PALO ALTO NETWORKS NEXT-GENERATION SECURITY PLATFORM

Guest Lecture at the
Munich University of Applied Sciences

Marc Meckel, CISSP, CISM
Systems Engineer
12/09/2016

paloalto NETWORKS®

Palo Alto Networks At-a-Glance

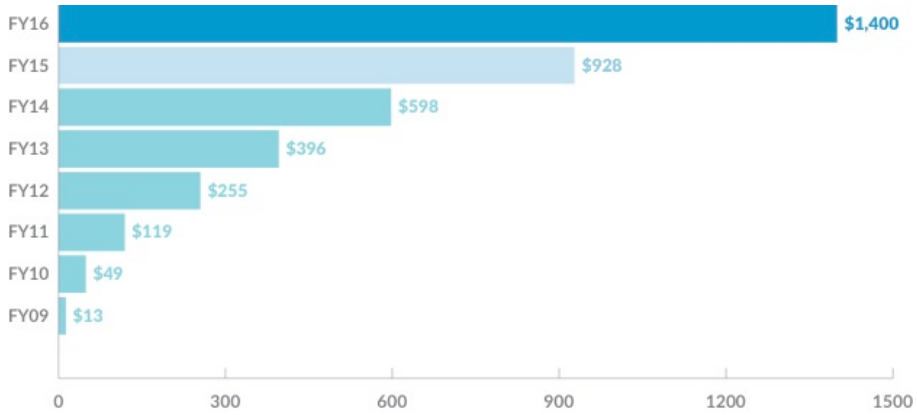
CORPORATE HIGHLIGHTS

- Founded in 2005; first customer shipment in 2007
- Safely enabling applications and preventing cyber threats
- Able to address all enterprise cyber security needs
- Exceptional ability to support global customers
- Experienced team of 3,800+ employees
- Globally 34,000+ customers
- Q4 FY16: $401.8M revenue

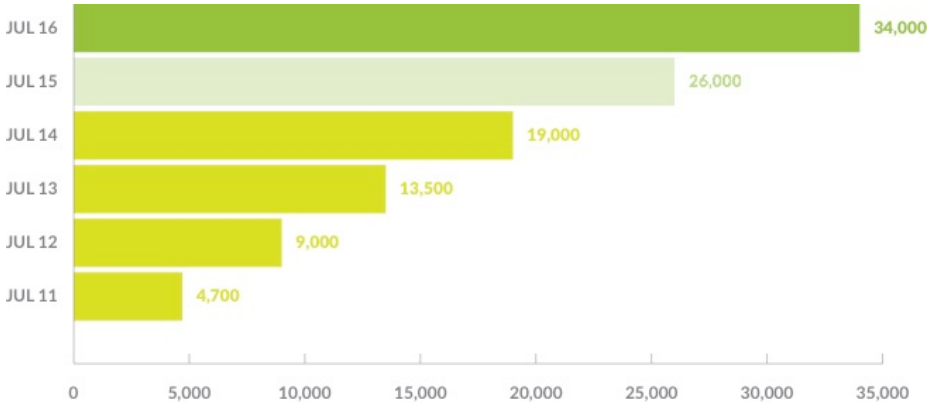
Q4 FY'16 Highlights

- Total revenue grew **41%** year-over-year to a record **$401.8Mn**
- Recurring services revenue grew **61%** year-over-year to **$209.7Mn**
- Deferred revenue grew **74%** year-over-year to **$1.2 billion**
- Billings grew **45%** year-over-year to **$572.4Mn***
- Non-GAAP operating margin grew **400 bps** year-over-year to **18.1%***
- Generated free cash flow of **$171.2 million***

REVENUE



ENTERPRISE CUSTOMERS



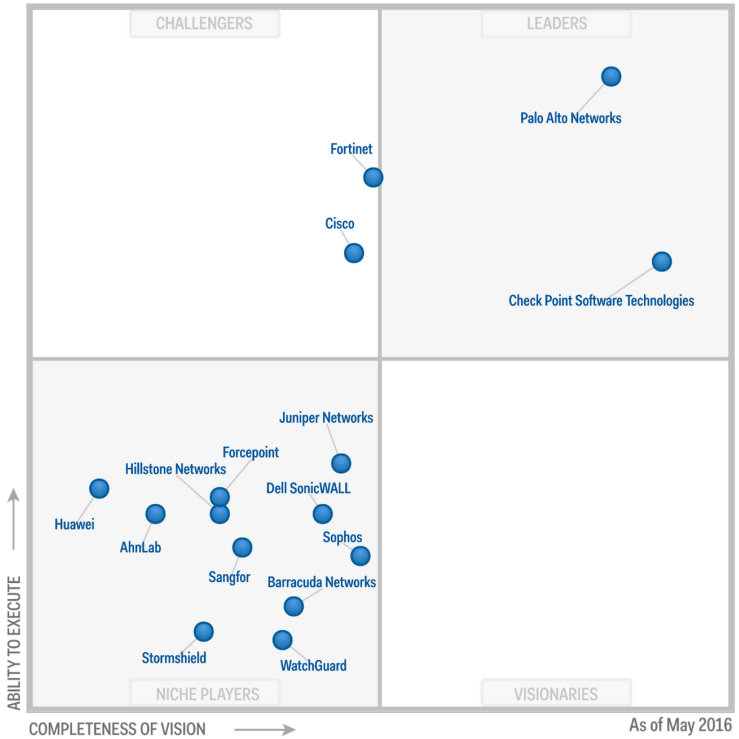
** Non-GAAP financial measures. See appendix for reconciliation to most comparable GAAP measure.*

Gartner Magic Quadrant for Enterprise Network Firewalls 2014-2016

2014

2015

2016

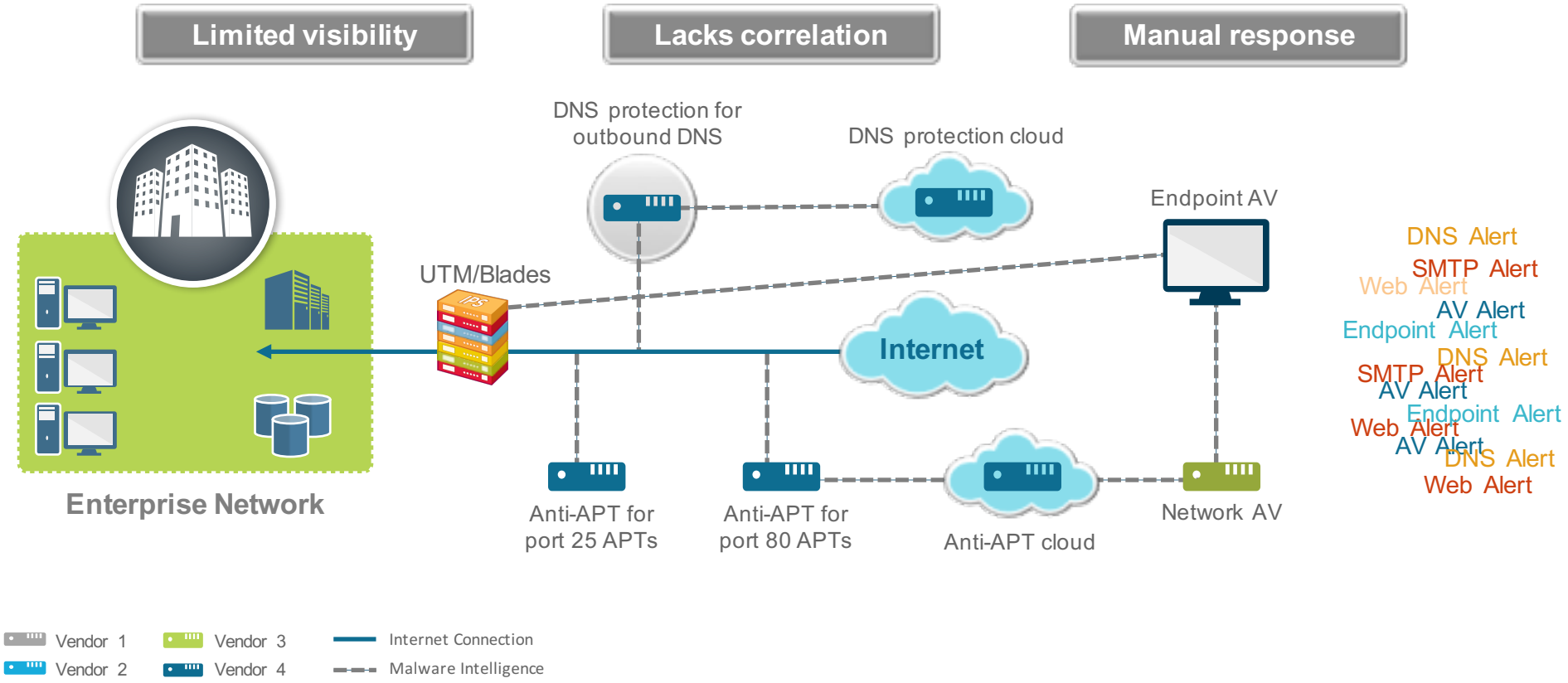


A Typical Cyber Attack Life Cycle

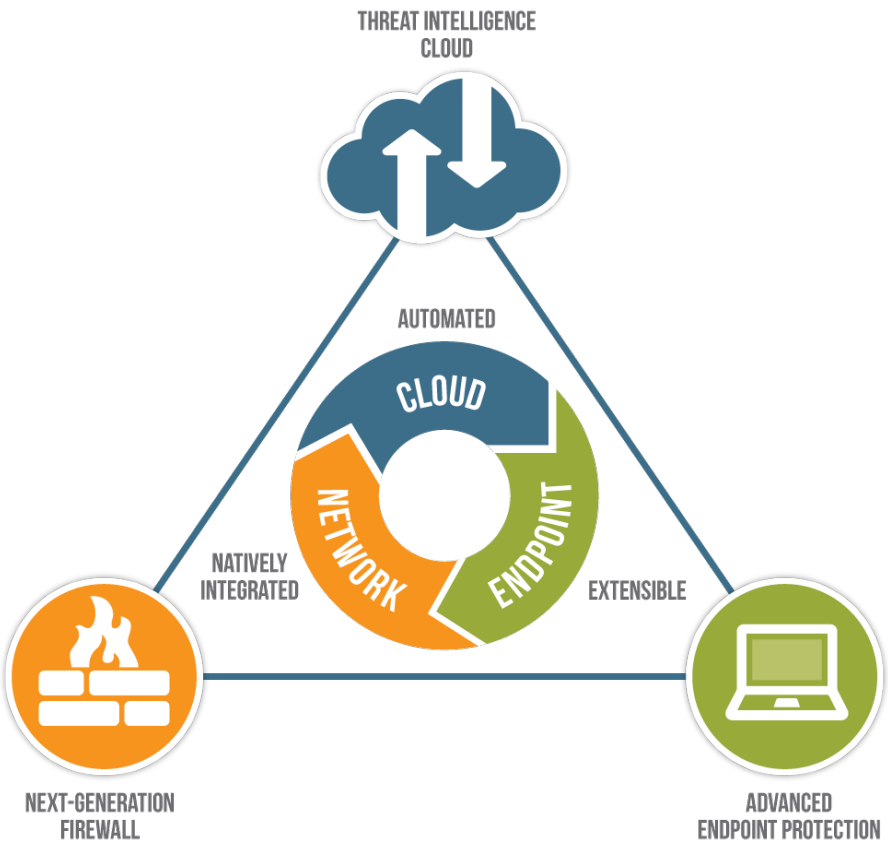
Prevention of an Attack at the Earliest Stage is Critical

Preventive Controls **Reactive Controls**

Failure of legacy security architectures



Palo Alto Networks: an integrated & automated security platform



- Safely enable applications, users and content
- Visibility into all traffic
- Prevent known and unknown cyber threats
  - All users
  - All devices
- Correlated threat intelligence
- Natively integrated extensible platform

Preventing attacks at every stage of the Attack Life Cycle

Breach the perimeter

Next-Generation Firewall / GlobalProtect

- Visibility into all traffic, including SSL
- Enable business-critical applications
- Block high-risk applications
- Block commonly exploited file types

Threat Prevention

- Block known exploits, malware and inbound command-and-control communications

URL Filtering

- Prevent use of social engineering
- Block known malicious URLs and IP addresses

WildFire

- Send specific incoming files and email links from the internet to public or private cloud for inspection
- Detect unknown threats
- Automatically deliver protections globally

Deliver the malware

Traps / WildFire

- Block known and unknown vulnerability exploits
- Block known and unknown malware
- Provide detailed forensics on attacks

Lateral movement

Next-Generation Firewall / GlobalProtect

- Establish secure zones with strictly enforced access control
- Provide ongoing monitoring and inspection of all traffic between zones

WildFire

- Detecting unknown threats pervasively throughout the network

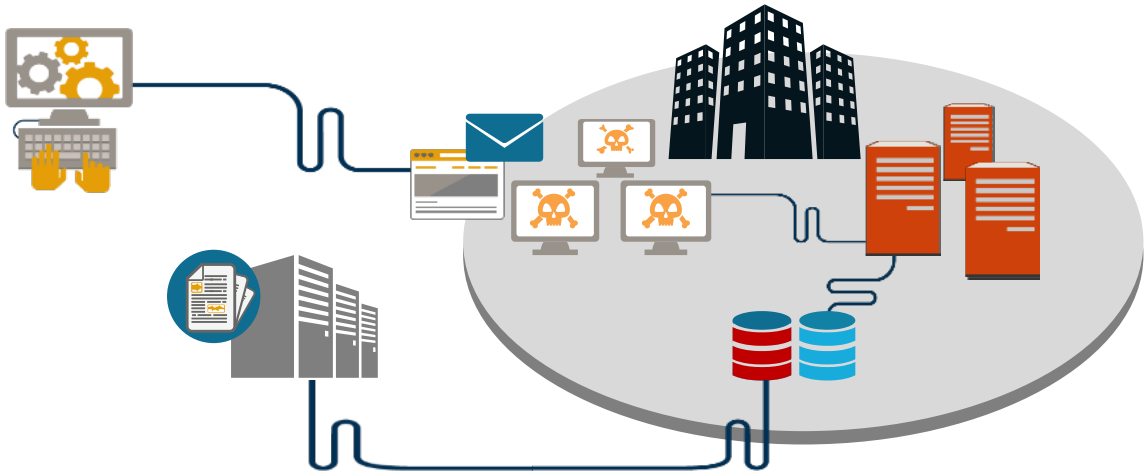
Exfiltrate data

Threat Prevention

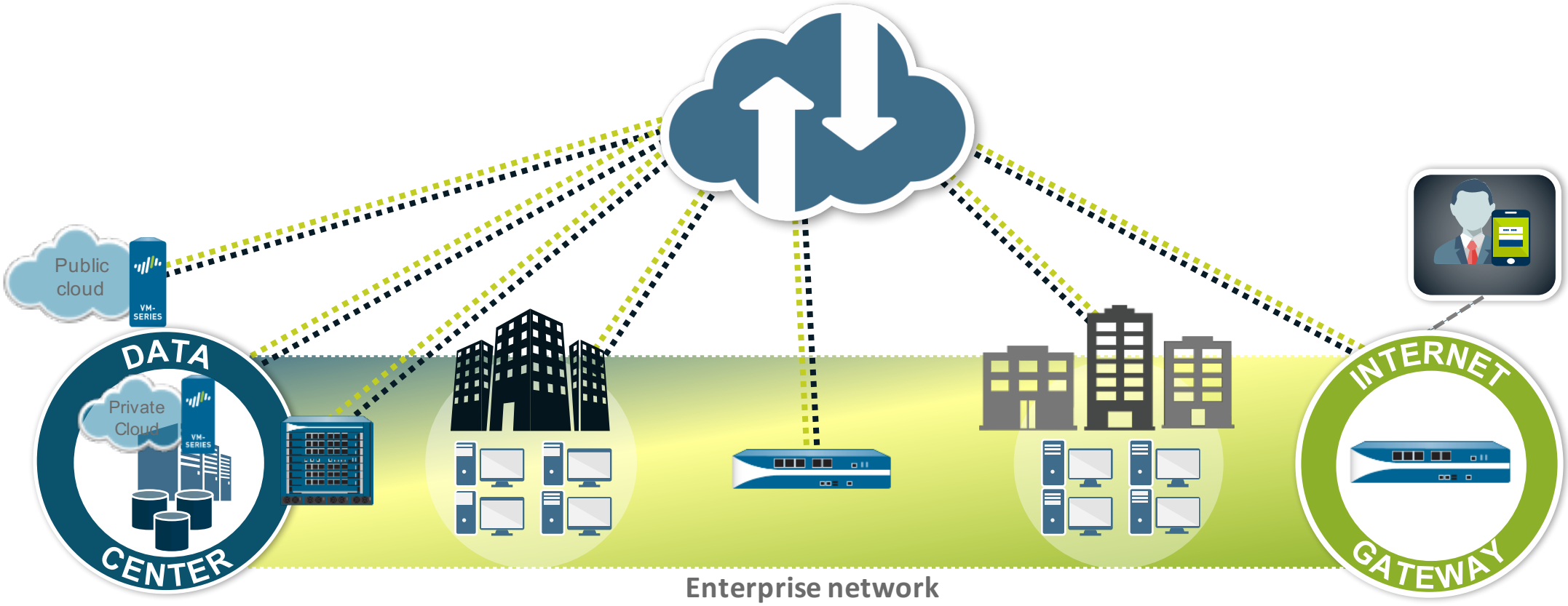
- Block outbound command-and-control communications
- Block file and data pattern uploads
- DNS monitoring and sinkholing

