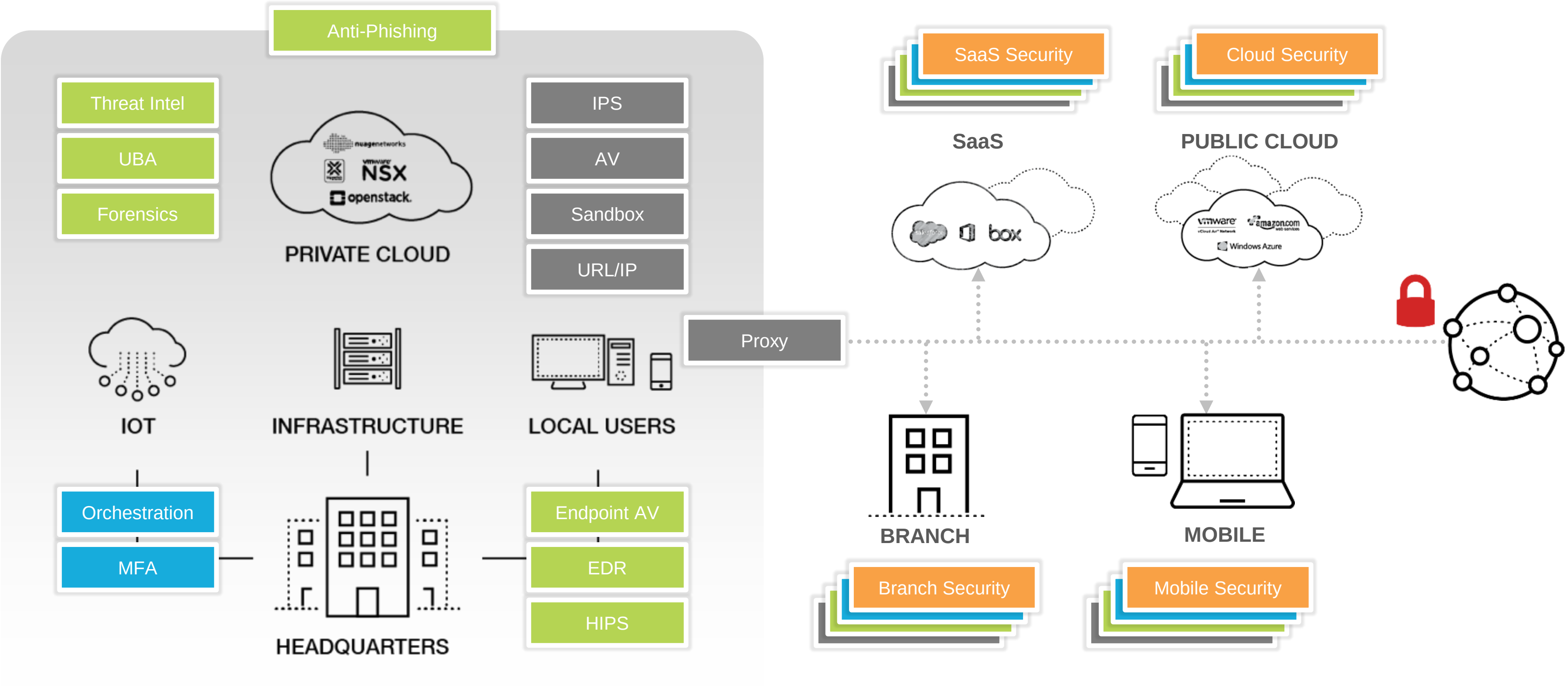
INTRODUCING PAN-OS 8.1

Timo Laue

SE EMEA

EXPANDING SECURITY CHALLENGE



Anti-Phishing

Threat Intel

UBA

Forensics

PRIVATE CLOUD

IPS

AV

Sandbox

URL/IP

IOT

INFRASTRUCTURE

LOCAL USERS

Proxy

Orchestration

MFA

HEADQUARTERS

Endpoint AV

EDR

HIPS

SaaS Security

SaaS

Cloud Security

PUBLIC CLOUD

BRANCH

Branch Security

MOBILE

Mobile Security

INEFFECTIVE LEGACY PRODUCTS

Limited Visibility

Lack of Automation

Difficult to Consume Innovations

A TRUE NGFW ….

Provides effective protections you can use

Automates tasks so you can focus on what matters

Consumes innovation quickly

A TRUE NGFW - BUILT FROM THE GROUND UP

NETWORK

USER

APPLICATION

CONTENT

ANALYTICS

COMPLETE CONTEXT

AUTOMATED PROTECTIONS

BUILT FOR INNOVATION

SECURITY THAT ACTUALLY WORKS

Single Pass Architecture…

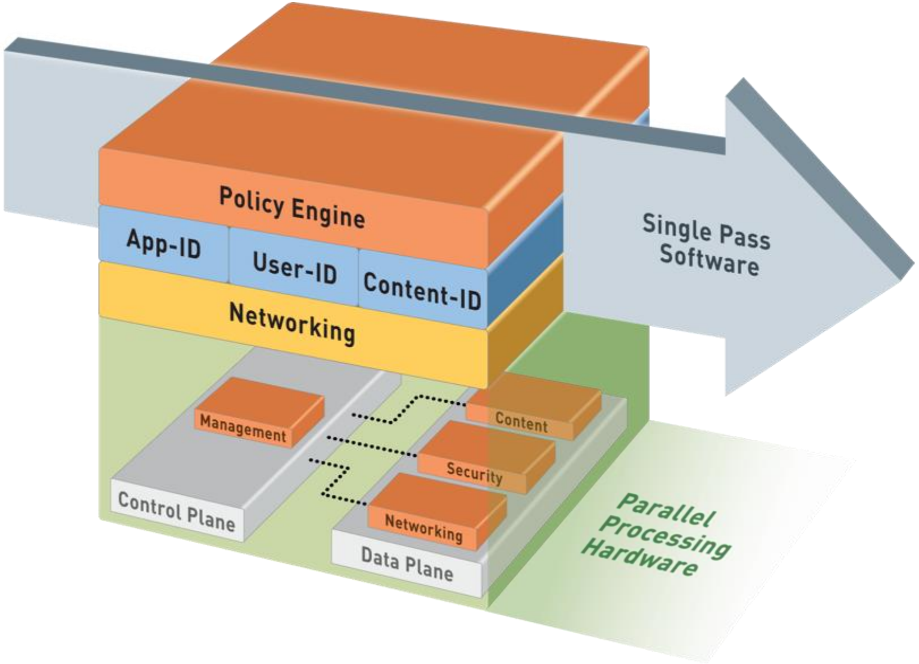
Palo Alto Networks: Single Pass Architecture

Single Pass (Palo Alto Networks)

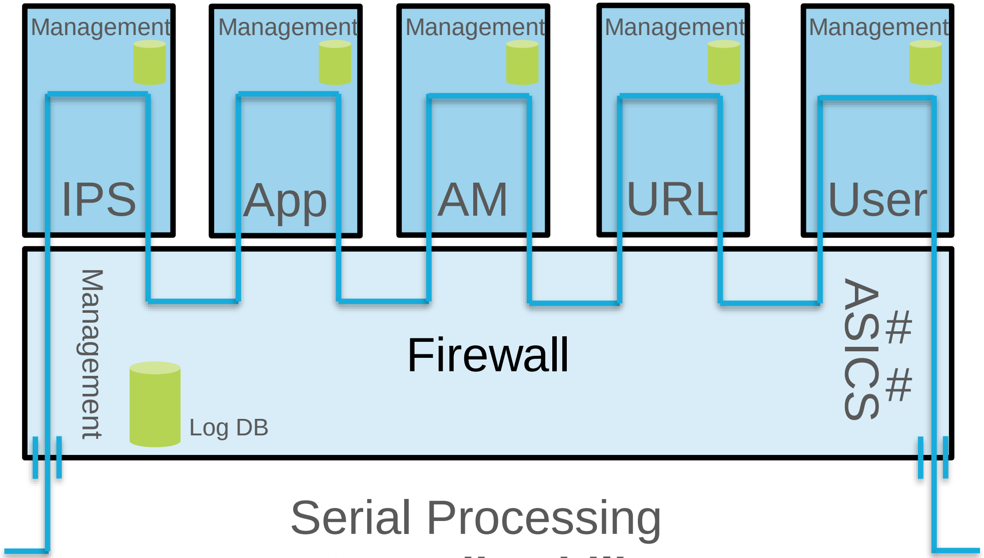
- Operations per packet
  - Traffic classification with App-ID
  - User/group mapping
  - Content scanning – threats, URLs, confidential data
- All in one Security Policy
- One OS Update for the Firewall

Parallel Processing

- Function-specific parallel processing hardware engines
- Separate data/control planes



