University of Pittsburgh

SAC-PA Workshop

“Firewalls” and ScienceDMZ applications

Brian Pasquini

Director Information Security - University of Pittsburgh

Kenny Holmes, CISSP ®

Cyber Security Evangelist and Director Public Sector

paloalto

Objectives

- **Trust**
- We have a **consumption** issue
- **Automation, Orchestration, and Leverage**
- The **third-evolution** of Cyber-Security
- Philosophy of **prevention** oriented security
- Minimize the spread of attacks by providing protection based on comprehensive global, industry, and organizational threat data
- Enforce automated preventative measures with a security platform in tap mode or in-line

TECHNOLOGY IS PART OF OUR LIVES

paloalto


TRUST

Breaches reported in 2017

5,207

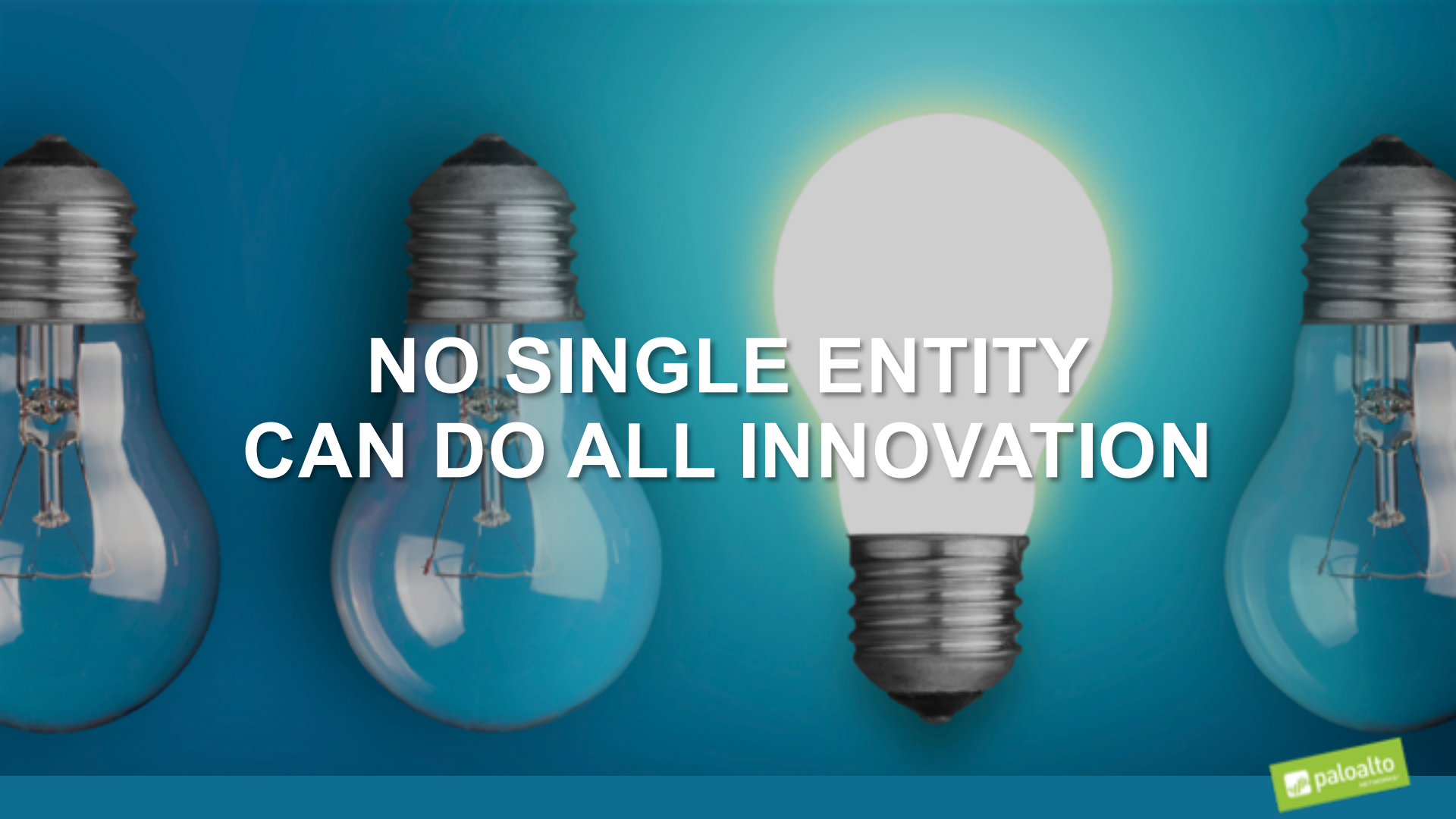
US breach cost 2016, up to

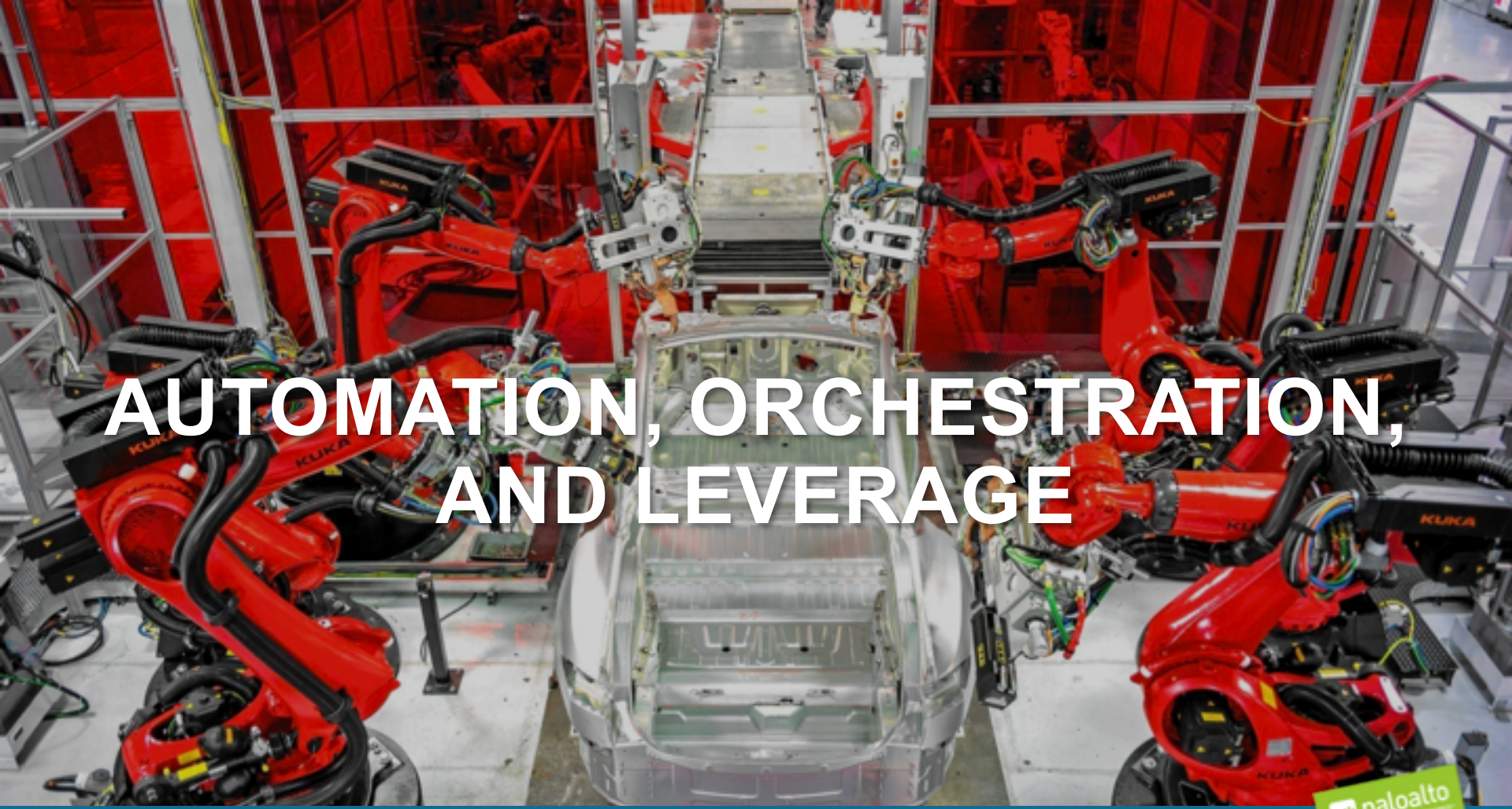
$109Bn

Source identity @2018 Dark Reading: 2017 Smashed World's Records for Most Data Breaches, Exposed Information by Kelly Jackson Higgins.
White House Council of Economic Advisers Report. February 2018

paloalto


OFFICE OF THE CISO
CONSUMING CYBERSECURITY IS BECOMING IMPOSSIBLE
paloalto


NO SINGLE ENTITY
CAN DO ALL INNOVATION



AUTOMATION, ORCHESTRATION, AND LEVERAGE