URL Filtering

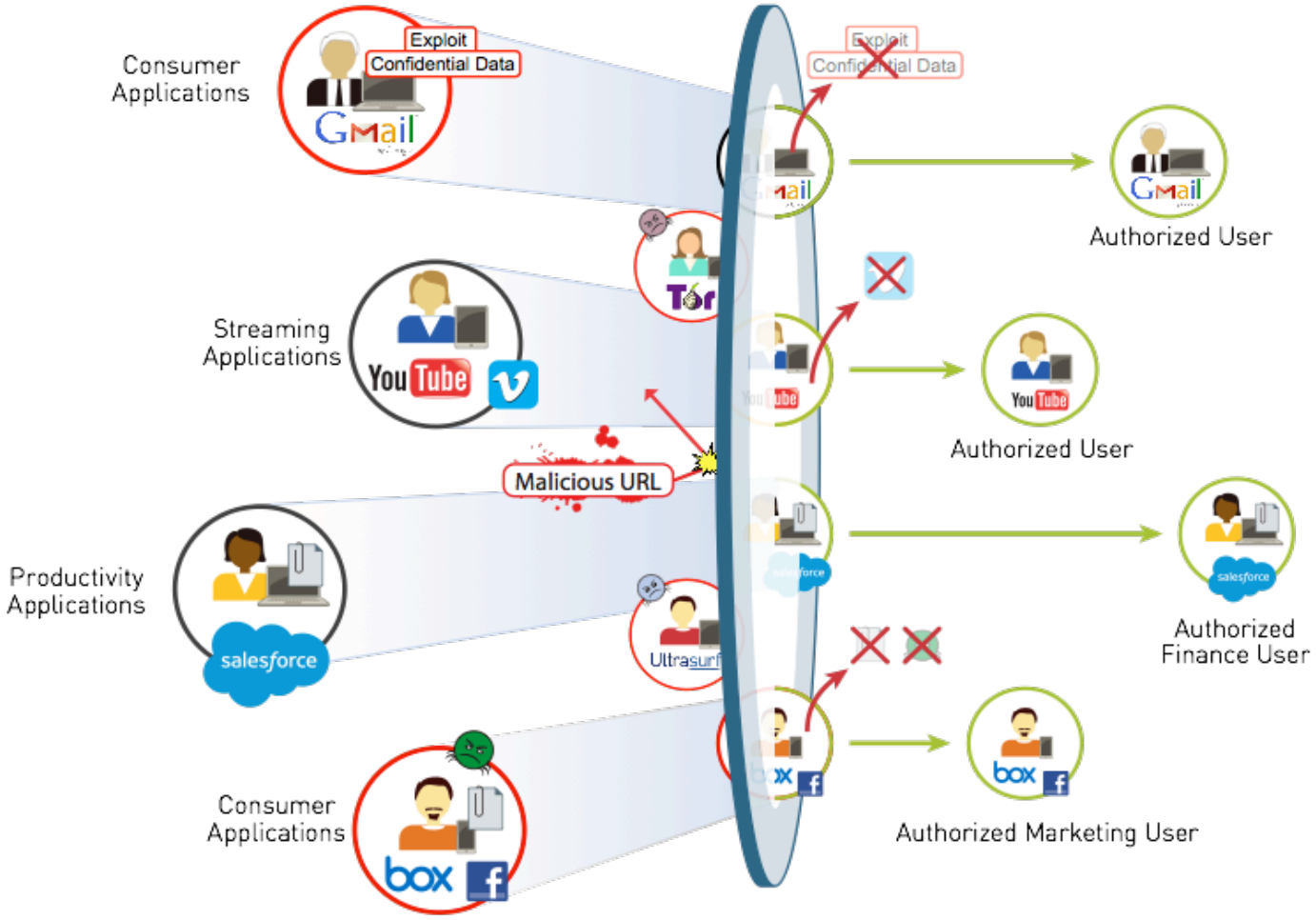
- Block outbound communication to known malicious URLs and IP addresses



A complete security architecture

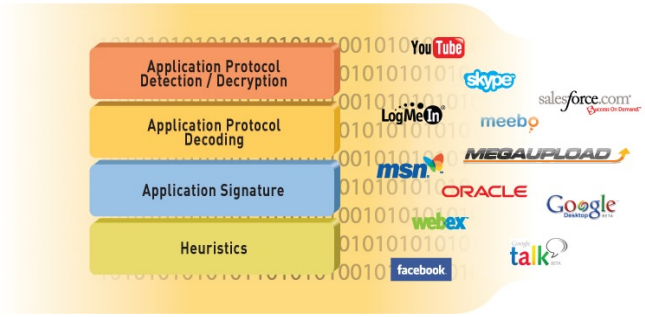


Enabling Applications, Users and Content



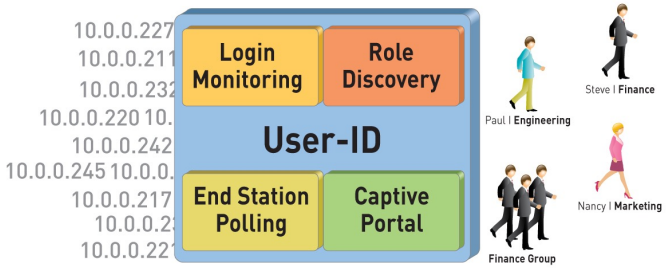
App-ID™

Identify the application



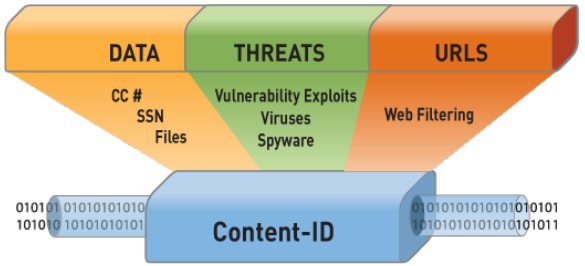
User-ID™

Identify the user



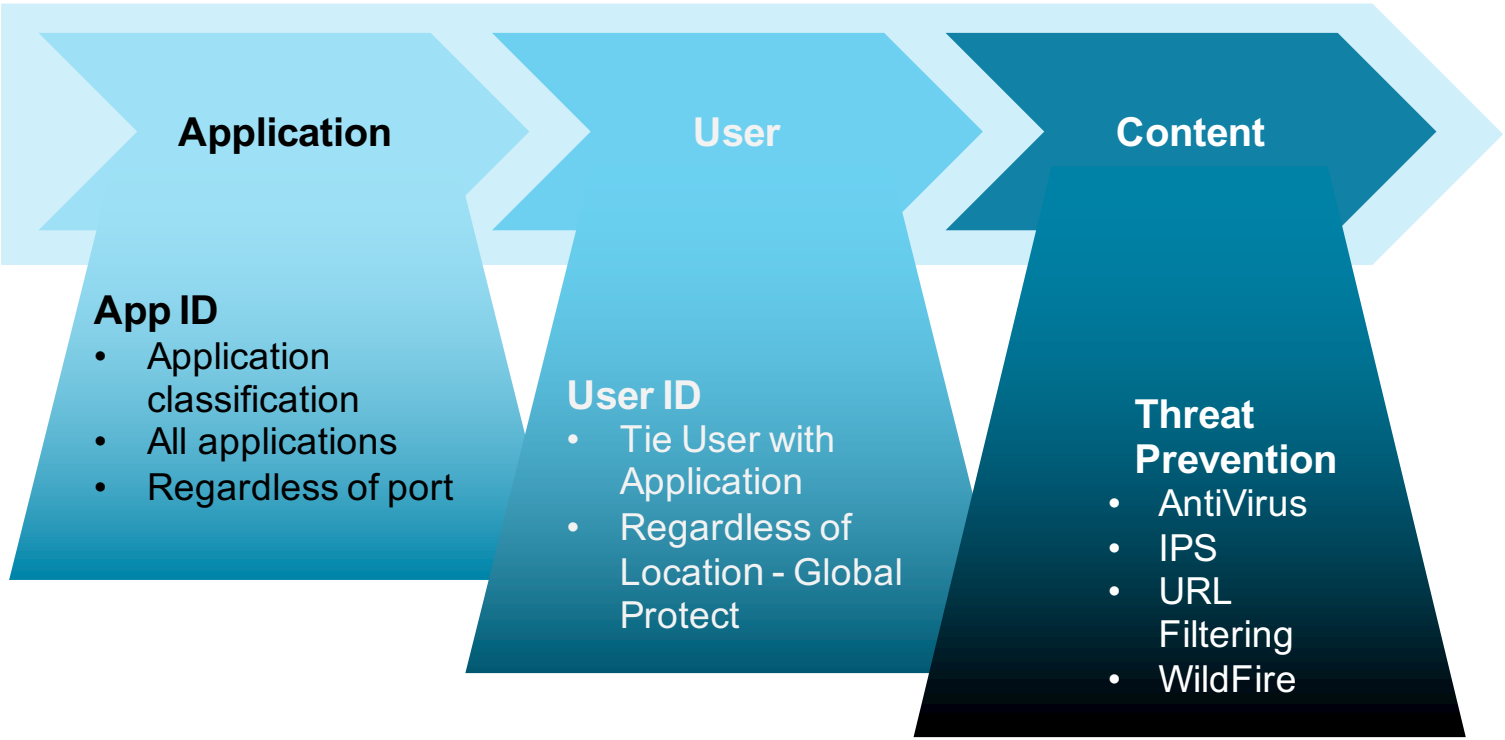
Content-ID™

Scan the content



Efficient Threat Prevention

SINGLE PASS ARCHITECTURE



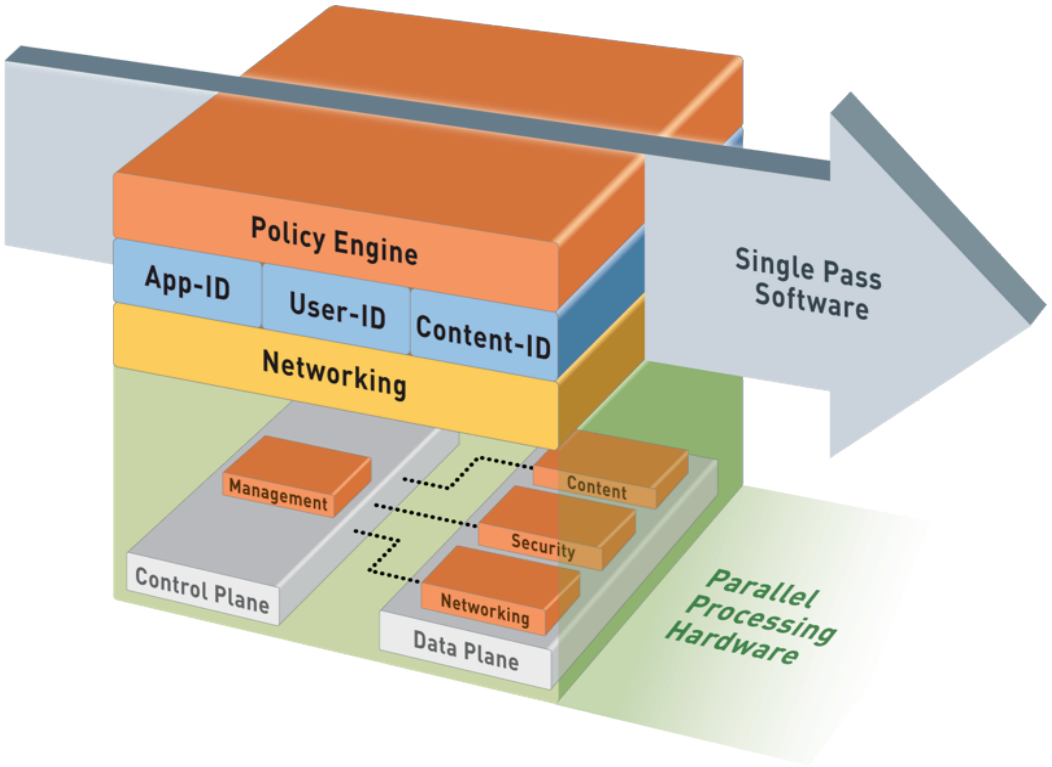
Palo Alto Networks Single Pass Platform Architecture

Single Pass

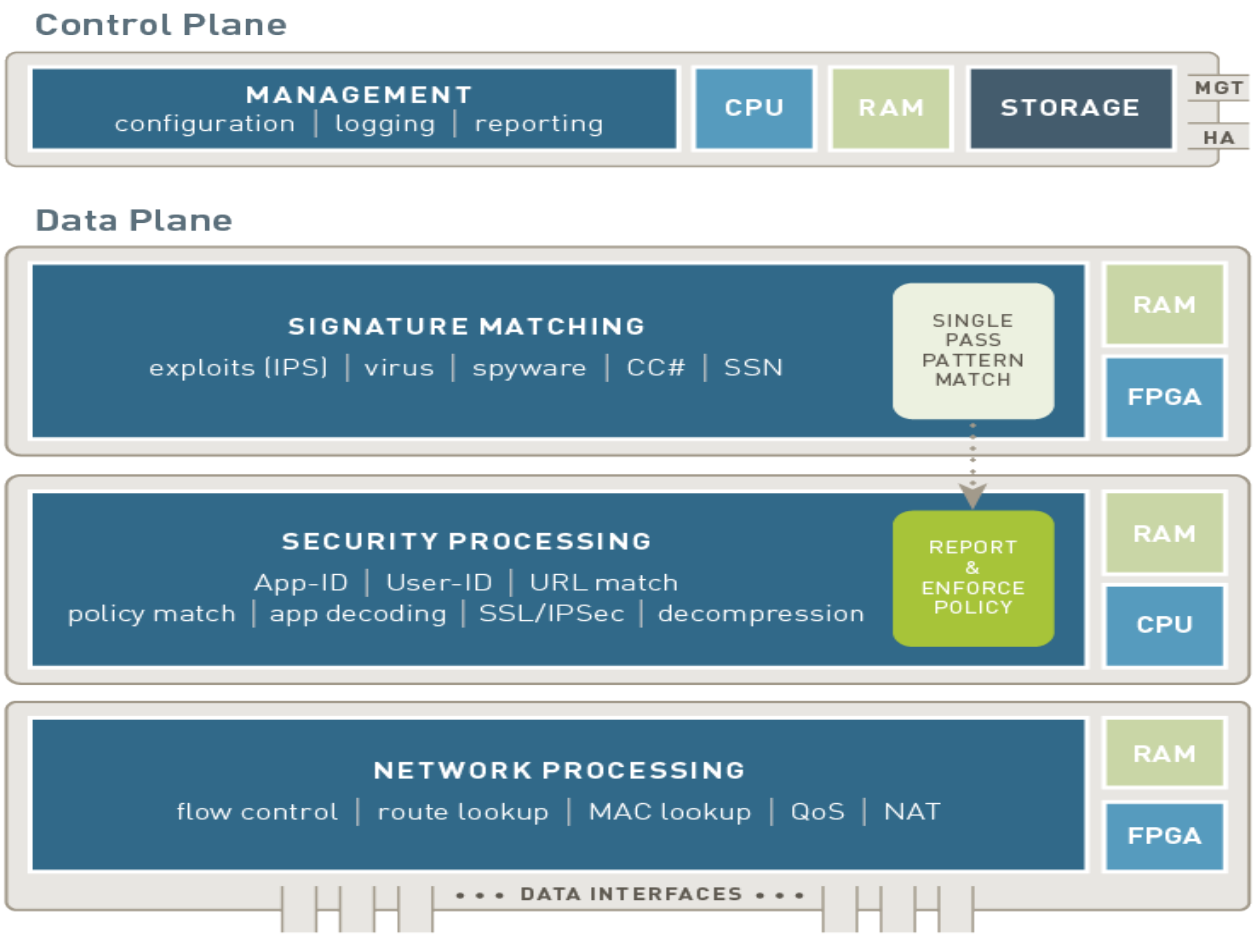
- Operations per packet
  - Traffic classification with App-ID
  - User/group mapping
  - Content scanning – threats, URLs, confidential data
- One policy

