INTRODUCING PAN-OS 8.1

Eirik Valderhaug
Systems Engineer Specialist - CSS

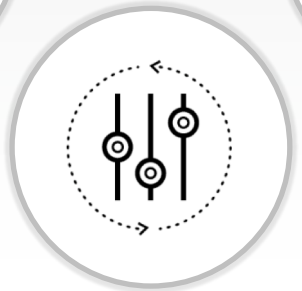
paloalto NETWORKS®

BOOST SECURITY EFFECTIVENESS & PERFORMANCE

Simplified app-based security

Streamlined SSL decryption

Performance boost for diverse deployments



Improved efficiency & performance for management

Advanced threat detection and prevention

BOOST SECURITY EFFECTIVENESS & PERFORMANCE

Simplified app-based security

Streamlined SSL decryption

Performance boost for diverse deployments

Improved efficiency & performance for management

Advanced threat detection and prevention

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

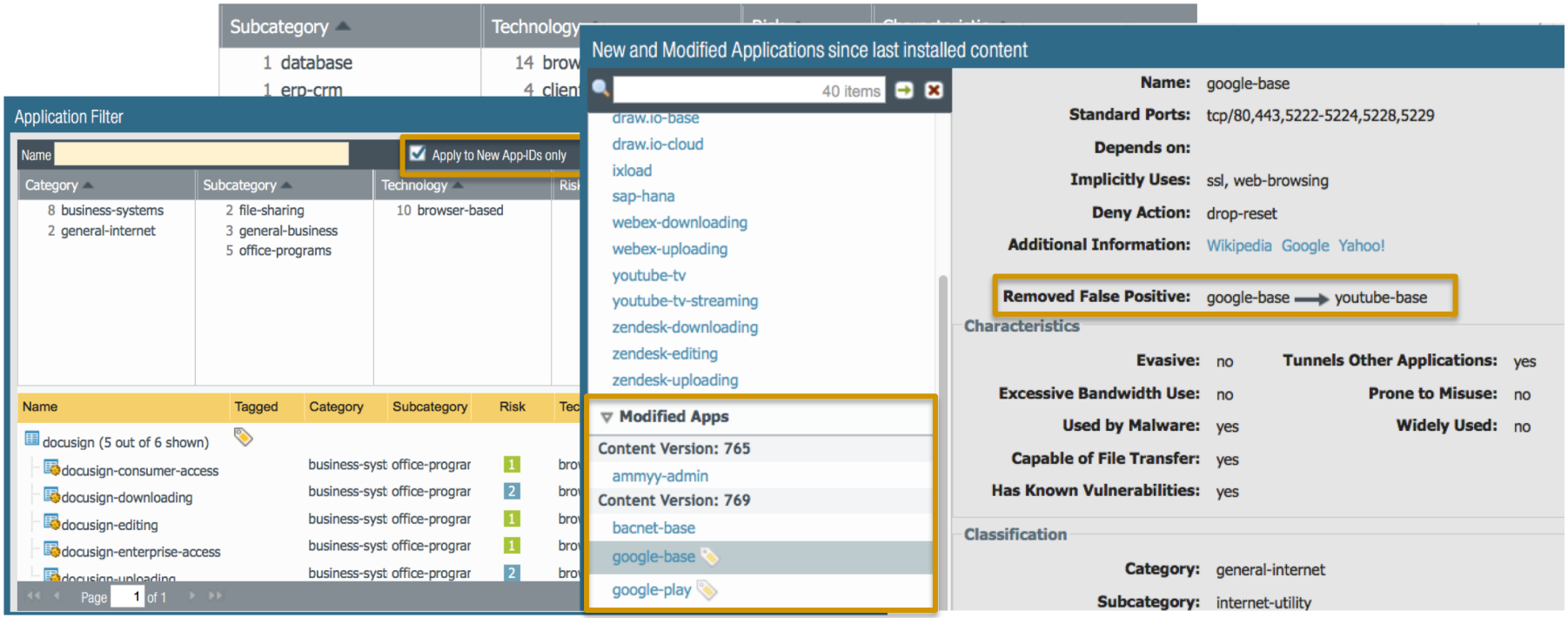
EASIER ADOPTION OF THREAT UPDATES & NEW APPS

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 NEW APPS



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

ENTERPRISE ACCOUNTS

Enterprise account

FREE / CONSUMER ACCOUNTS

Home / personal accounts

Same application, but are the risks different?