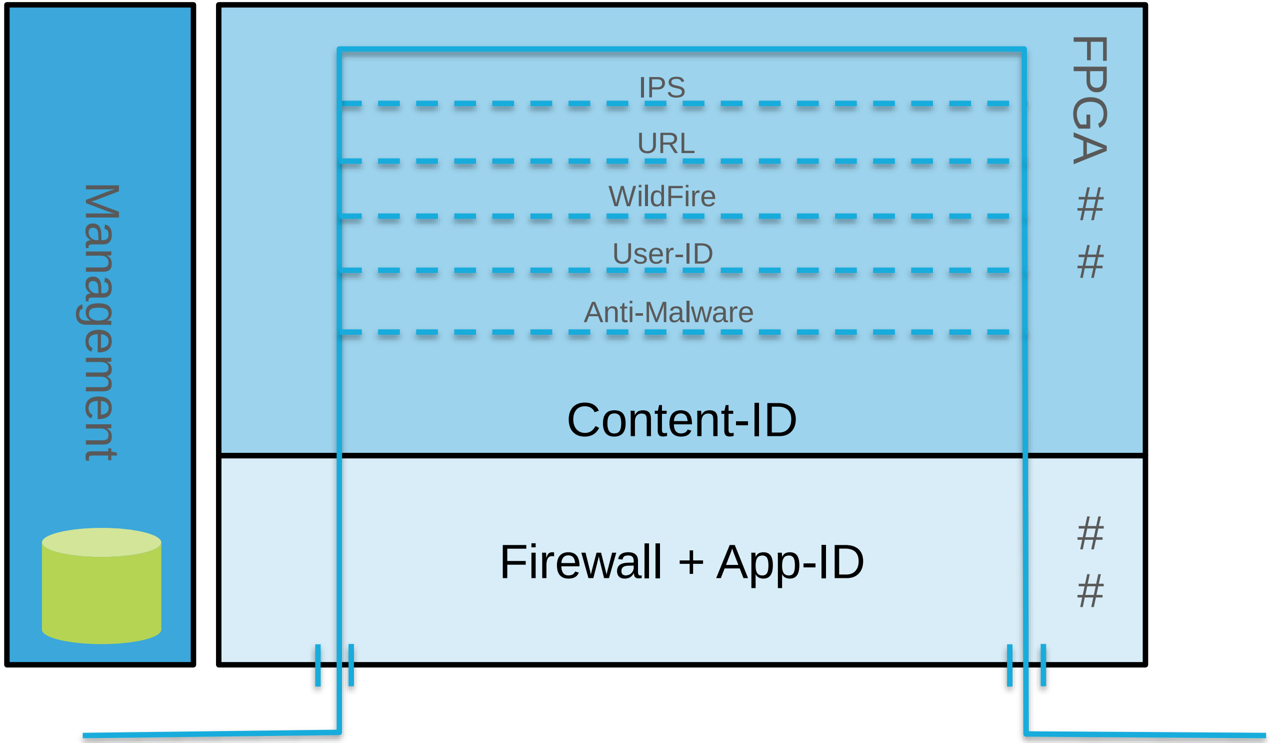
UTM Architecture



Serial Processing

NO Predictability

NGFW Architecture

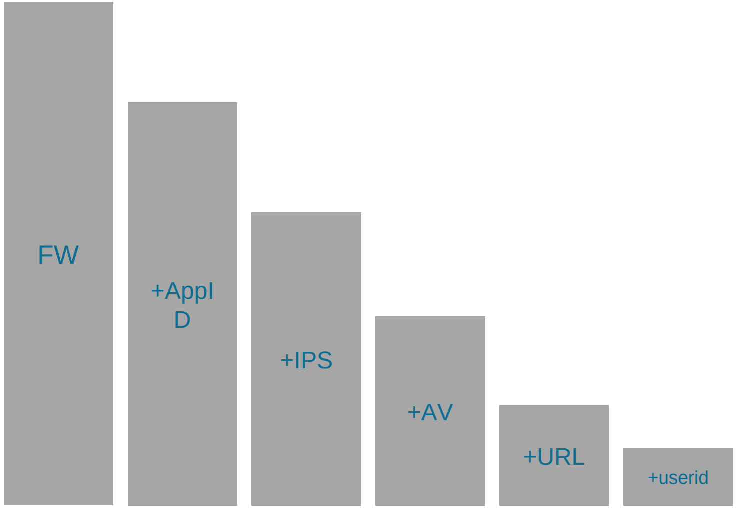


Single Pass Parallel Processing

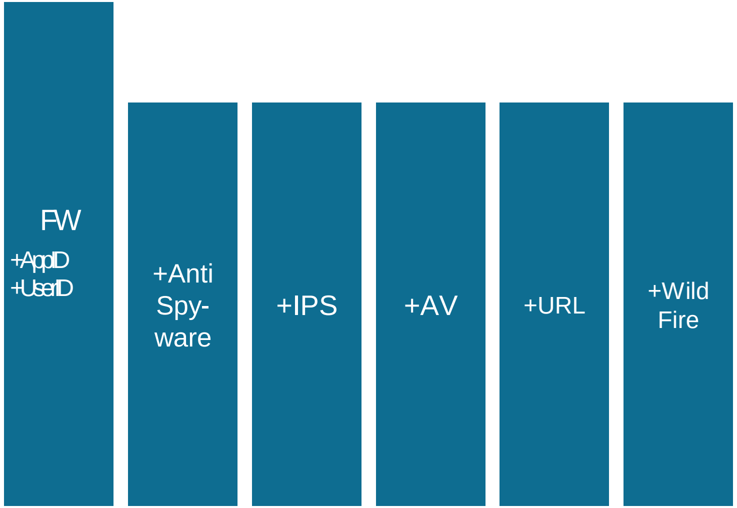
Predictability

Benefit of the Single Pass Architecture

High Performance = Low Risk

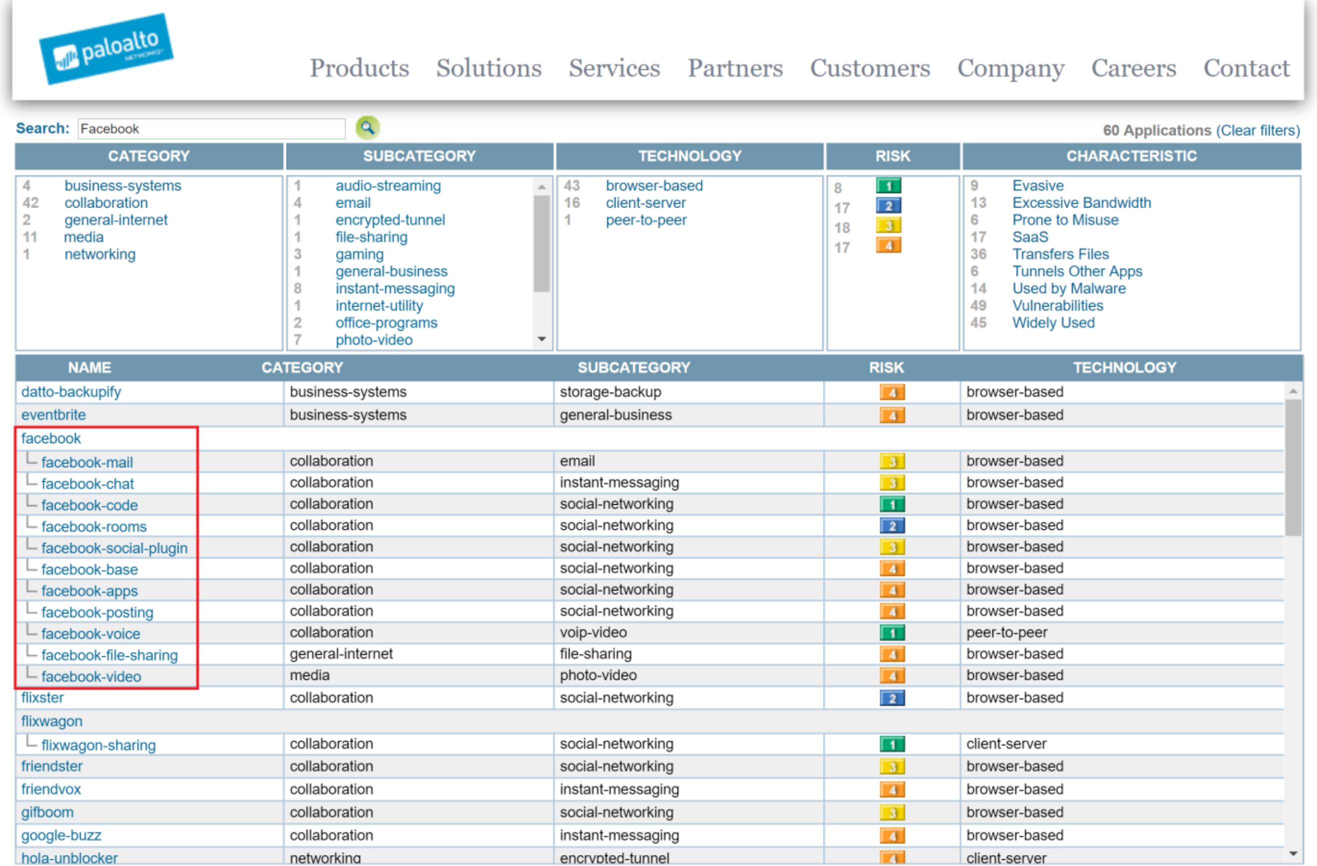


UTM - PROCESS BASED FW



NGFW – SP3 PARALLEL PROSSESING

App-ID: Example for Facebook



Products Solutions Services Partners Customers Company Careers Contact

Search: Facebook

60 Applications (Clear filters)

CATEGORY	SUBCATEGORY	TECHNOLOGY	RISK	CHARACTERISTIC
4 business-systems	1 audio-streaming	43 browser-based	8 1	9 Evasive
42 collaboration	4 email	16 client-server	17 2	13 Excessive Bandwidth
2 general-internet	1 encrypted-tunnel	1 peer-to-peer	18 3	6 Prone to Misuse
11 media	1 file-sharing		17 4	17 SaaS
1 networking	3 gaming			36 Transfers Files
	1 general-business			6 Tunnels Other Apps
	8 instant-messaging			14 Used by Malware
	1 internet-utility			49 Vulnerabilities
	2 office-programs			45 Widely Used
	7 photo-video			

NAME	CATEGORY	SUBCATEGORY	RISK	TECHNOLOGY
datto-backupify	business-systems	storage-backup	4	browser-based
eventbrite	business-systems	general-business	4	browser-based
facebook				
└ facebook-mail	collaboration	email	3	browser-based
└ facebook-chat	collaboration	instant-messaging	3	browser-based
└ facebook-code	collaboration	social-networking	1	browser-based
└ facebook-rooms	collaboration	social-networking	2	browser-based
└ facebook-social-plugin	collaboration	social-networking	3	browser-based
└ facebook-base	collaboration	social-networking	4	browser-based
└ facebook-apps	collaboration	social-networking	4	browser-based
└ facebook-posting	collaboration	social-networking	4	browser-based
└ facebook-voice	collaboration	voip-video	1	peer-to-peer
└ facebook-file-sharing	general-internet	file-sharing	4	browser-based
└ facebook-video	media	photo-video	4	browser-based
flixster	collaboration	social-networking	2	browser-based
flixwagon				
└ flixwagon-sharing	collaboration	social-networking	1	client-server
friendster	collaboration	social-networking	3	browser-based
friendvox	collaboration	instant-messaging	4	browser-based
gifboom	collaboration	social-networking	3	browser-based
google-buzz	collaboration	instant-messaging	4	browser-based
hola-unblocker	networking	encrypted-tunnel	4	client-server