Parallel Processing

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



Single Pass Platform Architecture – Hardware View

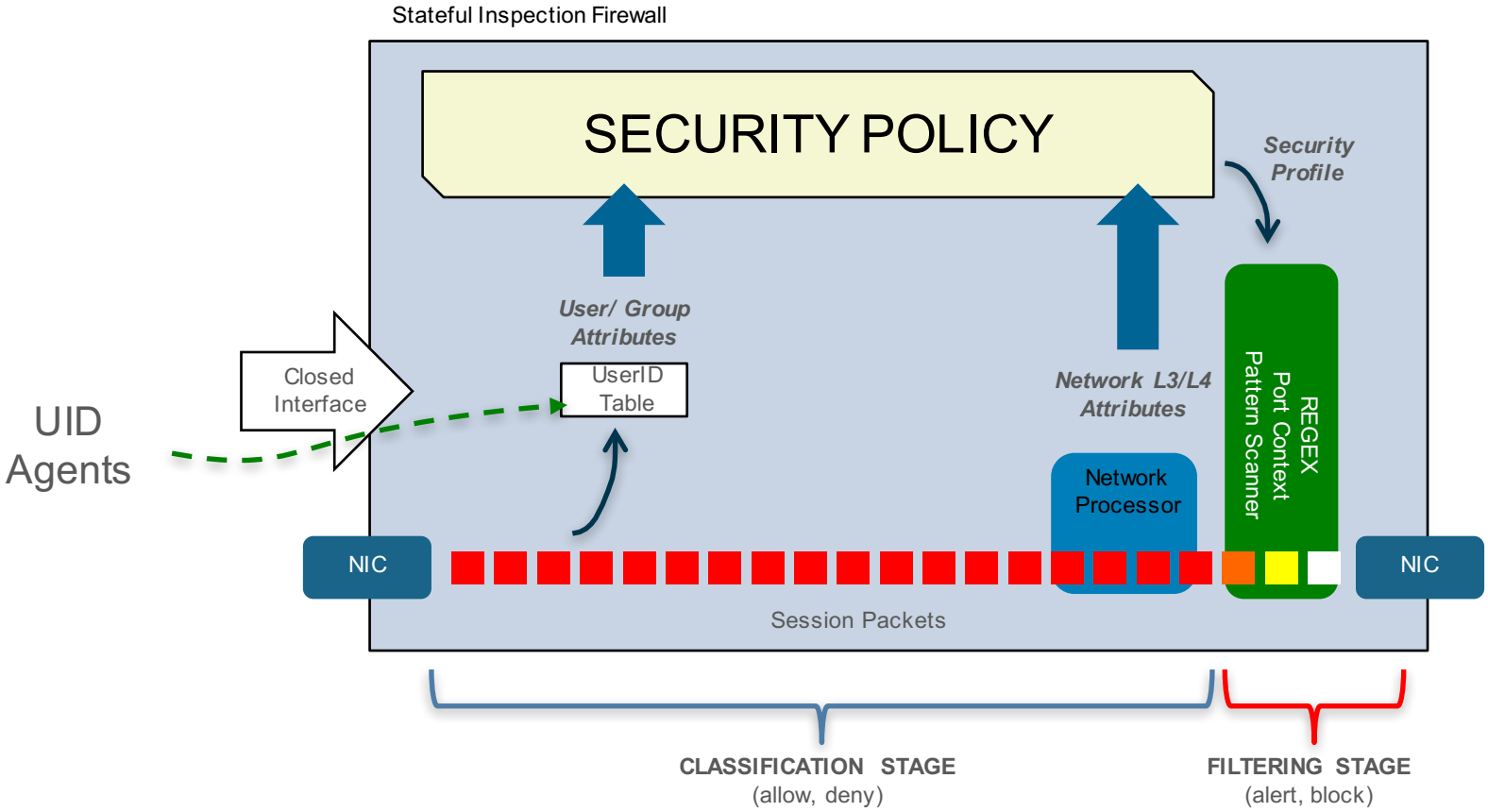


Signature Matching
Stream-based, uniform signature match provides full context to policy engine in a single pass

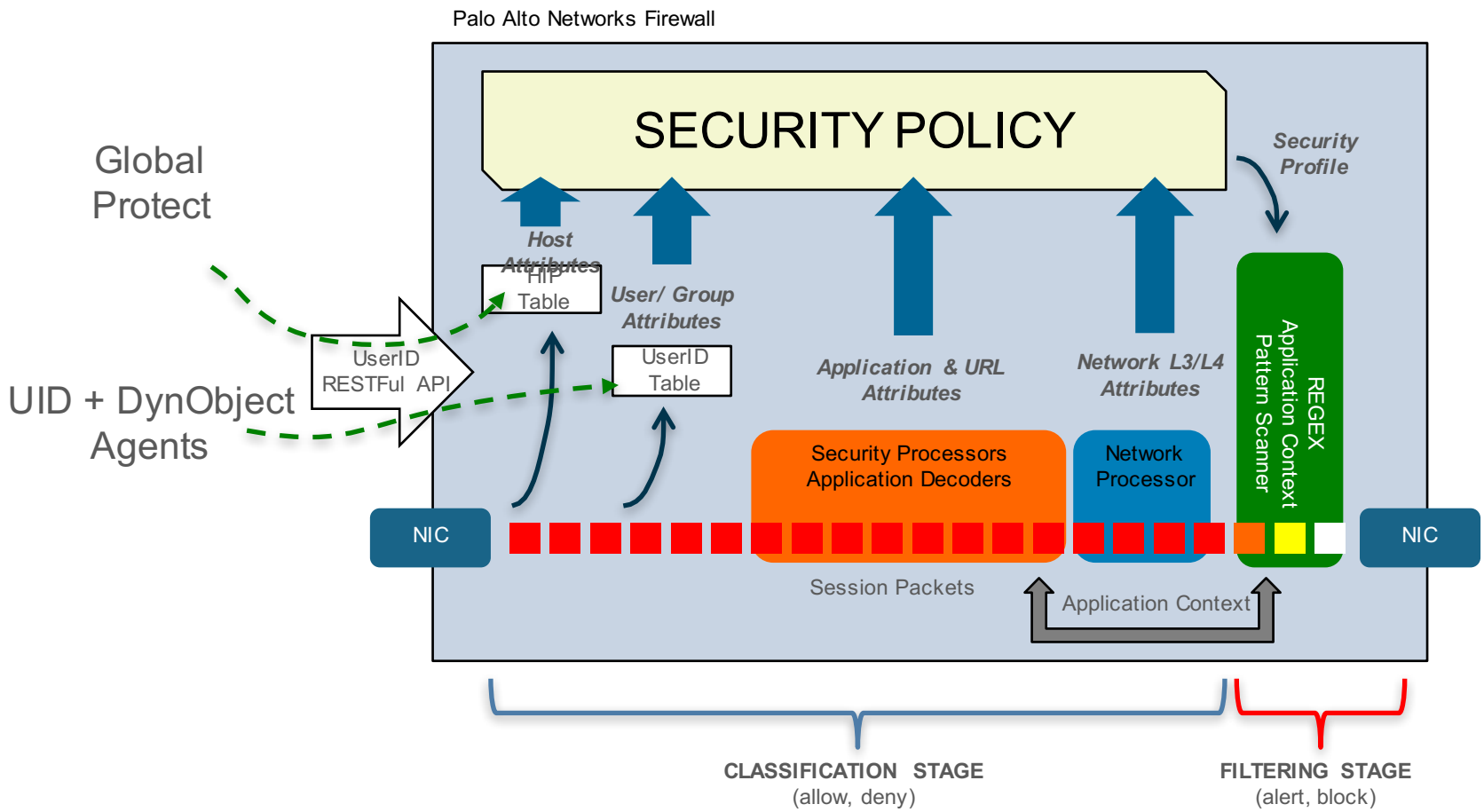
Security Processing
High density parallel processing for flexibility, hardware-acceleration for standardized complex functions

Network Processing
Front-end network processing, hardware accelerated per-packet route lookup, MAC lookup and NAT

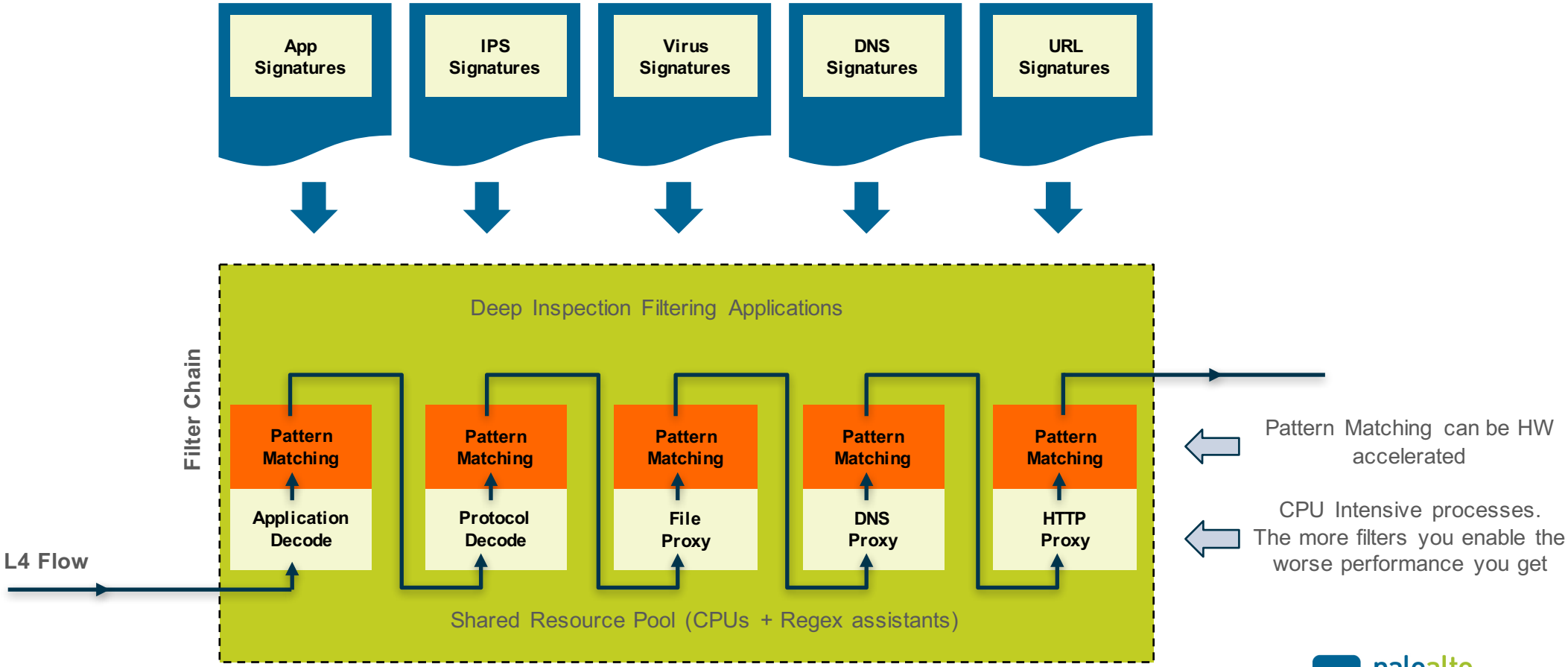
How does a NGFW-like firewall work?
(All self-claimed NGFW except Palo Alto Networks)



How does a Palo Alto Networks Firewall work?