paloalto NETWORKS

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

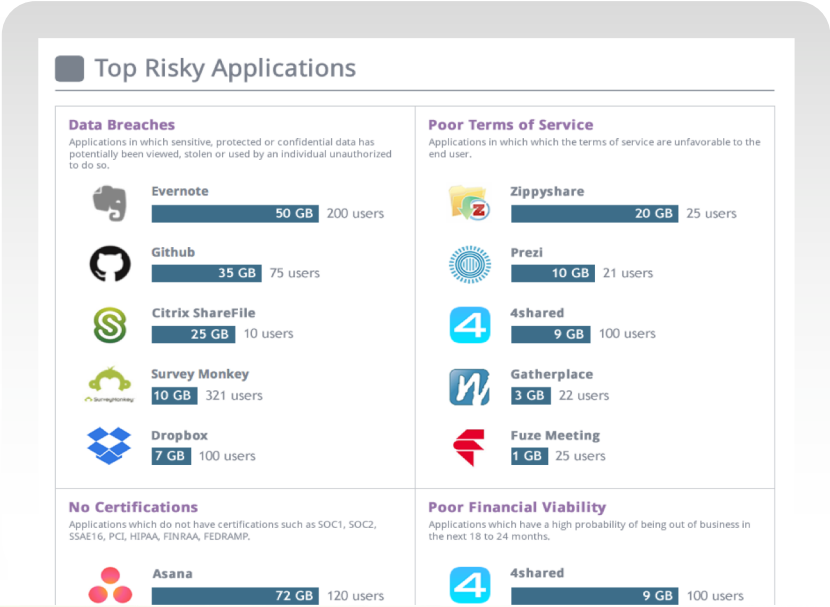
NGFW inserts HTTP header in the request

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

paloalto NETWORKS

ENABLING SAFE USAGE OF SANCTIONED SAAS APPS

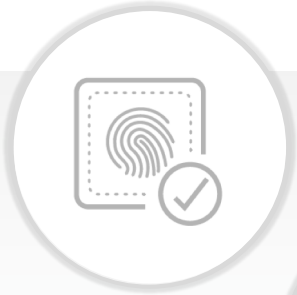
- Application function
- Application characteristics
- Deep visibility
- SaaS app characteristics