PAN-OS 8.1: BOOST SECURITY EFFECTIVENESS & PERFORMANCE

Simplified app-based security

Improved efficiency & performance for management

Streamlined SSL decryption

Advanced threat detection and prevention

Performance boost for diverse deployments

PAN-OS 8.1: BOOST SECURITY EFFECTIVENESS & PERFORMANCE

Simplified app-based security

Improved efficiency & performance for management

Streamlined SSL decryption

Advanced threat detection and prevention

Performance boost for diverse deployments

UNNECESSARY RULES CREATE A SECURITY RISK

RULE	FROM	User-ID	TO	PORT	App-ID
12	…	…	…	…	…
13	Any	Software engineers	Source code servers	app-default	perforce
14	10.100.20.0/22	-	Source code servers	1666	-
15	Any	DB admins	SQL servers-dynamic group	app-default	mssql-db mssql-mon
16	Any	IT Admins	132.34.3.0/24	app-default	SSH

Can I retire legacy port-based rules without an outage?

Are any of these rules obsolete, leaving open entry points for an attacker?

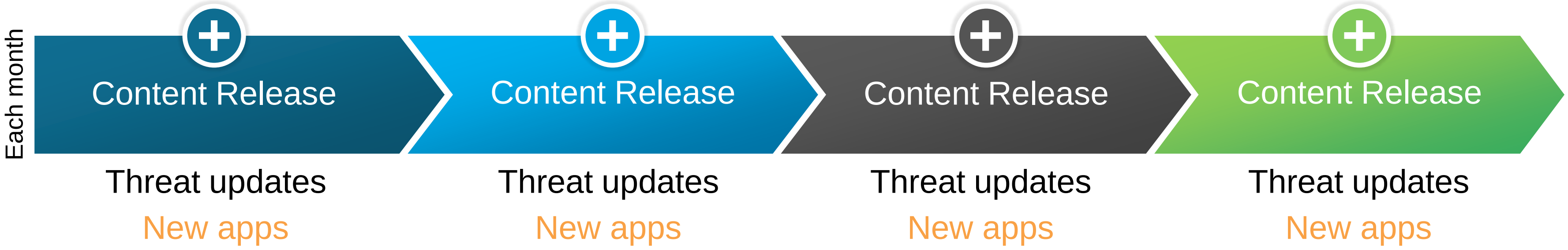
UNNECESSARY RULES CREATE A SECURITY RISK

RULE	FROM	User-ID	TO	PORT	App-ID	LAST HIT	HIT COUNT
12	…	…	…	…	…		
13	Any	Software engineers	Source code servers	app-default	perforce	30 seconds ago	1,832
~~14~~	~~10.100.20.0/22~~	~~-~~	~~Source code servers~~	~~1666~~	~~-~~	~~187 days ago~~	~~110~~
15	Any	DB admins	SQL servers-dynamic group	app-default	mssql-db mssql-mon	Yesterday	23
~~16~~	~~Any~~	~~IT Admins~~	~~132.34.3.0/24~~	~~app-default~~	~~SSH~~	~~1 year ago~~	~~392~~

Retire legacy rules confidently

Remove obsolete rules to reduce attack entry points

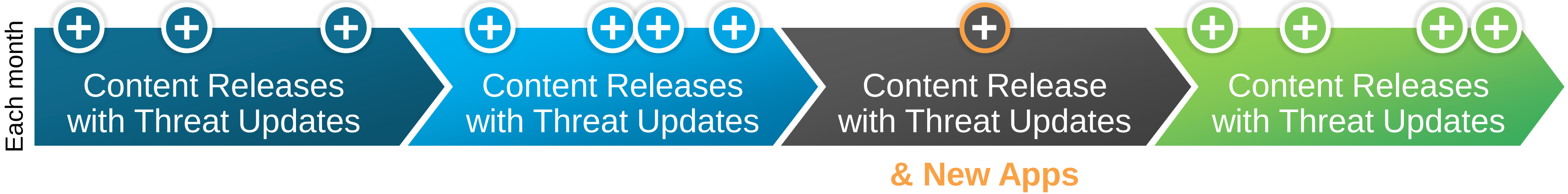
Before 8.1 -> ADOPTING THREAT UPDATES & NEW APPS



Adopt threat updates immediately, ensuring up-to-date protection

Adopting new apps in each update requires weekly policy review

After 8.1 EASIER ADOPTION OF THREAT UPDATES & NEW APPS



Each month

Content Releases with Threat Updates

Content Releases with Threat Updates

Content Release with Threat Updates

& New Apps

Content Releases with Threat Updates

Adopt threat updates immediately, ensuring up-to-date protection

To adopt new apps, perform policy updates once a month

Plan better using early announcement of new apps

EASIER ADOPTION OF THREAT UPDATES & NEW APPS

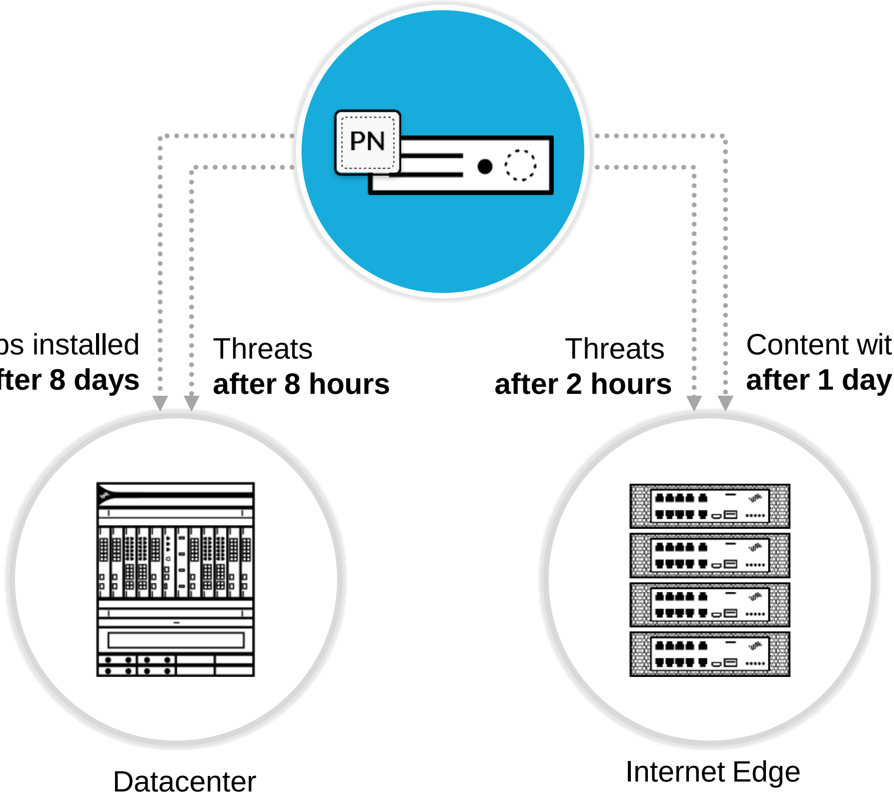
New Applications (11)

Risk	Name	Category	Subcategory	Technology	Depends On	Previously Identified As	Minimum PAN-OS Version
1	isilon-synciq	business-systems	storage-backup	client-server		unknown-tcp	5.0.0
2	jamf	business-systems	management	browser-based	apple-appstore, apple-push-notifications, itunes-base, ssl, web-browsing	ssl, web-browsing	5.0.0
1	matlab	general-internet	internet-utility	browser-based	ssl, web-browsing	ssl, web-browsing	5.0.0
1	paloalto-directory-sync	business-systems	management	client-server	ssl, web-browsing	ssl, web-browsing	5.0.0
2	tableau-downloading (functional)	general-internet	internet-utility	browser-based	ssl, tableau-base, web-browsing	tableau-base	5.0.0
1	tableau-editing (functional)	general-internet	internet-utility	browser-based	ssl, tableau-base, web-browsing	tableau-base	5.0.0
2	tableau-uploading (functional)	general-internet	internet-utility	client-server	ssl, tableau-base, web-browsing	tableau-base	5.0.0
2	yammer-downloading (functional)	collaboration	social-networking	browser-based	ssl, web-browsing, yammer-base	yammer-base	5.0.0
1	yammer-editing (functional)	collaboration	social-networking	browser-based	ssl, web-browsing, yammer-base	yammer-base	5.0.0
1	yammer-sharing (functional)	collaboration	social-networking	browser-based	ssl, web-browsing, yammer-base	yammer-base	5.0.0
2	yammer-uploading (functional)	collaboration	social-networking	browser-based	ssl, web-browsing, yammer-base	yammer-base	5.0.0