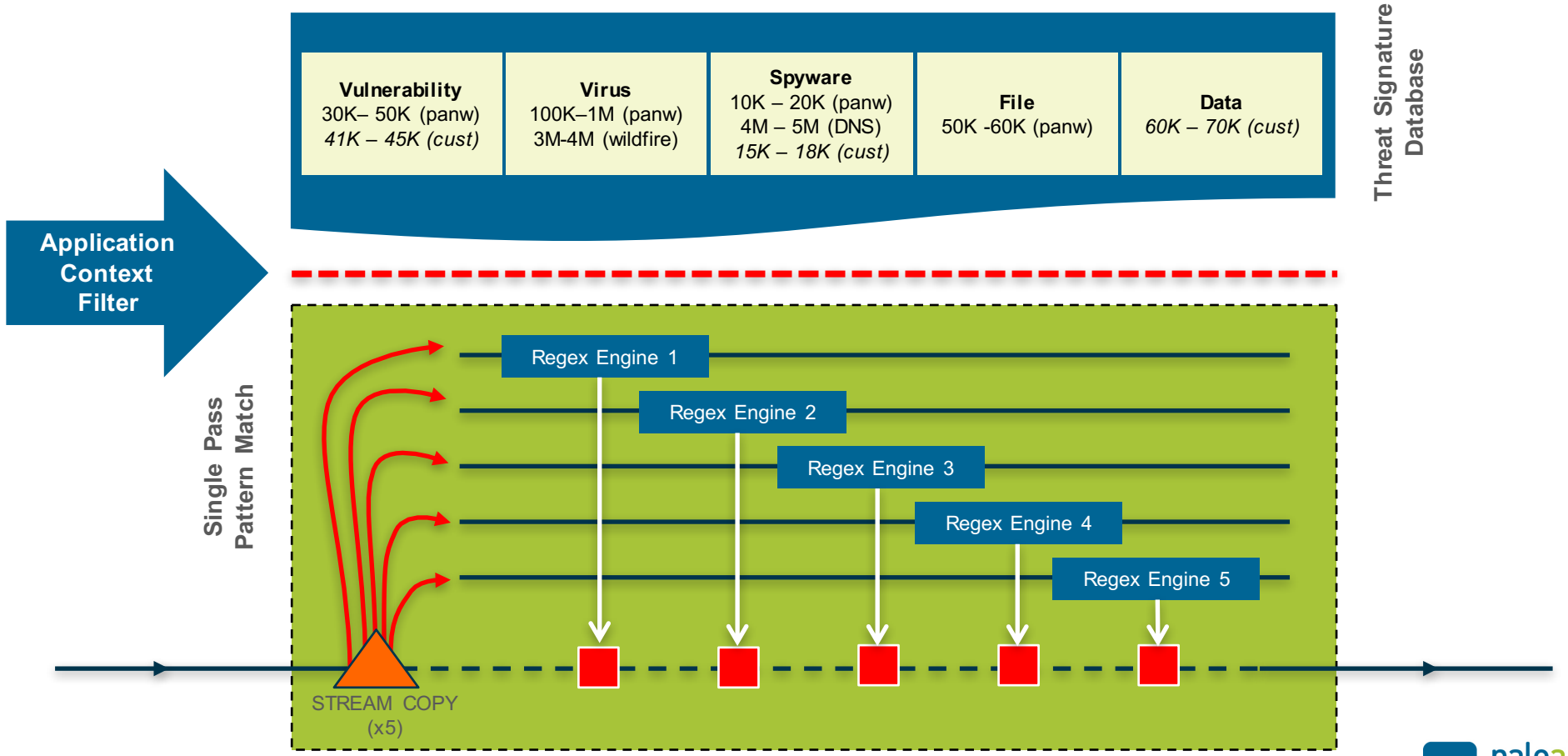


UTM Filter Chain: Fighting for the same shared resources



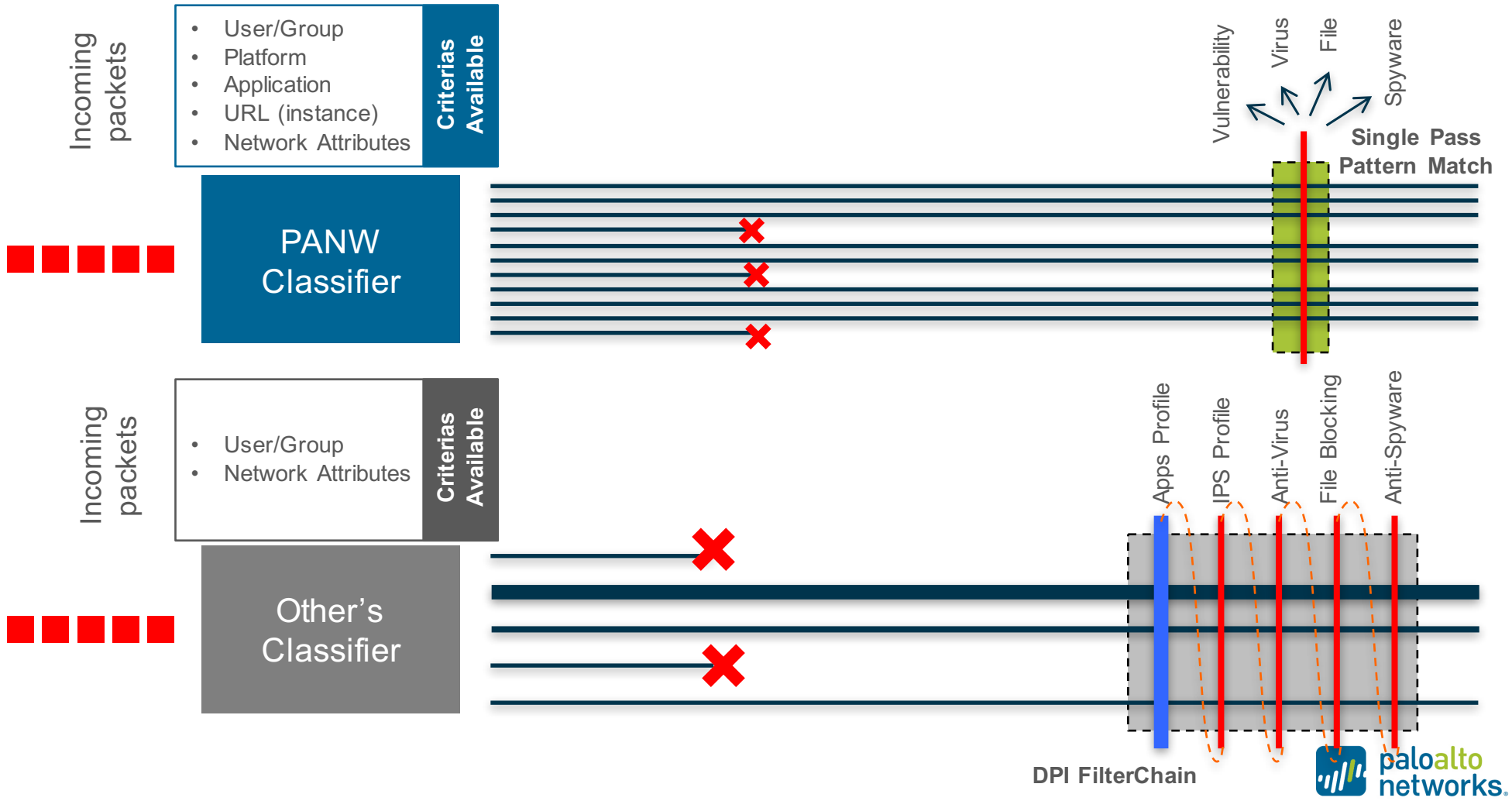
paloalto networks

SP3: High-performance low-latency parallel deep inspection. Easy when you've classified the traffic by app.



paloalto networks

Classify Applications vs Application Filter

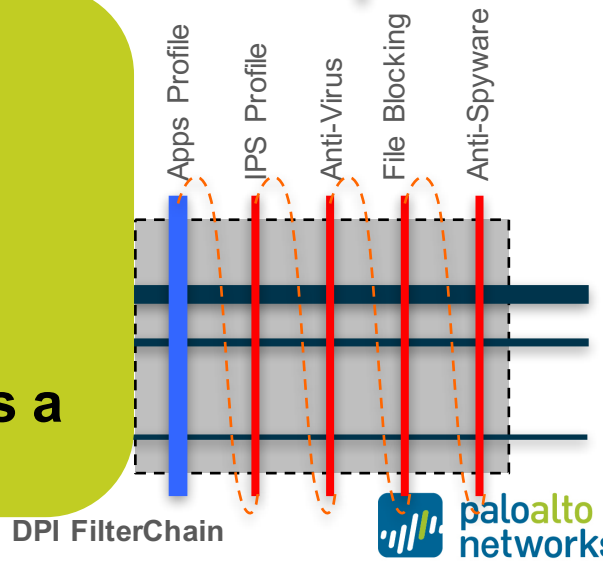


Classify Applications vs Application Filter

The key is

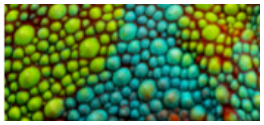
THEY WILL NEVER BE CAPABLE

to apply a different "security profile" based on application because the application control (filter) is a component of the "security profile" itself



paloalto networks

Our Approach: Seek First to Understand
The Power of Context



- classify all traffic to app level
  even encrypted traffic
- determine who (users)
- continually update this understanding
  includes content inspection

Then Enforce

Better decisions based on full situational awareness

Fully Understand + *Enforce*

document xfer

Fred (finance group)

other context

Allow

or

Deny

or

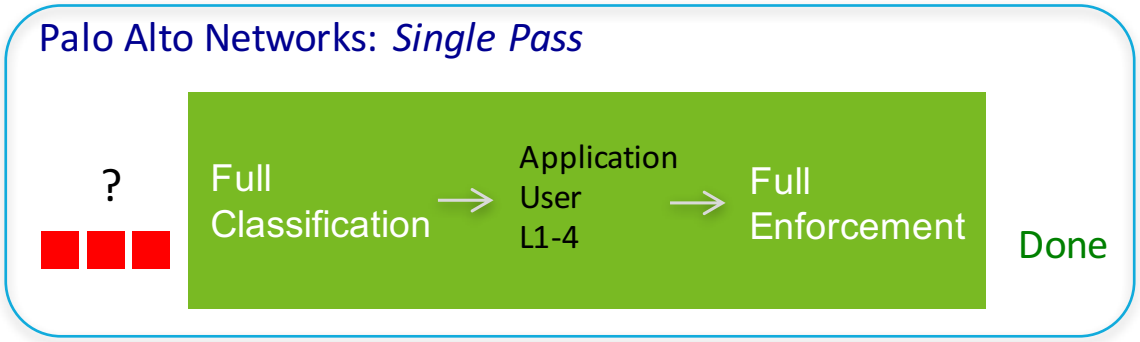
Allow, **but**:

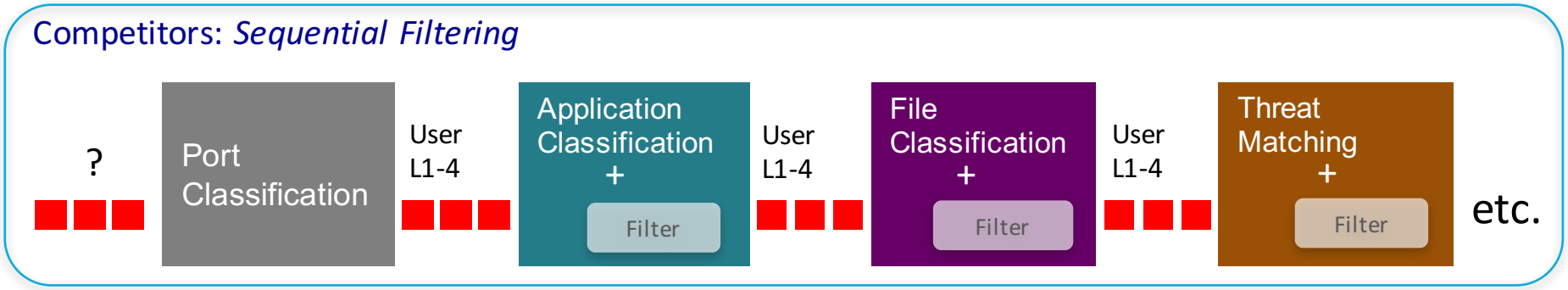
scan for threats
block files
per schedule
etc.

(Enables)

- a positive enforcement model
- stepwise refinement
- systematic management of unknown

A Fundamentally Different Architecture





Safe Applications Enablement – control each application independently

Web-browsing

e.g. CNN.com NBC NEWS

Block all file types

Cloud Backup

e.g. Dropbox SkyDrive

Allow all file types

Web Mail

e.g. Gmail Yahoo! Mail

Block all web mail like applications

Ms SharePoint

or salesforce SAP SAP NetWeaver

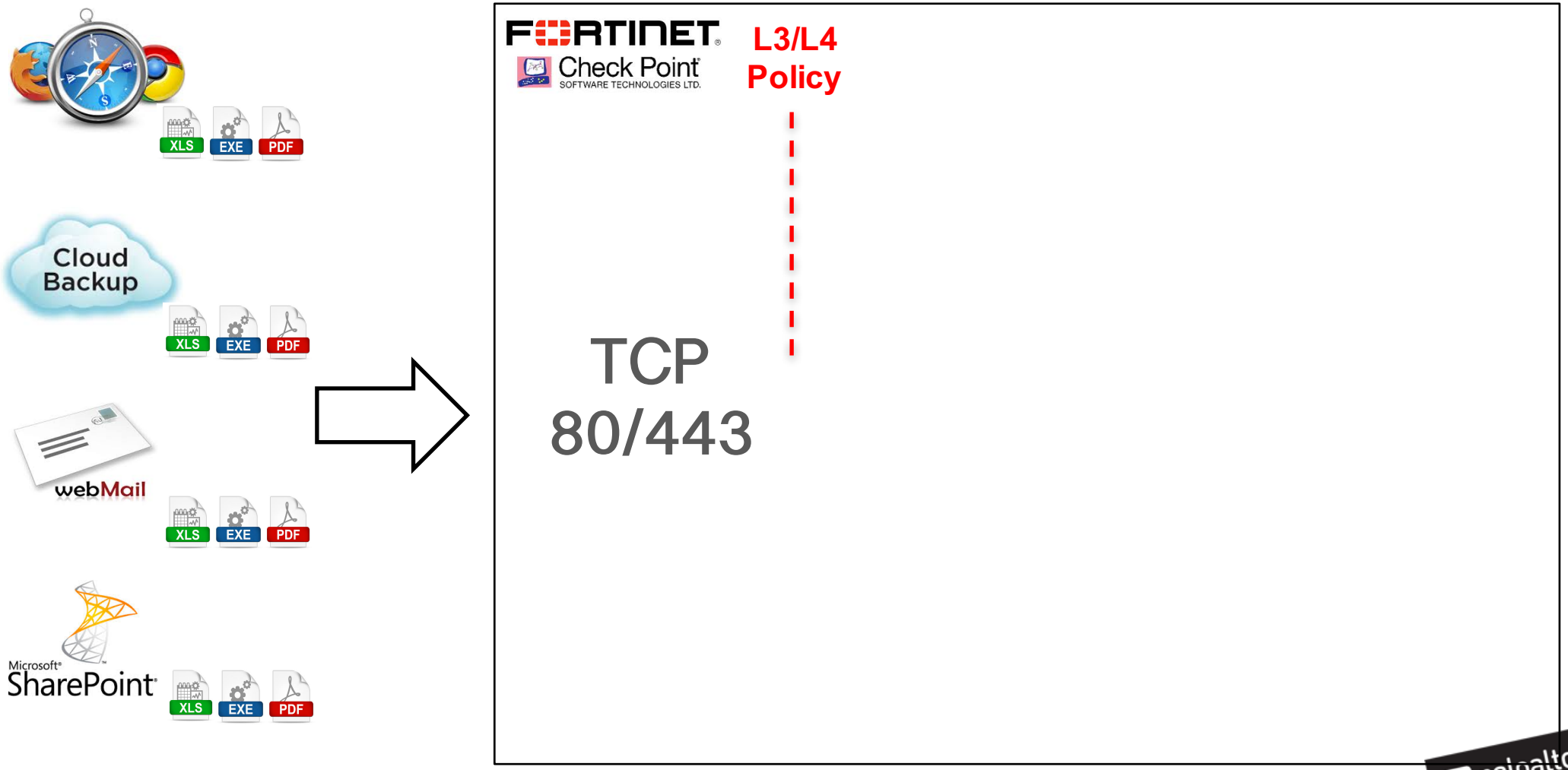
Block only EXE files

paloalto NETWORKS

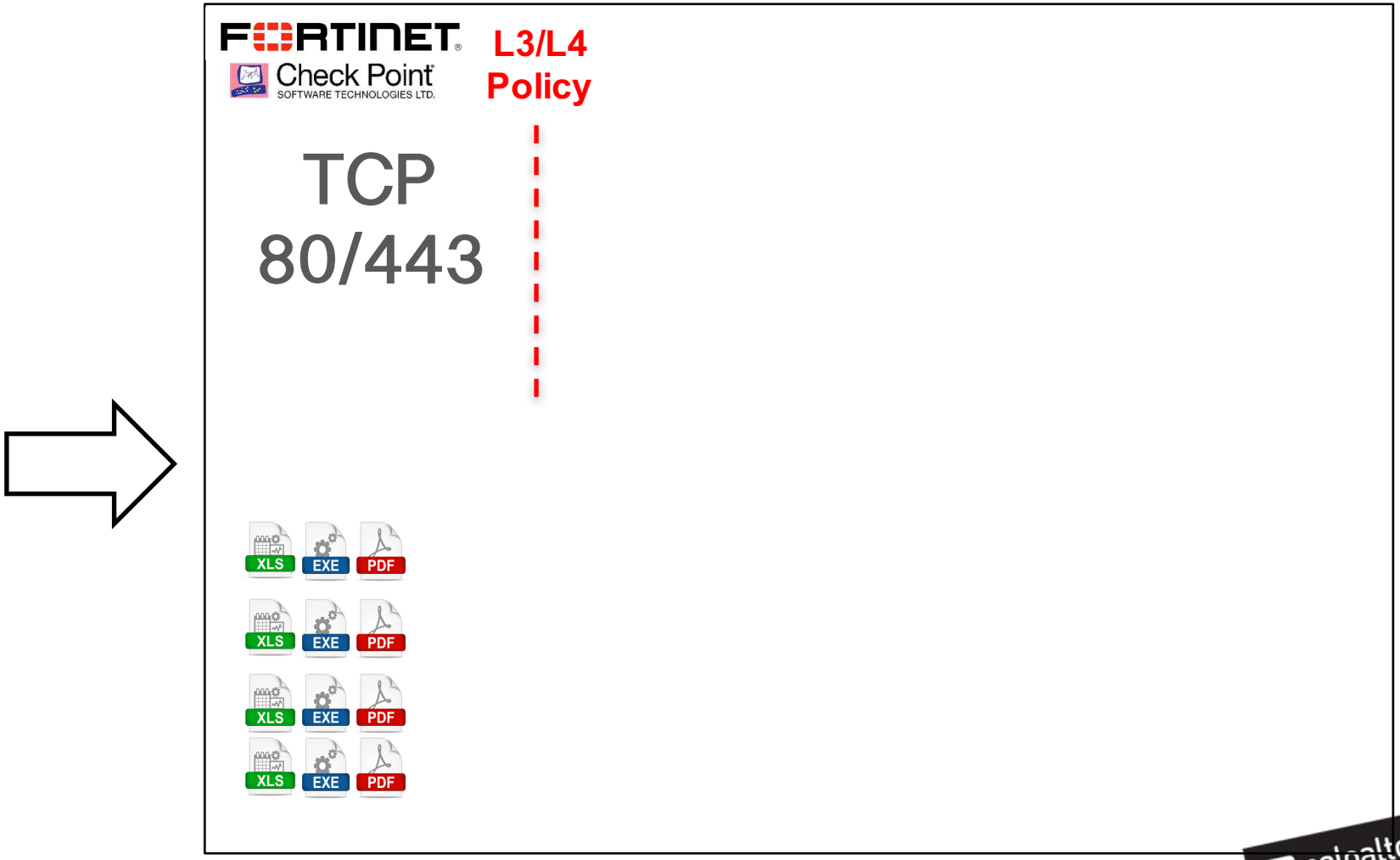
Safe Applications Enablement – control each application independently

Let's check if we can get the same configuration and how easy it is to setup such requirements using different vendors solutions