NEW

NETWORK SECURITY ENHANCEMENTS: FOCUS AREAS

Simplified app-based security



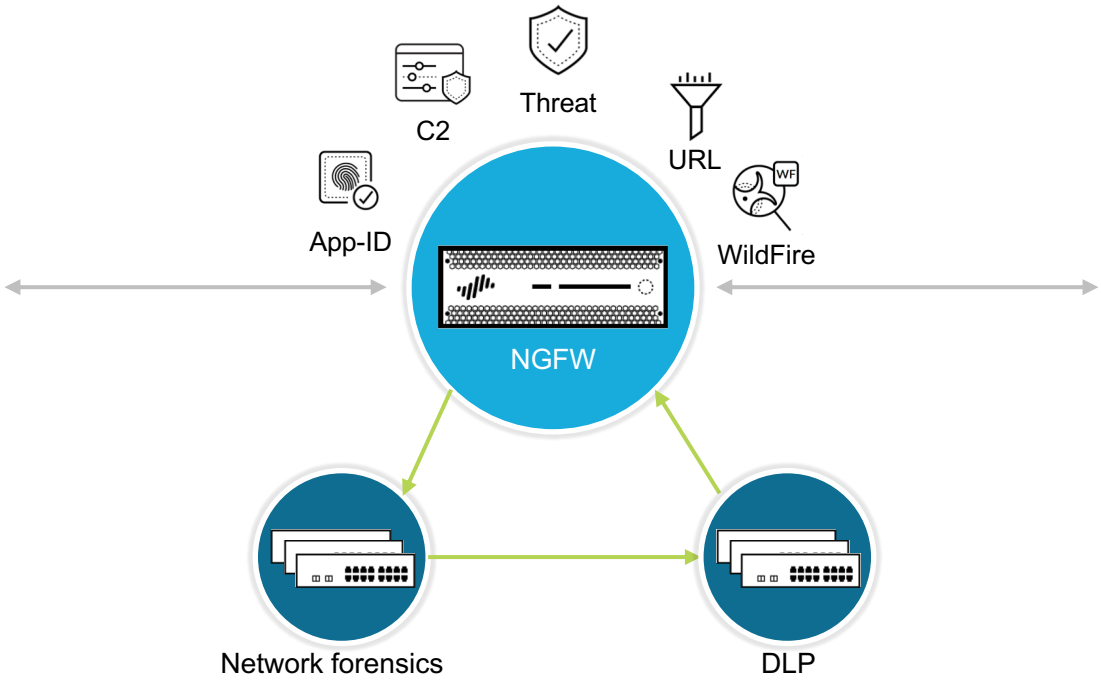
Streamlined SSL decryption

Performance boost for diverse deployments

Improved efficiency & performance for management

Advanced threat detection and prevention

NGFW DECRYPTION BROKER: SIMPLE AND SECURE



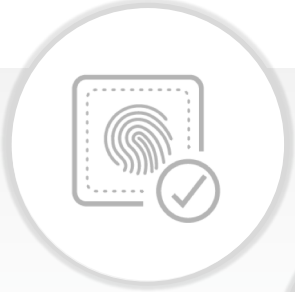
Eliminate dedicated SSL offloaders, simplifying the network

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



Streamlined SSL decryption

Performance boost for diverse deployments

Improved efficiency & performance for management

Advanced threat detection and prevention

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

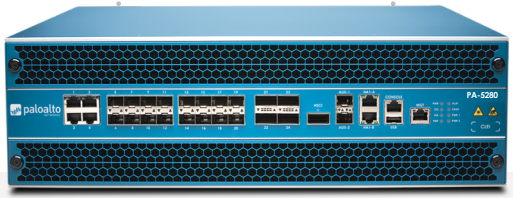
Power Generation

- **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



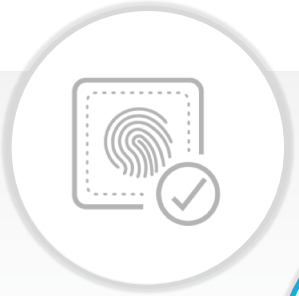
68 Gbps App-ID
29 Gbps threat
64 M sessions

LTE-IoT Security

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

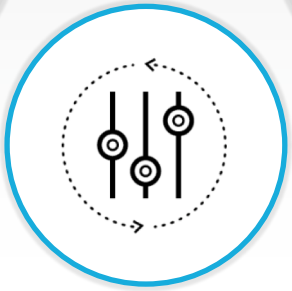
NETWORK SECURITY ENHANCEMENTS: FOCUS AREAS

