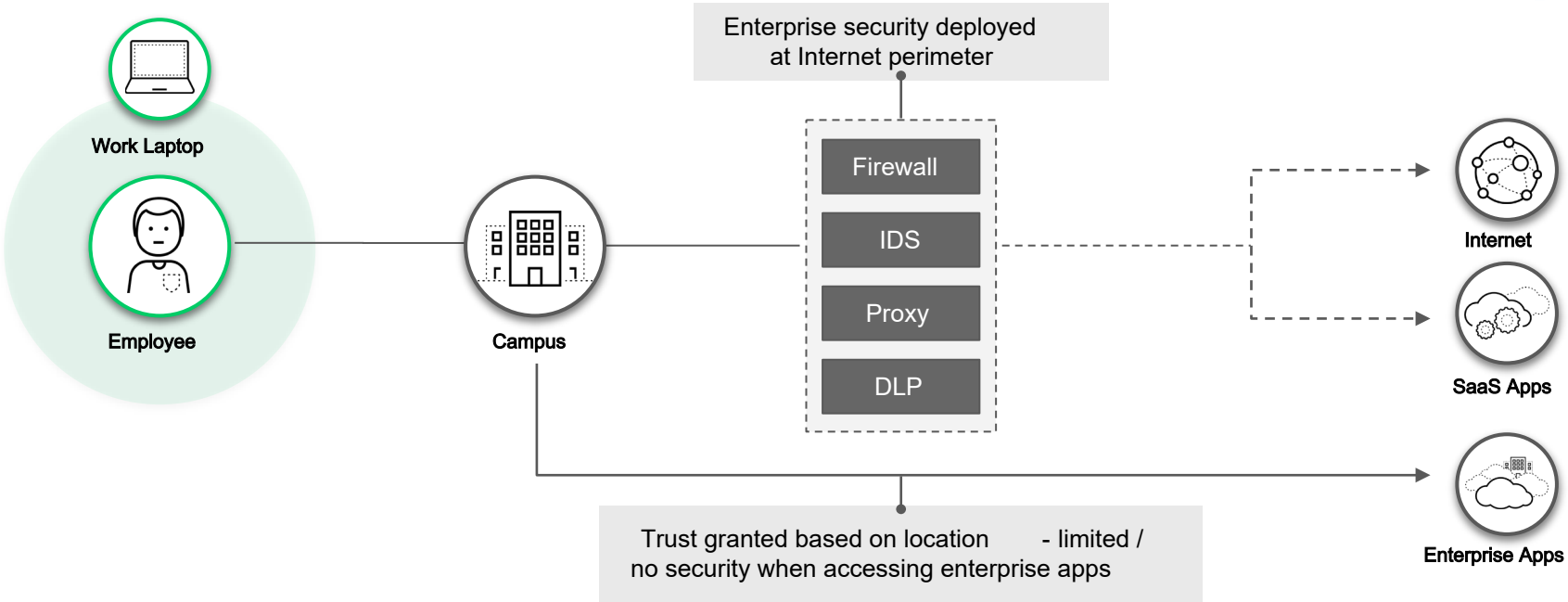
Complete Zero Trust Network Security

What's New in PAN-OS 10.1, Security Services, and ML-Powered NGFW Platforms

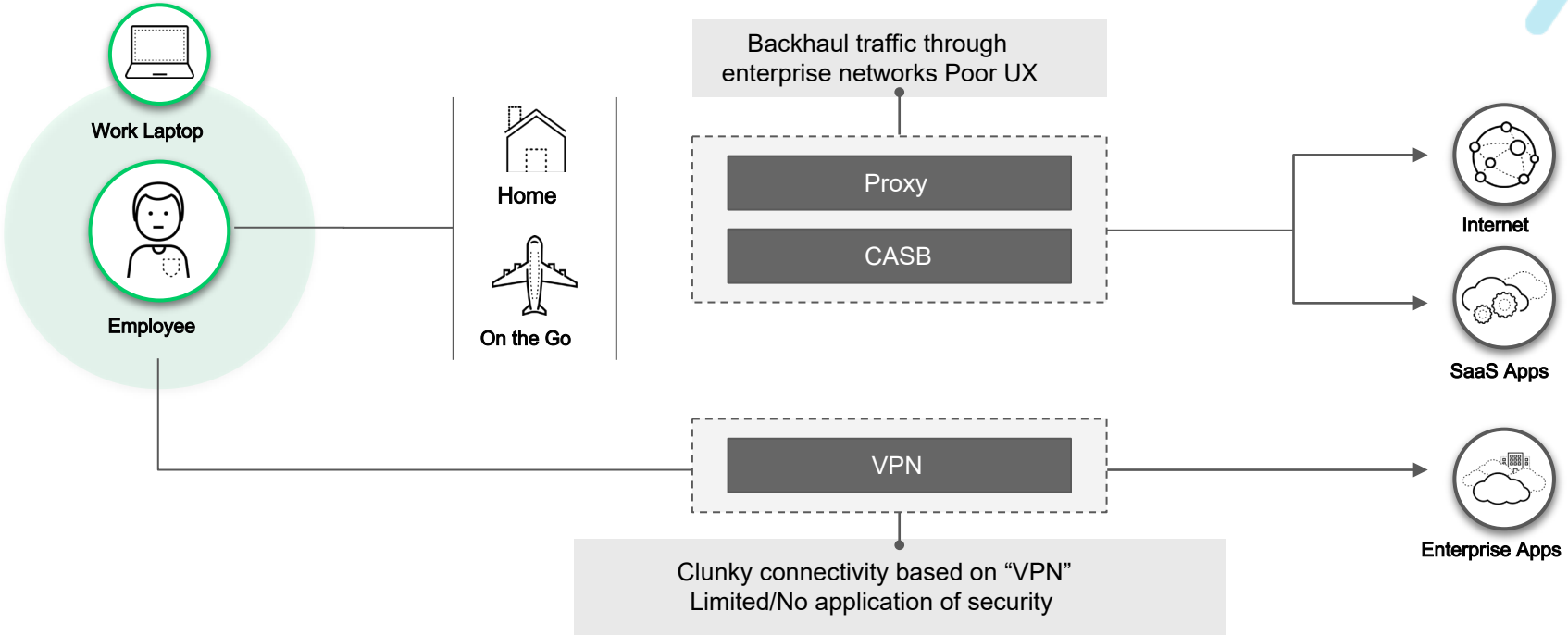
paloalto NETWORKS

Back In The Day, Everyone On Corporate Network Was Implicitly Trusted



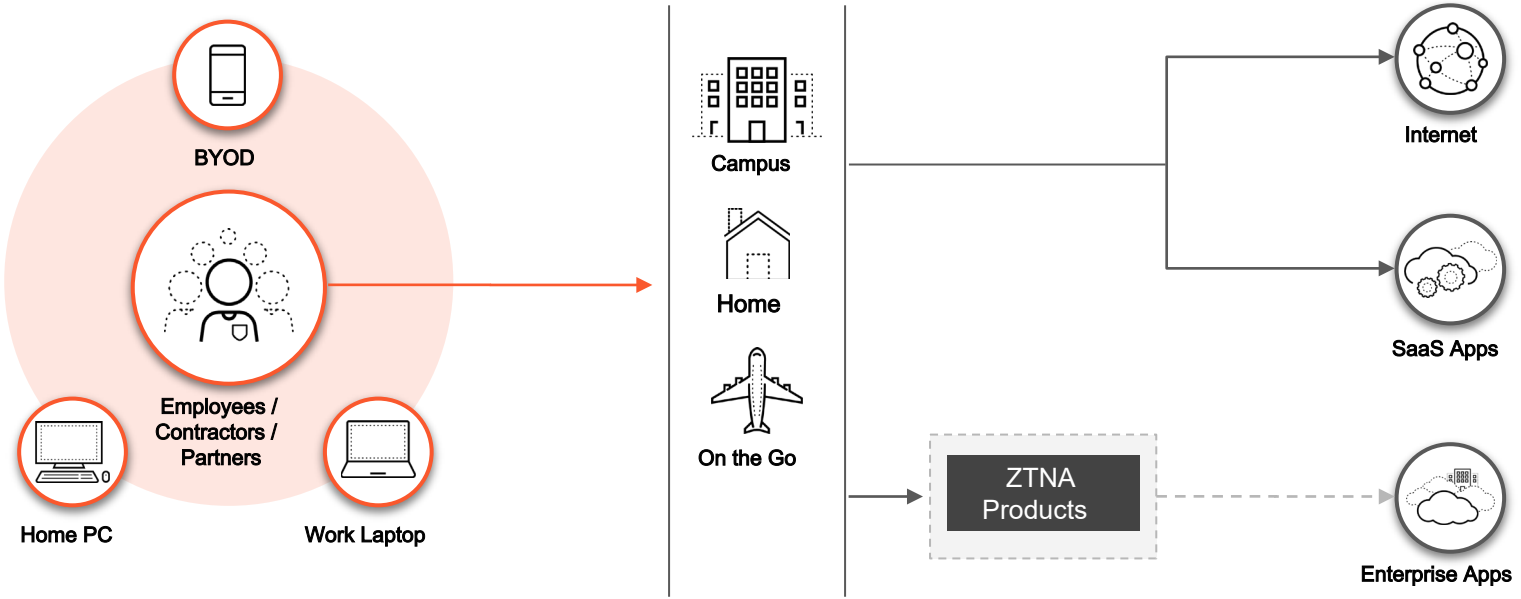
PROBLEM: POOR SECURITY

And Everyone Off Corporate Network Was Implicitly Untrusted



PROBLEM: POOR SECURITY & USER EXPERIENCE

Even Today, The Apparent Solution - ZTNA - Is Incomplete



Remote Users Only

Users roam - campus, branches, homes, mobile locations and shared spaces

Access Control Only

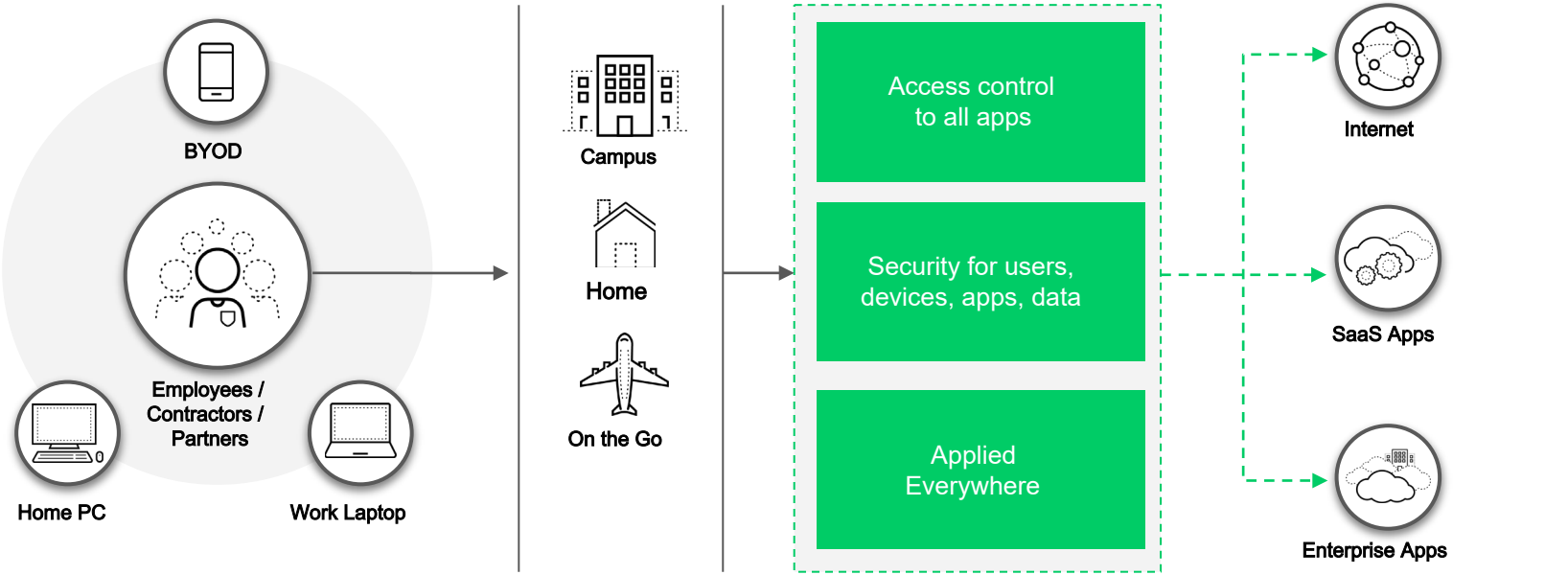
Access control is just one aspect of security

Enterprise Apps Only

Excludes SaaS apps and Internet access

To deliver the promise of Zero Trust , you need a comprehensive approach.

Introducing Complete Zero Trust Network Security



