



SHIELD vzw

The changing landscape of cybersecurity and the countermeasures within the Palo alto networks portfolio

by Tomas Van Beek & Jo Vander Schueren



Cybersecurity

Networking

Cloud

Managed services

About us

Who are we?

+30 passionate trusted advisors in Cybersecurity, networking and managed services.

What do we solve?

Problem of insufficient resources & knowledge in Cybersecurity & Networking.

What is our vision?

Intelligent use of AI/ML technology & automation can reduce workloads & optimize resources.

Where are we active?

- Belgium with offices in Ghent & Antwerp
- Netherlands with offices in Amsterdam

Who are our customers?

Public and private midsize organizations in the Benelux with extensive experience in healthcare.

Build resilience to manage incidents and avoid breaches

Cybersecurity

Implementing 3 layers of defense to answer OT & IT cybersecurity challenges

Networking

Building self-managed & end-user driven networks to create optimal experiences.

Cloud Security

Extending your security posture in the cloud for applications & infrastructure.



Managed Services

JUNIPER
NETWORKS

SentinelOne

VECTRA

infoblox

AVANAN
A Check Point Company

paloalto
NETWORKS

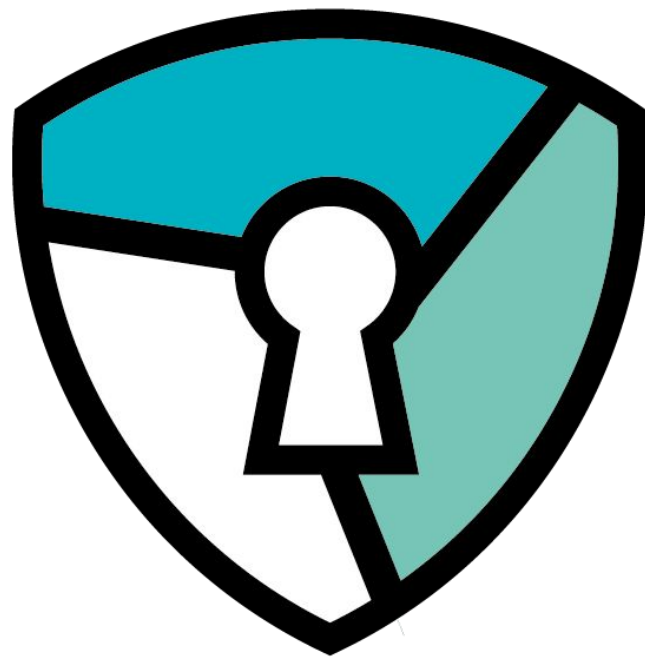
SILVERFORT

ATTACKIQ

ARMIS

f5

Blyott



SHIELD vzw

Framework agreement for
NEXTGEN/NETWORK FIREWALLS



JARVISS®
When Your OT & IT Security Get Personal



paloalto®
NETWORKS

Scope

1. Nextgen firewall platform based on Palo Alto Networks

- I. **Flexible platform:** branch, datacenter, segmentation, cloud, ...
- II. **Cloud delivered security services:** URL security, DNS security, Threat prevention, Saas, DLP, IOT, SDWAN, ...
- III. **Central (cloud) management**

2. Consultancy services

- I. Design & architecture
- II. Implementation & onboarding
- III. Security Control Baseline Testing (SCBT)
- IV. Certification training
- V. Project management

3. Support & managed services

- i. Basic
- ii. Advanced
- iii. Managed



Support services for NGFW

1. Basic

- I. Builds upon the vendor support
- II. Includes a pay as you go 8x5 Jarvis helpdesk
- III. Only recommended if extensive Palo Alto Networks knowledge is present

2. Advanced

- I. Direct Jarvis support with fix price
- II. Different SLA's possible (NBD, 8x5, 24x7)
- III. Different scope's possible (support, best practice checks, changes, ...)

3. Managed


- I. Full managed by Jarvis in a fix price model
- II. Jarvis takes full responsibility
- III. Different SLA's possible (NBD, 8x5, 24x7)

Get in touch!

 <https://www.shield-vzw.be>

 <https://www.jarviss.be>

 info@jarviss.be

 +32 (0)9 394 99 11

 <https://www.linkedin.com/company/jarviss/>



LOOKING FORWARD TO MEET YOU!

The threat landscape is intensifying

Elevated attacker motivation

\$8T cost of cybercrime ¹

Integral part of modern warfare

Nation-state economic gain

Tech is enabling attacks at scale

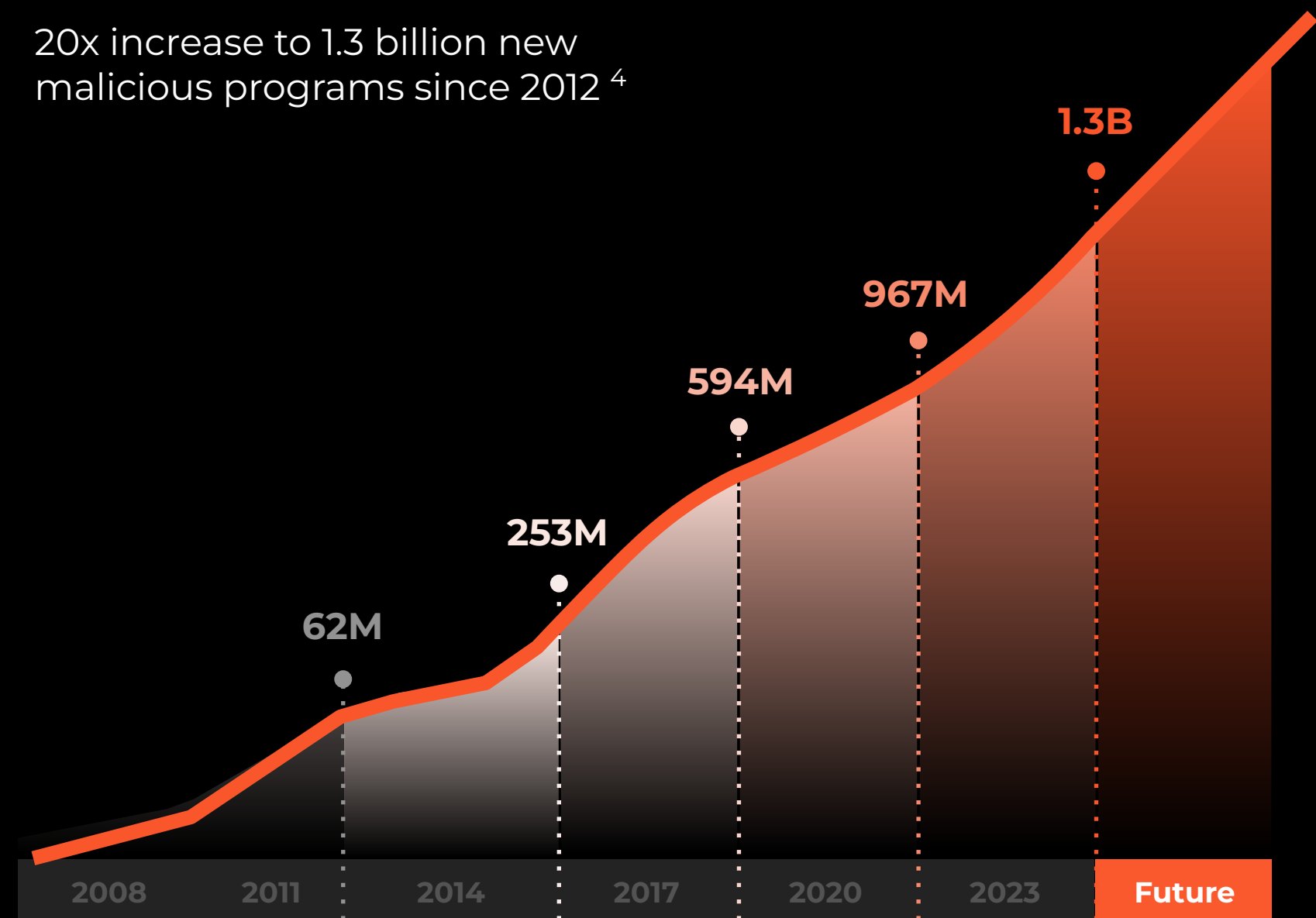
Automated attacks executed across regions within 1 hour of initial compromise ²

>10 million people and >1,700 organizations affected by supply chain attacks in 2022 ³

Near-instant “trickle down” of attack techniques

Organizations are heavily impacted... and it's getting worse

20x increase to 1.3 billion new malicious programs since 2012 ⁴



Sources:

¹ <https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/>;

² Unit 42 research: <https://unit42.paloaltonetworks.com/purpleurchin-steals-cloud-resources/>;

³ https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf

⁴ <https://portal.av-atlas.org/malware>.