Simplified app-based security



Streamlined SSL decryption

Performance boost for diverse deployments



Improved efficiency & performance for management

Advanced threat detection and prevention

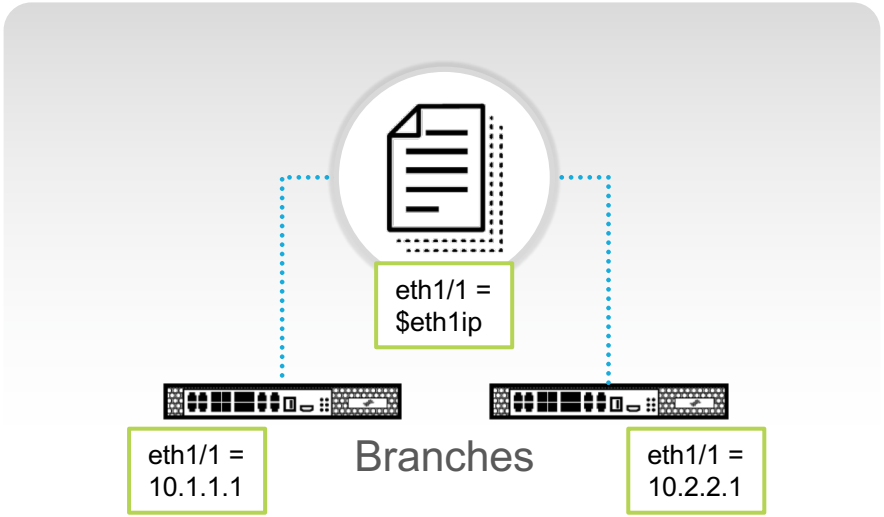
MANAGEABILITY

Simplifying management of large deployments

Proactive monitoring and alerting

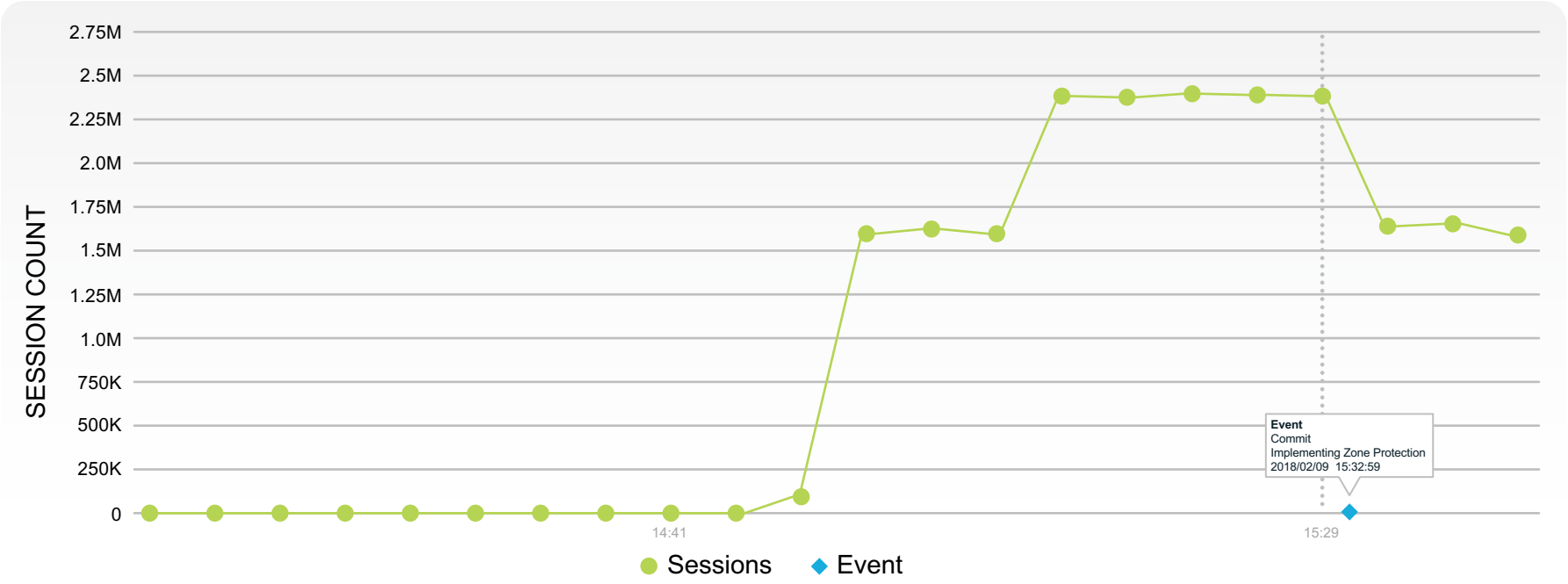
High-performance management

SIMPLIFYING LARGE SCALE CONFIG MANAGEMENT



Reuse configuration with templates,
account for differences with variables