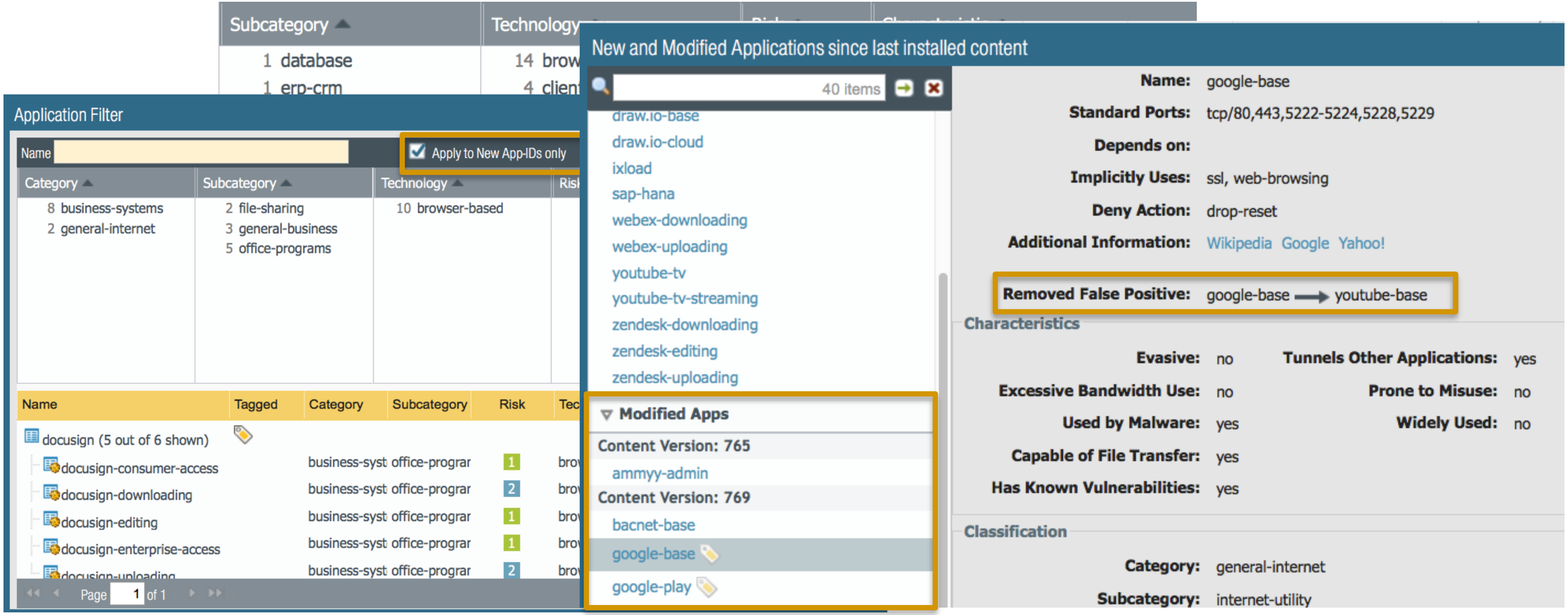
Modified Applications (8)

Risk	Name	Category	Subcategory	Technology	Type of Change	Change	Depends On	Minimum PAN-OS Version
1	opc-da	business-systems	management	client-server	expanded coverage	from msrpc to opc-da	msrpc	5.0.0
1	pnrp	networking	ip-protocol	peer-to-peer	expanded coverage	from unknown-udp to pnrp		5.0.0
2	progress-openedge	business-systems	database	client-server	expanded coverage	from unknown-tcp to progress-openedge		5.0.0
3	spotflux	networking	encrypted-tunnel	client-server	removed false positive	from spotflux to open-vpn	open-vpn	5.0.0
1	tableau-base	general-internet	internet-utility	client-server	expanded coverage	from ssl to tableau-base	ssl, web-browsing	5.0.0
3	teamviewer-base	networking	remote-access	client-server	expanded coverage	from unknown-udp to teamviewer-base	adobe-flash-socketpolicy-server, ssl, web-browsing	5.0.0
2	teamviewer-remote-control (functional)	networking	remote-access	client-server	expanded coverage	from teamviewer-base to teamviewer-remote-control	teamviewer-base	5.0.0
2	teamviewer-sharing (functional)	networking	remote-access	client-server	expanded coverage	from teamviewer-base to teamviewer-sharing	teamviewer-base	5.0.0

EASIER ADOPTION OF THREAT UPDATES & NEW APPS



EASIER ADOPTION OF NEW APPS



Subcategory	Technology
1 database	14 brow
1 erp-crm	4 client

Application Filter

Name: ☑ Apply to New App-IDs only

Category	Subcategory	Technology
8 business-systems	2 file-sharing	10 browser-based
2 general-internet	3 general-business	
	5 office-programs	

Name	Tagged	Category	Subcategory	Risk	Tec
docusign (5 out of 6 shown)					
docusign-consumer-access		business-syst	office-prograr	1	brov
docusign-downloading		business-syst	office-prograr	2	brov
docusign-editing		business-syst	office-prograr	1	brov
docusign-enterprise-access		business-syst	office-prograr	1	brov
docusign-uploading		business-syst	office-prograr	2	brov

Page 1 of 1

New and Modified Applications since last installed content

40 items

- draw.io-base
- draw.io-cloud
- ixload
- sap-hana
- webex-downloading
- webex-uploading
- youtube-tv
- youtube-tv-streaming
- zendesk-downloading
- zendesk-editing
- zendesk-uploading

Modified Apps

Content Version: 765

- ammyy-admin

Content Version: 769

- bacnet-base
- google-base
- google-play

Name: google-base
Standard Ports: tcp/80,443,5222-5224,5228,5229
Depends on:
Implicitly Uses: ssl, web-browsing
Deny Action: drop-reset
Additional Information: Wikipedia Google Yahoo!

Removed False Positive: google-base → youtube-base

Characteristics

Evasive:	no	**Tunnels Other Applications:**	yes
Excessive Bandwidth Use:	no	**Prone to Misuse:**	no
Used by Malware:	yes	**Widely Used:**	no
Capable of File Transfer:	yes		
Has Known Vulnerabilities:	yes		

Classification

Category: general-internet
Subcategory: internet-utility

Create rules for new App-IDs

Understand the effect of new and modified App-IDs on policy

Monitor new App-ID activity in ACC

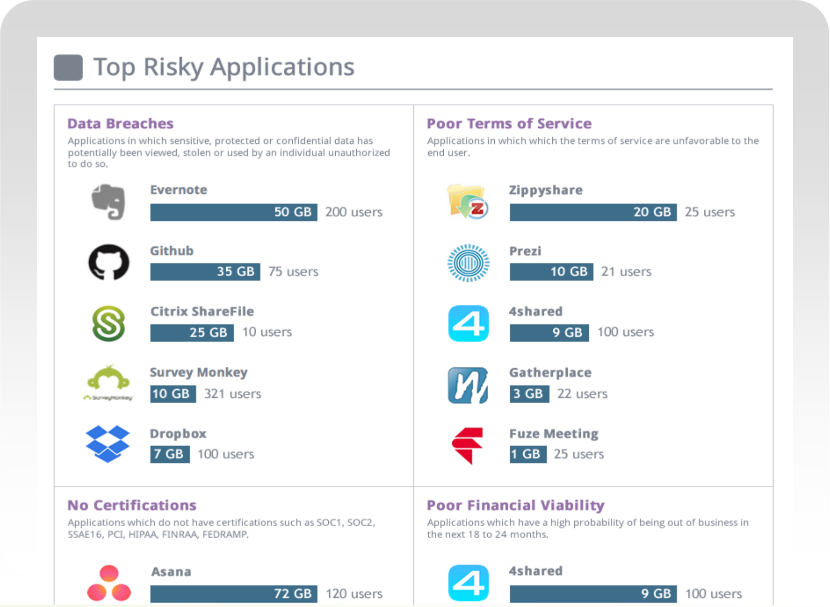
ENABLING SAFE USAGE OF SANCTIONED SAAS APPS

Application function

Application characteristics

Deep visibility

SaaS app characteristics



Top Risky Applications

Data Breaches

Applications in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an individual unauthorized to do so.

Evernote	50 GB	200 users
Github	35 GB	75 users
Citrix ShareFile	25 GB	10 users
Survey Monkey	10 GB	321 users
Dropbox	7 GB	100 users

Poor Terms of Service

Applications in which which the terms of service are unfavorable to the end user.

Zippyshare	20 GB	25 users
Prezi	10 GB	21 users
4shared	9 GB	100 users
Gatherplace	3 GB	22 users
Fuze Meeting	1 GB	25 users

No Certifications

Applications which do not have certifications such as SOC1, SOC2, SSAE16, PCI, HIPAA, FINRAA, FEDRAMP.

Asana	72 GB	120 users

Poor Financial Viability

Applications which have a high probability of being out of business in the next 18 to 24 months.

4shared	9 GB	100 users

NEW

ENABLING SAFE USAGE OF SANCTIONED SAAS APPS

AP

ENTERPRISE ACCOUNTS

✓ Office 365

Enterprise account

✓ G Suite

FREE / CONSUMER ACCOUNTS

✓ Office 365

Home / personal accounts

✓ Gmail

Same application, but are the risks different?

ENABLING SAFE USAGE OF SANCTIONED SAAS APPS

AP

ENTERPRISE ACCOUNTS

✓ Office 365

Enterprise account

✓ G Suite

FREE / CONSUMER ACCOUNTS

✗ Office 365

Home / personal accounts

✗ Gmail

NGFW inserts HTTP header in the request

SaaS app allows access to enterprise account	SaaS app denies access to free/consumer accounts

NETWORK SECURITY ENHANCEMENTS: FOCUS AREAS

Simplified app-based security

Improved efficiency & performance for management

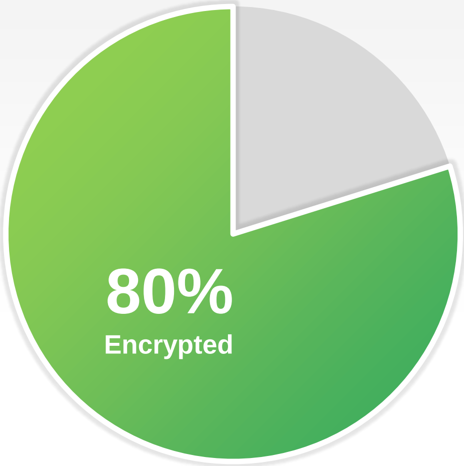
Streamlined SSL decryption

Advanced threat detection and prevention

Performance boost for diverse deployments

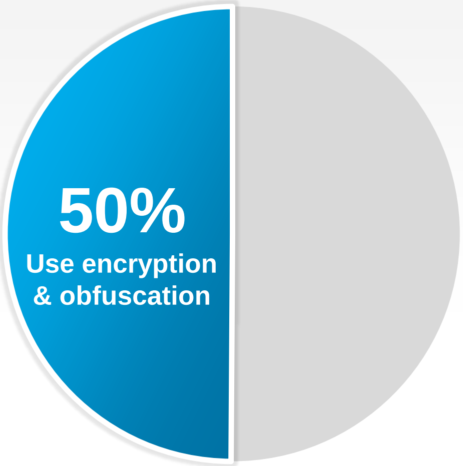
SECURING ENCRYPTED TRAFFIC IS A MUST

ENCRYPTED TRAFFIC, 2019



"Through 2019, more than 80% of enterprises' web traffic will be encrypted."