All Users & Devices

All Locations

Consistent Access Control & Security

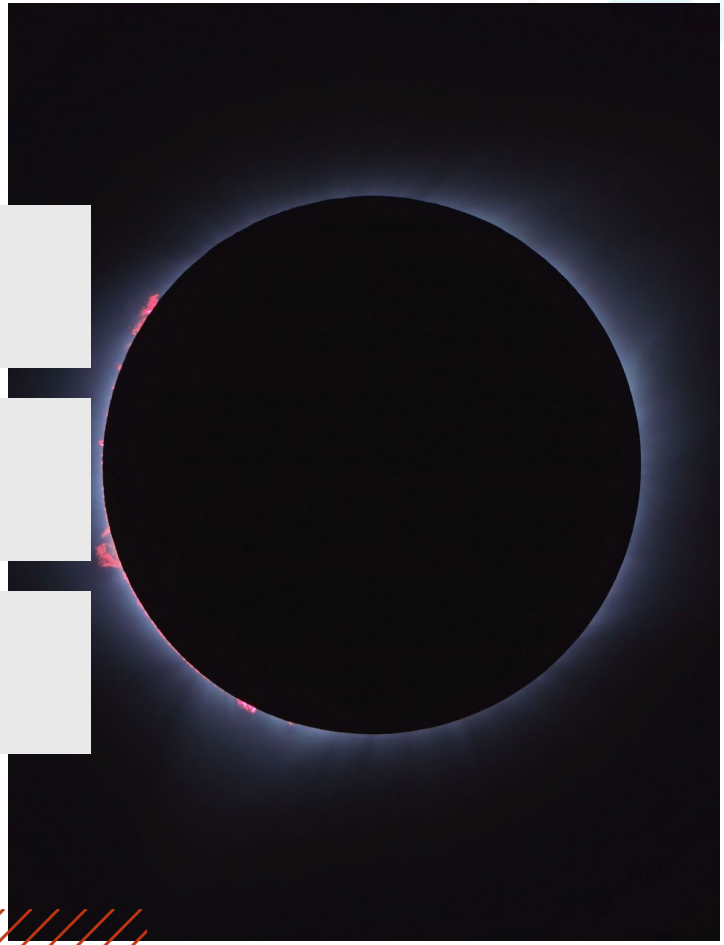
All Apps & Internet

3 Core Capabilities Needed To Adopt Zero Trust Network Security

1. Provide Context -based Access

2. Make Access Safe

3. Consistent Access & Security, Available Globally



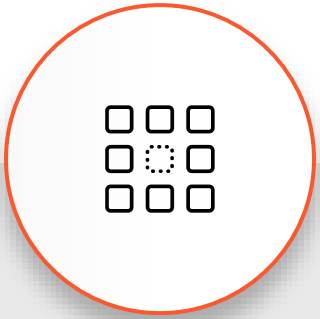
Core Capability 1: Provide Context -based Access

ALL Users

- Contractor
- Employee
- Partner

ALL Devices

- BYOD
- Corp Laptop
- Home PC

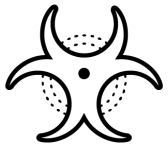


ALL Applications

- Enterprise Apps
- Internet
- SaaS

Core Capability 2: Make Access Safe

Secure ALL users, devices and applications against threats

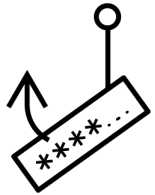


Exploits

- Vulnerability Exploits
- Phishing & Email Compromise
- Malicious Downloads

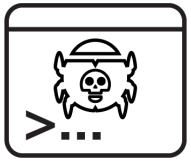
Malware

- Host Compromise
- Lateral Movement
- ...



