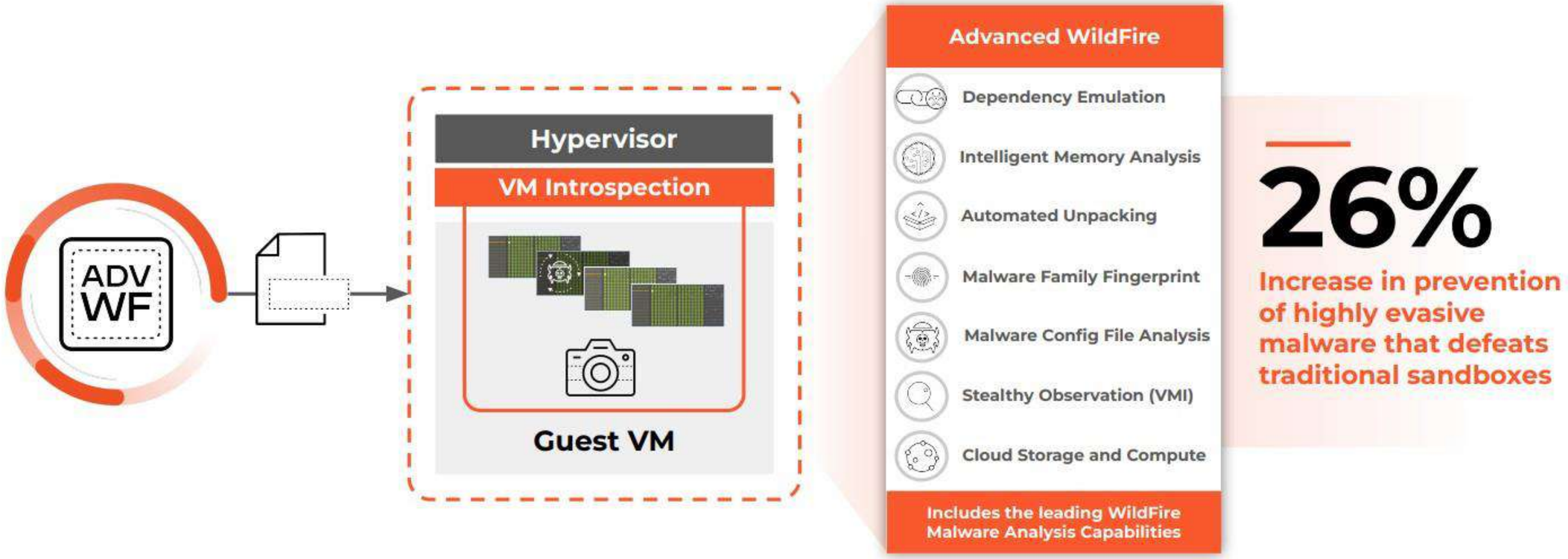
③ PAN-DB checks cloud based- inline security engine **for url detection in real-time**

④ Blocked the URL if Identified malicious otherwise Set the flag for content analysis

⑤ Send the request & receive the response from the server

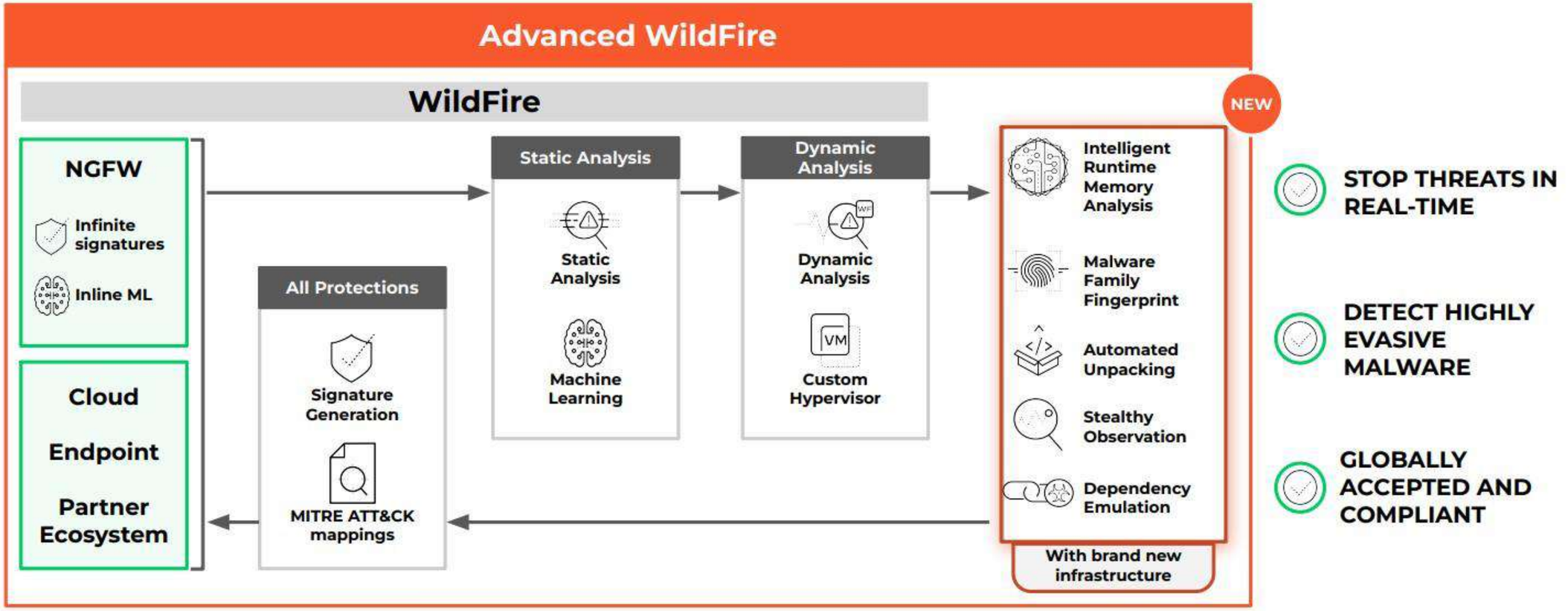
⑥ Forward the web-content for real-time analysis and blocked the request if identified malicious