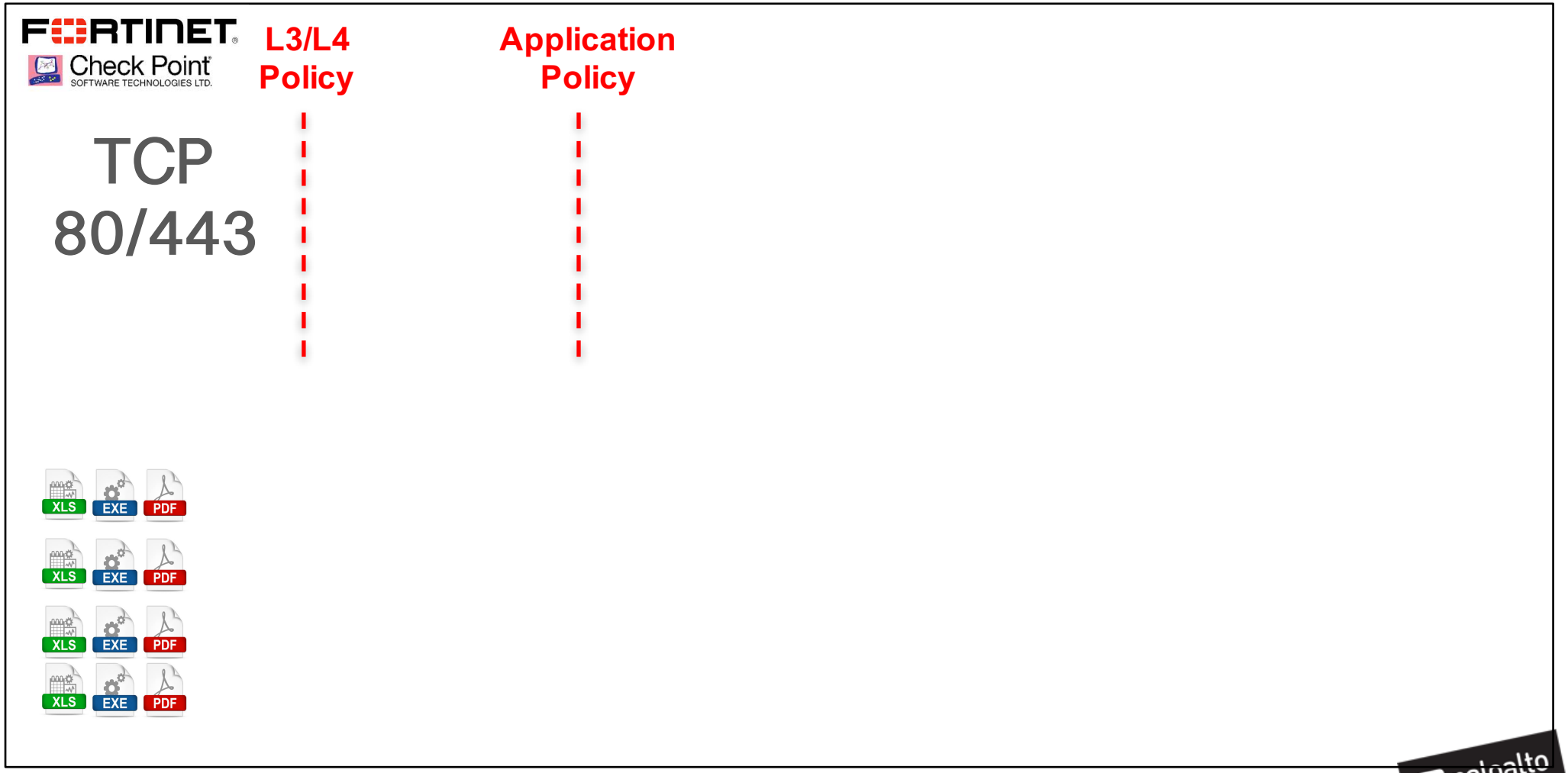
Safe Applications Enablement – control each application independently



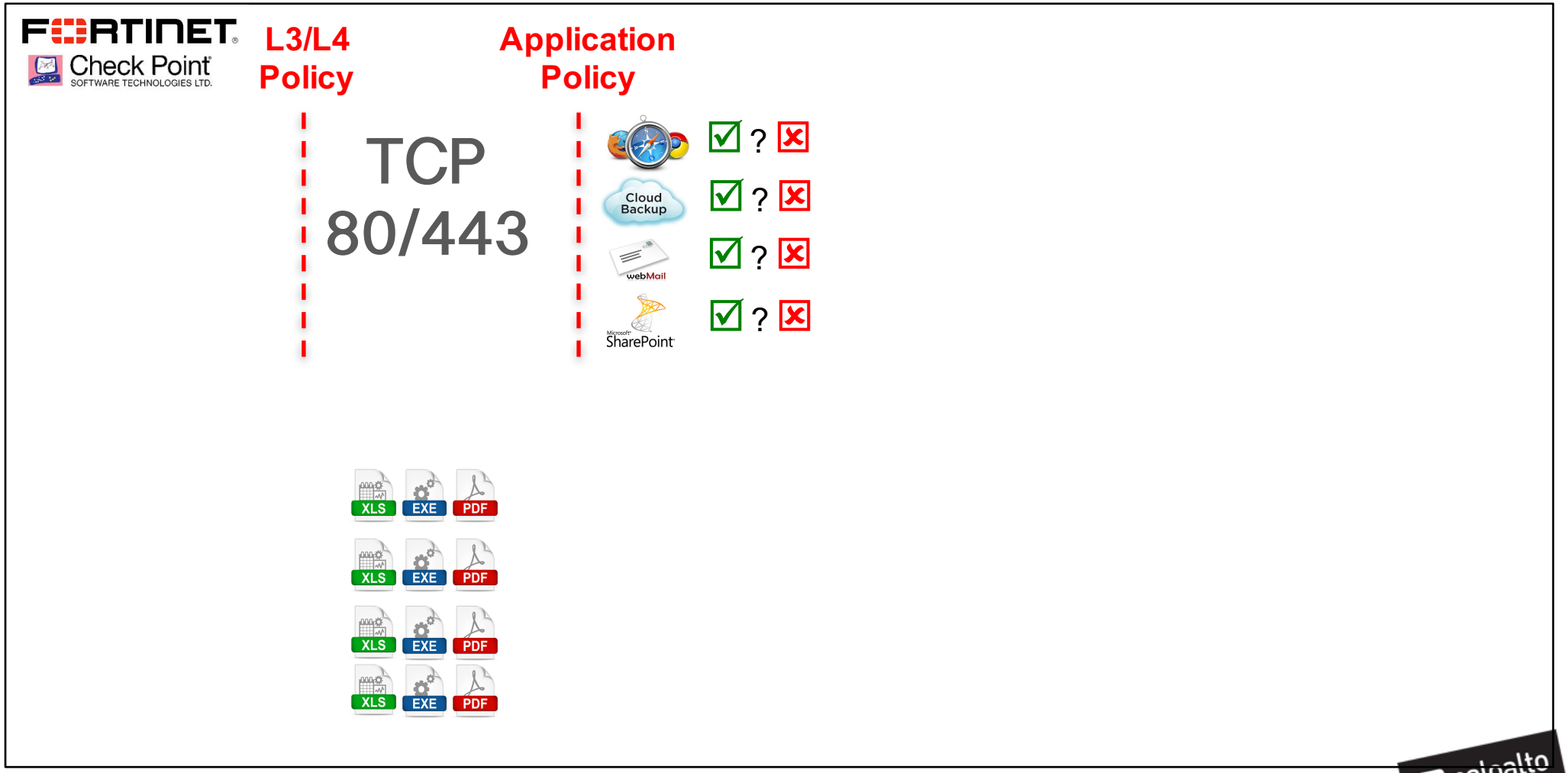
Safe Applications Enablement – control each application independently



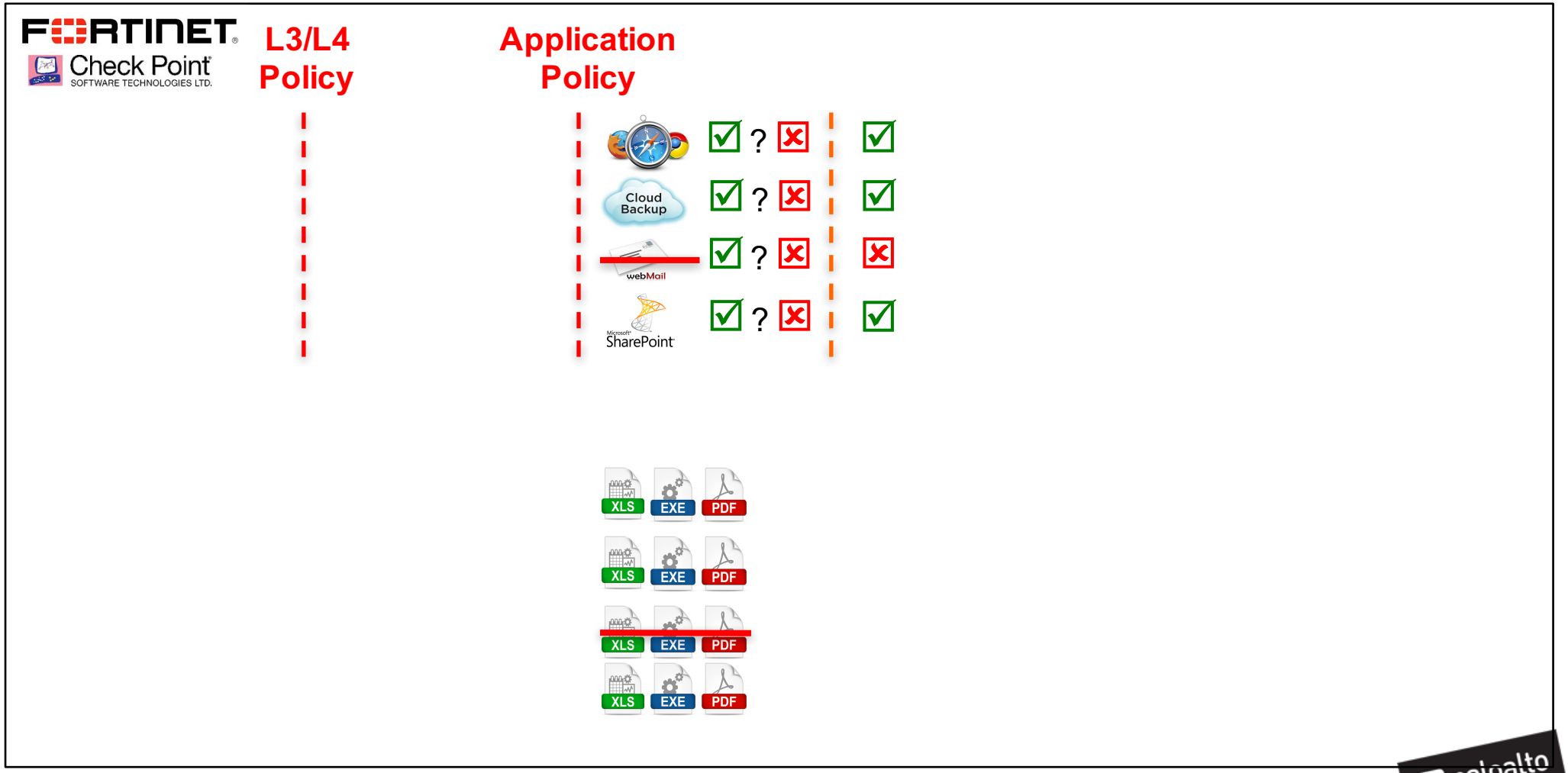
Safe Applications Enablement – control each application independently



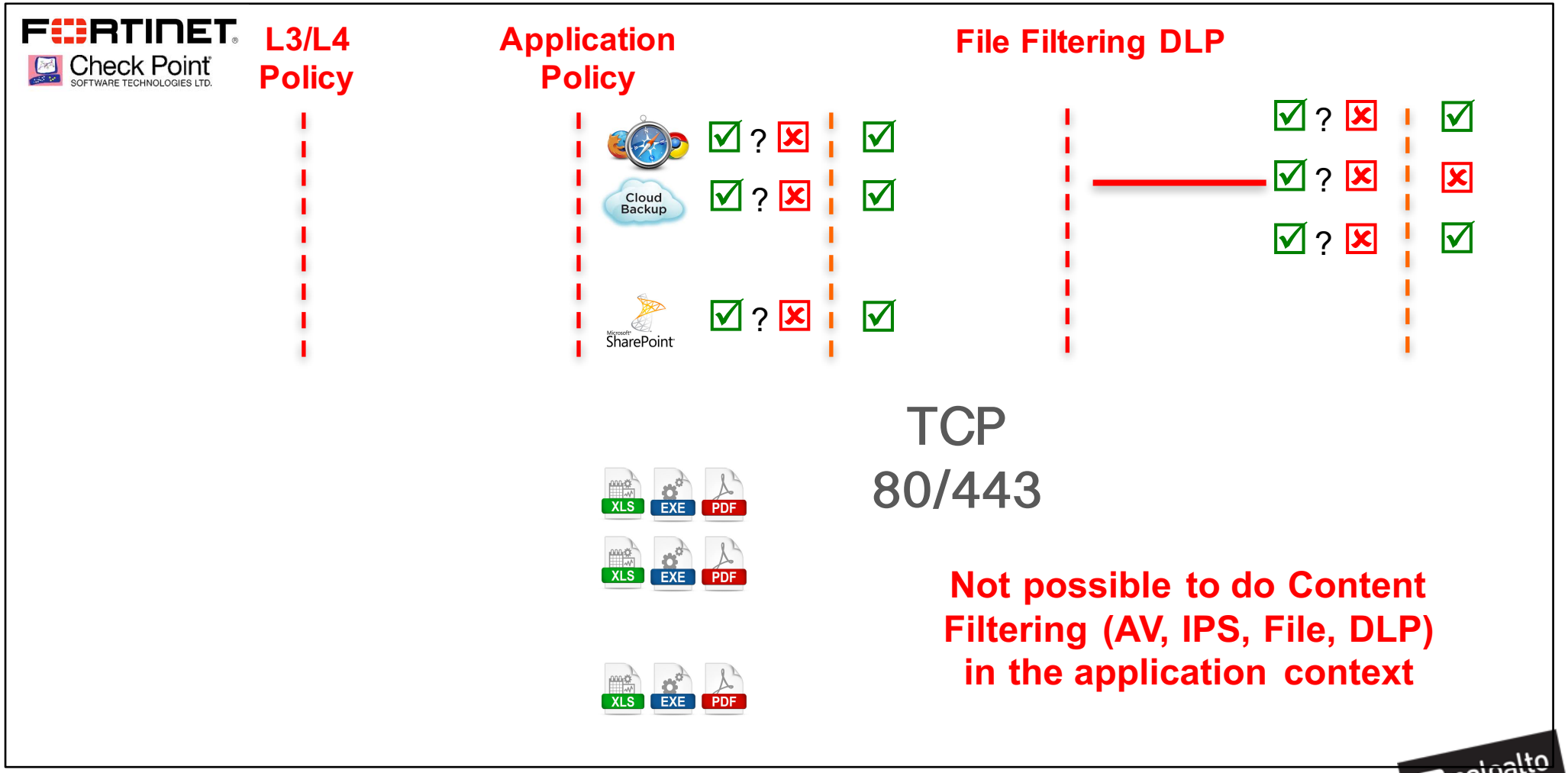
Safe Applications Enablement – control each application independently



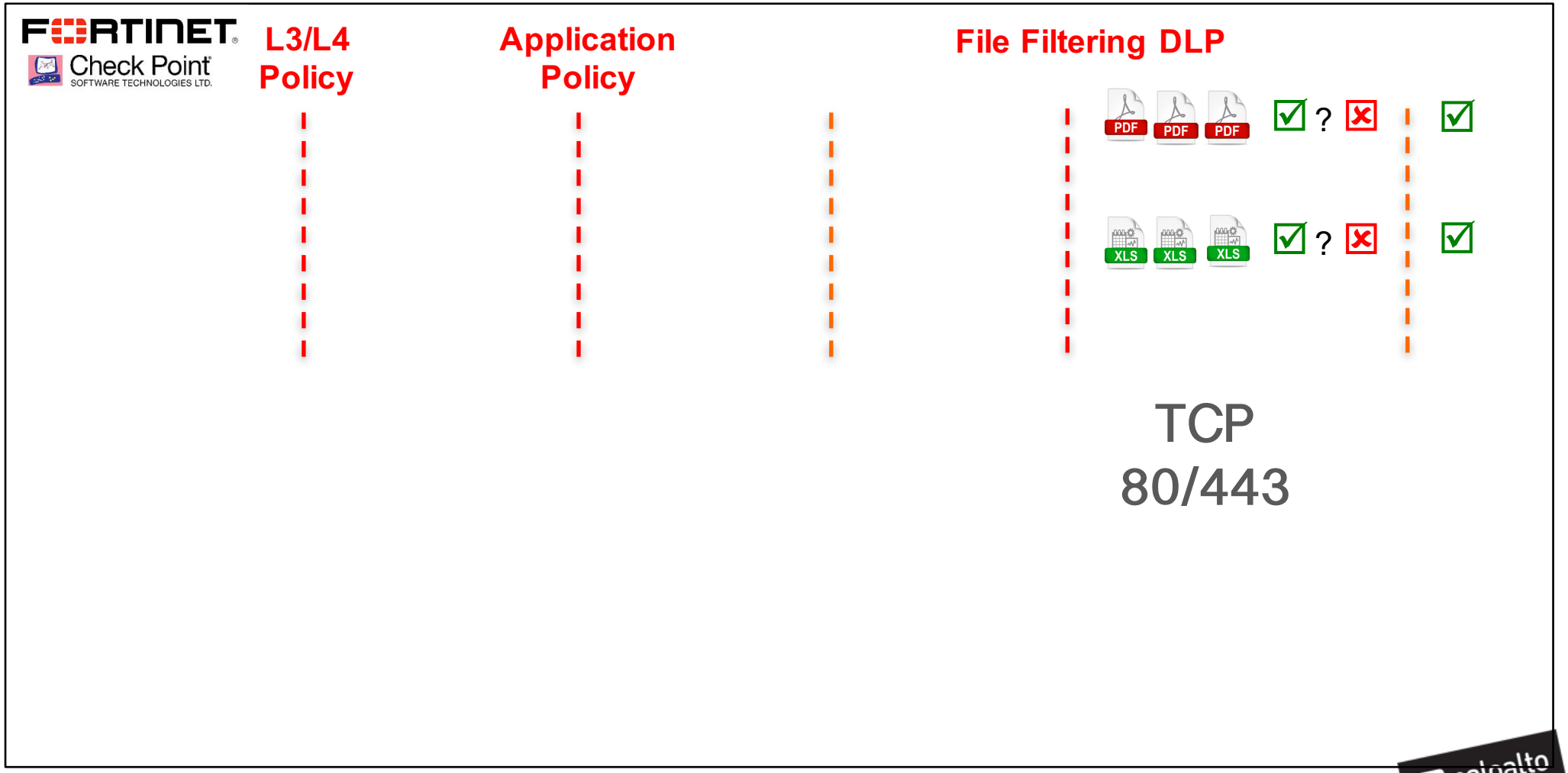
Safe Applications Enablement – control each application independently