...and “AI” Will Only Speed Up the Attackers



**Accelerated
Attacks**



**Scaled
Attacks**



**Utilizing
New Vectors**



Number of security tools organizations use:



32

Average # of security tools organizations use today
In the Germany it is **84**

56%

Work with 20 or more
Germany **78%**

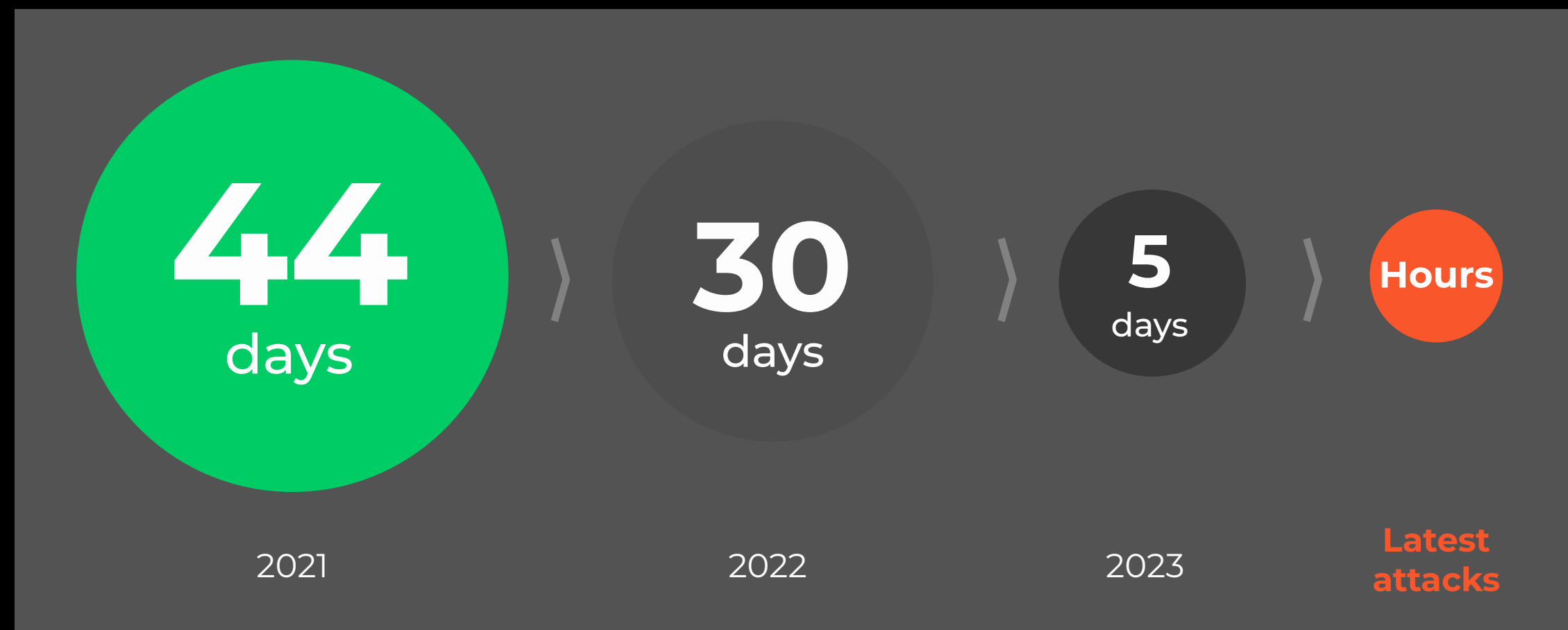
Did you know:

Only 13% of NAM responders use 50 or more tools, compared to **27% of EMEA (32% Netherlands)**

70% of BeNeLux companies work with 10 or more security-vendors, worldwide average is 41%

Attacks are happening faster than organizations can respond

Average Days from “Compromise” to “Exfil”¹



Sources:

¹ Unit 42 Cloud Threat Report - Volume 7, 2023, Unit 42 Engagement Experience;

² Under the new SEC Rules, the occurrence of a cybersecurity incident must be reported within four business days of when the incident is determined to be material by the reporting company.



Industry average

6 DAYS

to remediate

SEC adopted rule

4 DAYS

to disclose material cybersecurity incident²

EU GDPR

72 Hours

to disclose incident to Supervisory Authority

WHAT WE KNOW

Best of Breed ~~and or~~ 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

Only a platform approach will work



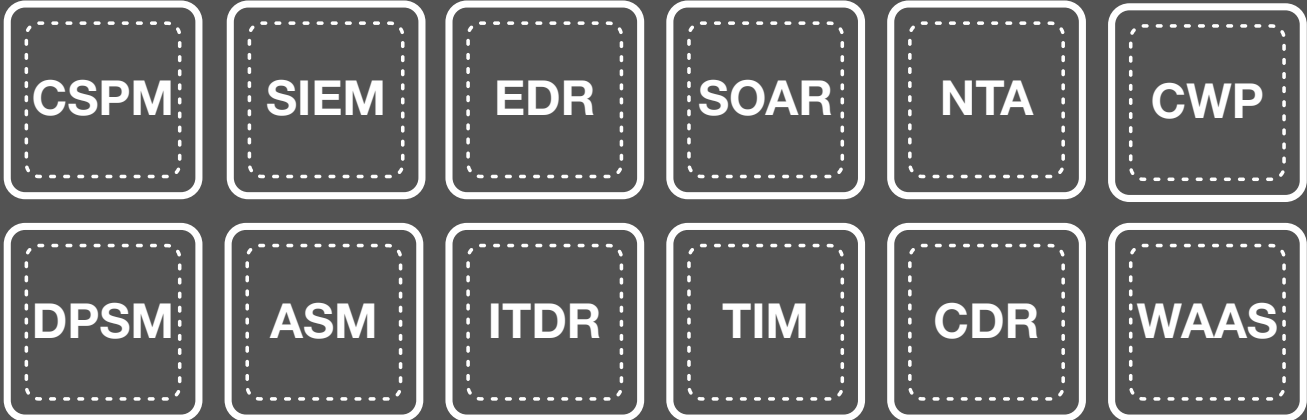
ZERO TRUST PLATFORM

Inspect connections and block attacks with Precision AI



CODE TO CLOUD TO SOC™ / SECOPS PLATFORM

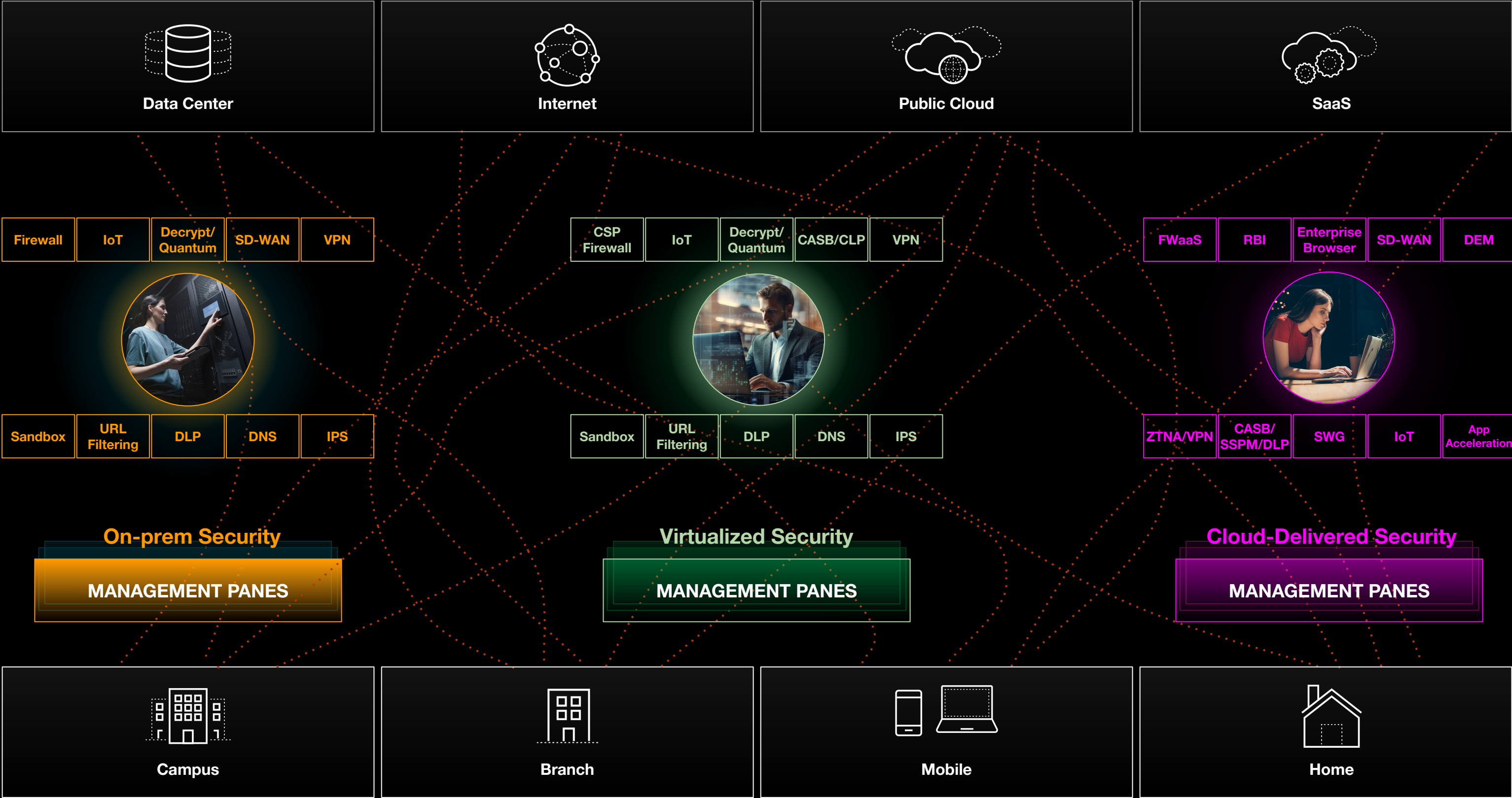
From Dev to Prod: real-time detection, investigation, and remediation with Precision AI