EVOLUTION III

PALO ALTO NETWORKS APPS

3rd PARTY PARTNER APPS

CUSTOMER APPS

CLOUD-DELIVERED SECURITY SERVICES

Threat Prevention | URL Filtering | Malware Analysis

APPLICATION FRAMEWORK & LOGGING SERVICE

NETWORK SECURITY

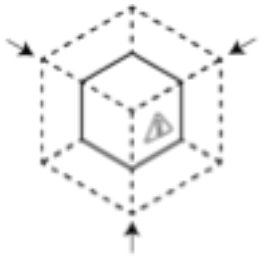
ADVANCED ENDPOINT PROTECTION

CLOUD SECURITY

Philosophy for prevention

Complete visibility

- All applications
- All users
- All content
- Encrypted traffic
- SaaS
- Cloud
- Mobile



Reduce attack surface area

- Enable business apps
- Block “bad” apps
- Limit app functions
- Limit file types
- Block websites
- Require multi-factor authentication

Prevent all known threats

- Exploits
- Malware
- Command & control
- Malicious websites
- Bad domains
- Credential theft

Detect & prevent new threats

- Dynamic Analysis
- Static Analysis
- Attack techniques
- Anomaly detection
- Analytics

Automated Prevention Touch Points
Continuous Protection

AutoFocus
3rd Party Intelligence Correlation and Aggregation

Cloud Security Services

Static Machine Dynamic Bare metal

Next Generation Security Platform

Next-Generation Firewall

GP TP UF AP TR VM

ENDPOINT IOT

Network Device w/ ACL

High-Fidelity IOC's

IP
URL
Domain
Hash
Regex
And More..