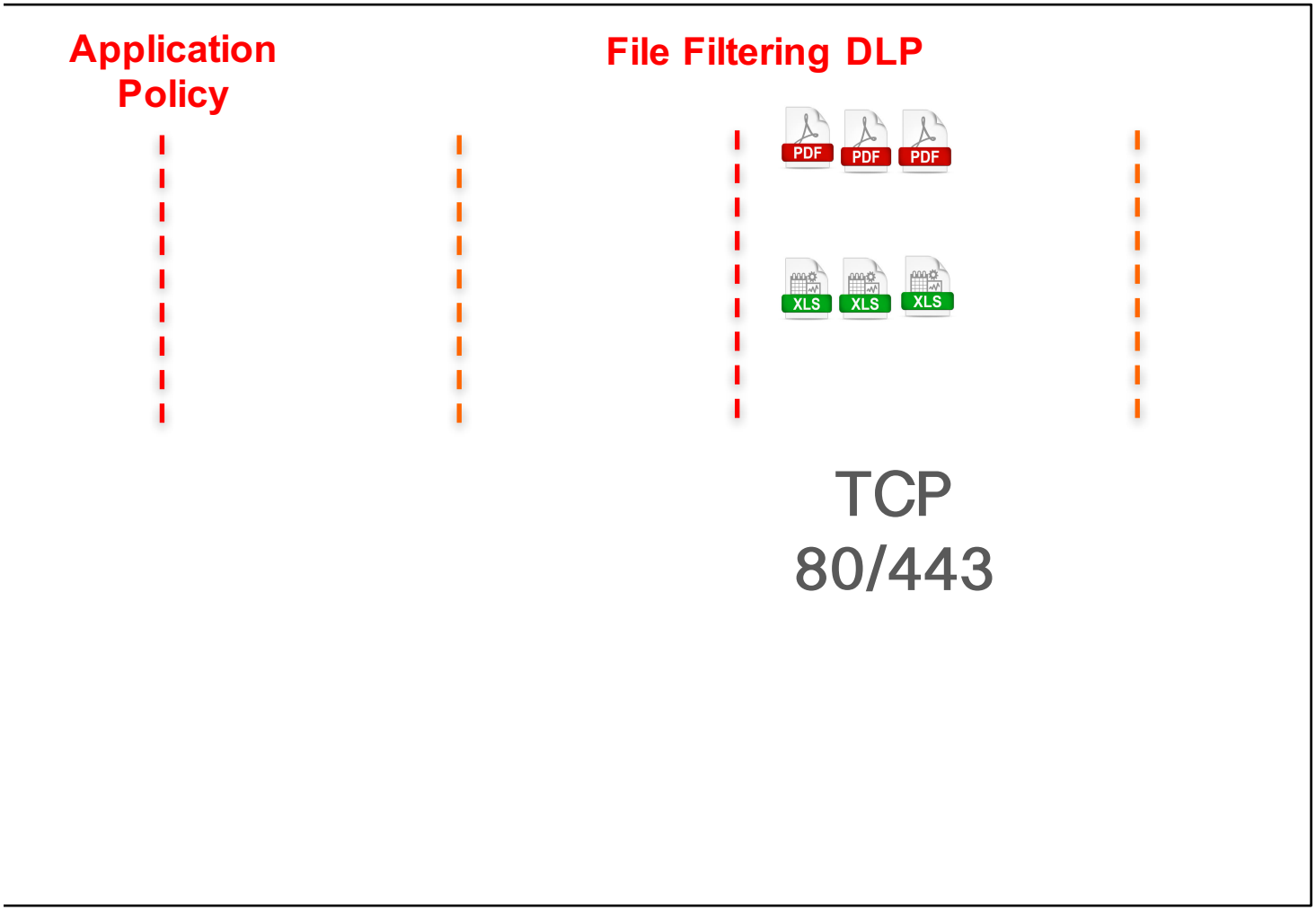
Safe Applications Enablement – control each application independently



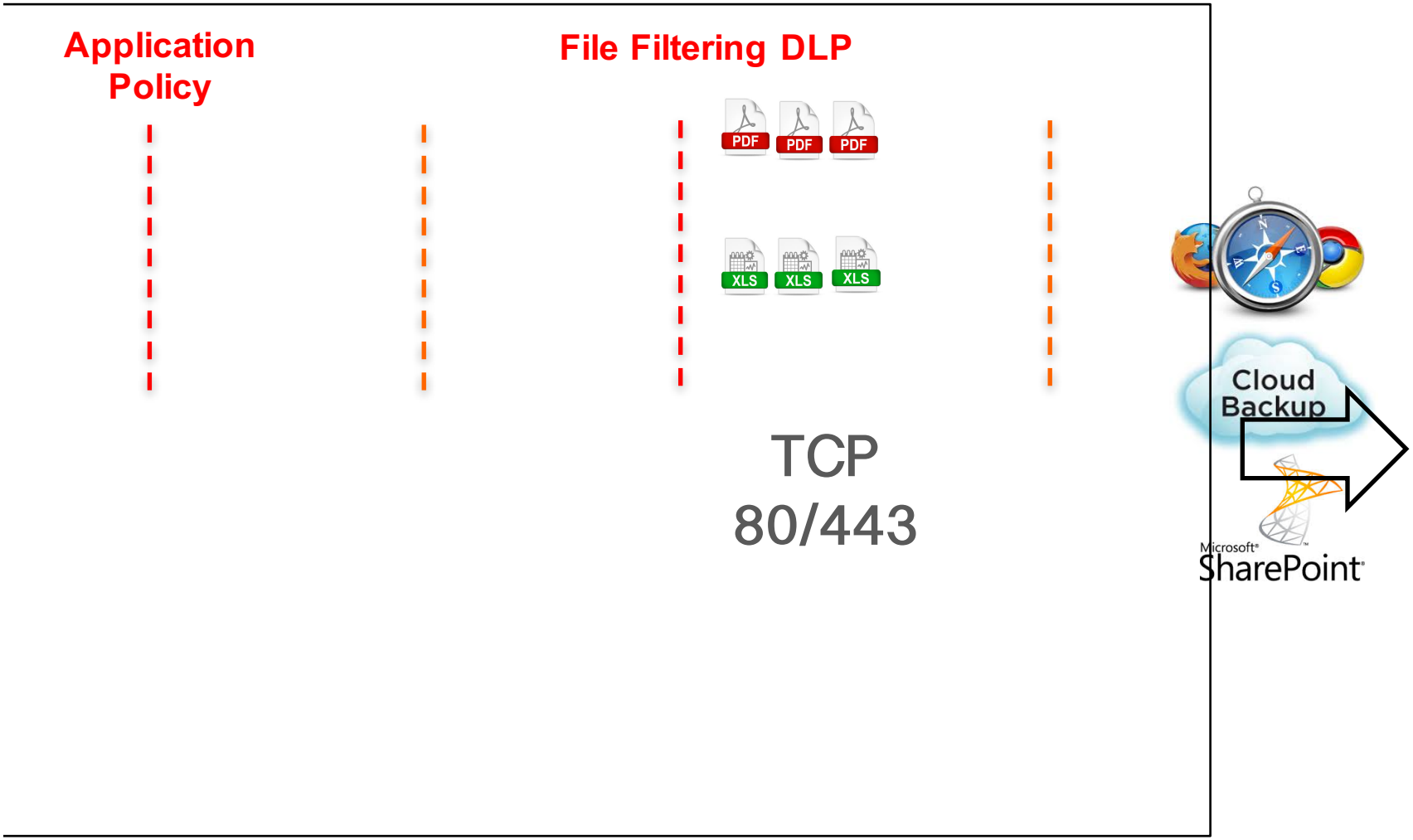
Safe Applications Enablement – control each application independently



Safe Applications Enablement – control each application independently



Safe Applications Enablement – control each application independently

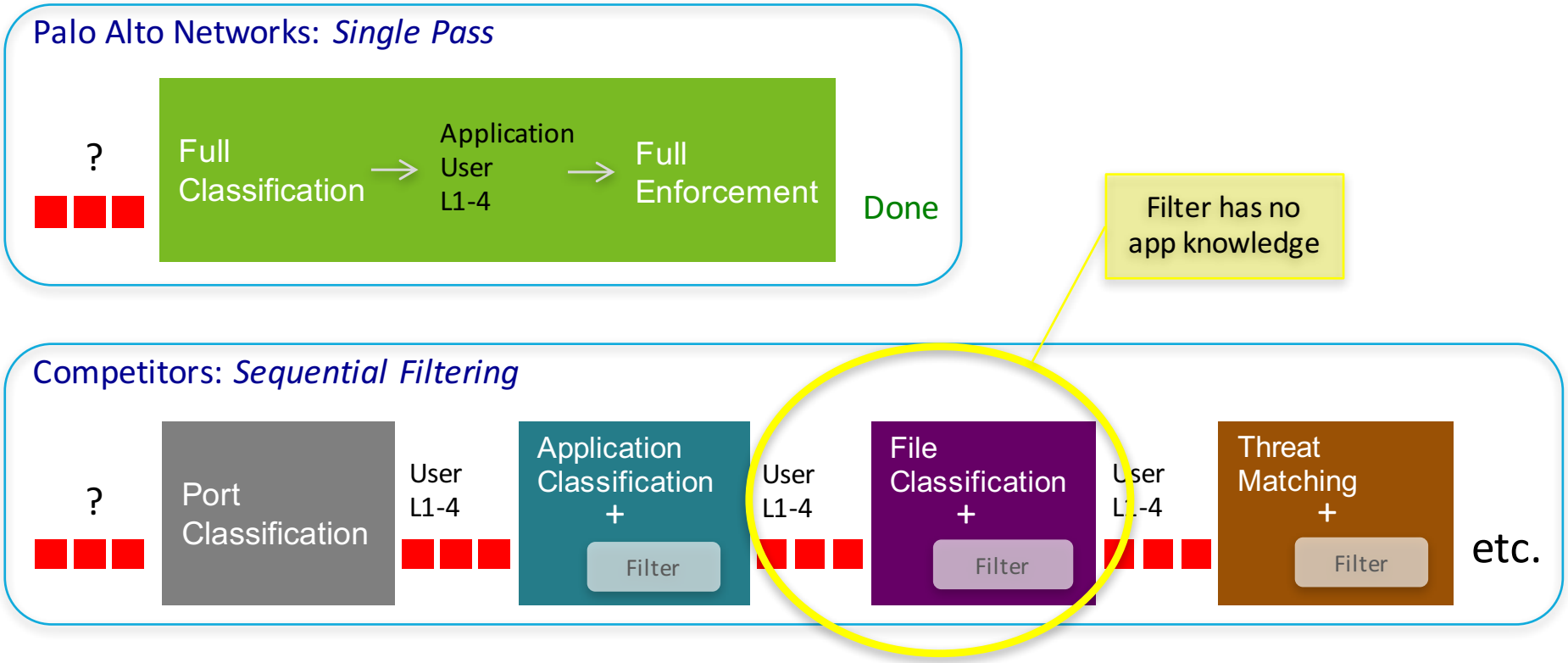


Please note that
Safe Application Enablement
is not only about File Blocking

It is about ALL content filtering features in
Application Context such as:

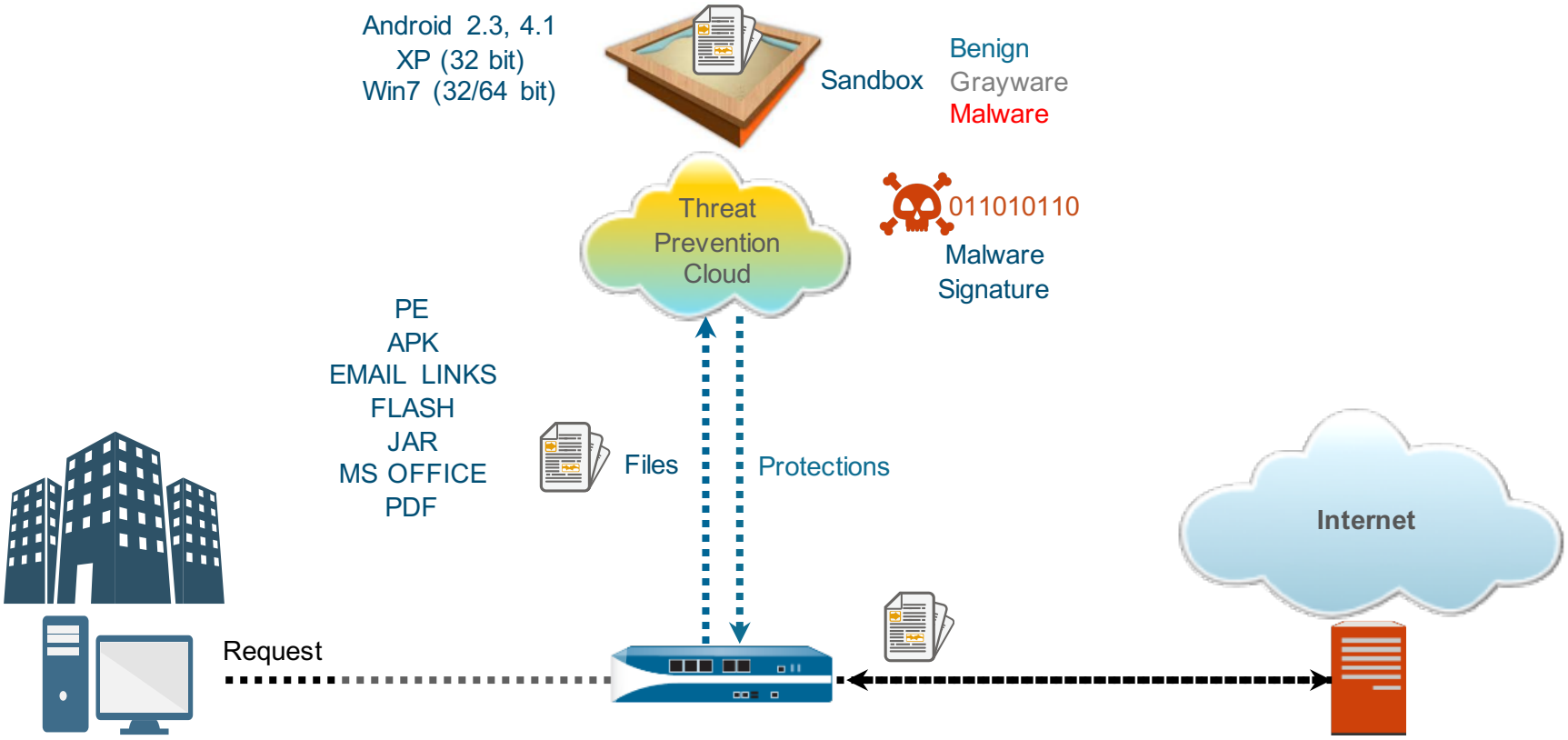
IPS, AV, anti-spyware, URL filtering,
DLP, Wildfire (zero-day attacks protection)

Why? The Architecture.