NEW MALWARE CAMPAIGNS, 2019



"During 2019, more than 50% of new malware campaigns will use various forms of encryption and obfuscation to conceal delivery, and to conceal ongoing communications, including data exfiltration."

Gartner's Predicts 2017: Network and Gateway Security, 13 December 2016
By Lawrence Orans, Adam Hils, Jeremy D'Hoinne, Eric Ahlm

DECRYPTION WITH MULTIPLE SECURITY DEVICES

Complex, expensive

Dedicated SSL offloaders

Unworkable

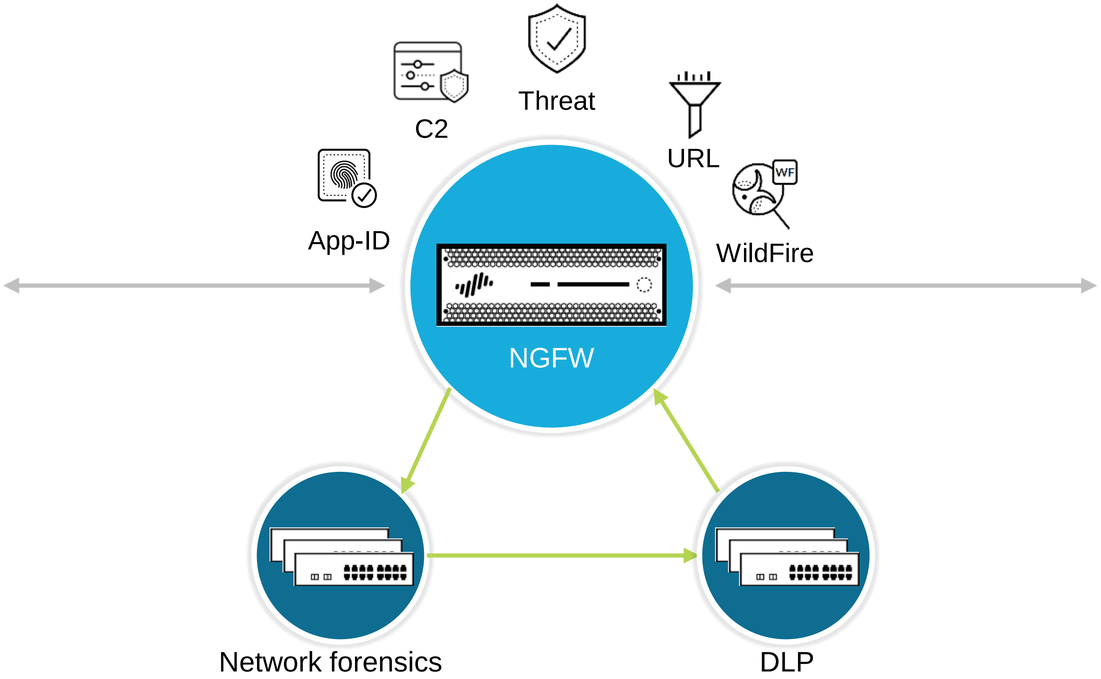
Decrypt, re-encrypt on every device

Detect-only mode*

Port-mirroring on the NGFW

** NGFW in enforcement mode, other devices in detect-only mode*

NGFW DECRYPTION BROKER: SIMPLE AND SECURE



Eliminate dedicated SSL offloaders, simplifying the network

Load balance decrypted flows across multiple stacks of security devices for add’l enforcement

Decrypt once, reducing latency

NETWORK SECURITY ENHANCEMENTS: FOCUS AREAS

Simplified app-based security

Improved efficiency & performance for management

Streamlined SSL decryption

Advanced threat detection and prevention

Performance boost for diverse deployments

TRENDS DRIVING NEW HARDWARE REQUIREMENTS

Increased encrypted traffic

Attacks requiring threat prevention

Increased throughput needs

NEW HARDWARE FOR HIGH-PERFORMANCE INTERNET EDGE

PA-3200 Series

PA-3220
5.0 Gbps App-ID
2.2 Gbps threat

PA-3250
6.3 Gbps App-ID
3.0 Gbps threat

PA-3260
8.8 Gbps App-ID
4.7 Gbps threat

- ✓ **Up to 5x performance increase**
- ✓ **Front-to-back cooling**
- ✓ **Interface speeds up to 40G for flexible connectivity**
- ✓ **Up to 7x decryption performance increase**
- ✓ **Up to 20x decryption session capacity increase**

CONSISTENT SECURITY FOR INDUSTRIAL DEPLOYMENTS

Water Utilities

Electric Transmission & Distribution

Oil & Gas

PA-220R

Manufacturing

Transportation

Power Generation

- Extended operating range for temperature
- Certified for industrial use in harsh environments
- Fan-less design, no moving parts for higher reliability
- Prevention of known and unknown threats, including ICS-specific threats
- Range of ICS / SCADA App-IDs supported with PAN-OS
- High availability and dual DC power supplies for redundancy

NEW HARDWARE FOR HIGH-PERFORMANCE MOBILE NETWORKS

Mobile Network Deployments

PA-5280

68 Gbps App-ID
29 Gbps threat
64 M sessions

LTE-IoT Security

- ✓ **100G Interfaces, high performance and session count**
- ✓ **GTP packet inspection (GTP-U and GTP-C)**
- ✓ **SCTP, SS7, Diameter signaling traffic inspection**
- ✓ **Supports deployments across key mobile network use cases**
- ✓ **Certified for use in service provider datacenters**
- ✓ **High availability and dual power supplies for redundancy**