Strata Network Security Platform

Tomas Van Beek | Domain Consultant Manager

Today's network security can be **complex** and **fragmented**



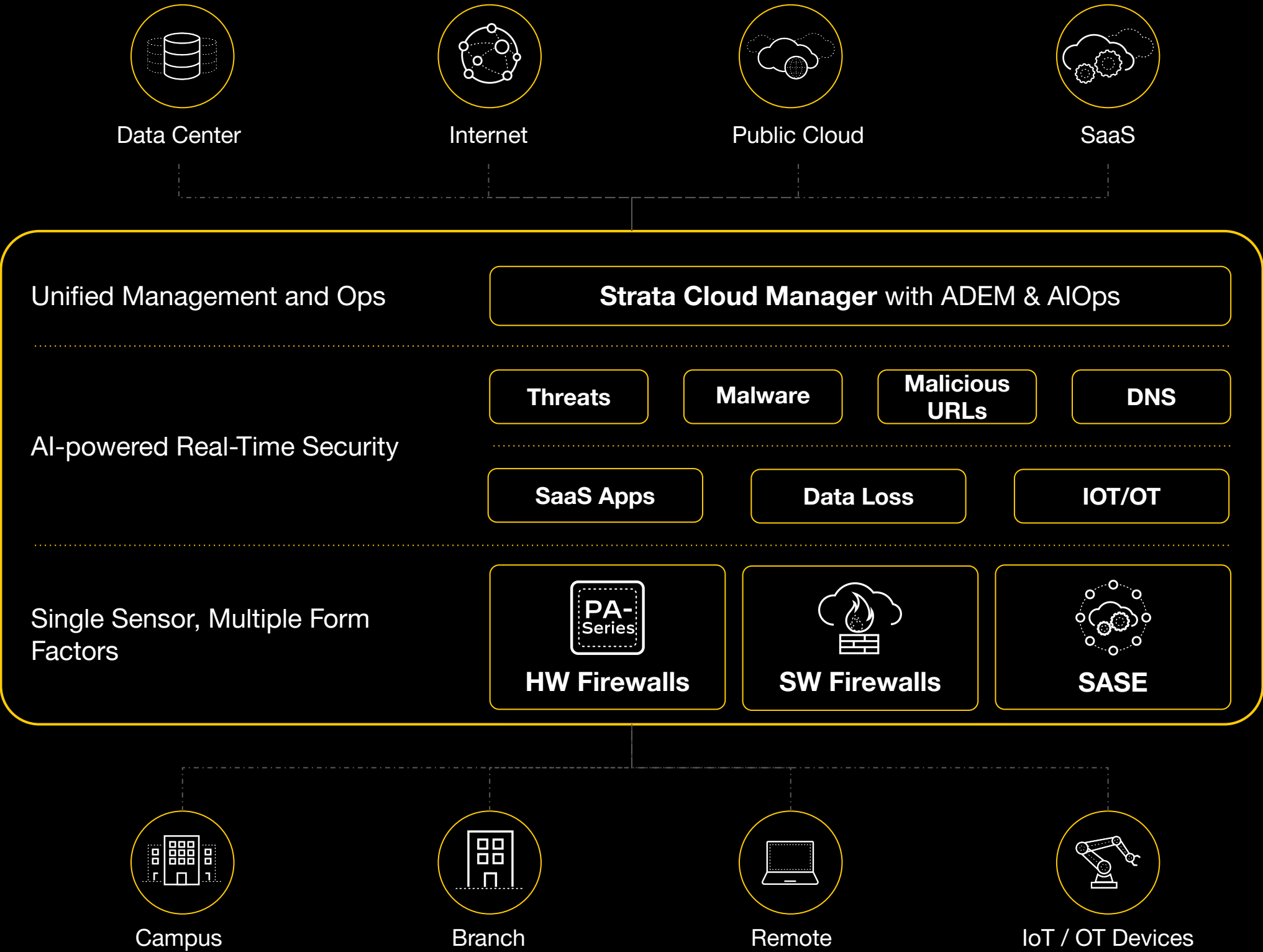
Simplify and unify network security with the Strata Network Security Platform

SUB-CATEGORY	ONE PLATFORM
Firewall	 Strata Network Security Platform
Intrusion Prevention	
URL Filtering	
Sandbox	
DNS Security	
IoT / OT Security	
Data Loss Prevention (DLP)	
Cloud Access Security Broker	
Remote Access	
Secure Web Gateway	
SD-WAN	
Remote Browser Isolation	
Enterprise Browser	
Digital Experience Monitoring	
Posture and Health Management	

#platformization

Strata Network Security Platform

Simple & unified. Prevents threats in real time everywhere.



Unified management and operations

Unify policies for all users, apps, devices. Deploy best practices to avoid human error.

AI-powered real-time security

Prevent threats in real time using AI & ML applied to rich data from 65,000+ customers

Single sensor, multiple form factors

Simplify security with consistent operating system. Protect every location with a fitting form factor.

174% ROI over three years: Forrester TEI Report

Core Cloud-Delivered Security Services

AI-powered real-time security

Continuous Trust Verification of App, User and Device



App-ID

Verify thousands of apps and app functions regardless of what port or protocol is used