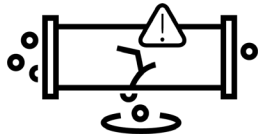
Phishing

- C2
- Behavioral Indicators
- User/Device Risk



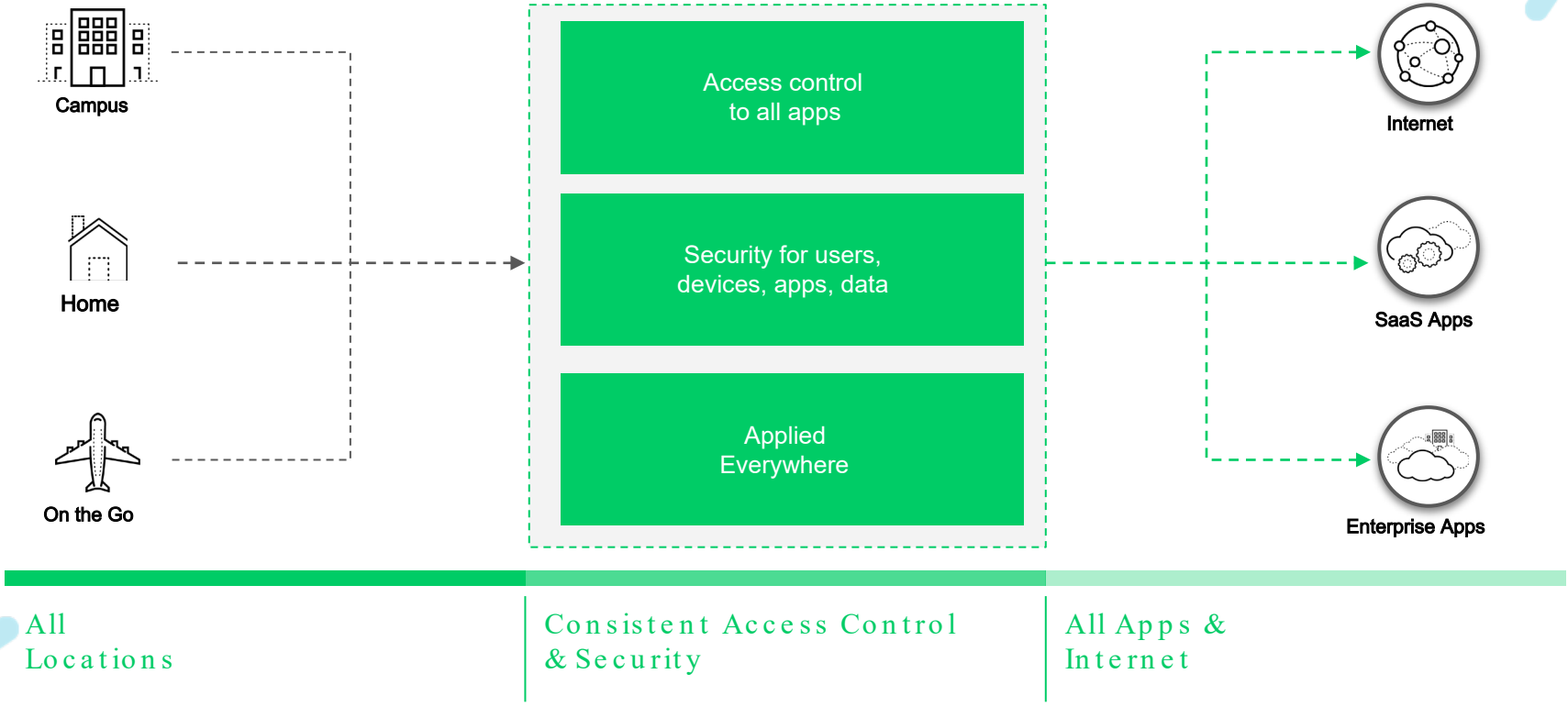
Malicious Websites

- Social Engineering
- Shadow IT
- ...



Data Loss

Core Capability 3: Consistent Access & Security, Available Globally



New Innovations Aligned To 3 Zero Trust Network Security

Core Capabilities

Cloud Identity

Simplified identity controls for adopting Zero Trust

SaaS Security

Integrated CASB to keep pace with the SaaS explosion

Internet Security

Industry -first inline ML to prevent unknown and emerging attacks

ML-Powered NGFW Platforms

Best-in-class, ML-Powered NGFW to protect your enterprise

Context-Based Access

Make Access Safer

Global, Consistent Availability

Enable identity-based controls in a cloud-first world.

paloalto NETWORKS

We've Been Delivering Industry -Leading Identity Innovations

Enable users to access apps they need.

Always know that the user is who they claim to be.

Prevent users from getting phished for credentials.

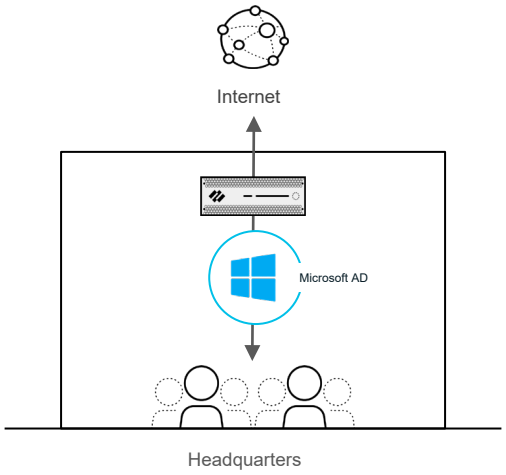
Enable rapid SOC responses with identity context.

While the blueprint hasn't changed, identity stores are undergoing significant disruption.

Problem | Managing Identity Has Become Challenging

A few years ago

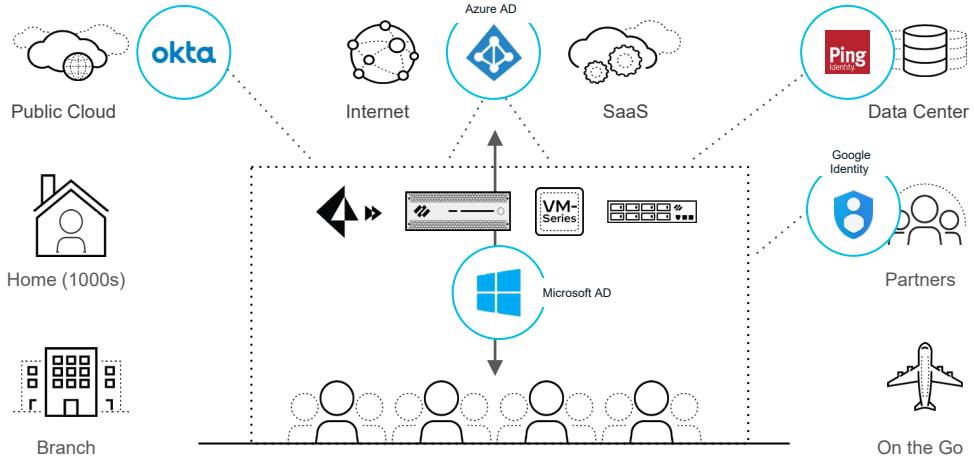
Deploying user -based policies was straightforward.



One identity source.
All employees worked from an office.

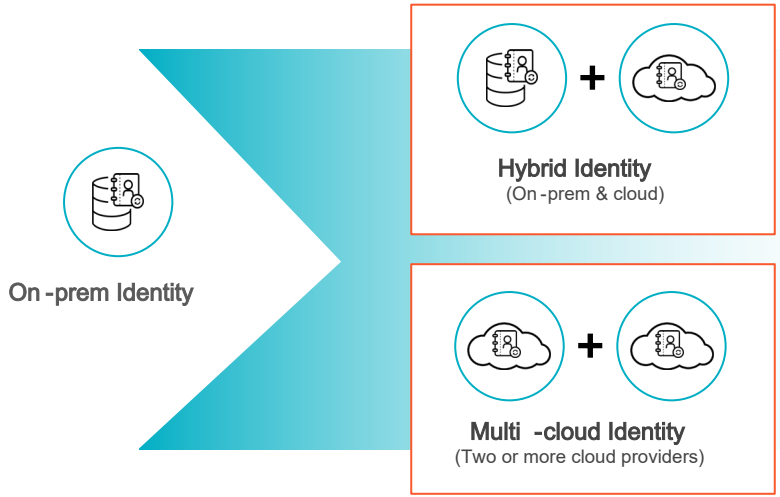
Now

Deploying user -based policies is highly complicated and laborious.



Identity has federated as apps moved to cloud.
10-1,000s of users work from everywhere.

Problem | Enterprise Identity is Migrating From On -prem to Cloud



87%

of organizations use or plan to use cloud -based directory service.*

Source: * ESG Survey, Trends in IAM . Dec 2020

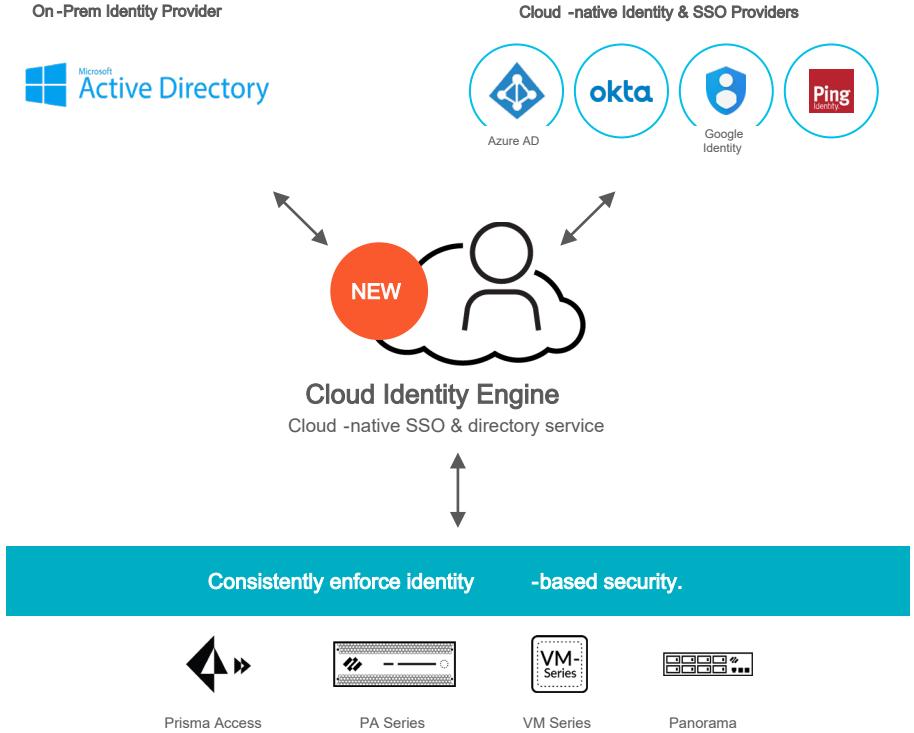
ZERO TRUST

Zero Trust is a security strategy to minimize the risk of breaches by eliminating assumed trust in the digital world and consistently verifying all users, devices, applications, and data based on context and user activity.