Automated Protection #1

-5 min updates
WF-AV, C2, DNS, URL
230K+ protections daily

1

Automated Protection #2

API, External Dynamic List
-5min updates
IP, URL, Domain

Python/EEM/TCL ACL Updates

2

•JSON
•JSON-SEQ
•STIX/TAXII

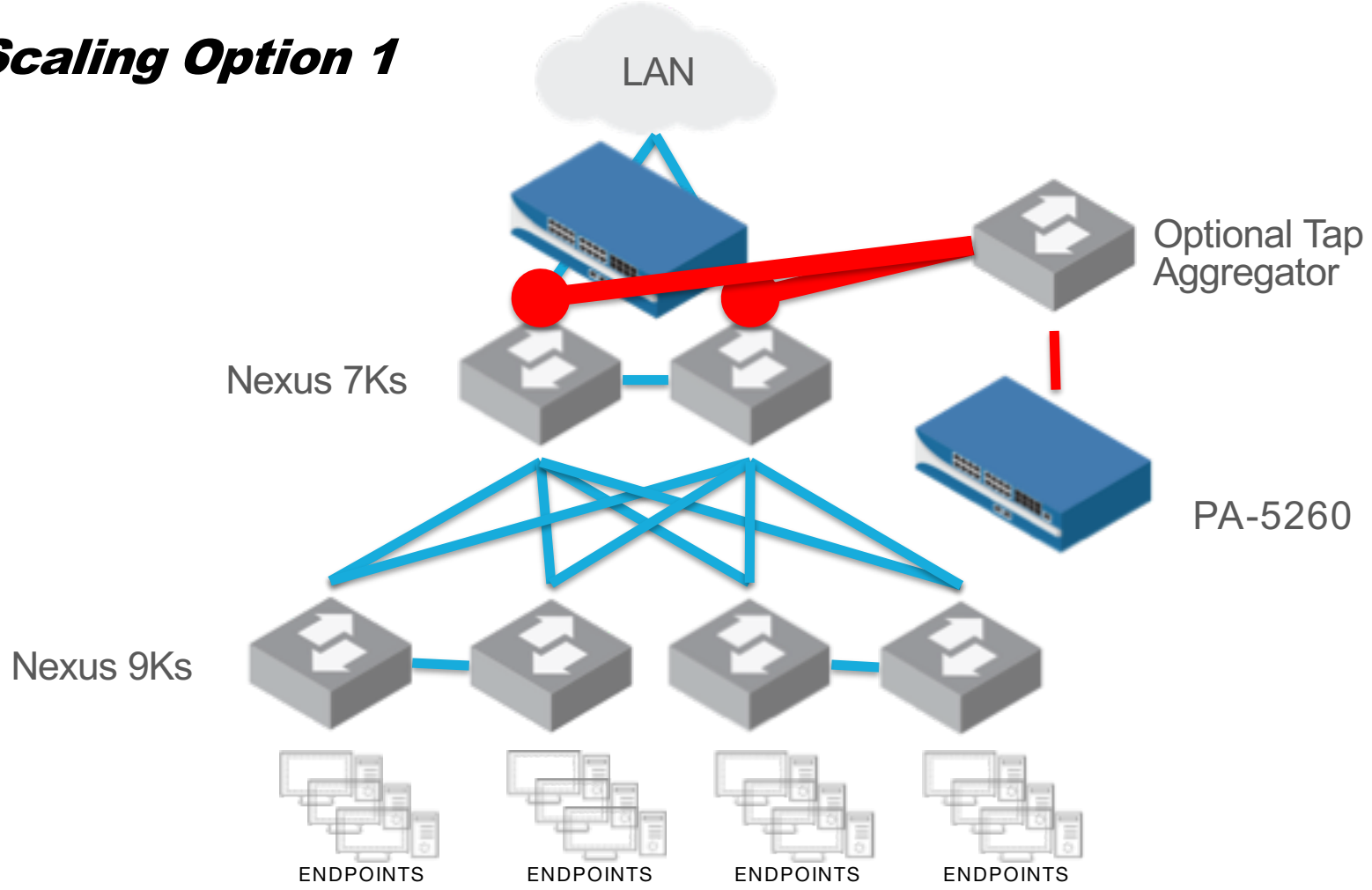
3rd Party Solutions
EDR | SIEM | IR Systems | O365