User-ID

Verify all users regardless of IP address or where user identity is stored



Device-ID

Verify all devices connected to the network

Continuous Security Inspection

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

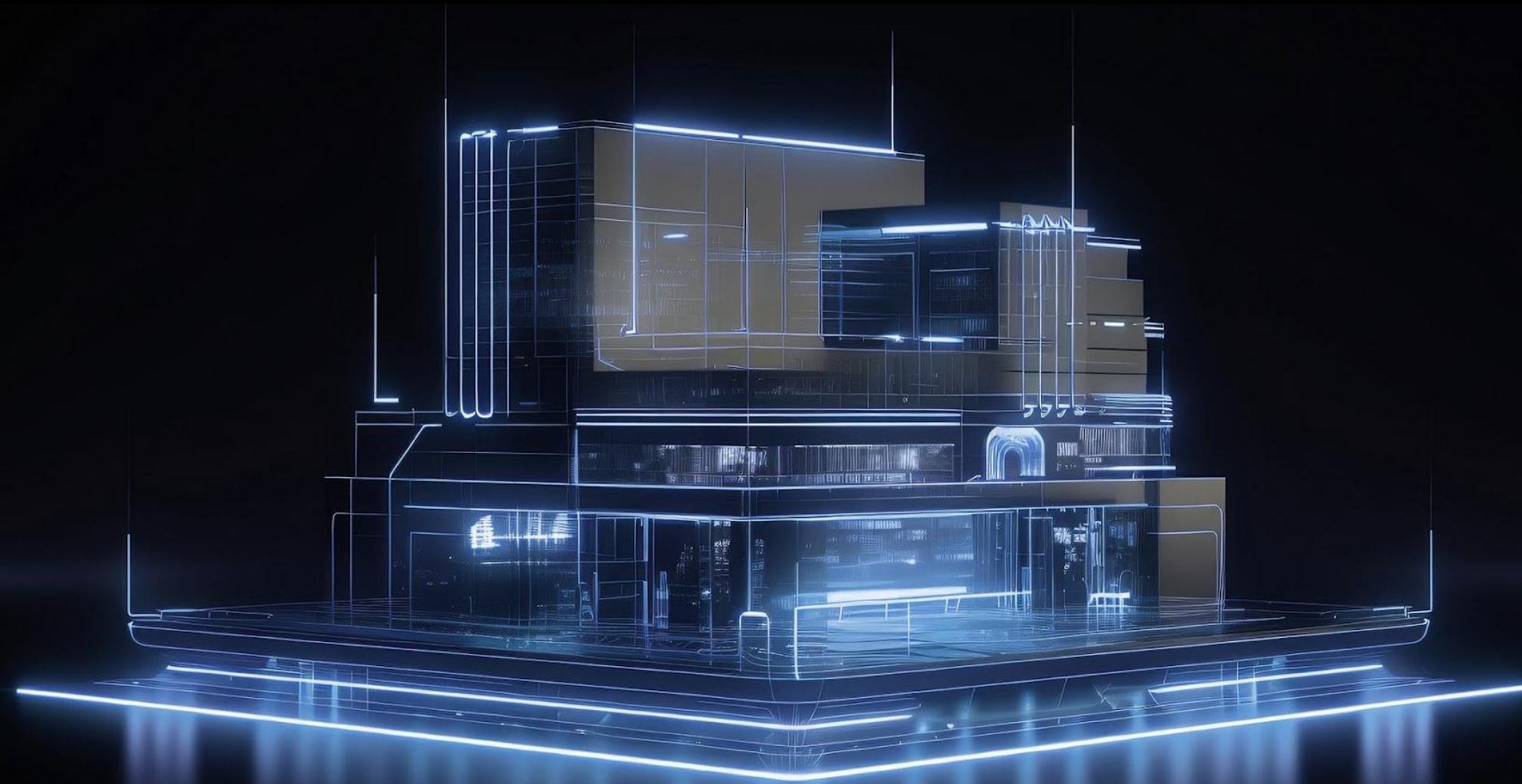
Users

Devices

Applications

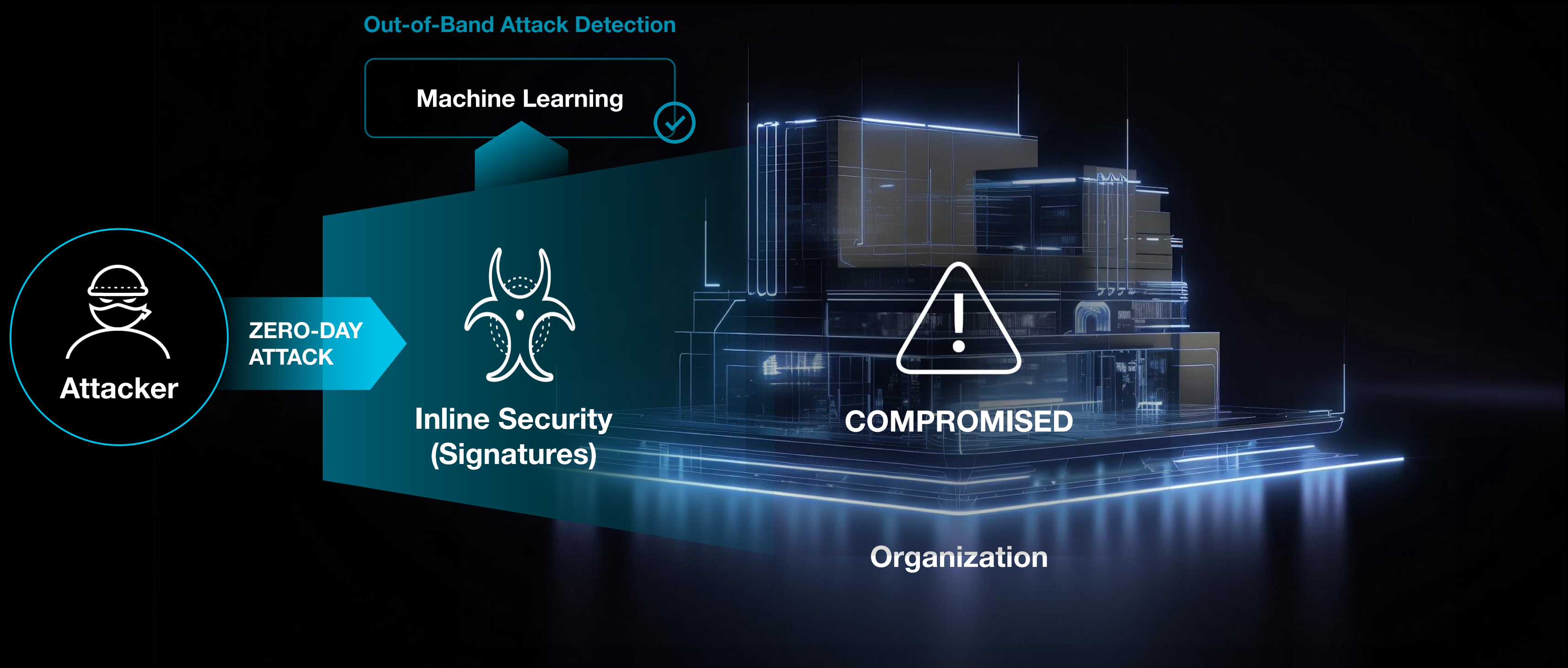
All Security Subscriptions

Traditional Approaches Can't Stop New Attacks; There's Always a "Patient Zero"



Organization

Traditional Approaches Can't Stop New Attacks; There's Always a "Patient Zero"



Combining Two Innovations: Precision AI & Inline Protection to Prevent Even the First Attack



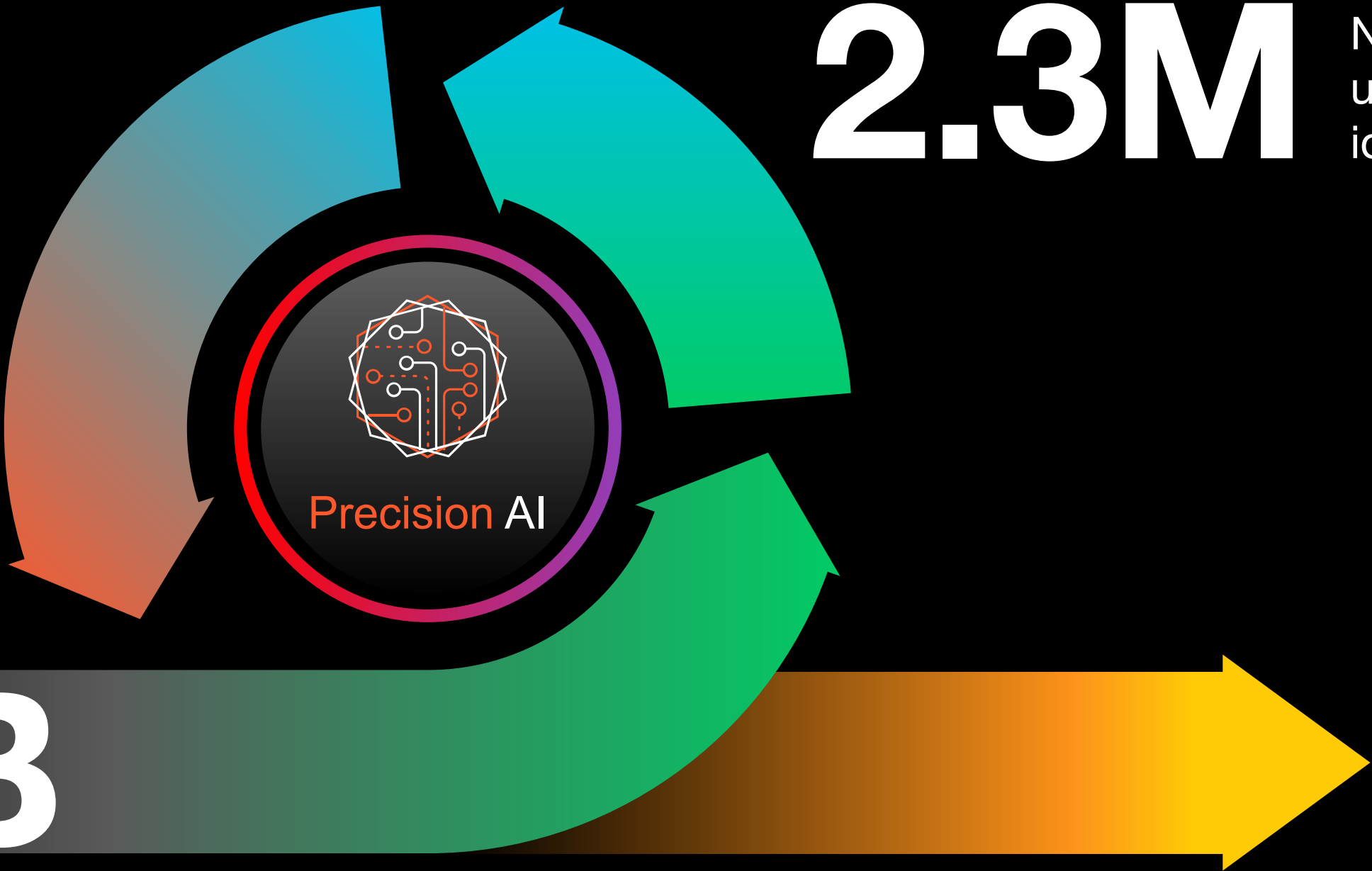
Extending the Network Effect of Detection and Prevention