To achieve Zero Trust for identity, we need something that can easily and consistently verify users across…

Campus/HQ | Branch | Remote Workplace | Data Center/ Private Cloud | SaaS | Public Cloud

Introducing Cloud Identity Engine



Always -on identity for Zero Trust Network Security

Global, resilient cloud -native engine

Your global network security footprint integrated with identity providers in 10 mins

Point -and -click IdP integrations

Instant MFA for all your data center apps

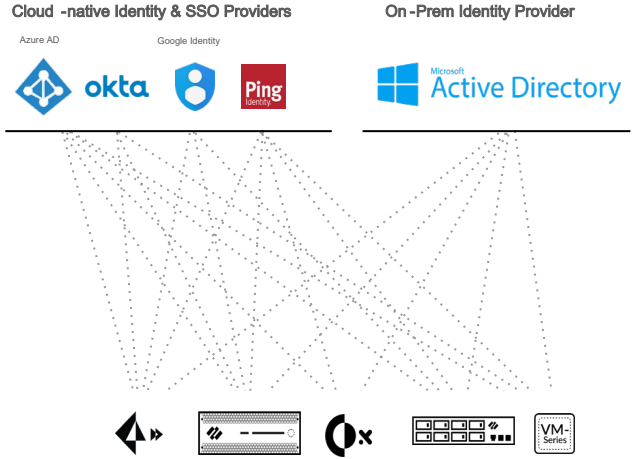
Use your cloud identity provider's MFA (multi -factor authentication) for all your data center apps instantly

Our Approach | Transition from On -prem to Cloud Identity with Ease

A few years ago

Up to 1,000s of Security Devices

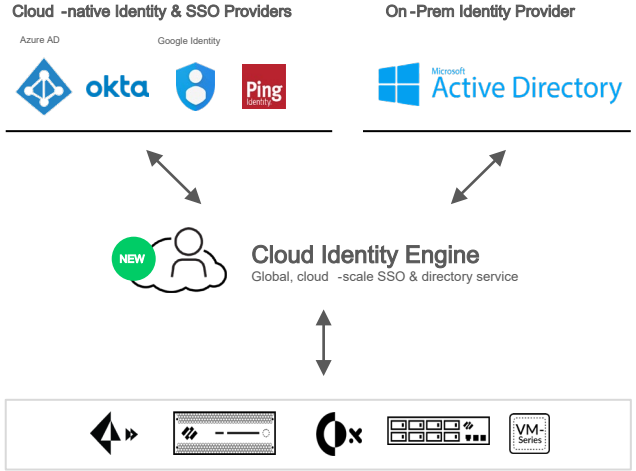
Now



Up to 1,000s of Security Devices

Months to years.

With Cloud Identity Engine

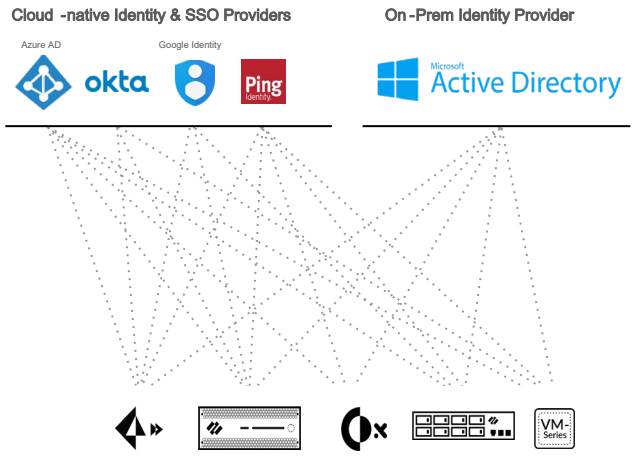


Up to 1,000s of Security Devices

Can be achieved in 10 minutes.

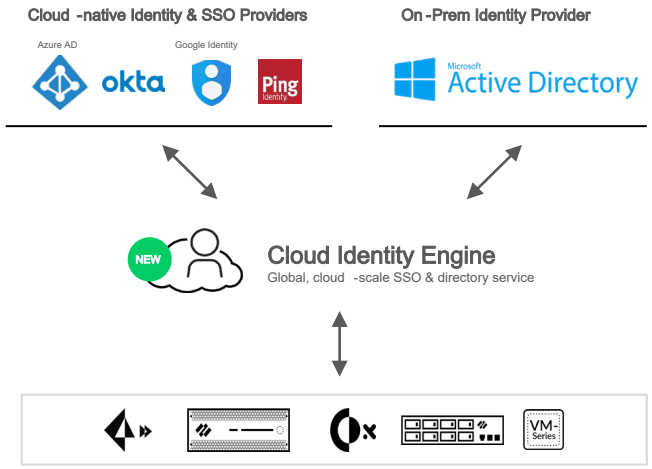
Use Case 1 | Simplifying Identity -based Group Policies

Before
Without Cloud Identity Engine



Up to 1,000s of Security Devices

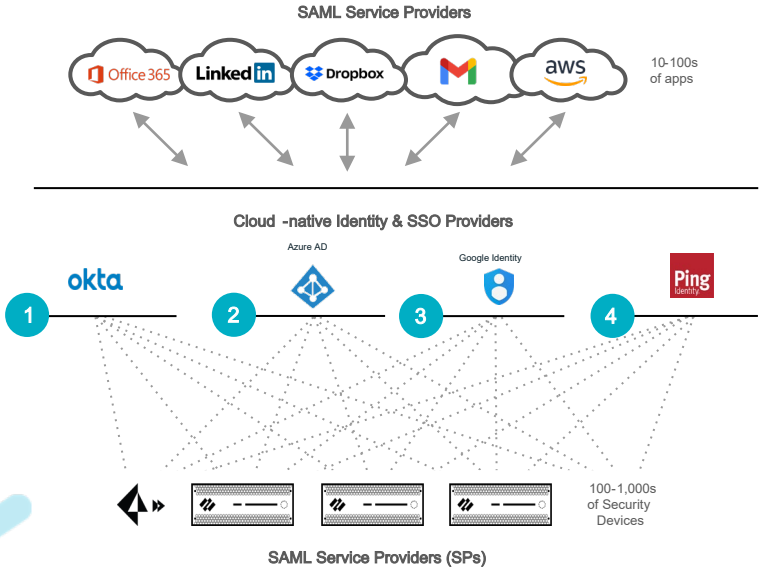
After
With Cloud Identity Engine



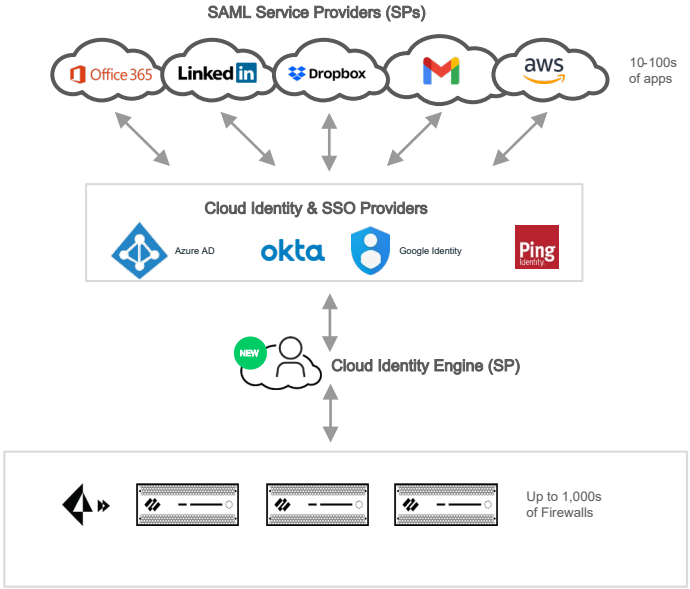
Up to 1,000s of Security Devices

Use Case 2 | Simplifying Cloud Authentication Set Up and Management

Before
Multiple SPs



After
Single SP



Cloud Identity Engine

Empowering organizations to move to Zero Trust Network Security.