NETWORK SECURITY ENHANCEMENTS: FOCUS AREAS

Simplified app-based security

Improved efficiency & performance for management

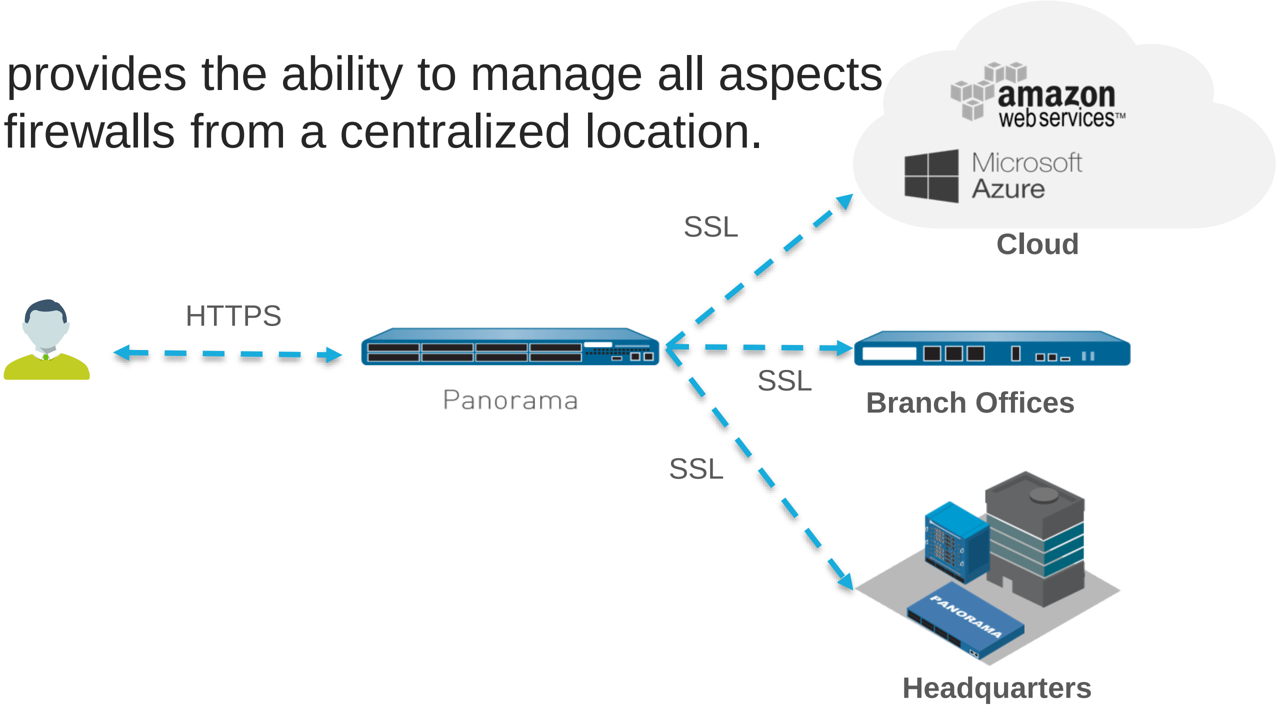
Streamlined SSL decryption

Advanced threat detection and prevention

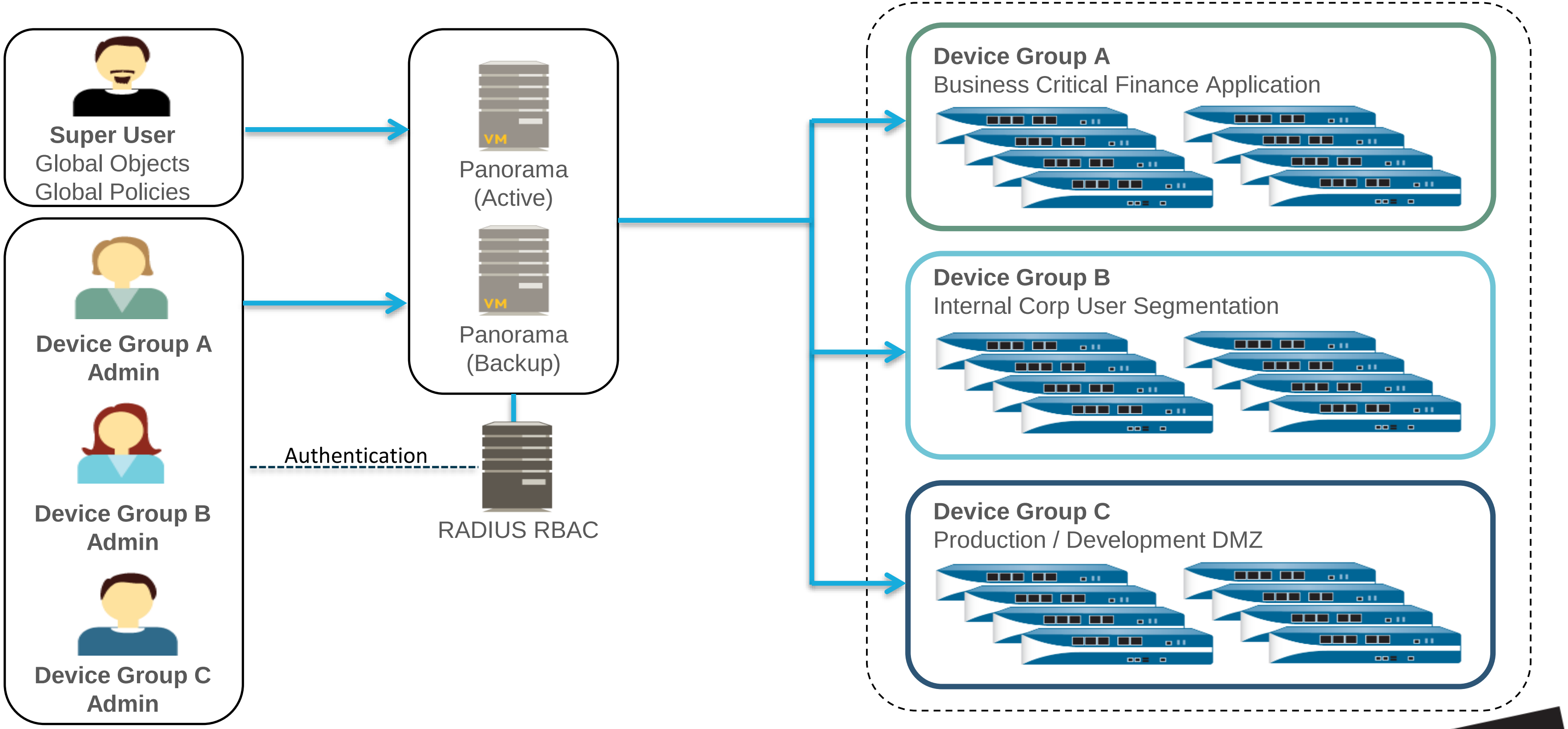
Performance boost for diverse deployments

Panorama

- Panorama is the central management Platform for our NGFW
- Panorama provides the ability to manage all aspects of multiple firewalls from a centralized location.



Panorama: Role Based Administration & Segmentation



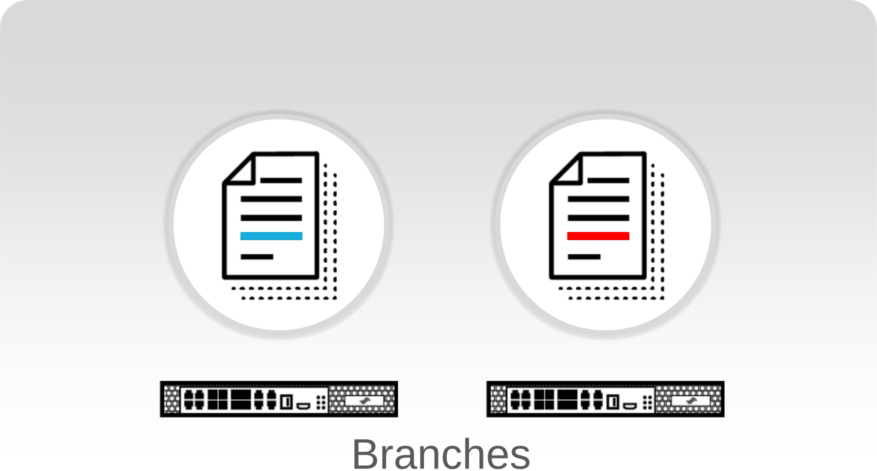
MANAGEABILITY

Simplifying management of large deployments

Proactive monitoring and alerting

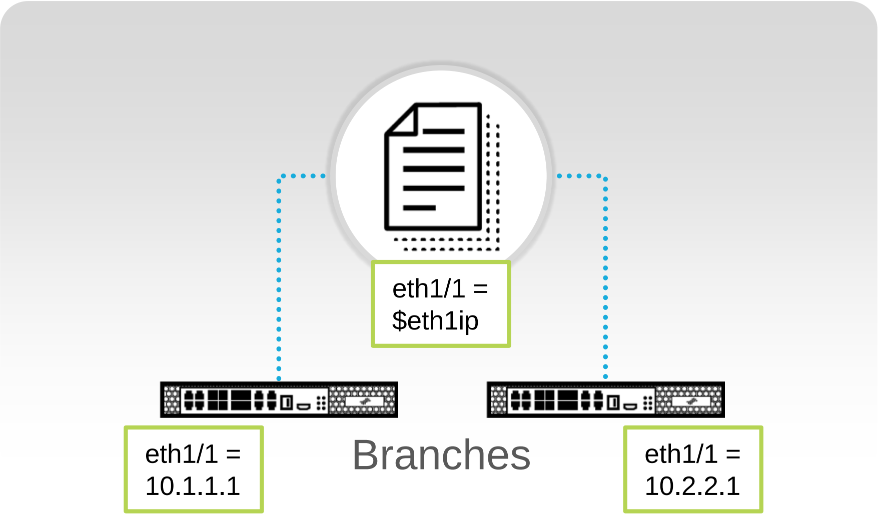
High-performance management

LARGE SCALE CONFIG MANAGEMENT IS COMPLEX



Minor differences complicate centralized configuration

SIMPLIFYING LARGE SCALE CONFIG MANAGEMENT



Reuse configuration with templates,
account for differences with variables

DIAGNOSING FIREWALL UTILIZATION CHANGES IS HARD

!