3

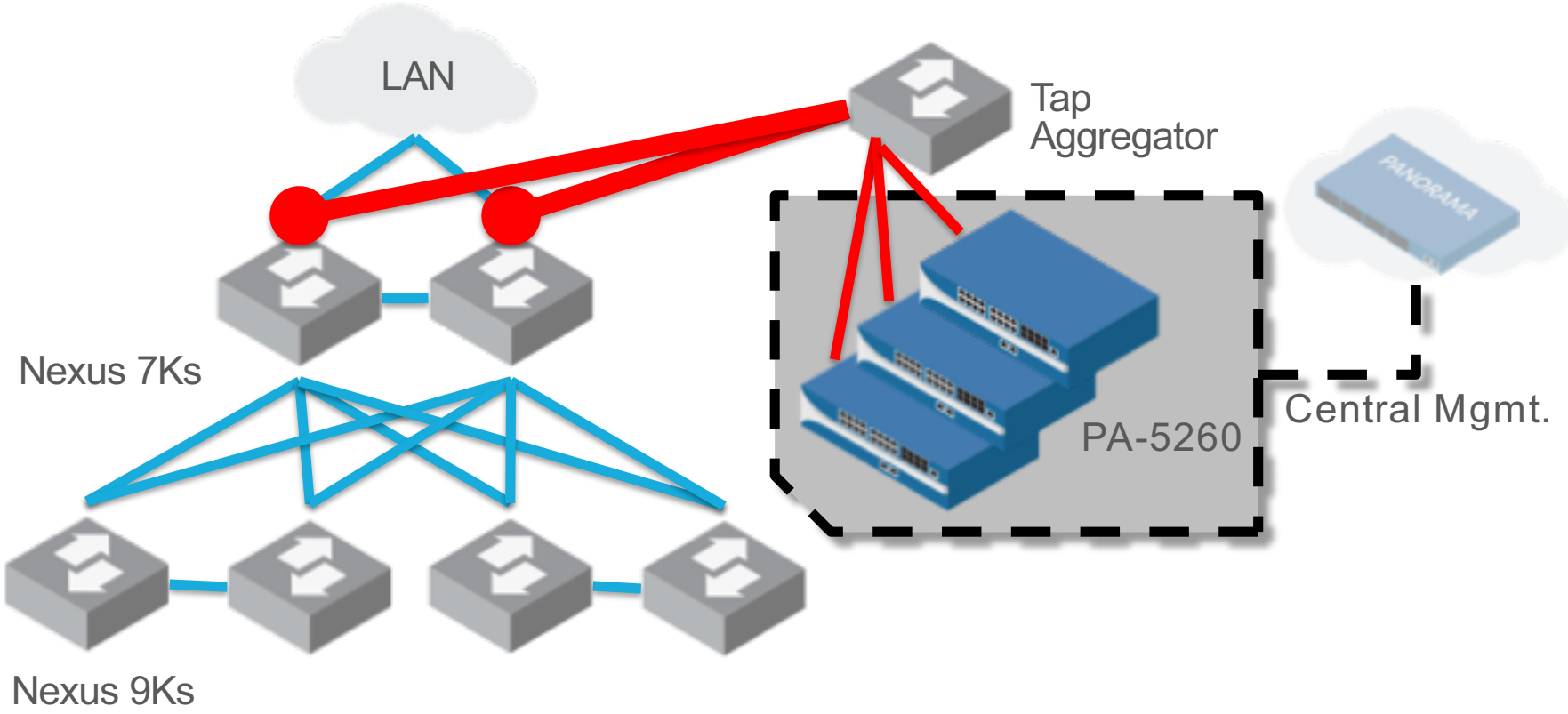
Automated Protection #3

API/External Dynamic List
White List OR Black List
Python/EEM/TCL ACL Updates

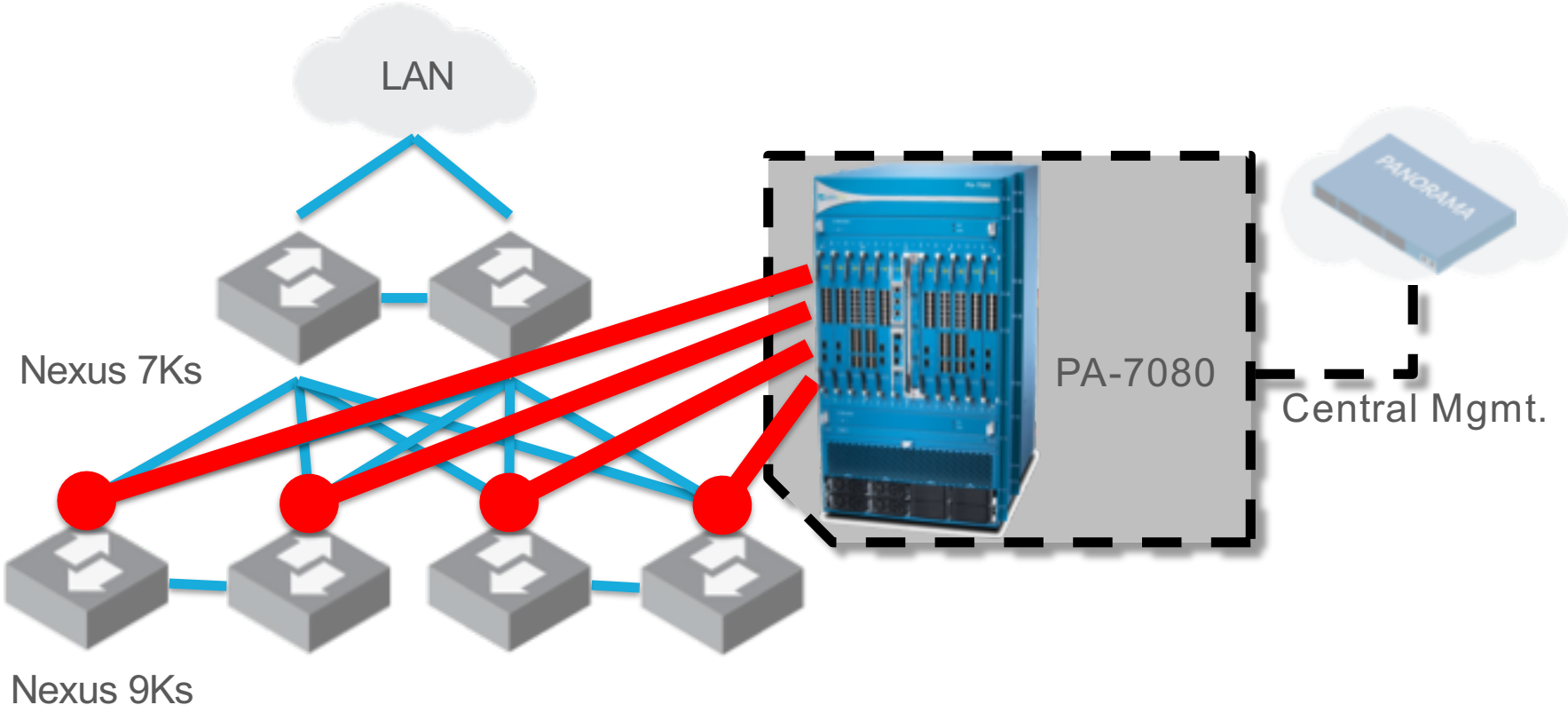
Scaling Option 1



Scaling Option 2



Scaling Option 3




#CyberMoonshot
OUR MISSION AS A SOCIETY IS TO MAKE THE INTERNET SAFE IN TEN YEARS
THANK YOU
paloalto