NEW ADVANCED WILDFIRE:
Industry's Largest Malware Prevention Engine



Stopping Highly Evasive Threats With Speed And Scale

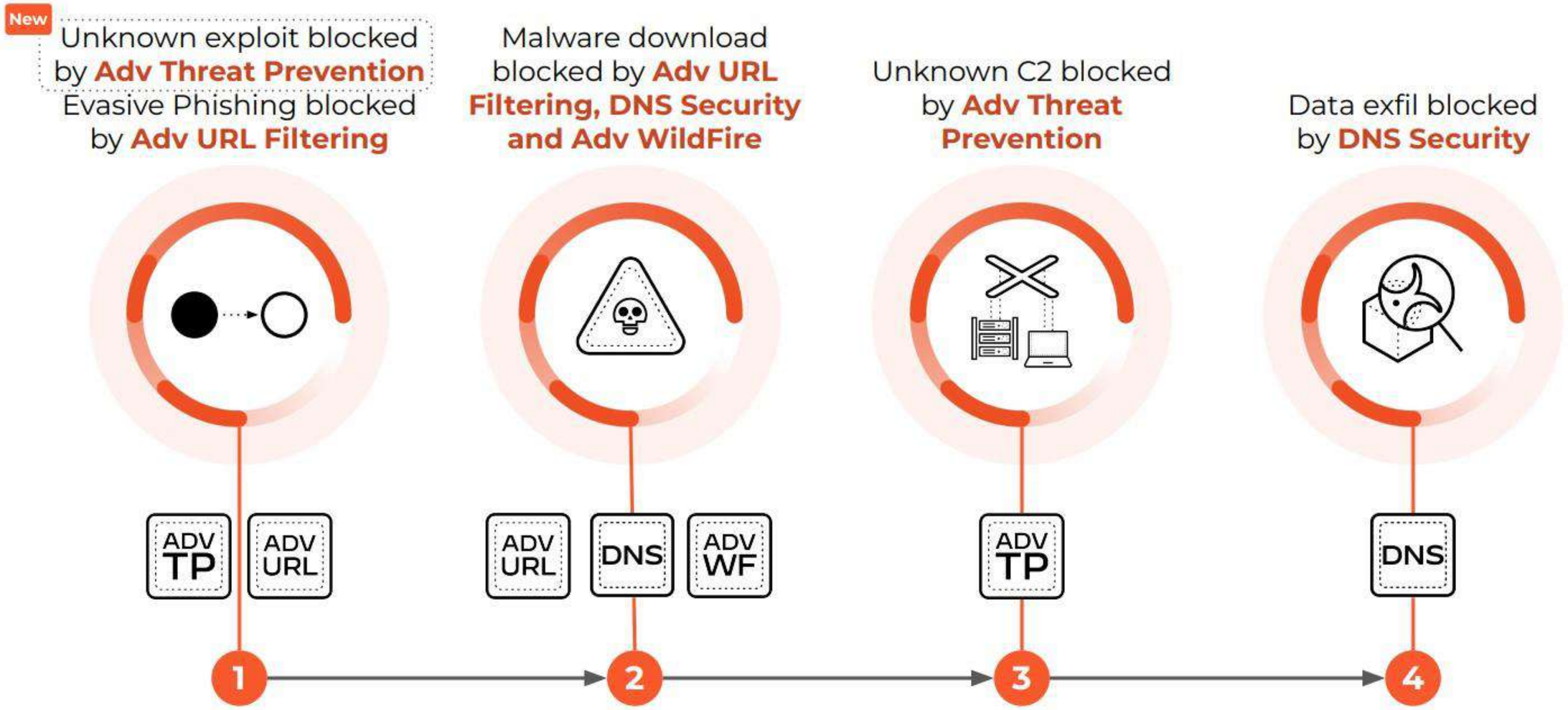
NEW ADVANCED WILDFIRE:
Industry's Largest Malware Prevention Engine