11.3B

Attacks blocked inline daily

2.3M

New and unique attacks identified daily



4.6B

New events analyzed daily

Cloud Delivered Security Services

Powering All Core Security Services with Precision AI



Prevent Zero Day
Injection and
C2 Attacks



Protect Against
Evasive Malware

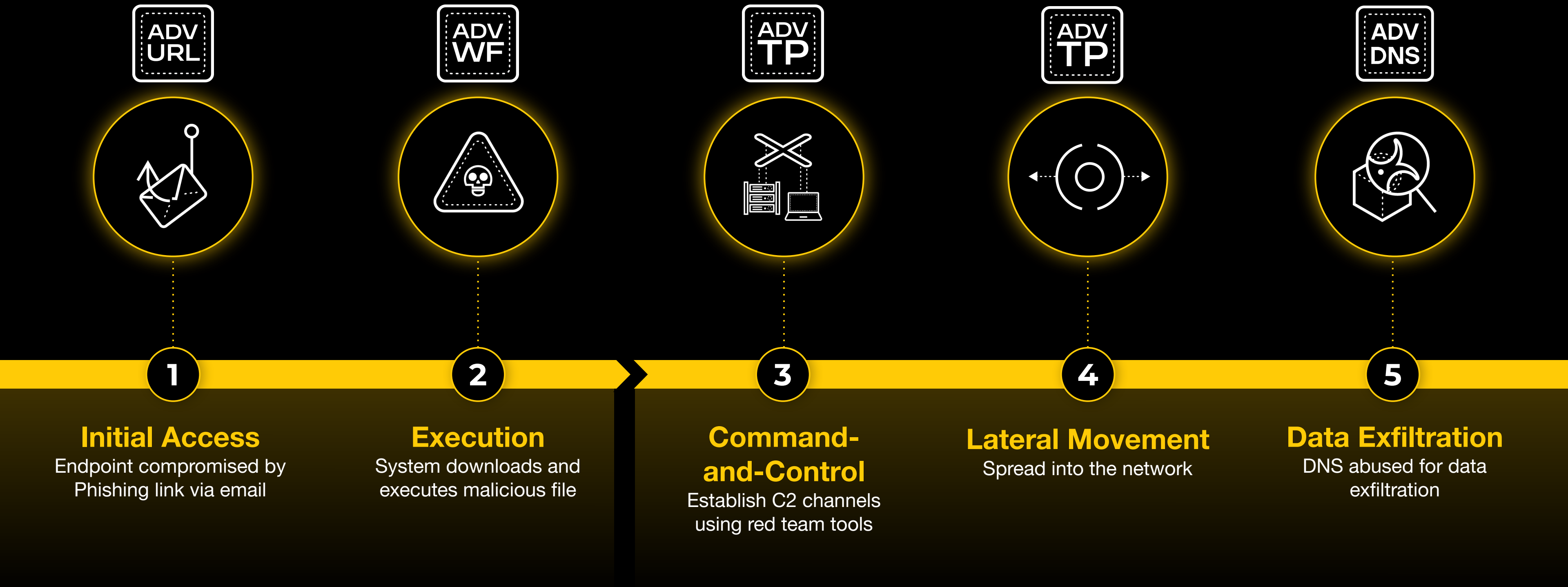


Defend Against
Evasive Web Phishing



Expanded Protection
Against Latest DNS
Hijacking Attacks

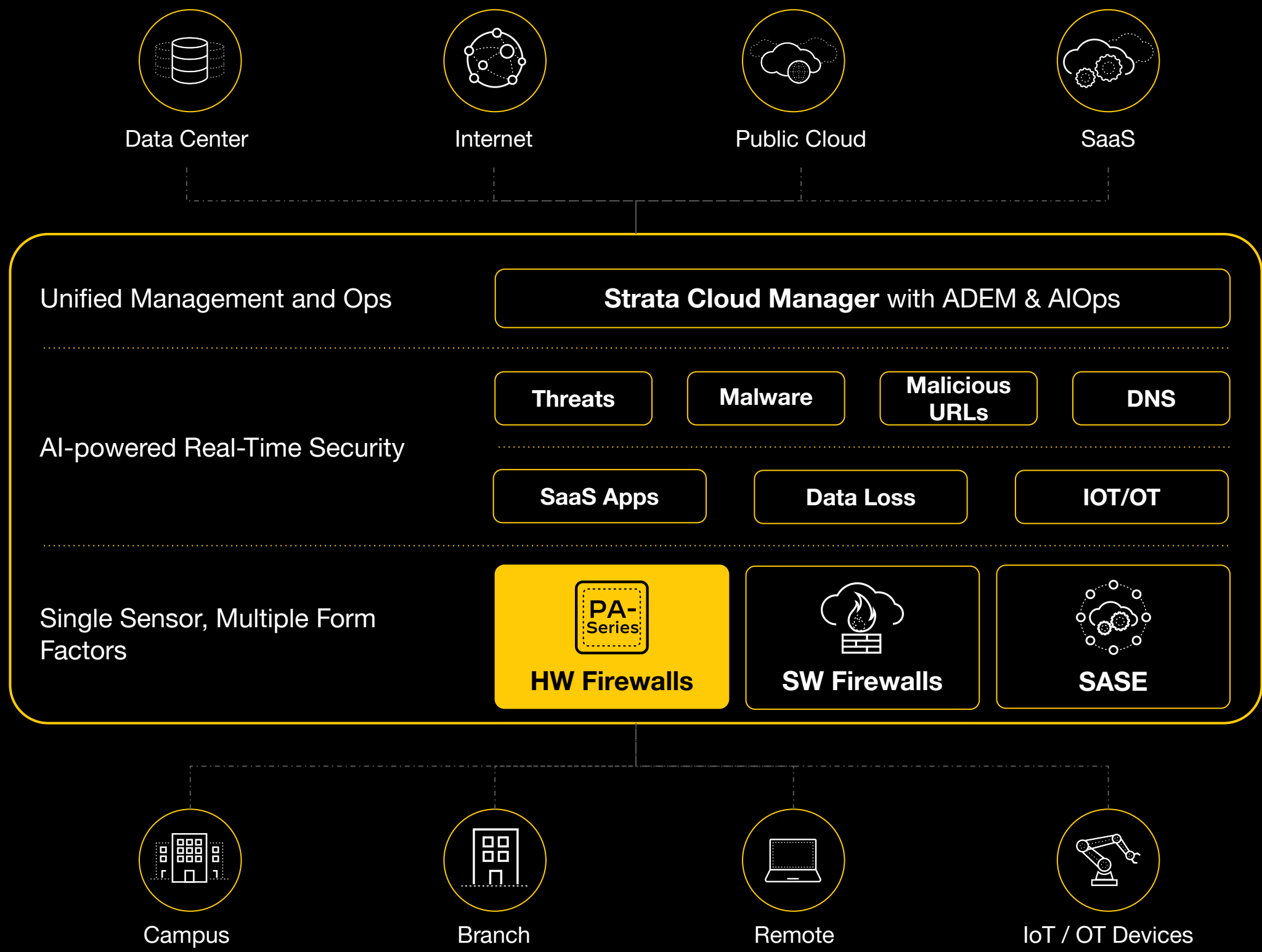
They are designed to work together to disrupt the threat lifecycle



Next Generation Firewalls

Secure all traffic at scale. Secure every location.

Palo Alto Networks Hardware Firewalls



Unified management and operations

Unify policies for all users, apps, devices. Deploy best practices to avoid human error.