THANK YOU

Additional Information

CONSISTENT AND FRICTIONLESS PREVENTION EVERYWHERE

PALO ALTO NETWORKS SECURITY OPERATING PLATFORM

PREVENT SUCCESSFUL CYBERATTACKS

Operate with ease using best practices

FOCUS ON WHAT MATTERS

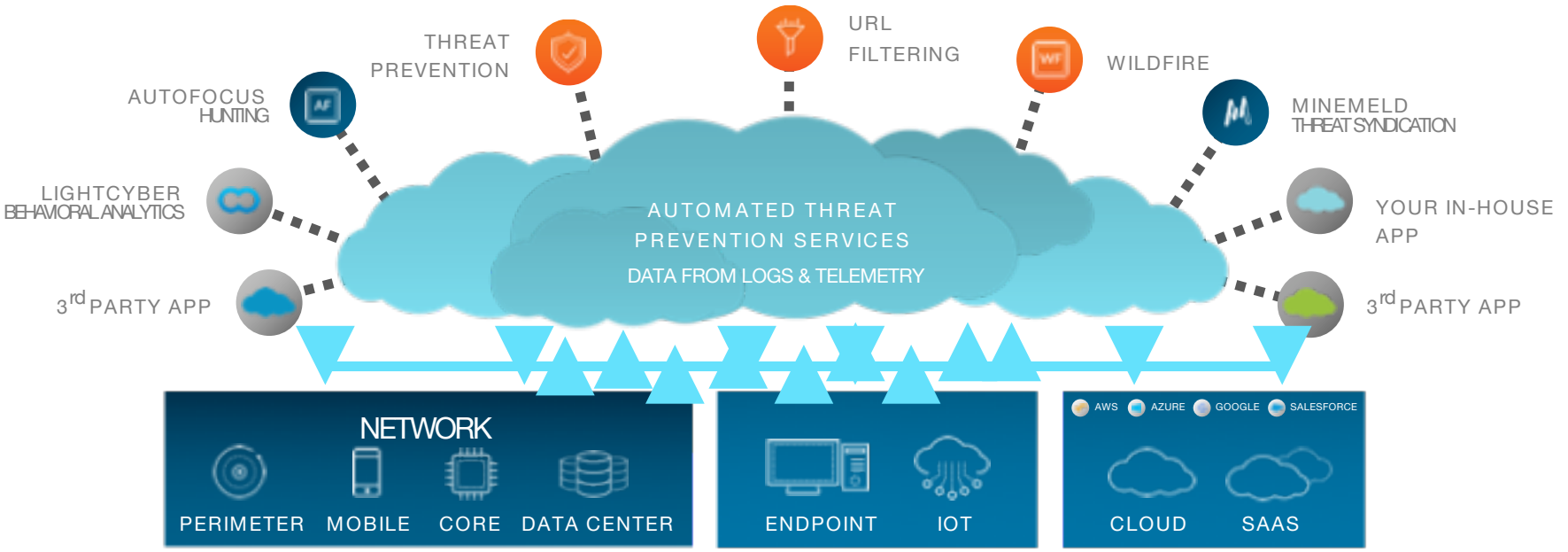
Automate tasks using context and analytics

CONSUME INNOVATIONS QUICKLY

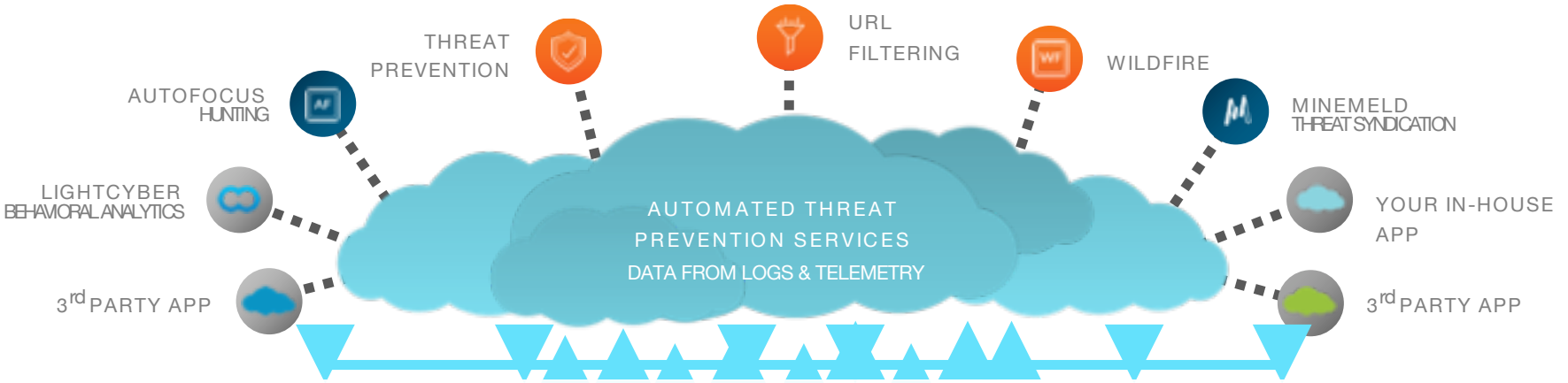
Palo Alto Networks, 3rd party, and customer delivered

BUILT FOR AUTOMATION

Disrupting the cyber-security consumption model



Disrupting the cyber-security consumption model



~19K Wildfire customers
(> 45K NGFW Customers)

350 Million
Unique Protections

>6M New files
scanned/day

>3.1 Billion
files scanned

5 minute
automated updates

~50k New Protections
published/day

>1 Trillion
artifacts learned
(IP addr, processes, domains)