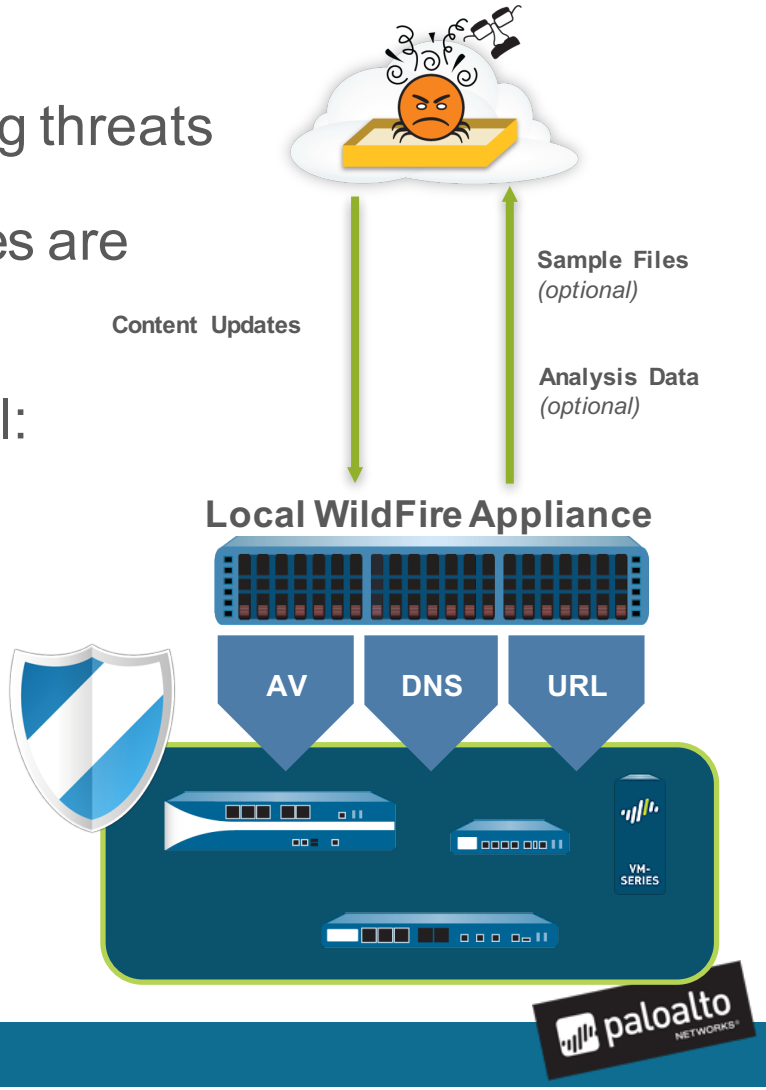
Wildfire

Wildfire


Android 2.3, 4.1
XP (32 bit)
Win7 (32/64 bit)
Sandbox
Benign
Grayware
Malware
Threat Prevention Cloud
011010110
Malware Signature
PE
APK
EMAIL LINKS
FLASH
JAR
MS OFFICE
PDF
Files
Protections
Internet
Request

Wildfire Retention

- We receive feeds from over 55 sources regarding threats
- 350,000 files per day from external threat sources are uploaded into WildFire
- We are refreshing signatures daily on the firewall:
  - Signature retention on the firewall
    - AV signatures – 1M
    - WF signatures – 100K
    - DNS signatures – 100K



WildFire Detects Malware Using Multiple Methods & Techniques

Static Analysis

- File Anomaly Detection
- Static Signatures
- String & Code Block Detection
- Machine Learning & Static Analysis

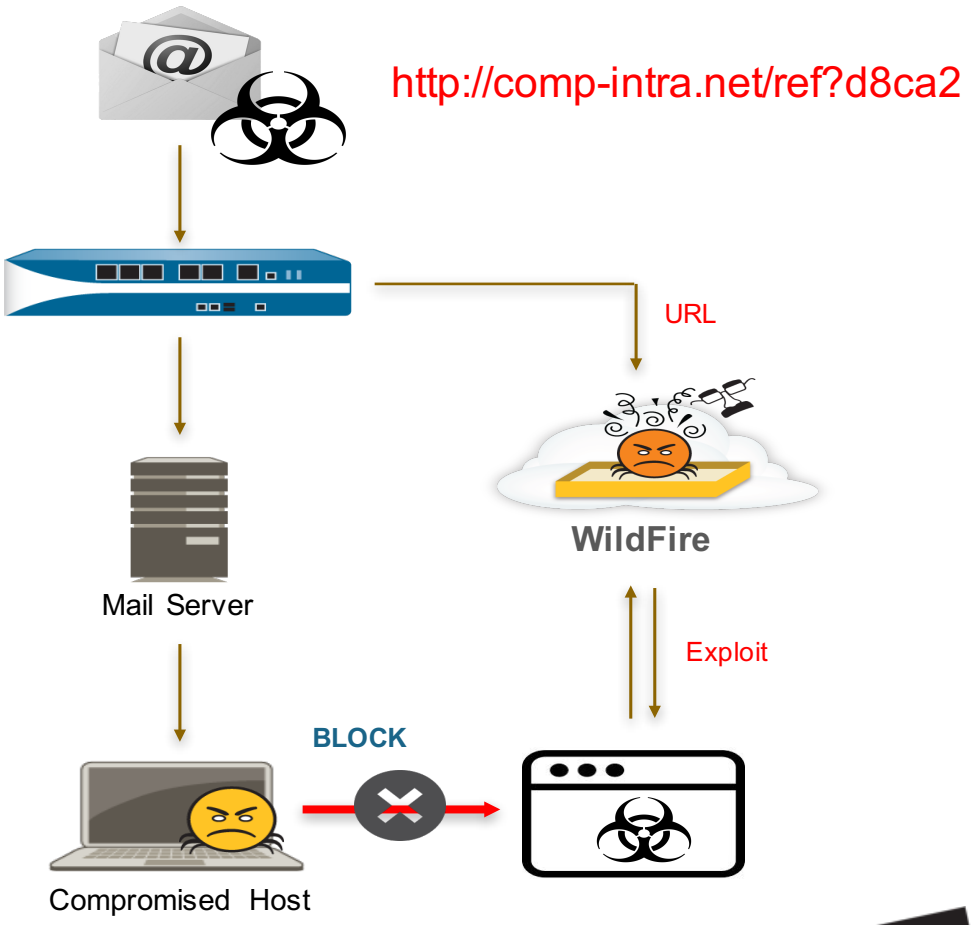
Dynamic Analysis

- Full Execution Analysis
- Multi-version Execution Environment
- Multi-dimensional Scoring
- Network Traffic Analysis

WildFire Turns the *Unknown* into the *Known* in About 5 Minutes

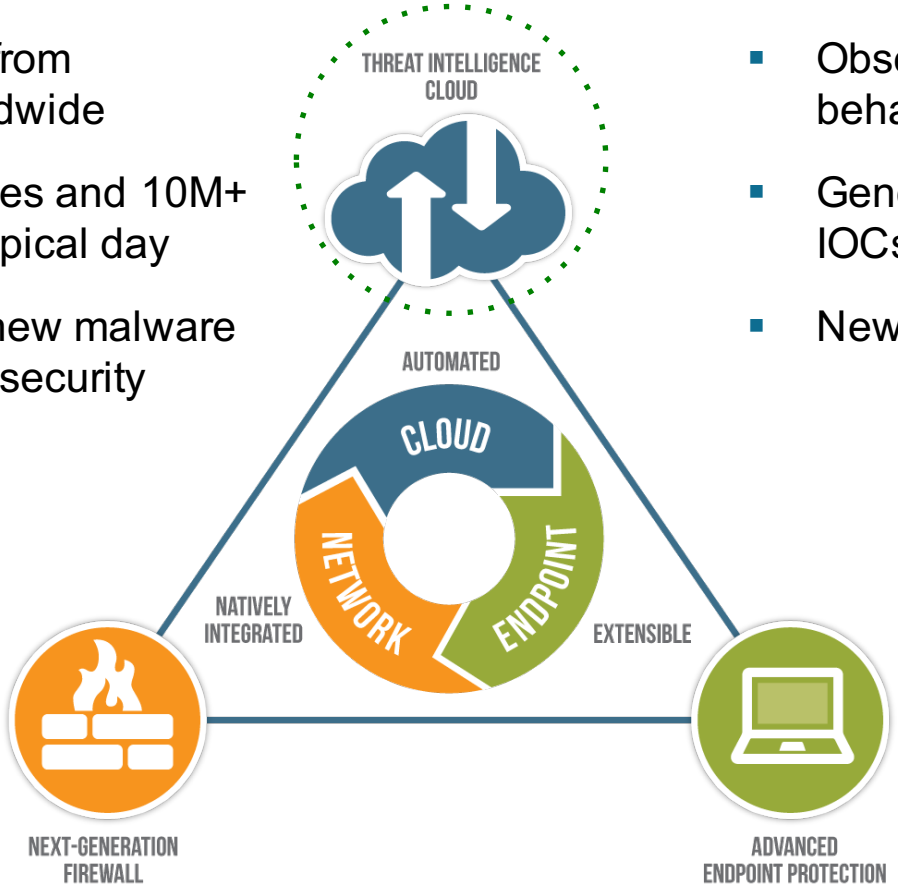
Identify and Protect Against Malicious Email Links

- PAN-OS firewalls detect and send Web links in suspicious emails to WildFire
- WildFire visits the Web page and analyzes the traffic to detect exploits and malware
- Available service with all solutions
  - WildFire public cloud
  - WildFire WF-500
  - Hybrid cloud solution



Palo Alto Networks WildFire cloud-based malware analysis and prevention service

- Powerful network effect from 15,000+ customers worldwide
- Analyzing 3M+ unique files and 10M+ unique email links in a typical day
- Uncovers thousands of new malware not prevented by legacy security products, daily.



- Observes 350+ malicious behaviors to identify malware
- Generates high fidelity IOCs
- New protections in as little as 5mins

Palo Alto Networks Threat Intelligence Cloud

Threat intelligence

- Malware
- Exploits
- Malicious URLs
- DNS queries
- Command & control
- Third-party data
- Unit42
- Community sharing