AI-powered real-time security

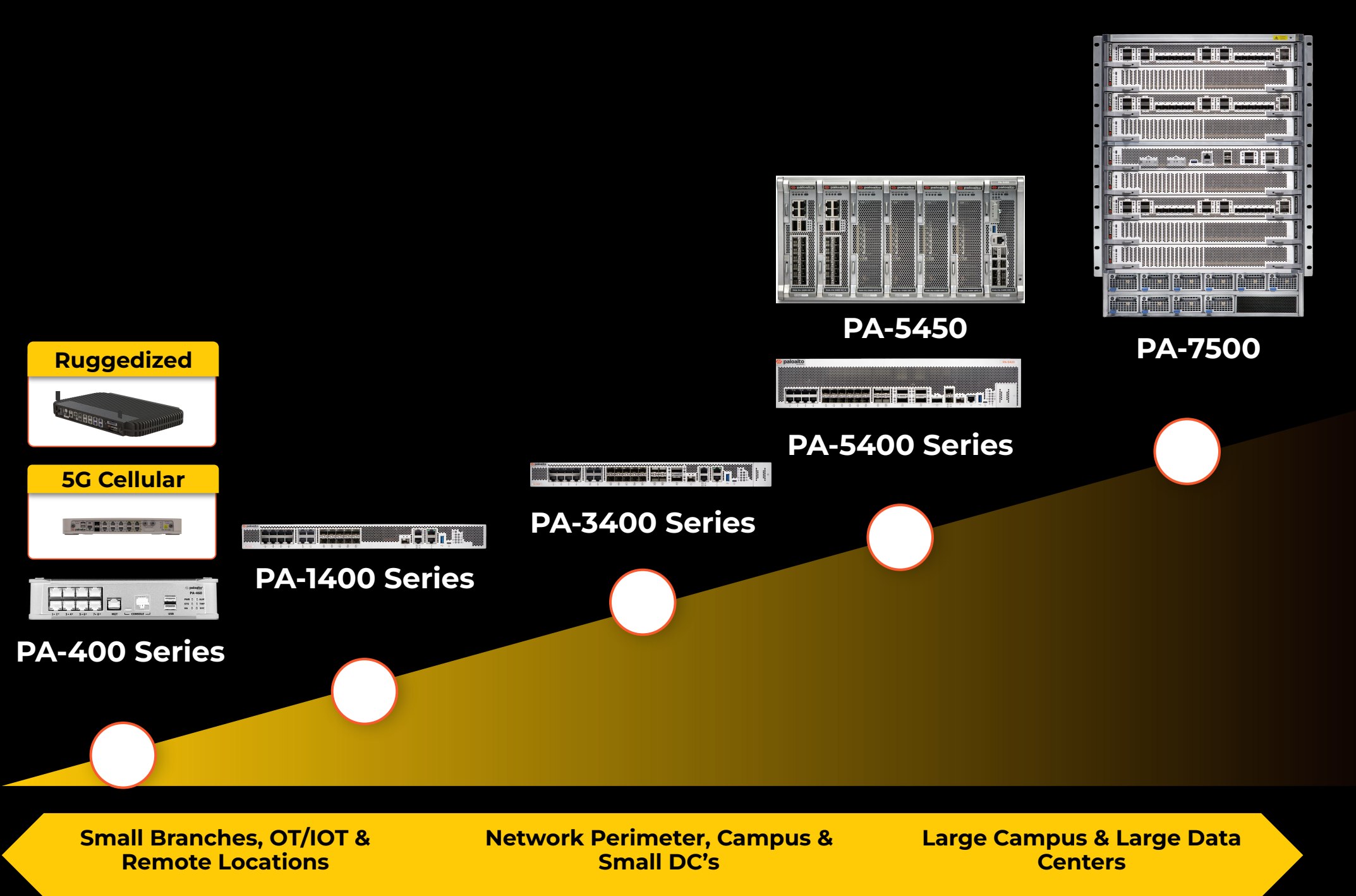
Prevent threats in real time using AI & ML applied to rich data from 65,000+ customers

Single sensor, multiple form factors

Simplify security with consistent operating system. Protect every location with a fitting form factor.

174% ROI over three years: Forrester TEI Report

High performance ML-Powered NGFWs for every use case



Fastest

Up to 1.5 Tbps throughput w/ single pass architecture and custom ASICs

Broadest range

Models for all use cases including 5G, 400G, PoE, Ruggedized

Inline AI

Cloud services work with inline ML models to deliver real-time security

Best price:performance

Scalable Layer 7 security and simplified operations

We Enable Multiple Security Services without Degrading Performance

Single-pass architecture

Enable multiple security services from a single enforcement point with no performance degradation

Competitive approach

Performance degradation from daisy-chaining security services drives need for additional sensors

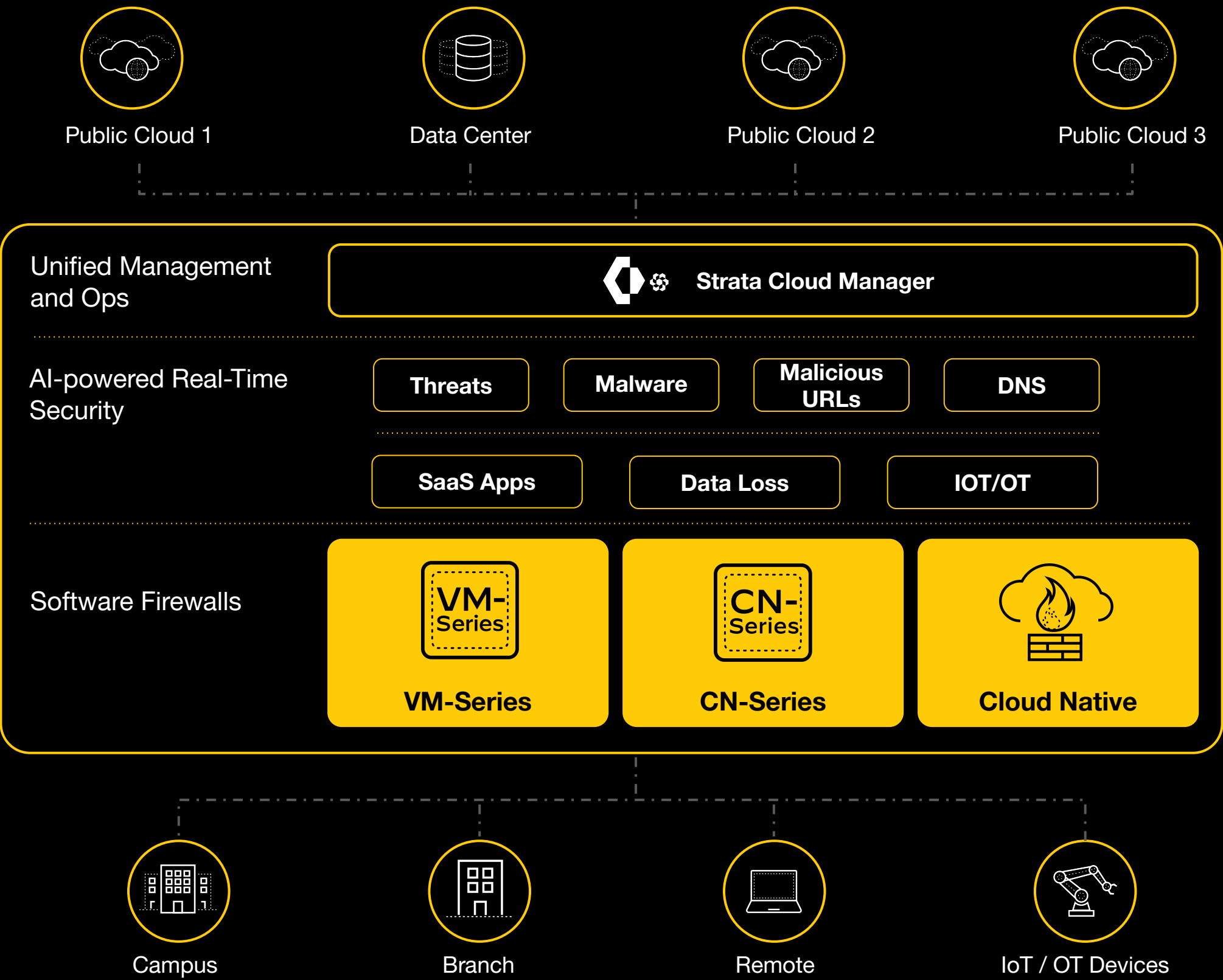


Up to 21% lower TCO
with security services enabled

87% throughput degradation
with security services enabled

[Miercom testing results](#)