>100
3rd party feeds

~250k Malware threats
learned/day

Threat Intelligence Cloud

215M+

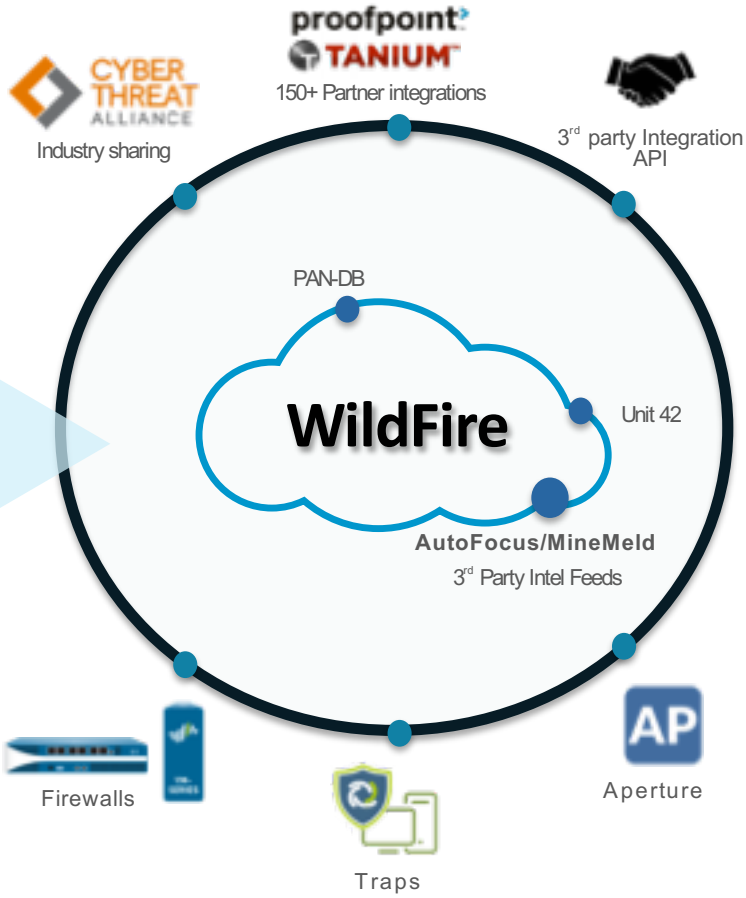
Never before seen samples every month

19,500+

Global customers actively submitting samples

230,000+

New protections delivered daily every 5 minutes



AutoFocus

3.1B
Sample Files in **AutoFocus**

1,500+
Unit 42 Malware Tags

1.2T
Artifacts in **AutoFocus**

150+ **Built in 3rd Party Feed Connectors**

Our approach to enterprise security

App-ID

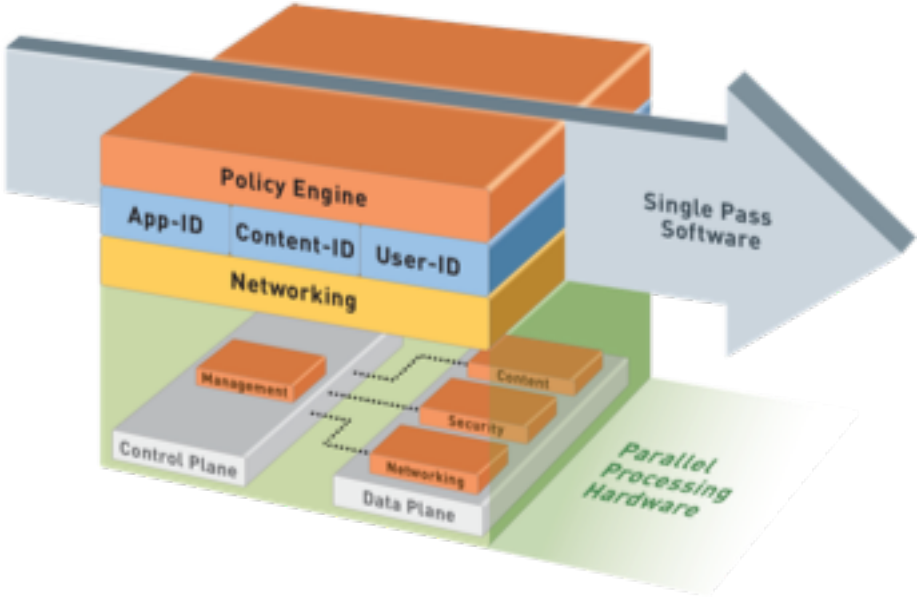
Identify the application

Content-ID

Scan the content

User-ID

Identify the user



PA-5200 Series

- New advanced architecture delivers up to 72 Gbps* (App-ID) and 30 Gbps* (Threat Prevention)
- Up to 32M sessions; 3.2M SSL decrypt session capacity
- Higher port density, 40G and 100G I/O support for diverse deployments

**Performance specs derived from HTTP traffic with 64K transaction size*

PA-5200 Series Specifications

PA-5260

- 72 Gbps App-ID
- 30 Gbps Threat Prevention
- 21 Gbps IPSec VPN
- 32,000,000 sessions
- (4) 40G/100G QSFP28
- (16) 1G/10G SFP/SFP+
- (4) 100/1000/10G Copper