Identity -based access

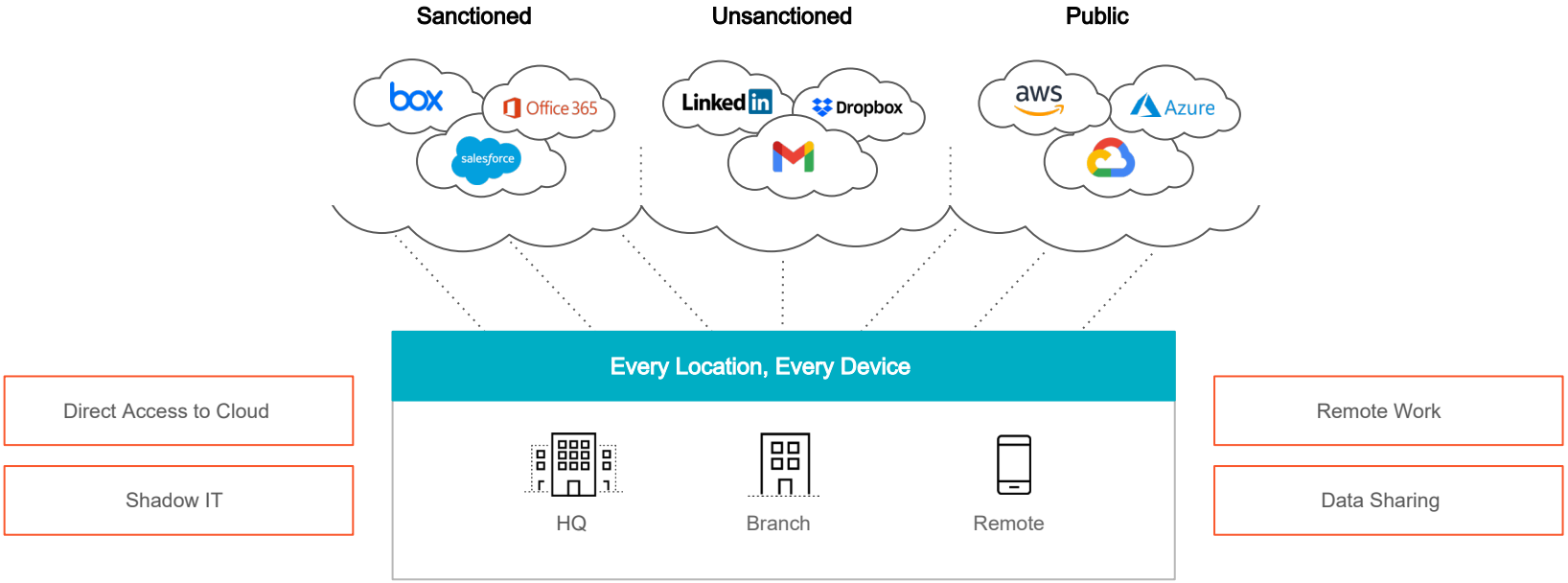
Real -time identity sync

Transition to cloud identity with ease


Securely enable
SaaS applications
with confidence.
paloalto
NETWORKS

SaaS Adoption is Elevating Cloud Security Risks

Cloud adoption brings shadow IT risks, excessive data exposure, and cloud threats



Existing solutions do a poor job at SaaS security.

Complex/costly | Can't scale | Poor security

Legacy architecture is complex and costly

Multiple, overlaid components with disjointed DLP policies

SaaS manual DB can't scale for SaaS hypergrowth

Current, manual approach can't keep up

Legacy CASB does not focus on security

Limited, disjointed security capabilities

The SaaS Application Landscape Continues to Evolve

In addition to best -in-class prevention, a risk -based security approach is needed for SaaS

Customers are required to allow use of 1000s of SaaS apps

The traditional allow -and-block method does not work for SaaS applications.

In addition to best -in-class prevention, A NEW risk-based security approach is needed

Current Best -of-Breed Protection

- Protection From Known & Unknown Threats
- Web Security

New Required Protection

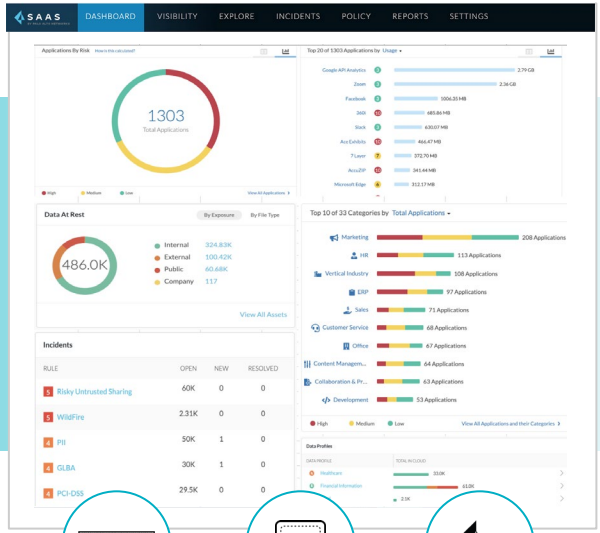
- Visibility & Control
  1000s of apps
- Regulate Shadow IT
- Meet Compliance Requirements
- Protect Data

Introducing The Only Integrated CASB
Without the Middleman

Automatically Keep Pace With The Explosion of SaaS Applications

Visibility for 15,000+ SaaS apps (5x increase)

Regulate shadow IT with granular risk -based control



NGFW

VM-Series

Prisma Access
(Aug '21)

Unified console for data protection across DLP and SaaS (inline & API controls)

Simple to deploy, faster time to value with lower TCO

To manage SaaS hypergrowth...

...we're delivering continuous discovery of new apps with crowdsourcing

Discover new apps with ML self -learning

Granular controls

Leverage community as sensors with cloud delivered App -ID

Palo Alto Networks now offers a simple, comprehensive, and cost -effective Data Protection Solution.

SaaS Security | Enterprise DLP

Fastest time -to -value and ease of deployment

Integrated Enterprise DLP and CASB services

Best -in -class CASB

Automatic visibility, granular inline and API controls

Cost effective

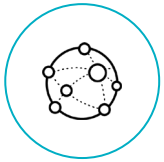
60% lower TCO

paloalto NETWORKS


Internet security
reinvented.
paloalto
NETWORKS

Securing the Internet Edge is Critical and Becoming Harder to Protect

The internet is a crucial business tool...



Web

Data

SaaS

...but attacks are getting harder to stop...

Malware attack

Phishing

C2 and data exfil

….and the edge is everywhere.

HQ

Hybrid

Mobile

Why the Internet Edge is Getting Harder to Secure

Modern web -based attacks are evading traditional URL filtering.

Thousands of new phishing URLs are created daily, and URL databases can't keep up.

Hackers Use Fake Google reCAPTCHA to Cloak Banking Malware

February 21, 2019
By Luke Leal

Malware Campaigns Come Back in Full Swing

September 9, 2020
Threat Intelligence Team

Attackers are increasingly using DNS to help carry out attacks.

Web access depends on DNS, yet typical web security solutions do not protect against the latest DNS -layer threats.

solarwinds

Half -a-Billion Enterprise Devices Exposed By DNS Rebinding

July 23, 2018
By Eduard Kovacs

Widespread DNS Hijacking Activity Targets Multiple Sectors

January 25, 2019
By Matt Dahl
Research and Threat Intel

Introducing industry -first innovations in Internet security.

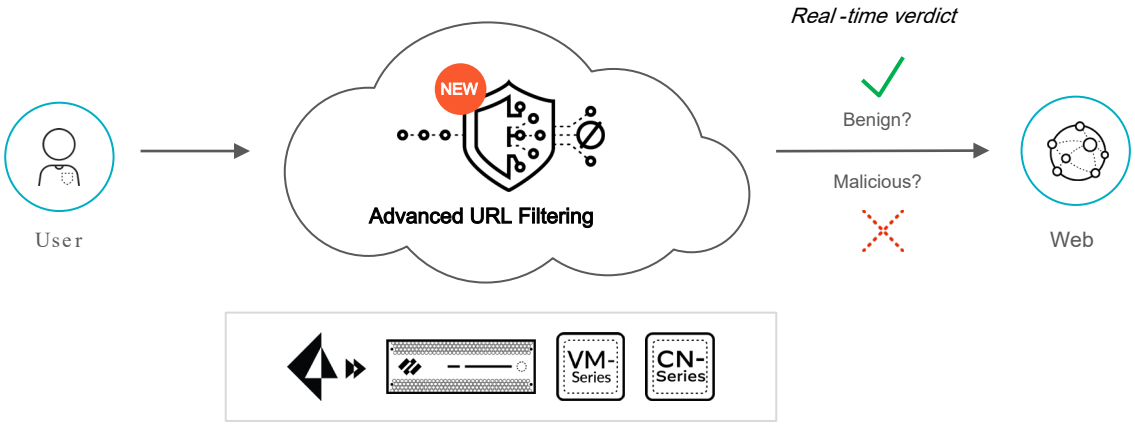
New Advanced URL Filtering service prevents modern web attacks with ML

New protections for the next - generation of advanced DNS - based attacks

Introducing Industry's First Inline ML -Powered Web Security

Prevent new, unknown attacks in real time with Advanced URL Filtering

Advanced URL Filtering



Benefits

Prevent **patient zero** by blocking **unknown malicious** URLs not in URL databases.