Palo Alto Networks Software Firewalls



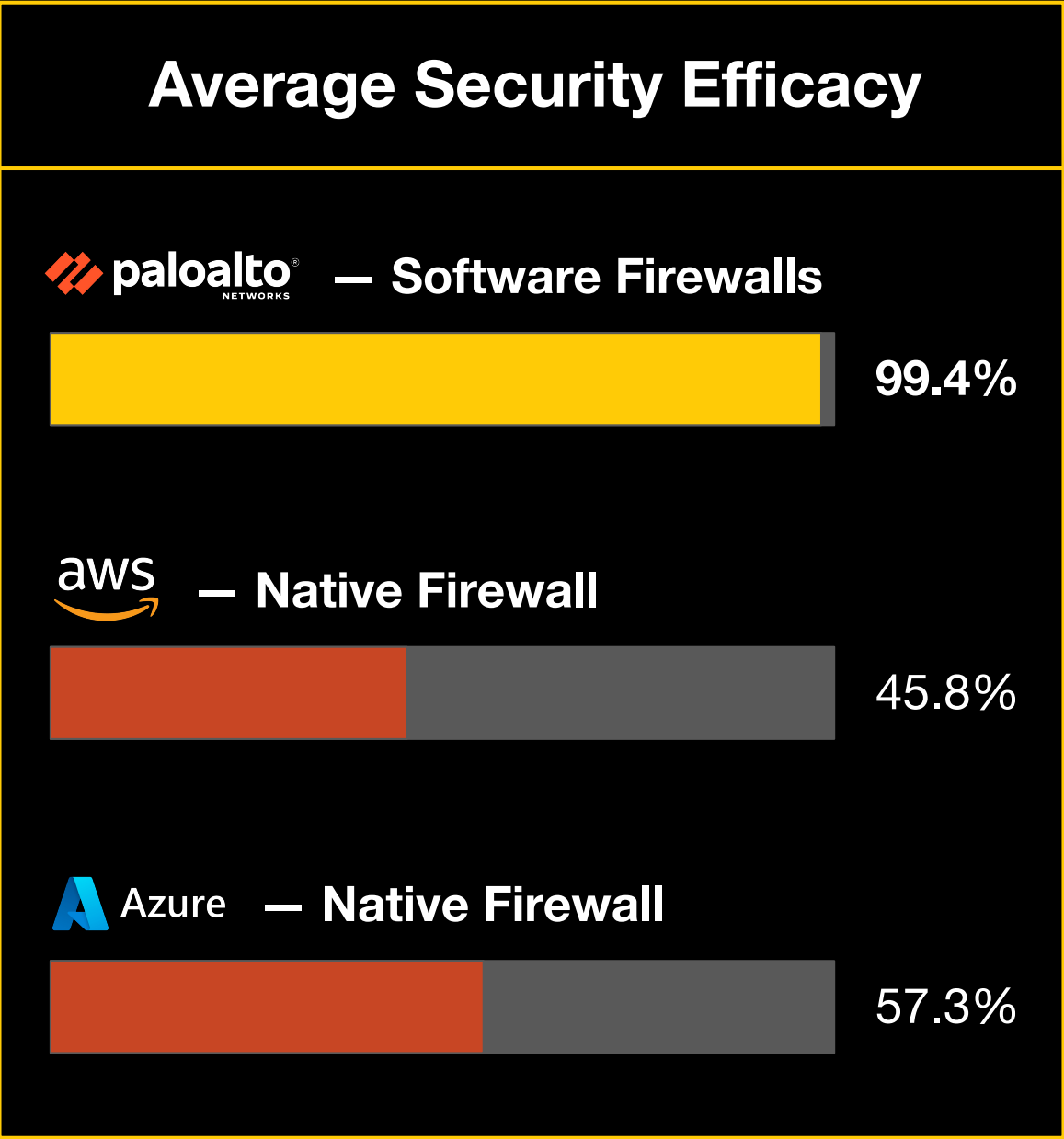
Unified management and operations
Unify policies across multi and hybrid cloud, integrates with premises FW estate

AI-powered real-time security
Prevent threats in real time using AI & ML applied to rich data from 65,000+ customers

Deployment options for every cloud
DIY or managed service across AWS, Azure, GCP, OCI, and private cloud/hypervisors.

163% ROI over three years: Forrester TEI Report

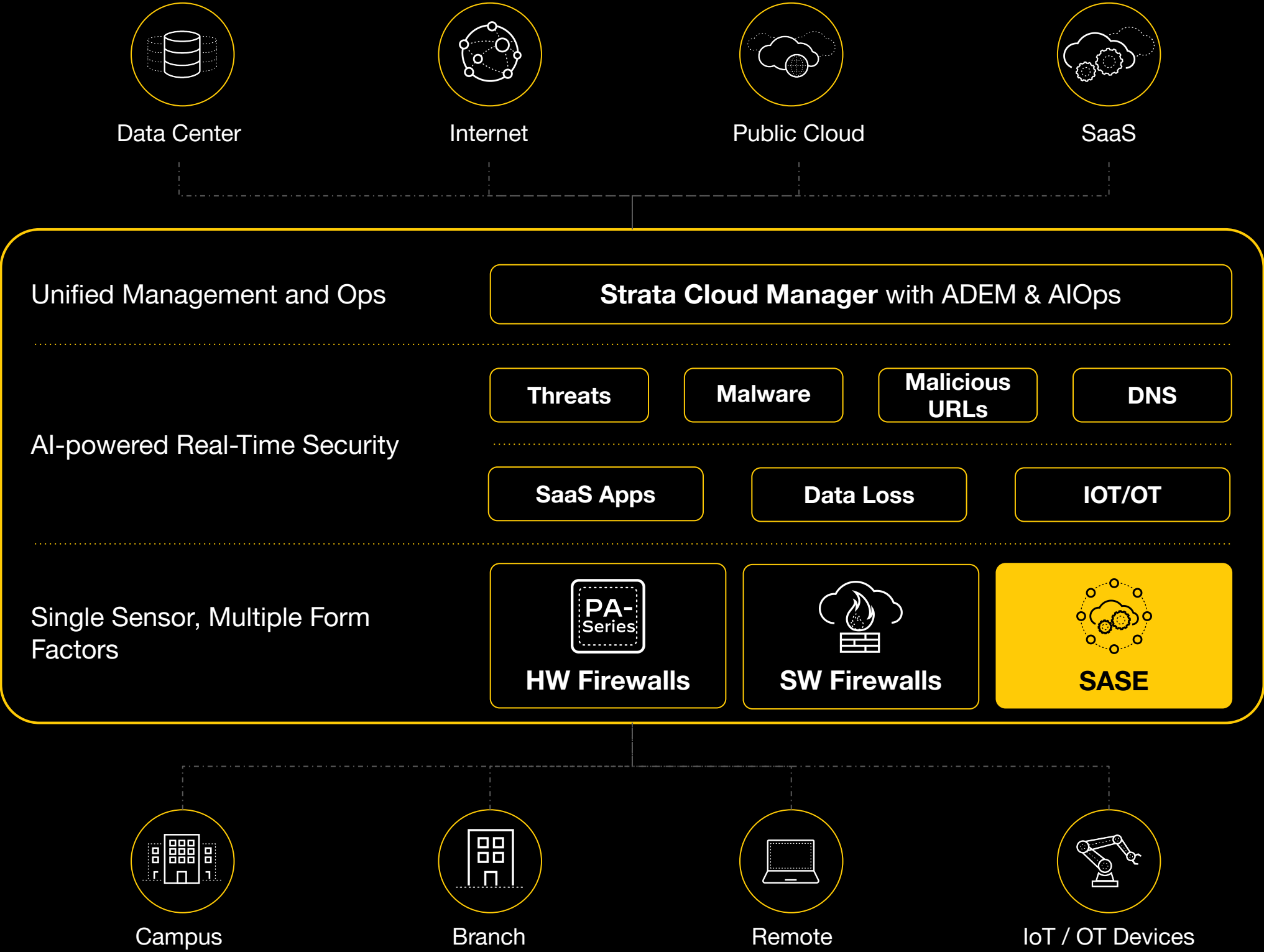
Security Outcomes Unattainable with Basic Cloud Provider Protection



Features	AWS Network Firewall	Azure Firewall Premium	Palo Alto Networks Software Firewall
Cloud native service and management	<div></div>	<div></div>	<div>✓</div>
Integrated with premises network security	<div></div>	<div></div>	<div>✓</div>
Multi-cloud Support	<div></div>	<div></div>	<div>✓</div>
User, Device, Application identity in policies	<div></div>	<div></div>	<div>✓</div>
Threat & Intrusion Prevention	<div></div>	<div></div>	<div>✓</div>
Malware Sandboxing & Prevention	<div></div>	<div></div>	<div>✓</div>
URL Security	<div></div>	<div></div>	<div>✓</div>
DNS Security	<div></div>	<div></div>	<div>✓</div>

Source: Mar 2024 [SecureIQ Lab Public Test](#) (Not Sponsored)

Palo Alto Networks SASE



Unified management and operations

Unify policies for all users, apps, devices. Deploy best practices to avoid human error.