PROACTIVE DEVICE HEALTH AND METRICS MONITORING



Understand baseline usage and get notified of deviations

Correlate device resource utilization with config changes and system events

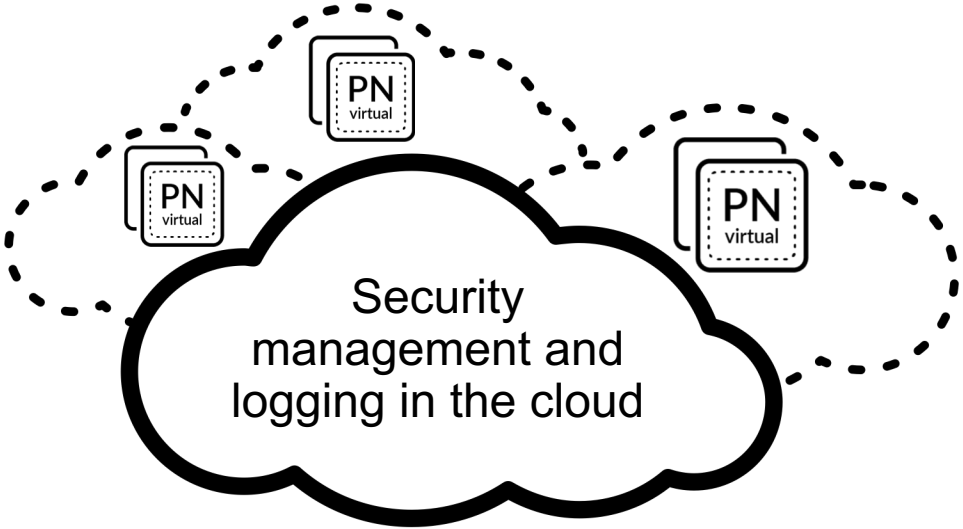
NEW M-SERIES FOR HIGH-PERFORMANCE MANAGEMENT

M-200

M-600

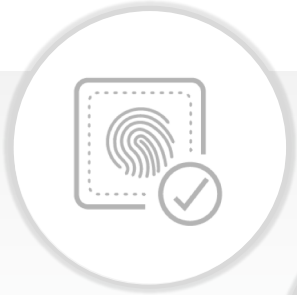
- **Improved responsiveness with faster CPU and more memory**
- **Twice the log ingestion rate** means better scalability of logging infrastructure
- Redundancy with dual power supplies
- Better serviceability with field-replaceable system drives