Defeat evasions of crawlers, including cloaking and **one-time -use links** .

Detection capabilities **improve over time** with more data, newer models.

Supported on PAN -OS 9.1+ software and Prisma Access (H2 '21)

Why is DNS Security so important?

DNS is now used in 80% of attacks

DNS runs everywhere and is a key tool for attackers

Web security alone doesn't secure DNS

Attackers Continue to Carry Out Attacks

Using DNS in New Ways

DNS is an overlooked attack vector; increasingly used to penetrate networks and steal data

Data Exfiltration

EXAMPLE TECHNIQUE

Ultra -slow tunneling

Growing in prevalence as a preferred technique.

Network Intrusion

EXAMPLE TECHNIQUE

DNS rebinding

Popular approach to launch lateral network attacks.

Domain Hijacking

EXAMPLE TECHNIQUE

Dangling DNS

Pervasive issue with growing cloud adoption.

DNS Security | Introducing Expanded Coverage

Stop new DNS attack types that others can't with the industry's most comprehensive DNS security

Existing Protections

- Known malicious domains
- High -risk domains
- DGA domains
- DNS tunneling

New Protections

- Fast-flux domains
- DNS rebinding attacks
- Dictionary DGA
- Dangling DNS attacks
- NSNX denial of service
- Prediction detection of new domains
- Ultra -slow DNS tunneling

Industry -first protections

Supported on PAN -OS 9.1+ software and Prisma Access (H2 '21)

DNS Security
is the right approach
to securing DNS.

Natively -integrated with NGFW and Prisma Access, requiring no change to DNS

Secures all DNS traffic, including unexpected DNS resolvers and malicious DNS servers

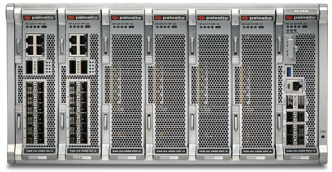
Comprehensive ML -powered protections for all types of DNS -based attacks


Secure the digital enterprise with ML-powered NGFW Platforms.
paloalto NETWORKS

Consistent Access & Security , Available Globally

From hyperscale data centers to branches and cloud

PA-5450



Best-in-class NGFW platform for DC and enterprise deployments

PA-400 Series

Secure the distributed enterprise with optimized price performance

Software Firewall

VM-Series CN-Series

5x performance increase and auto scaling for hyperscaling cloud and SP deployments

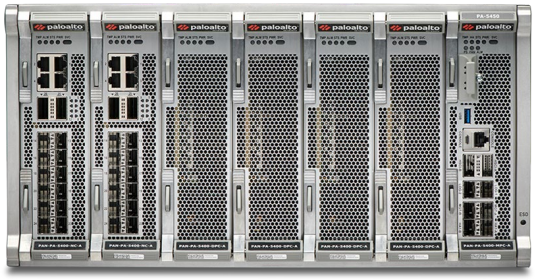
Consistent performance with any/all security services.

Unified policy and management.

Open and programmable platforms.

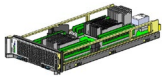
Introducing PA -5450 For Hyperscale Datacenter & Internet Edge

Enable high -performance Zero Trust Network Security at up to 70% lower TCO than competition*



PA-5450

Network Card



Data Processing Card

Up to **150 Gbps** of threat inspection

100M sessions

2X performance for Snort/Suricata signatures

25G*/100G interface

Optimized for ML inference performance

Benefits

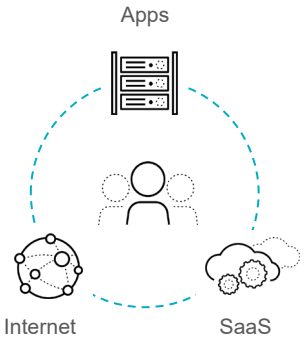
- **Stop latest threats** with ML -Powered NGFW, and consolidate security tools
- **Deliver incredible performance** with decryption and all security services
- **Scale security to match** your business needs using a modular design

* Compared to Cisco 9300 with 2 x SM -56 cards (128 Gbps NGFW)

PA-5450

Built for hyperscale DC, Internet edge, and campus segmentation deployments

Internet edge deployment

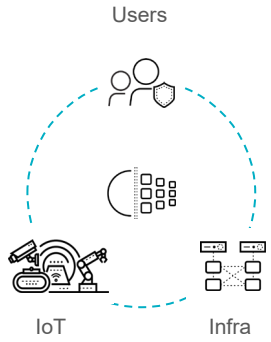


WF | TP | UF | DNS | DLP | SD-WAN | GP | SaaS

Hyperscale DC deployment

WF | TP | UF | DNS | DLP

Campus segmentation



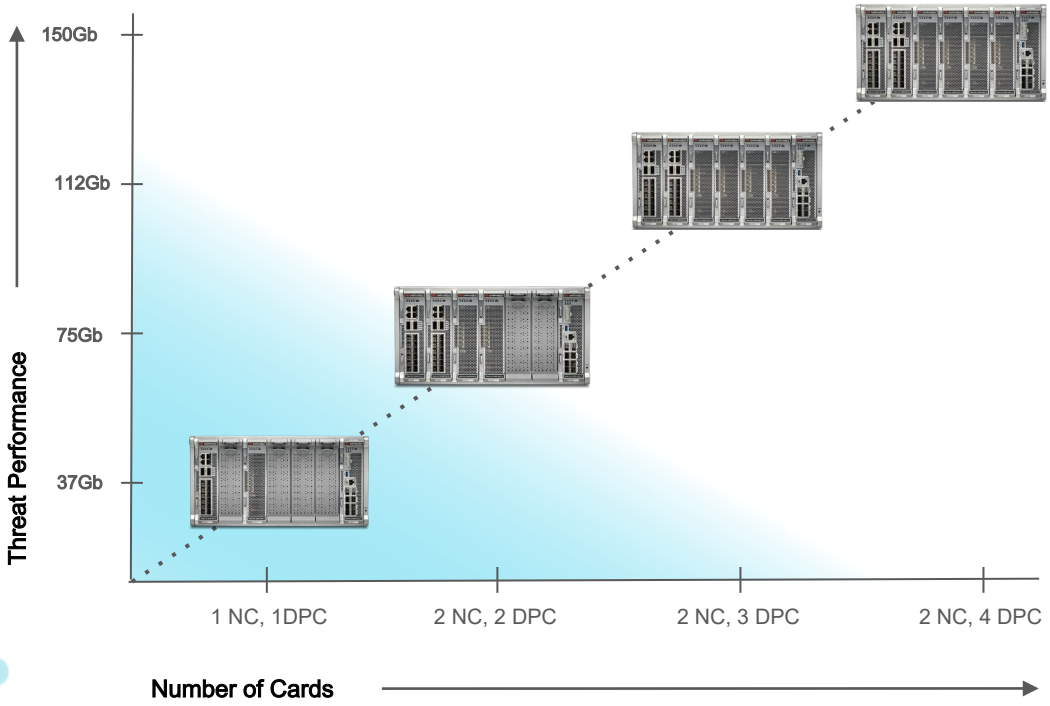
WF | TP | DNS | IoT | DLP

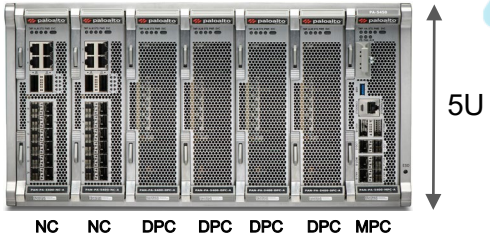
Prevention -first security.
Consolidate infrastructure.

Purpose -built for hyperscale.
Up to 70% TCO savings.

Context -aware segmentation.
Granular visibility of IoT.