PA-5250

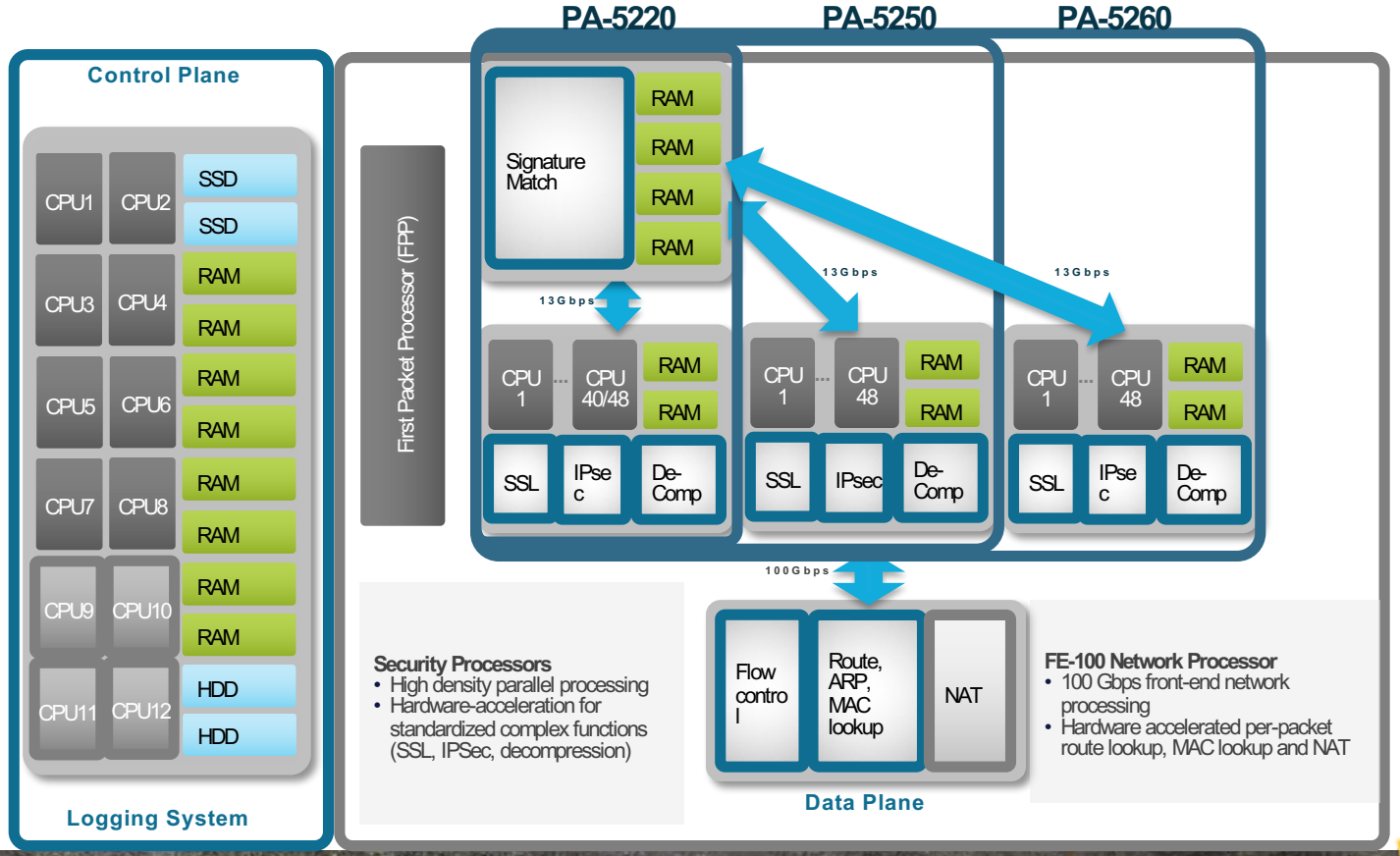
- 35 Gbps App-ID
- 20 Gbps Threat Prevention
- 14 Gbps IPSec VPN
- 8,000,000 sessions
- (4) 40G/100G QSFP28
- (16) 1G/10G SFP/SFP+
- (4) 100/1000/10G Copper

PA-5220

- 18 Gbps App-ID
- 9 Gbps Threat Prevention
- 5 Gbps IPSec VPN
- 4,000,000 sessions
- (4) 40G QSFP+
- (16) 1G/10G SFP/SFP+
- (4) 100/1000/10G Copper

- Hot swappable fans, power supplies
- Dual SSD system drives (240GB) and dual HDD logging drives (2TB)
- Dedicated HA and management interfaces
- 3U, 2 and 4 post rackmount units
- Front to back airflow with replaceable filters
- NEBS Level 3 Certified

PA-5200 Series Architecture

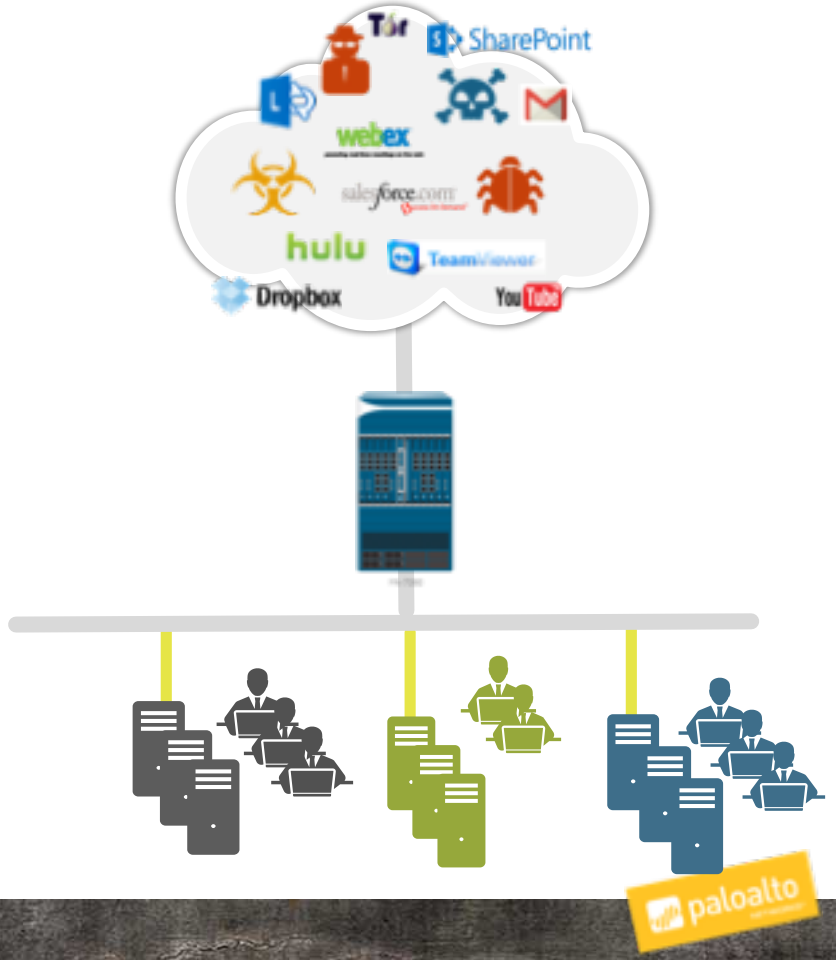


7080 Benefits

- Managed and licensed as a single system regardless of how many NPCs used
  - Consistent PAN-OS feature set
  - Managed by webUI, CLI, or Panorama
  - Support and subscriptions are system-wide
- Easily integrates into any network
  - Virtual wire means plug-n-play level integration into nearly any network
  - L2, L3 mode provide added integration options
  - Active/Active or Active Passive ensures resiliency