CLOUD RESIDENT MANAGEMENT WITH PANORAMA



NETWORK SECURITY ENHANCEMENTS: FOCUS AREAS

Simplified app-based security



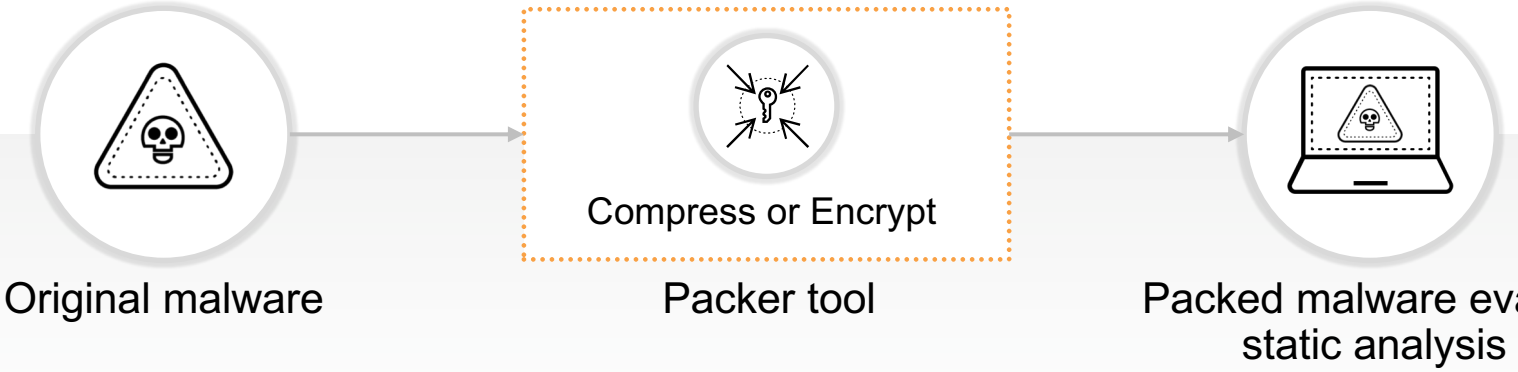
Streamlined SSL decryption

Performance boost for diverse deployments

Improved efficiency & performance for management

Advanced threat detection and prevention

MALWARE CAN AVOID ANALYSIS AND DETECTION

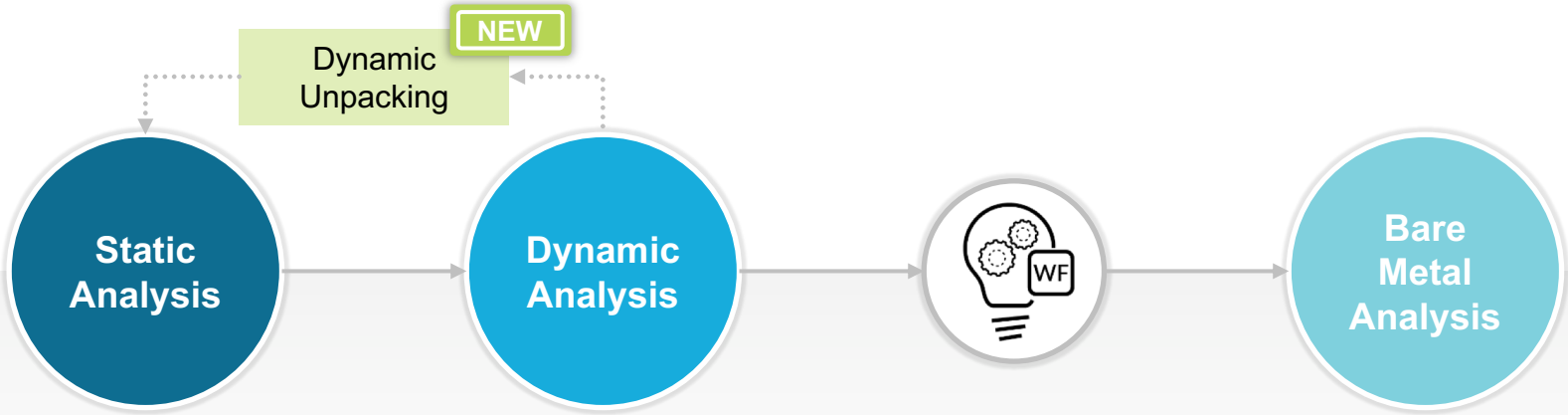


Attackers use packer tools to avoid malware analysis

Static analysis and machine learning alone are not enough

Defeating packing requires complementary analysis techniques

ADVANCING DETECTION: NEW WILDFIRE MODULE



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

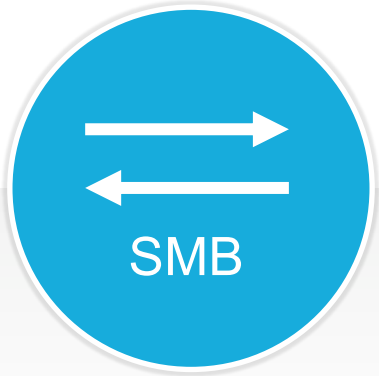
Identify VM-aware threats using hardware systems