Scaling Performance in a Modular 5U Appliance





Network Card (NC)

Data Processing Card (DPC)

Management Processing Card (MPC)

Introducing PA-400 Series For The Distributed Enterprise

Enable Zero Trust Network Security for your branches: Better security at the same price*

PA-410 PA-440 PA-450 PA-460

10x higher performance

Up to **5x** faster boot times

Redundant power

Noiseless operation with fanless design

Desktop form factor

NOTE: PA-410 general availability expected in Sep 2021

Benefits

- **Stop latest threats** with ML - Powered NGFW, in desktop form factor
- **Simplify operations** with zero touch provisioning — no need for specialized staff at branches
- **Cut servicing costs** with extremely resilient firewalls — no moving parts and dual power supplies

* When compared with Fortinet 60F, 80F and 100F appliances

Open and Programmable Platforms

Consistent experience for all hardware and software firewall form factors.

Programmable APIs and interfaces

XML and REST based APIs

New!

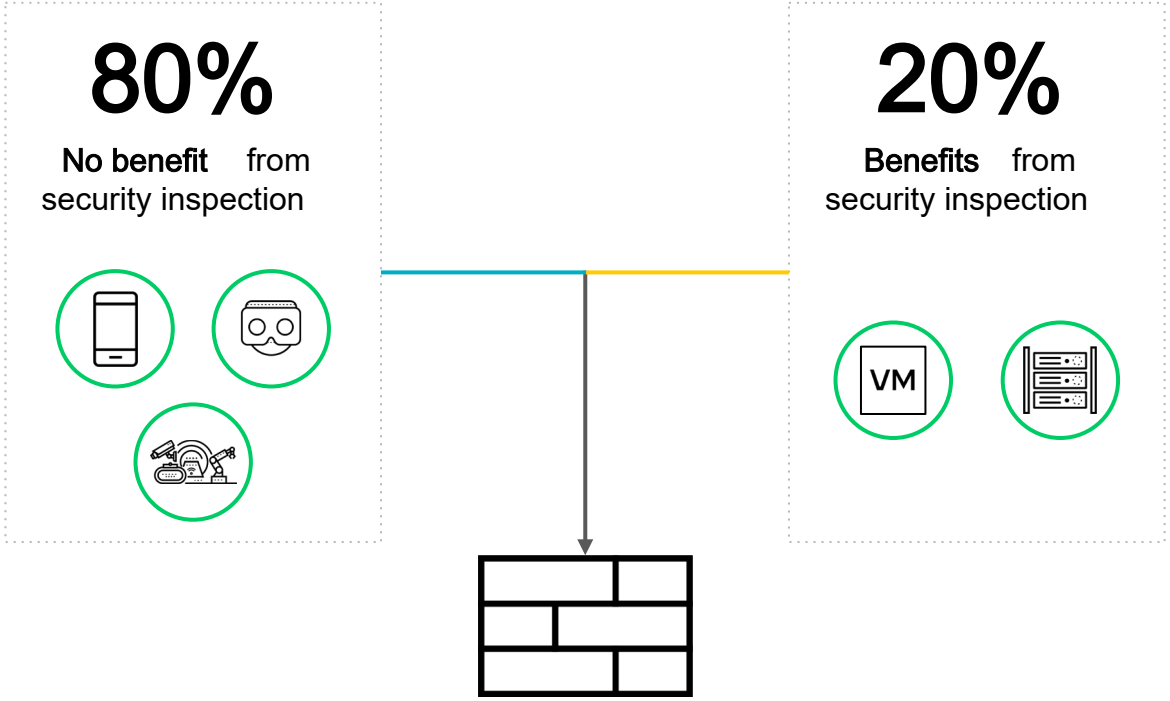
Standards -based Schema and Protocols

OpenConfig based configuration and telemetry interface (gNMI, gNOI)

VM -Series
Intelligent Traffic Offload Service

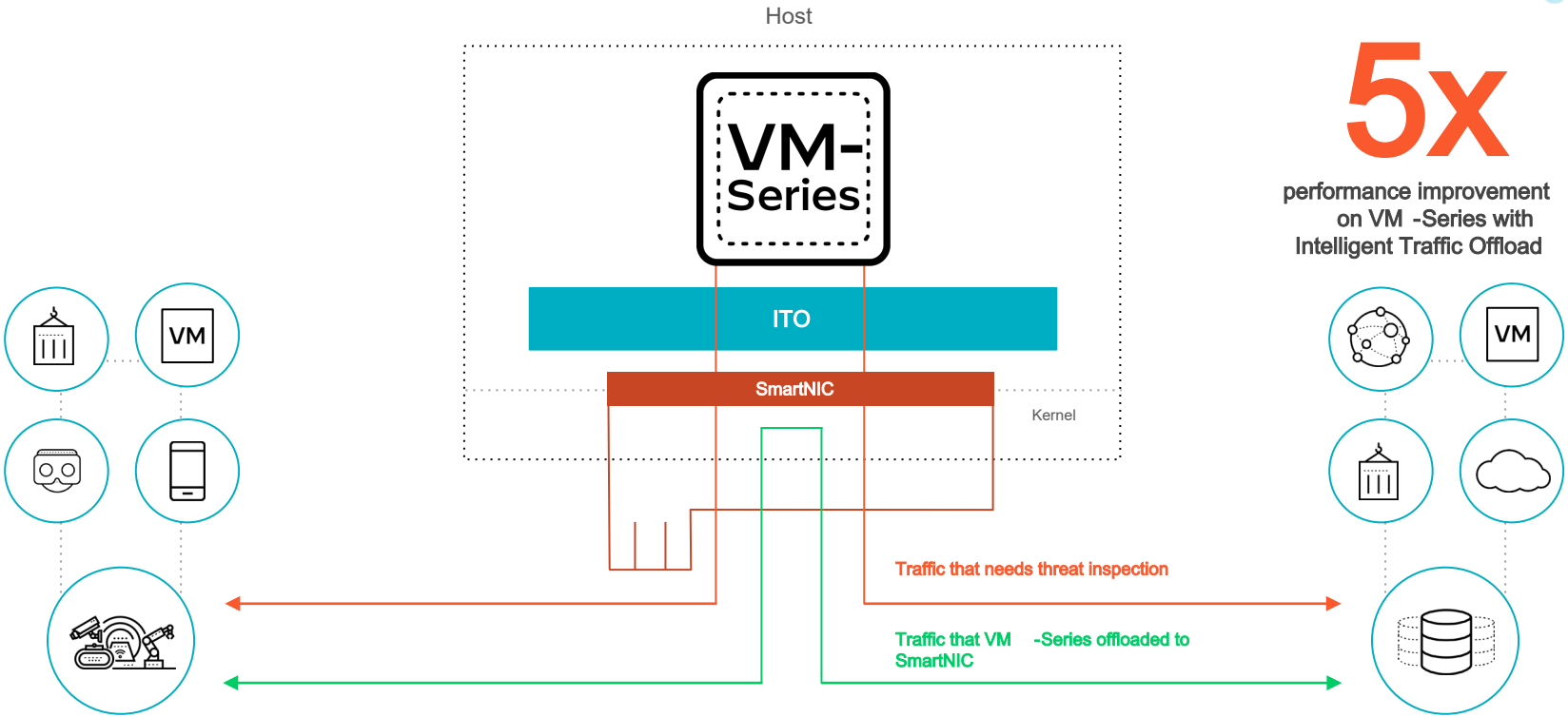
paloalto NETWORKS

Service Providers must compromise between security and cost



Firewall must be big enough to accommodate 100% of traffic

Intelligent Traffic Offload



5x

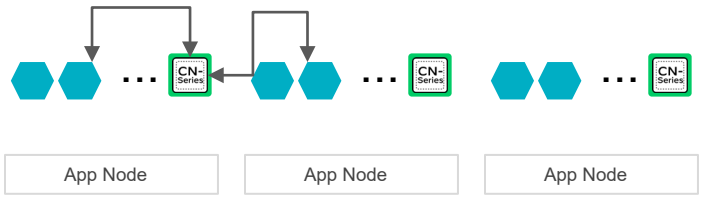
performance improvement on VM -Series with Intelligent Traffic Offload

CN-Series Updates

paloalto NETWORKS

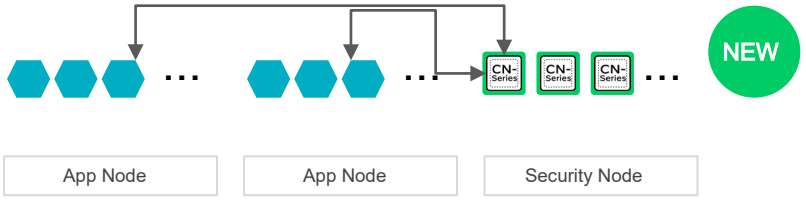
Flexible Deployment Options

Distributed Deployment (DaemonSet)



- **Reduce network latency** by implementing enforcement closer to the workloads
- **Node -based licensing** eliminates need to predict throughput and simplifies forecasting

Clustered Deployment (Kubernetes Service)



- Improve **utilization** , reduce **cost** , and increase **scale** with native K8s service -based deployment model
- **Autoscale** using native Kubernetes autoscale capabilities