Track important metrics over time

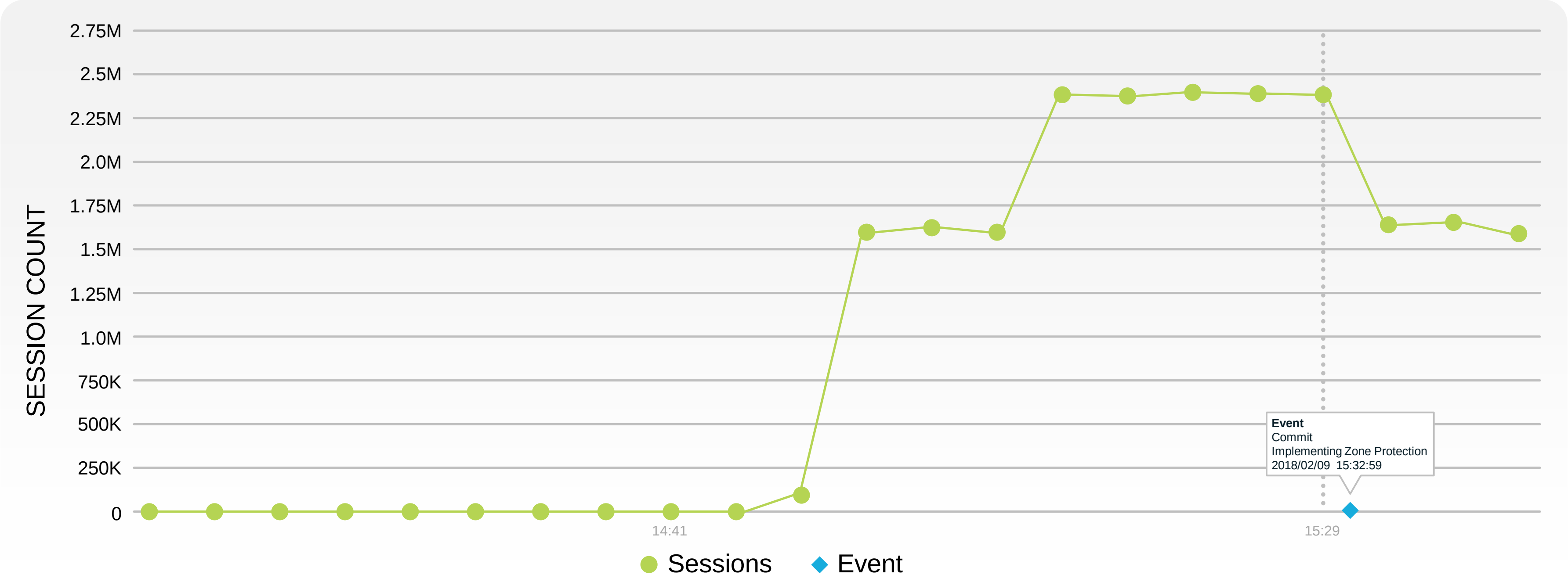
Identify when metrics exceed baseline

Diagnose the cause of the metrics’ change

REACTIVE

MANUAL

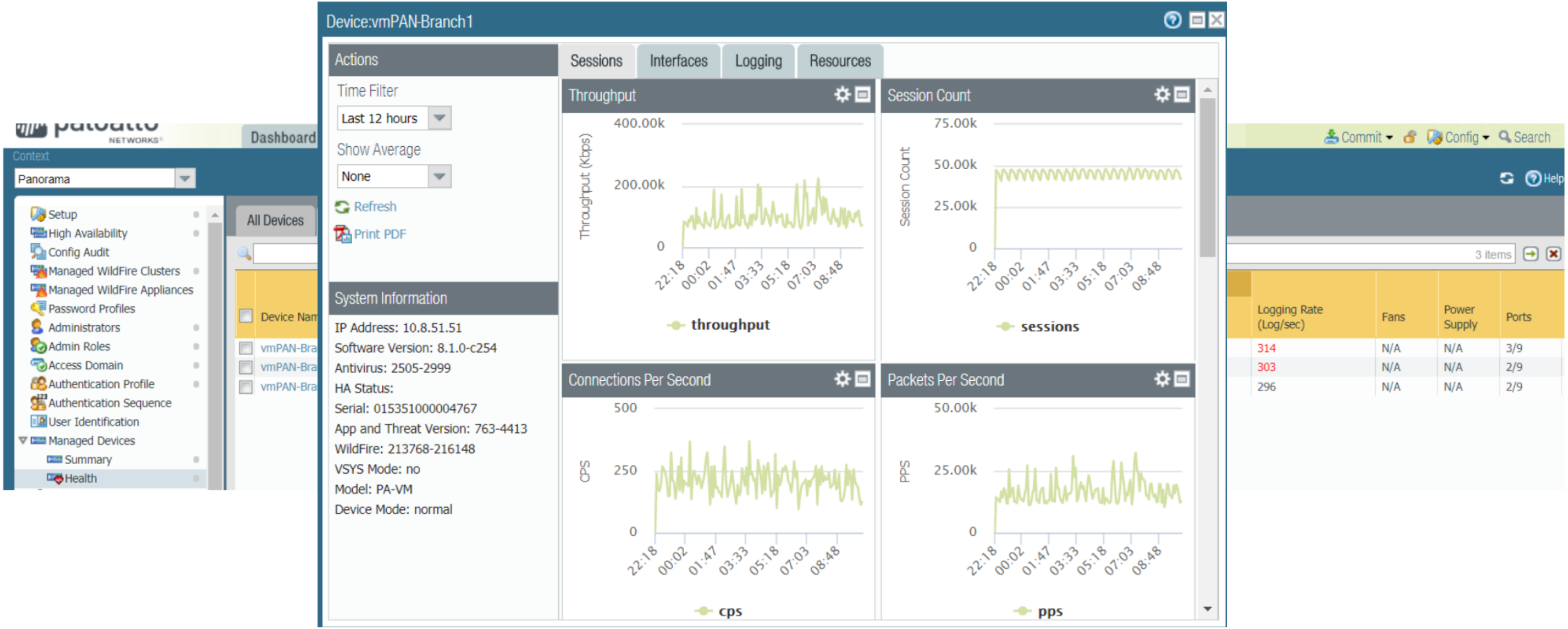
PROACTIVE DEVICE HEALTH AND METRICS MONITORING



Understand baseline usage and get notified of deviations

Correlate device resource utilization with config changes and system events

PROACTIVE DEVICE HEALTH AND METRICS MONITORING



Time Filter: Last 12 hours

Show Average: None

System Information

IP Address: 10.8.51.51
Software Version: 8.1.0-c254
Antivirus: 2505-2999
HA Status:
Serial: 015351000004767
App and Threat Version: 763-4413
WildFire: 213768-216148
VSYS Mode: no
Model: PA-VM
Device Mode: normal

Device Nam	Logging Rate (Log/sec)	Fans	Power Supply	Ports
vmPAN-Bra	314	N/A	N/A	3/9
vmPAN-Bra	303	N/A	N/A	2/9
vmPAN-Bra	296	N/A	N/A	2/9

NEED FOR HIGH-PERFORMANCE MANAGEMENT

Responsiveness and user experience

Visibility into large amounts of data

Managing networks at scale

NEW M-SERIES FOR HIGH-PERFORMANCE MANAGEMENT

M-200

M-600

✓ **Improved responsiveness with faster CPU and more memory**

✓ **Redundancy with dual power supplies**

✓ **Twice the log ingestion rate** means better scalability of logging infrastructure

✓ **Better serviceability with field-replaceable system drives**

Some other changes and features in 8.1...

- ✓ VM-Series Firewall on Google Cloud Platform
- ✓ Configuration Capacity Improvements
- ✓ Optimized Split Tunneling for GlobalProtect
- ✓ Tunnel Content Inspection
- ✓ FQDN IKE Gateways / Dynamic IP Destination NAT
- ✓ Content Update Revert from Panorama

NETWORK SECURITY ENHANCEMENTS: FOCUS AREAS

Simplified app-based security

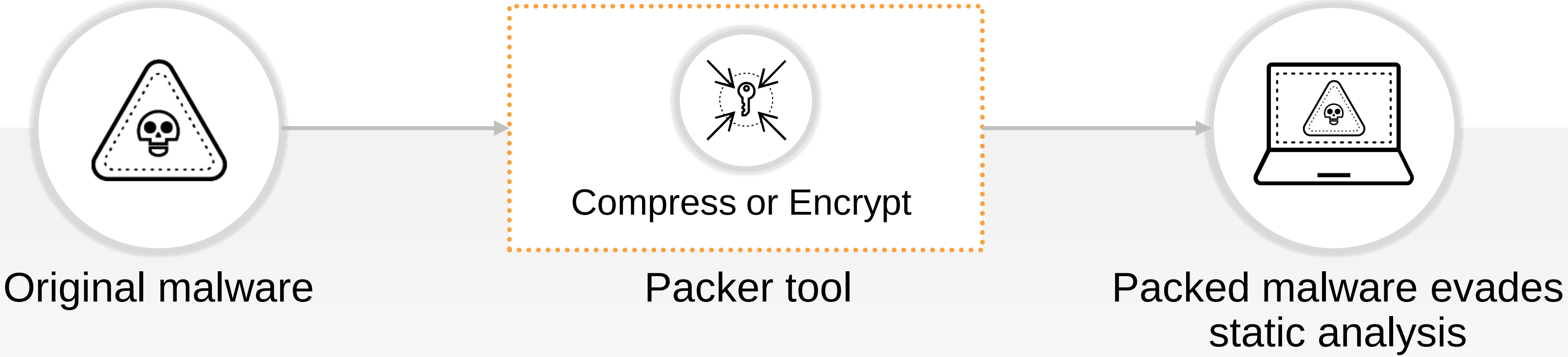
Improved efficiency & performance for management

Streamlined SSL decryption

Advanced threat detection and prevention

Performance boost for diverse deployments

MALWARE CAN AVOID ANALYSIS AND DETECTION



Compress or Encrypt

Original malware

Packer tool

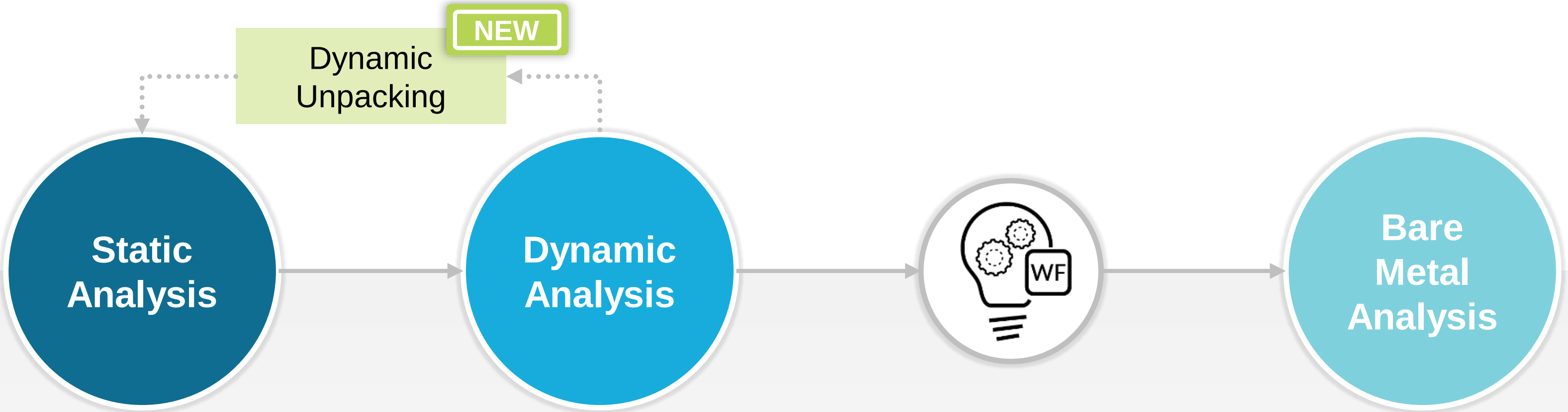
Packed malware evades static analysis

Attackers use packer tools to avoid malware analysis

Static analysis and machine learning alone are not enough

Defeating packing requires complementary analysis techniques

ADVANCING DETECTION: NEW WILDFIRE MODULE



NEW

Dynamic Unpacking

Static Analysis

Dynamic Analysis

Bare Metal Analysis

Detect known exploits, malware, and variants

NEW

- Memory analysis
- Machine learning
- File anomalies
- Malicious patterns
- Known malicious code

Find new zero-day exploits & malware through execution

- Custom hypervisor
- Behavioral scoring
- Multi-version analysis

Heuristic Engine
Steer evasive malware to bare metal

Identify VM-aware threats using hardware systems

- Full dynamic analysis
- Real desktop hardware
- No virtual environment
- No hypervisor

PREVENTION EVERYWHERE

SMB

7Z RAR

New analysis environments

Improved detection of malware targeting Linux servers and IoT devices

Prevent malware spreading inside the network

Detect and prevent zero-day malware moving freely inside the network with new SMB protocol support