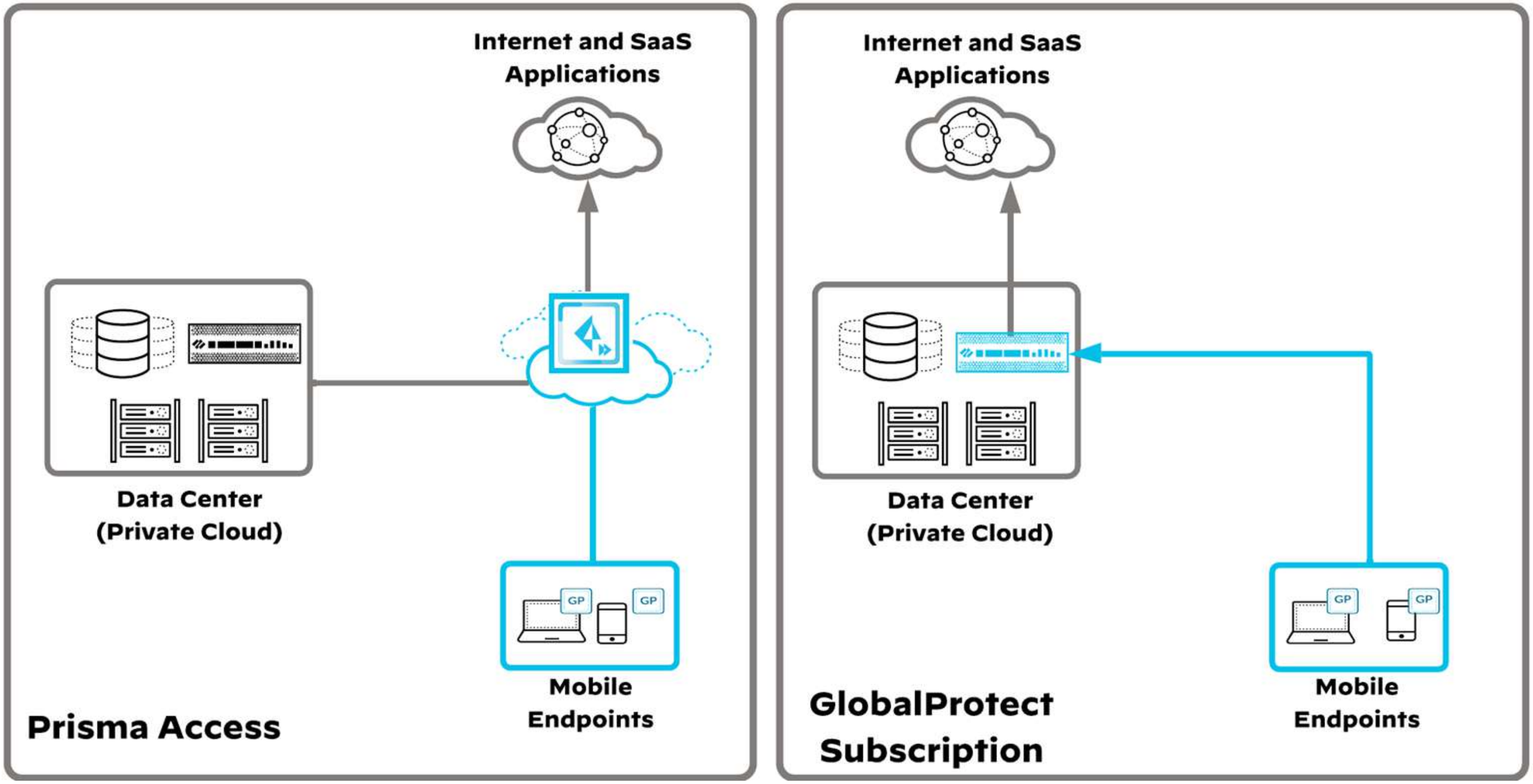
Stopping Highly Evasive Threats With Speed And Scale

NetOne TECHNOLOGY

Defense in Depth across the Attack Lifecycle



GlobalProtect



Palo Alto NGFW key features

- **NextGen Firewall with Machine Learning inside OS**
- Extensive use of inline Deep Learning
- Automated response when malicious traffic from a host or a user is recognized
- Policy Optimizer tool inside PanOS for optimizing security policies

- **Based on four Engines: App-ID, Content-ID, User-ID, Device-ID**
- IoT security
- **Wildfire is the biggest Sandbox in the world**
- Implicit communication with Palo Alto Cortex XDR through Wildfire

- The same GUI on any form factor platform, hardware, virtual, container
- Flex approach in buying VM and CN firewalls through credits
- Management from one GUI console – Panorama
- **Palo Alto embrace Zero Trust Security**

- **Over 800 implemented firewalls in the region in over 300 companies**
- Local vendor support and training center

NetPlus TECHNOLOGY

NetOO TECHNOLOGY

HVALA NA PAŽNJI

+381 11 36999 967
www.netpp.rs
Otokara Keršovanija 11/39, Beograd