Summary

New Innovations Aligned To 3 Zero Trust Network Security

Core Capabilities

Cloud Identity

Simplified identity controls for adopting Zero Trust

SaaS Security

Integrated CASB to keep pace with the SaaS explosion

Web Security

Industry -first inline ML to prevent unknown web attacks

ML-Powered NGFW Platforms

ML-Powered NGFW and Best -in-class security, to protect your entire enterprise

Context-Based Access

Make Access Safer

Global, Consistent Availability

Many New Capabilities in This Release

App -ID

- App -ID Cloud Engine
- SaaS Policy Recommendation

Identity

- Cloud Identity Engine

User -ID

- Group Mapping Centralization for Virtual System Hubs

Management

- Audit Tracking for Administrator Activity
- Persistent Uncommitted Changes on PAN -OS
- OpenConfig Support
  - Using standard models
  - gNMI protocol for configuration and streaming telemetry
  - gNOI for operational requests

SaaS Inline Security

- New Security Service to Secure SaaS Applications

Advanced URL Filtering

- New security service extends URL filtering to prevent evasive and targeted phishing and other web -based attacks

DNS Security

- New protections from emerging DNS attacks, including ultra -slow tunneling, dangling domains, and dictionary DGAs

Networking

- Aggregate Group Members on Multiple Cards
- Network Packet Broker
- Packet Diagnostics Resource Protection
- SD-WAN Support for AE and Layer 3 Subinterfaces

Panorama

- Authentication Enhancement for Onboarding Firewalls
- Scheduled Configuration Push to Managed Firewalls
- Unique Master Key for a Managed Firewall

Virtualization

- Intelligent Traffic Offload Service for VM -Series
- VM-Series Smart NIC integration
- CN-Series Cluster Mode deployments
- CN-Series Autoscale
- CN-Series performance enhancements

Mobile Infrastructure Security

- 5G Multi -Edge Security

And new hardware platforms PA -5450, PA -400 Series


Thank you.
paloalto
NETWORKS


Appendix

Network Packet Broker

paloalto NETWORKS

With PAN -OS 10.0, we had made Decryption on NGFW a lot easier...

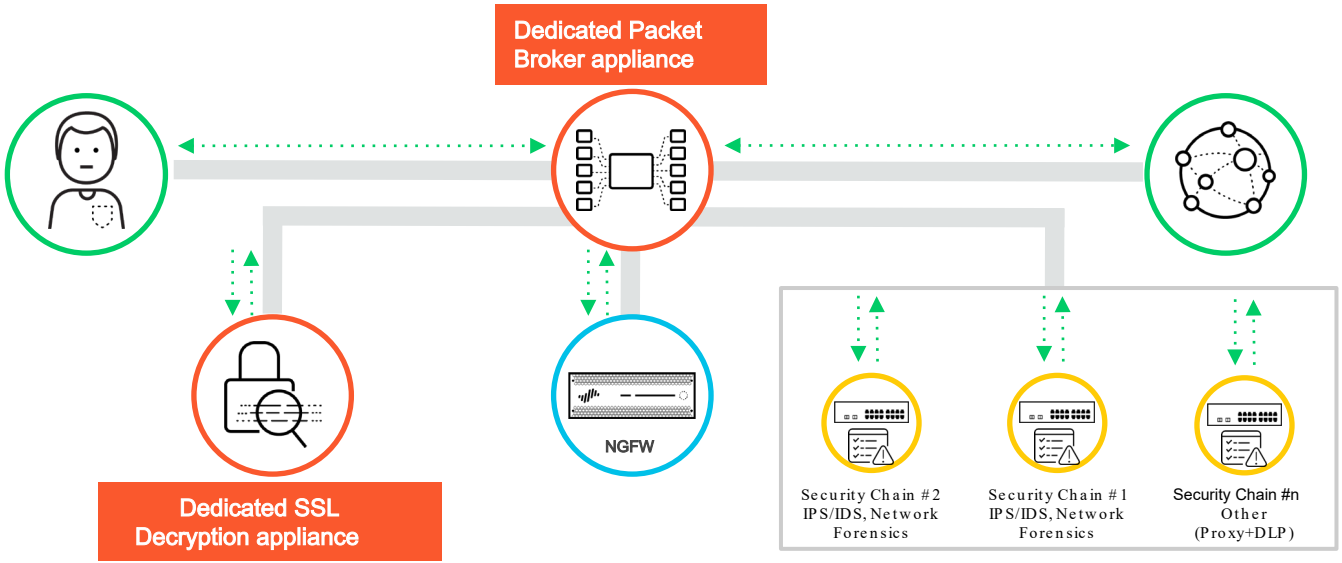
Customers no longer need to buy separate devices to Decrypt their traffic because:

- We added visibility into details of encrypted and decrypted traffic
- Added support for latest encryption protocols TLS 1.3 and HTTP/2
- Simplified troubleshooting
- Customers can leverage high Decryption performance with the new DPC's on PA-7000 series

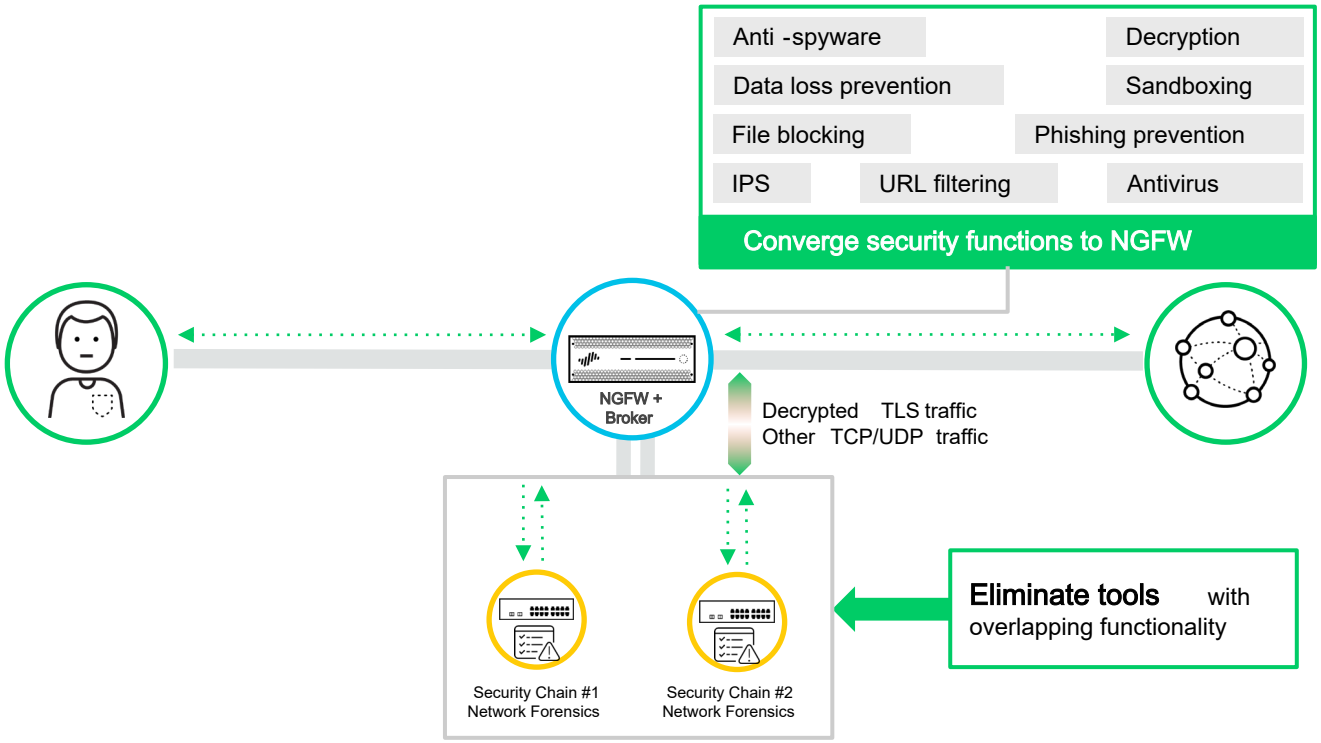
And now with PAN -OS 10.1..

Customers no longer need to purchase separate broker devices as well to send all traffic (decrypted TLS, encrypted TLS, non-TLS) to their security tools.

Problem| Complex, Multi -point Security Network



Simplify and Consolidate Decryption with Network Packet Broker



Scheduled Push

paloalto NETWORKS

Deploying Changes to Firewalls is Complex

Human Intervention Required

Additional Time Spent

Simplify Configuration Changes with Scheduled Push

Automate Changes

Automate routine changes using one -time or recurring schedules

No custom scripting required

Improve Efficiency

Reduce the need for human involvement at off -hours

Save time for deploying changes to Multi -VSYS firewalls

- Available for **all** NGFW form factors - Hardware, Software, Cloud Service
- Review and track changes with system logs
- **Requires** Panorama with OS 10.1+