More file types

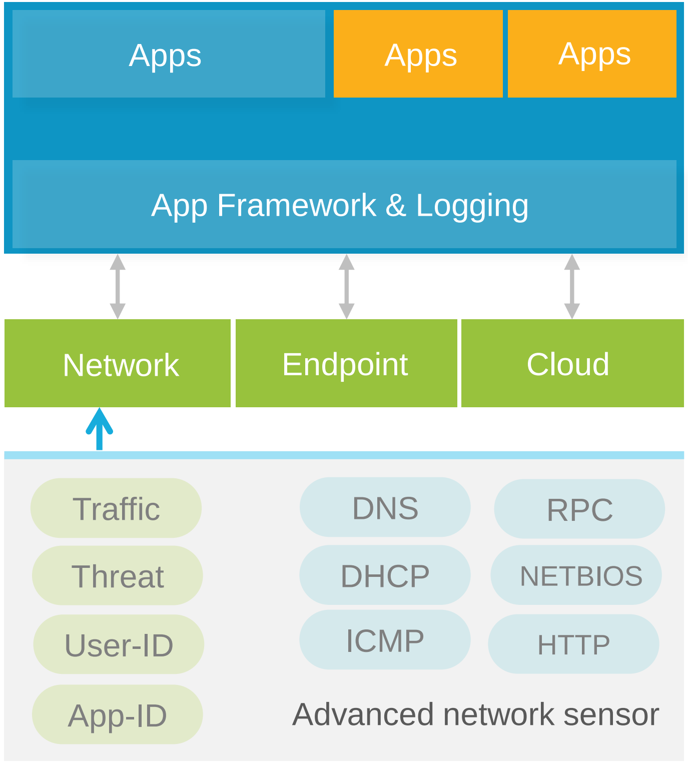
Find malware hiding in less common file archive formats, including RAR and 7zip

DATA FOR ANALYTICS: ENHANCED APPLICATION LOGS

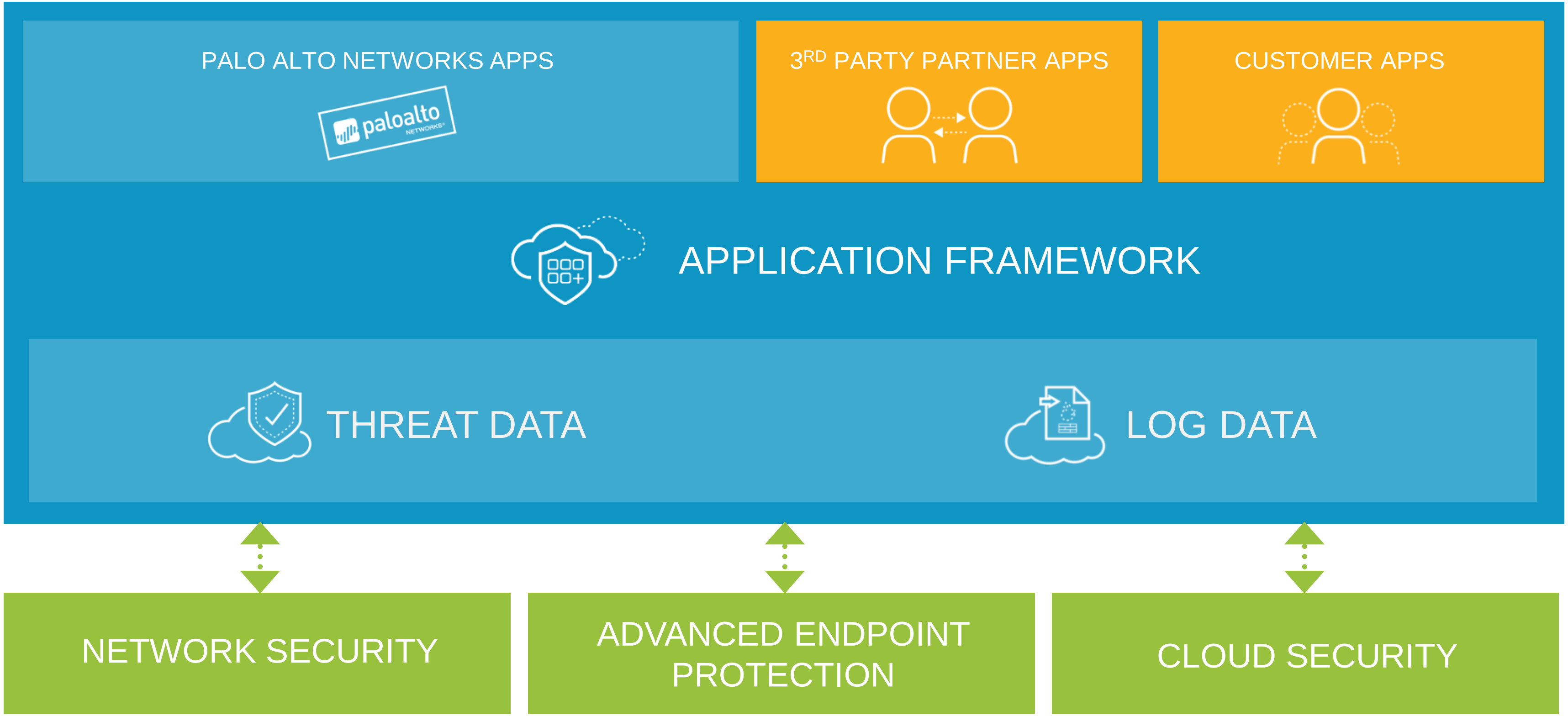
Evolves the next-generation firewall into an advanced network sensor to collect rich data for analytics with Enhanced Application Logs

Enables Magnifier and Application Framework apps to use enhanced data for advanced analytics

Content-based update to expand or modify the data that is collected from the Next-Gen Firewall



PALO ALTO NETWORKS APPLICATION FRAMEWORK



PALO ALTO NETWORKS APPS

3RD PARTY PARTNER APPS

CUSTOMER APPS

APPLICATION FRAMEWORK

THREAT DATA

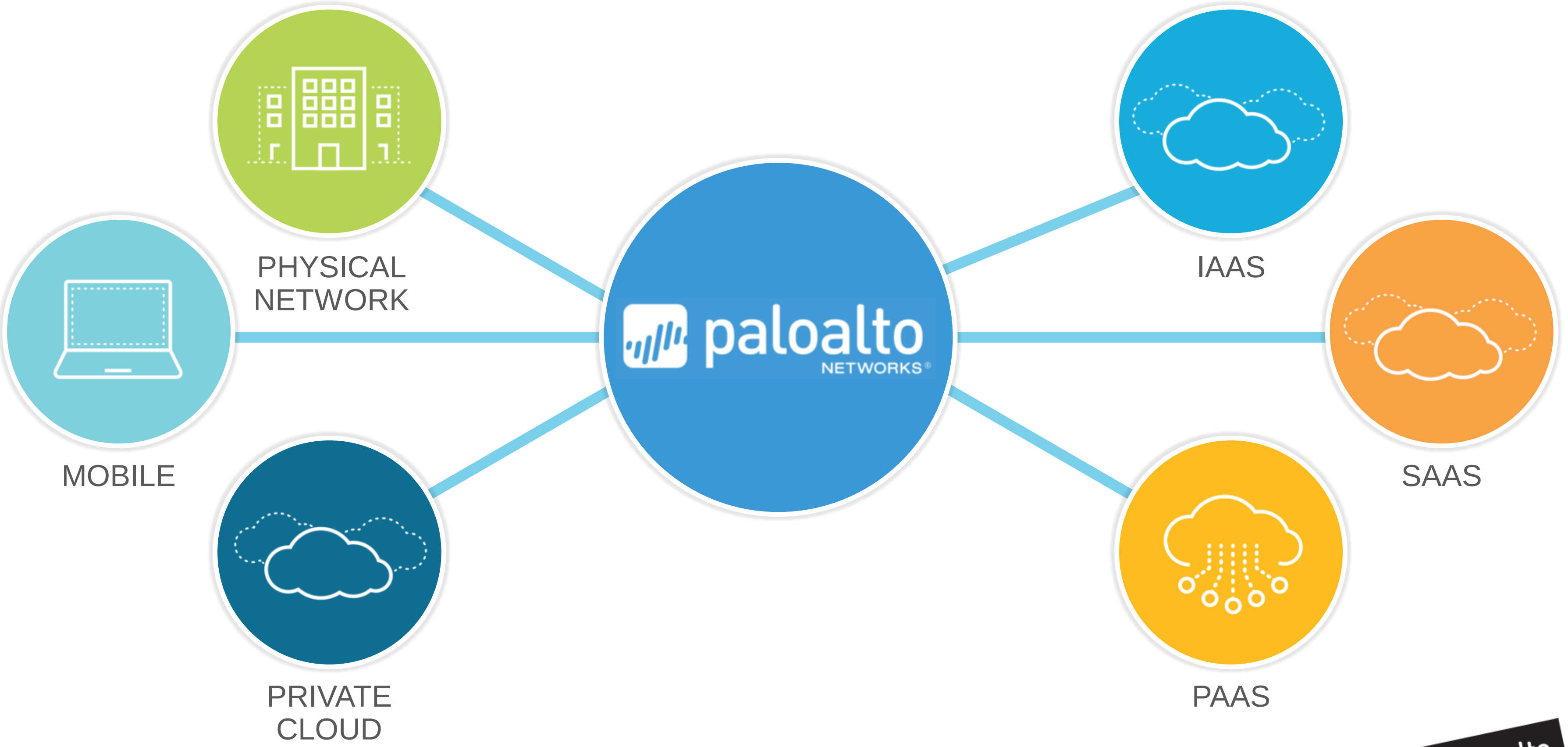
LOG DATA

NETWORK SECURITY

ADVANCED ENDPOINT PROTECTION

CLOUD SECURITY

CONSISTENT & FRICTIONLESS PREVENTION EVERYWHERE



PHYSICAL NETWORK

MOBILE

PRIVATE CLOUD

IAAS

SAAS

PAAS

paloalto

NETWORKS®