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

PREVENTION EVERYWHERE

New analysis environments

Improved detection of malware targeting Linux servers and IoT devices



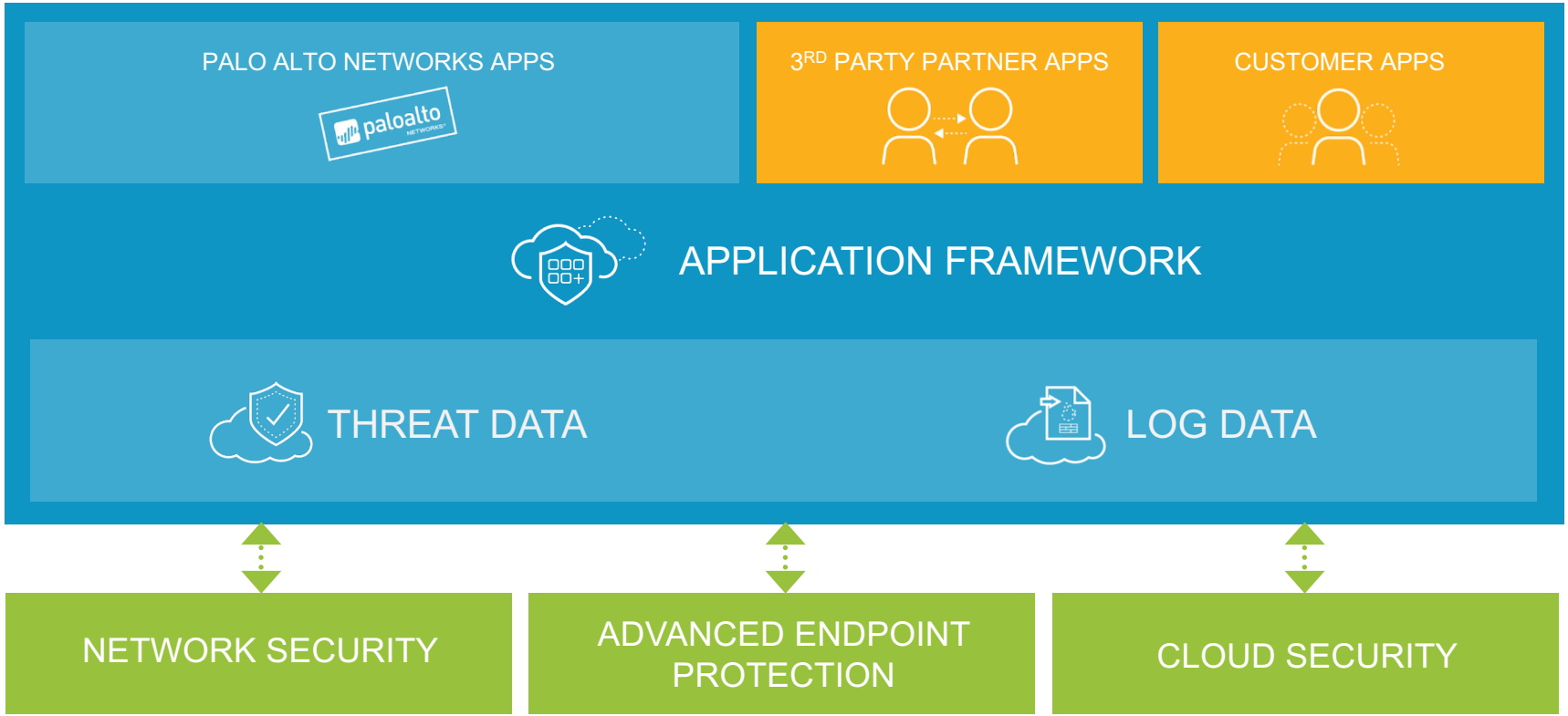
Prevent malware spreading inside the network

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

PALO ALTO NETWORKS APPLICATION FRAMEWORK

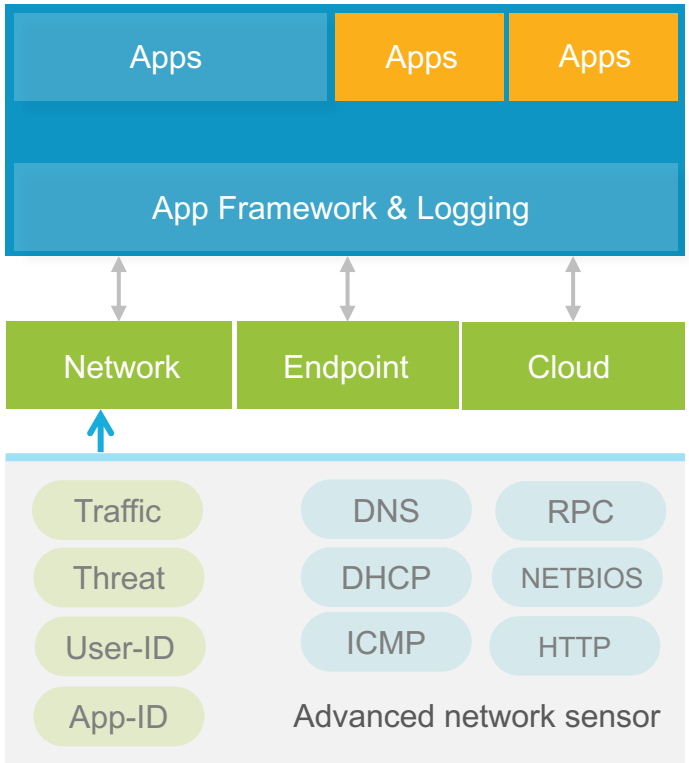


DATA FOR ANALYTICS: ENHANCED APPLICATION LOGS

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



CONSISTENT & FRICTIONLESS PREVENTION EVERYWHERE


paloalto
NETWORKS®