AI-powered real-time security

Prevent threats in real time using AI & ML applied to rich data from 65,000+ customers

Single sensor, multiple form factors

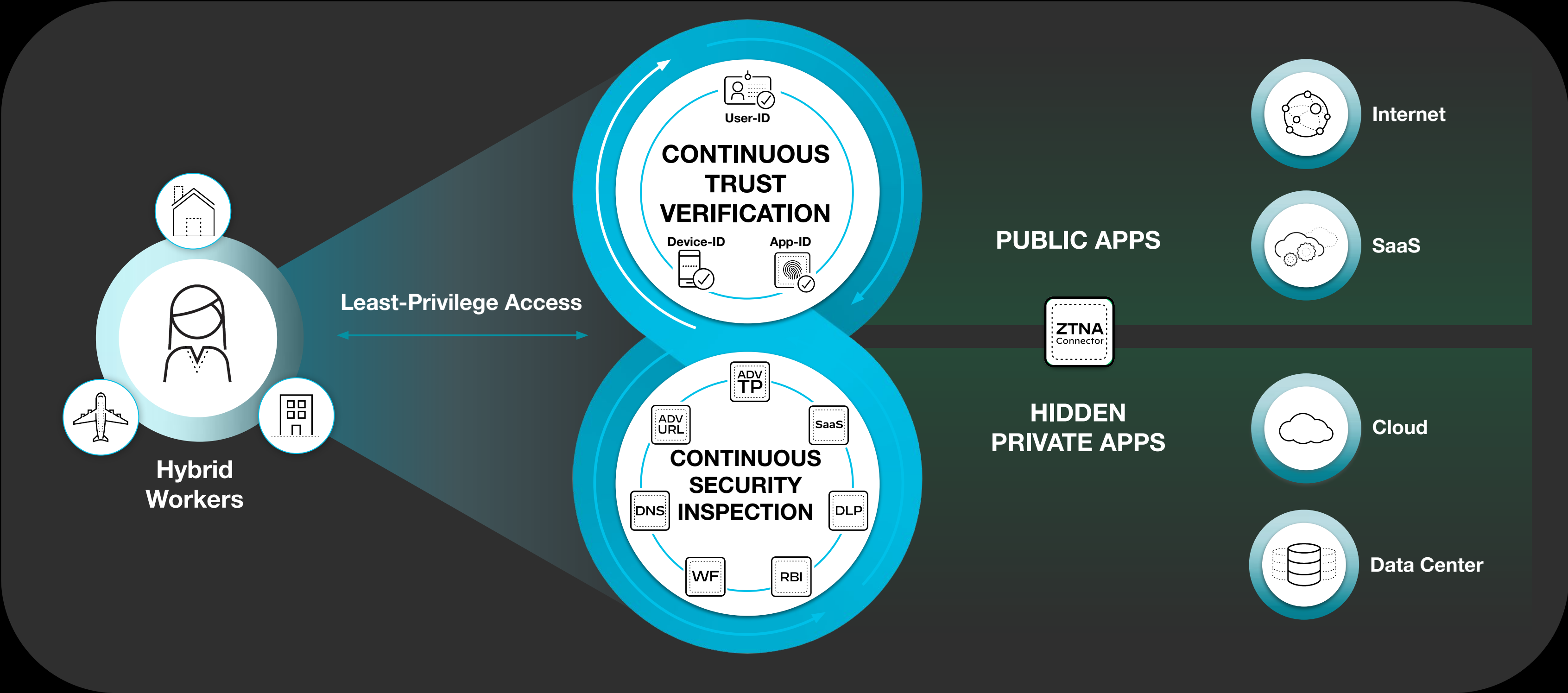
Simplify security with consistent operating system. Protect every location with a fitting form factor.

174% ROI over three years: Forrester TEI Report

Prisma Access is a Globally Distributed Service Securing All Users & All Applications



Continuous & AI-Powered Security Inspection of All Traffic



Unified management and operations for your entire network security estate



STRATA™ CLOUD MANAGER

BY PALO ALTO NETWORKS

AI-Powered Zero-Trust Management and Operations



Predict and Prevent
Network Disruptions



Strengthen Security
in Real-Time



Comprehensive Management for All
Deployments in a Single UI

Cloud-Delivered
Security Services



Hardware Firewalls



Software Firewalls
Cloud NGFW



SASE




SHIELD vzw


Thank you

by Tomas Van Beek & Jo Vander Schueren


Advanced Threat Prevention

Prevent Known and Unknown C2 attacks and Zero-Day Exploits In Real-Time





Prevent zero-day exploits that use techniques such as command and code injection by patented AI-powered detection models



Prevent evasive C2 traffic generated by popular red team tools such as Cobalt Strike and Empire



Purpose-built ML models to detect malicious encrypted payloads based on packet header information

98%

Prevention of C2 attacks propagated by Empire




Global network of 65k+ customers providing **crowd-sourced threat intelligence**




Robust database of signatures for prevention of known exploits, web-based threats, C2, and malware


Advanced WildFire

Prevent Known and Unknown File-Based Malware Inline






Detect and prevent evasive malware, resulting in **99.5% reduction** in systems infected




Defeat 26% more malware than traditional sandboxes using ML and advanced intelligent run-time memory analysis (IRMA)




Multiple patented counter-evasion techniques deployed, generating **99% detection** of known and unknown malware

180x

Faster prevention than the average competitor





16 regional clouds and **17 international certifications** to meet data and network latency requirements



Global network of 65k+ customers providing **crowd-sourced threat intelligence**

© 2024 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

Advanced URL Filtering

Ensure Safe Access to the Web and Stop Known and Unknown Phishing Attacks Inline

Inline analysis of user web traffic, instead of relying on databases generated by web crawlers to prevent evasion techniques used by attackers

AI-powered analysis identifies unique attributes of web pages to detect and prevent phishing pages hosted on legitimate SaaS platforms, all in real time

ML/DL detectors enable accurate detection of emerging phishing attacks and the toolkits used to create those attacks

88%

Malicious URLs prevented 48hrs before competitors

Global network of 65k+ customers and third-party databases providing **crowd-sourced threat intelligence**

40% more threats prevented than traditional filtering databases

ADNS Security

Prevent Sophisticated DNS-Layer Threats In Real-Time

AI-powered detection models continuously trained on billions of transactions for more accurate detection

Comprehensive coverage of modern-day DNS attacks; 68% more DNS-layer threat coverage than competitors

Inline inspection of *both* DNS request and response prevent DNS hijacking attacks

6x

Faster detection of known and unknown threats than public scanners



Global network of 65k+ customers and third-party databases providing **crowd-sourced threat intelligence**



Comprehensive visibility and inline analysis of all DNS traffic, including plain-text DNS, DoT, DoH, and those going to unknown resolvers

ML-Powered NGFWs

Ruggedized



**Ruggedized
PA-450R**
3.0 Gbps App-ID
Dual SFP



**Ruggedized
PA-220R***
540 Mbps App-ID

5G Cellular



PA-415-5G
1.5 Gbps App-ID

PA-400 Series



PA-460
4.4 Gbps App-ID



PA-455
3.6 Gbps App-ID



PA-450
2.9 Gbps App-ID



PA-445
2.2 Gbps App-ID



PA-440
2.2 Gbps App-ID



PA-415
1.2 Gbps App-ID



PA-410
1.1 Gbps App-ID

PA-1400 Series



PA-1420
9.5 Gbps
App-ID



PA-1410
6.8 Gbps
App-ID

PA-3400 Series



PA-3440
24 Gbps App-ID



PA-3430
20.5 Gbps App-ID



PA-3420
16.9 Gbps App-ID

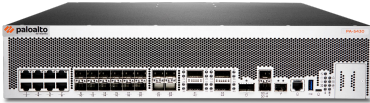


PA-3410
11 Gbps App-ID

PA-5400 Series



PA-5445
93 Gbps App-ID



PA-5440
72 Gbps App-ID



PA-5430
61 Gbps App-ID



PA-5420
56 Gbps App-ID



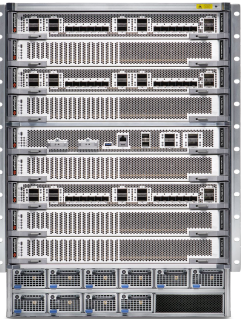
PA-5410
43.5 Gbps App-ID

PA-5450



PA-5450
Up to 200 Gbps
App-ID

PA-7000 Series



PA-7500
1 Tbps App-ID



PA-7080*
635 Gbps App-ID



PA-7050*
384 Gbps App-ID



Small Branches & Remote



Network Perimeter & Data Centers



Large Data Centers