At the perimeter

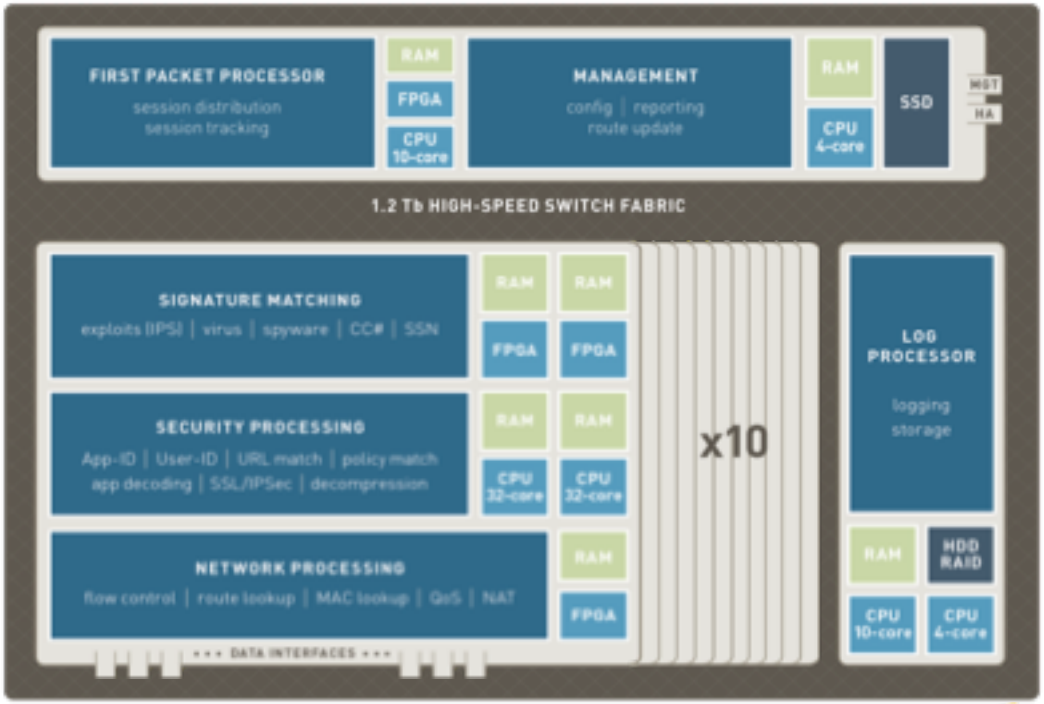
- Protect the network
  - Reduce threat exposure by blocking high risk applications
  - Enable applications based on need and user credentials
  - Block known/unknown threats
  - Control web activity
  - Inspect encrypted traffic
- Key features: System capacity and performance, zone-based architecture, networking, SSL decryption



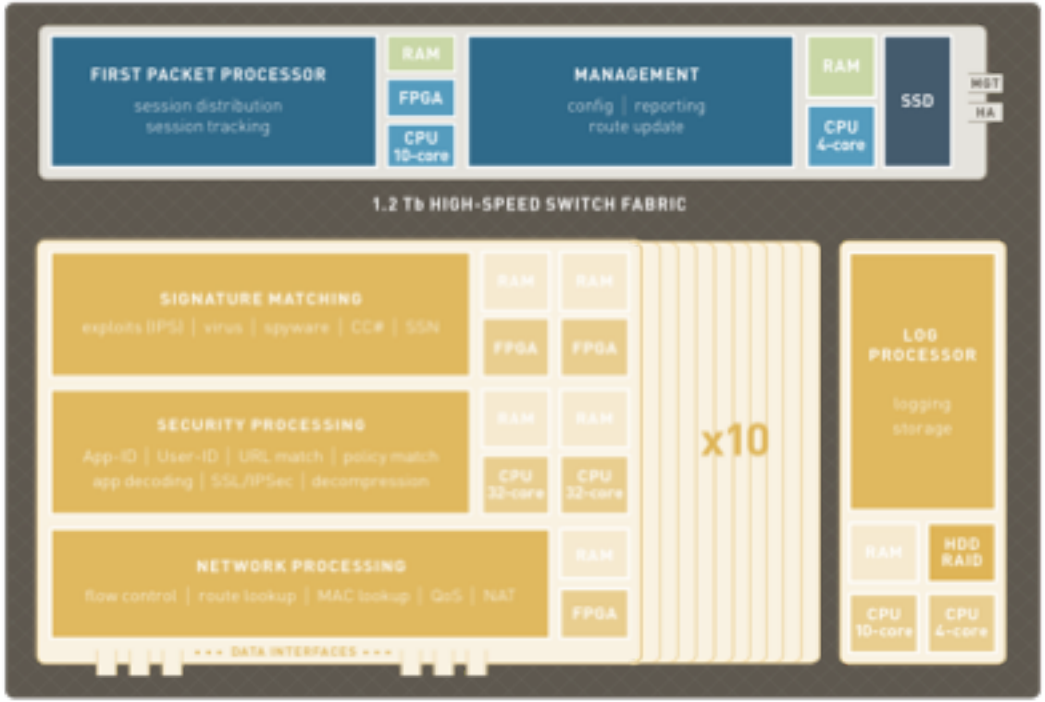
Power that predictably scales to 100 Gbps

Nearly 700 processors dedicated to protecting your data

- Network processing card (NPC)
  - 670 processors distributed across 10 NPCs
  - Executes all networking and security processing functions
  - Scales to 100 Gbps by adding an NPC as needed
- Switch management card (SMC)
  - 14 processors intelligently manage all traffic to maximize resource utilization
- Log processing card (LPC)
  - 14 processors dedicated to managing high volume log processing tasks



Intelligent traffic management



First Packet Processor

- Dedicated subsystem designed to deliver scalable connection setup
- Intelligently allocates security processing resources based on configurable administrative controls
- Automatically scales traffic processing as new cards are added