Automated protection

NGFW

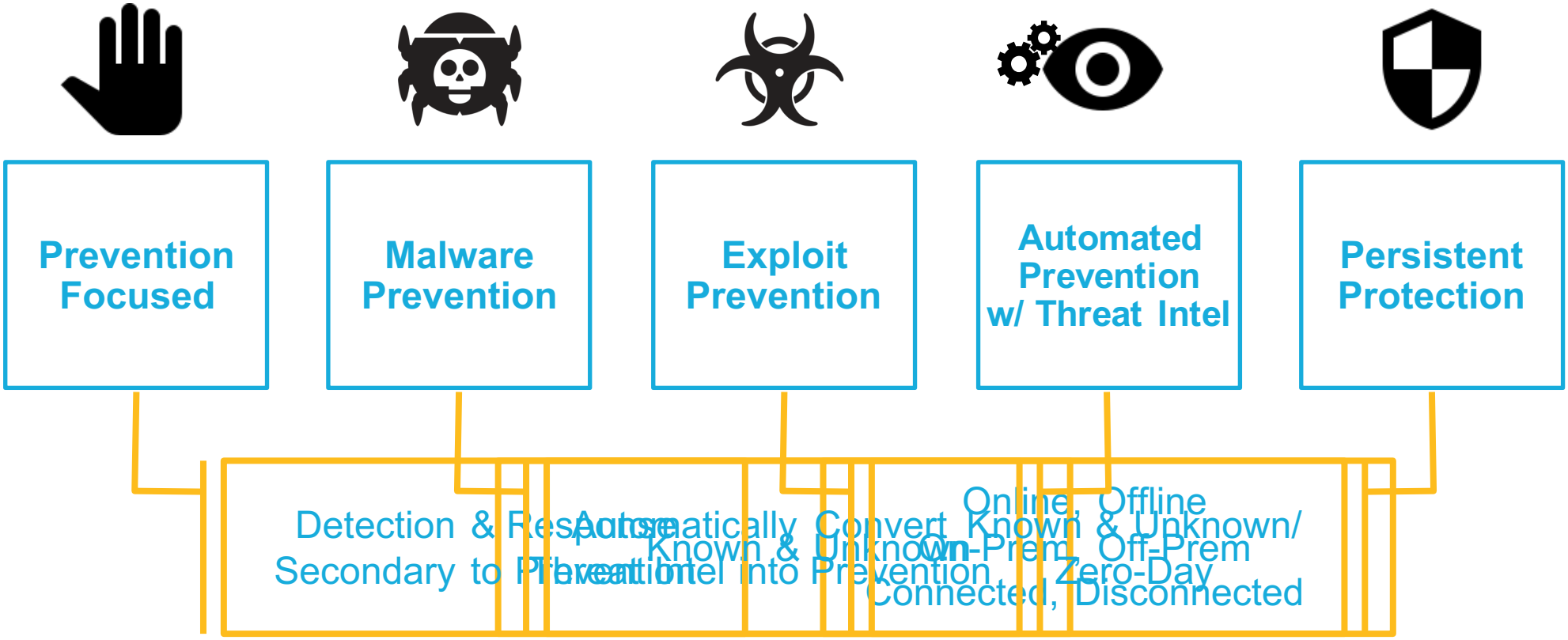
Traps
Advanced
Endpoint Protection

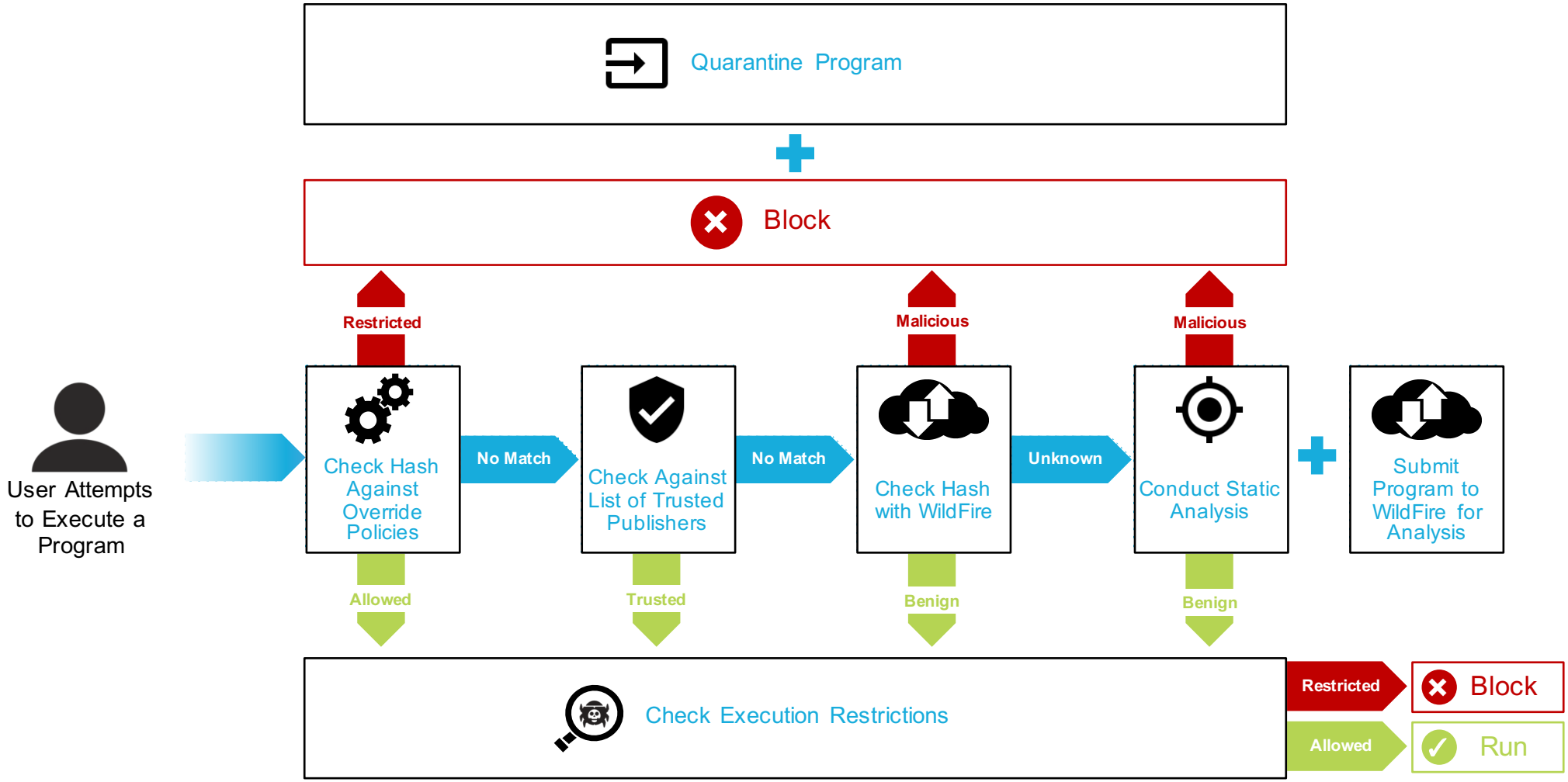
Aperture
Complete SaaS Security

paloalto NETWORKS

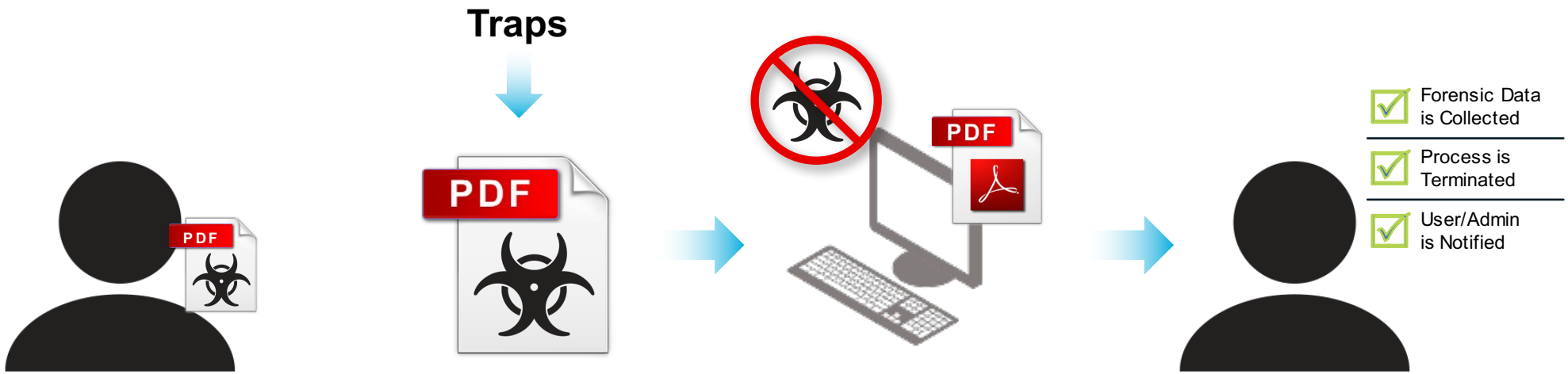
Traps:
Advanced Endpoint Protection
and
AV Replacement

Five Fundamental Capabilities Any AV Replacement Must Deliver





Exploit Prevention – The User Experience



Unsuspecting user opens infected document (Exploit evades Anti-Virus)

Traps injects itself seamlessly into the process

Exploit technique is attempted and blocked by Traps before any malicious activity is initiated

Traps reports the event and collects detailed forensics

Traps is Transparent to the User Until an Exploitation Attempt is Made

Traps Philosophy

Block the core techniques – not individual attacks

Software Vulnerability Exploits

Thousands of new vulnerabilities and exploits a year

Exploitation Techniques

Only 2-4 new exploit techniques a year

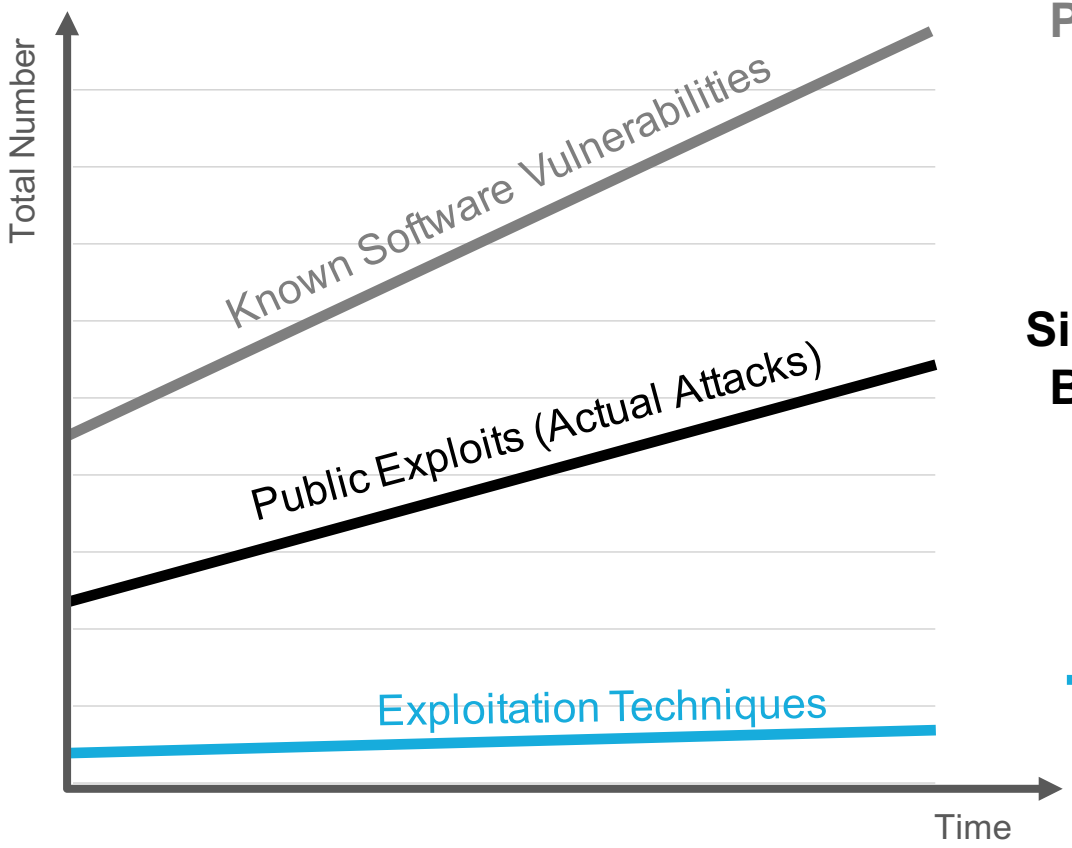
Malware

Millions of new malware every year

Malware Techniques

10's – 100's of new malware sub-techniques every year

Traps Prevents Exploits At Their Core



Patching

Requires Prior Knowledge, Proactive Application

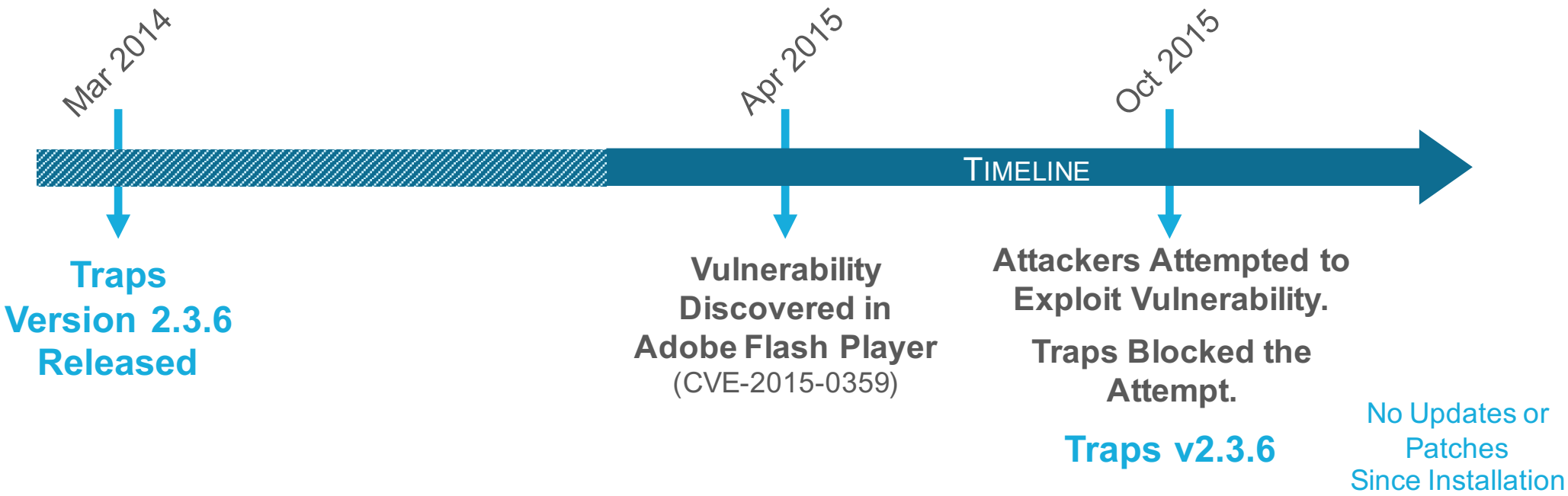
Signature / Behavior

Requires Prior Knowledge of Weaponized Exploits

Traps

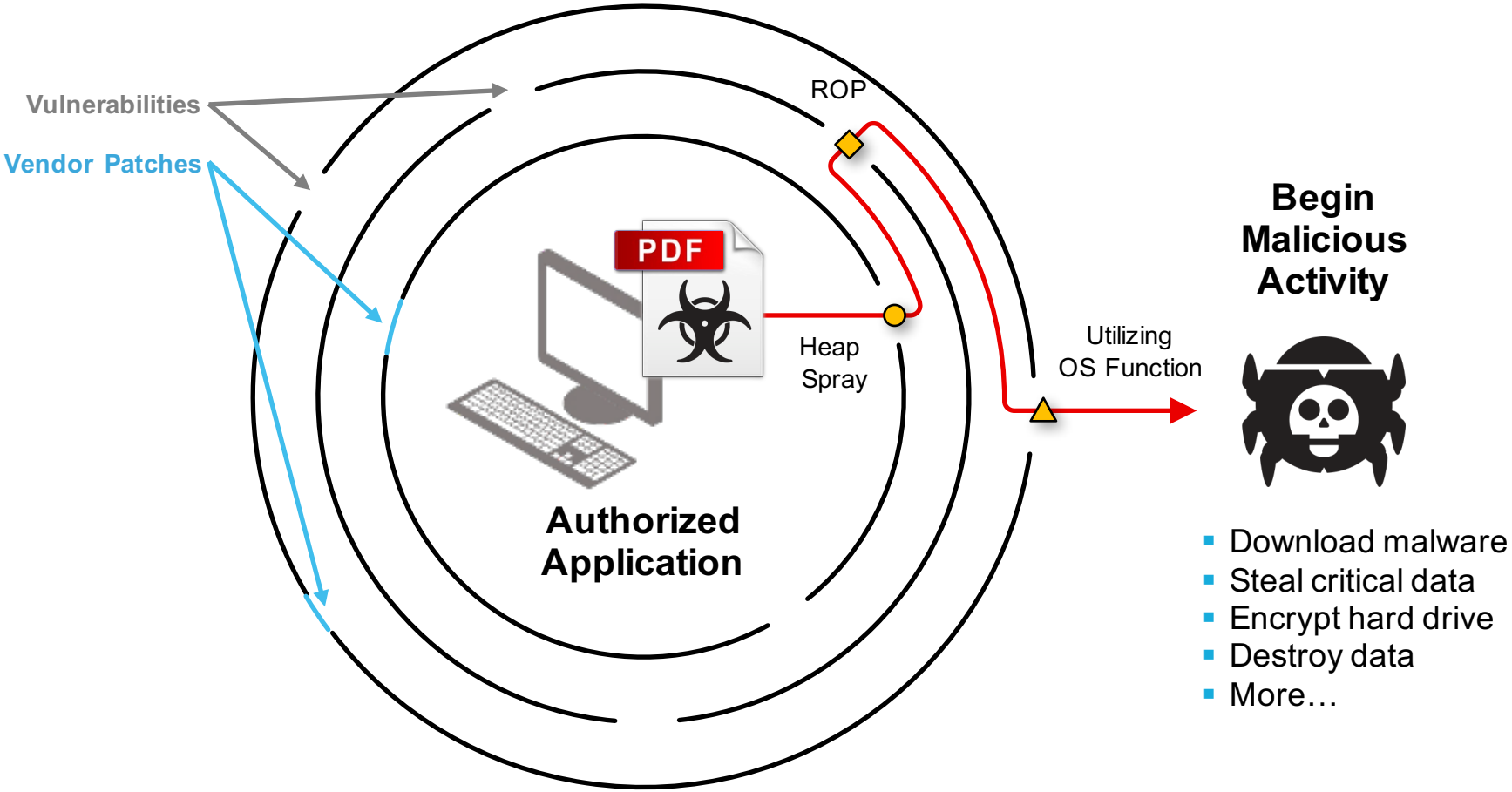
Requires No Patching, No Prior Knowledge of Vulnerabilities, and No Signatures

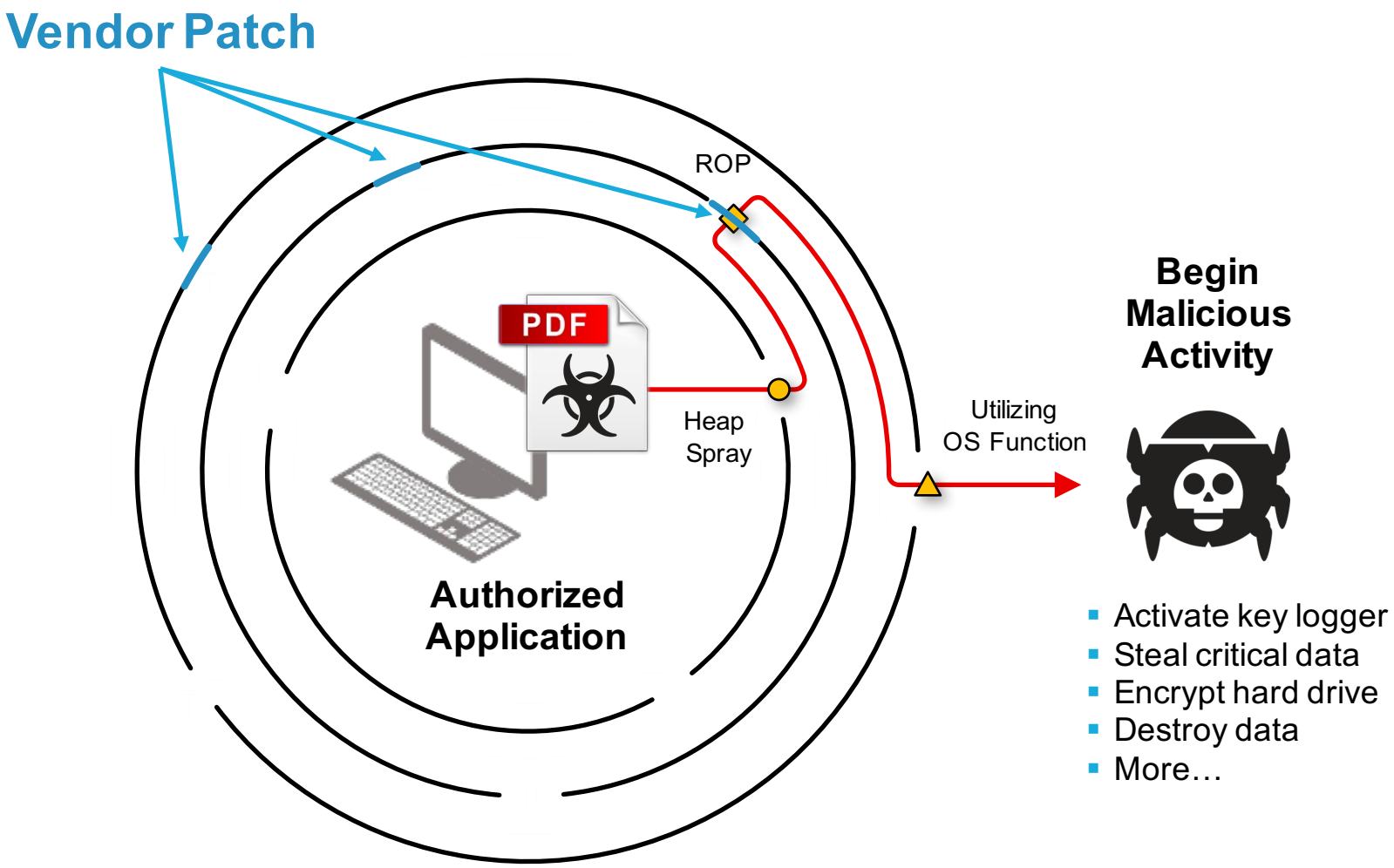
Value of Technique-based Exploit Prevention



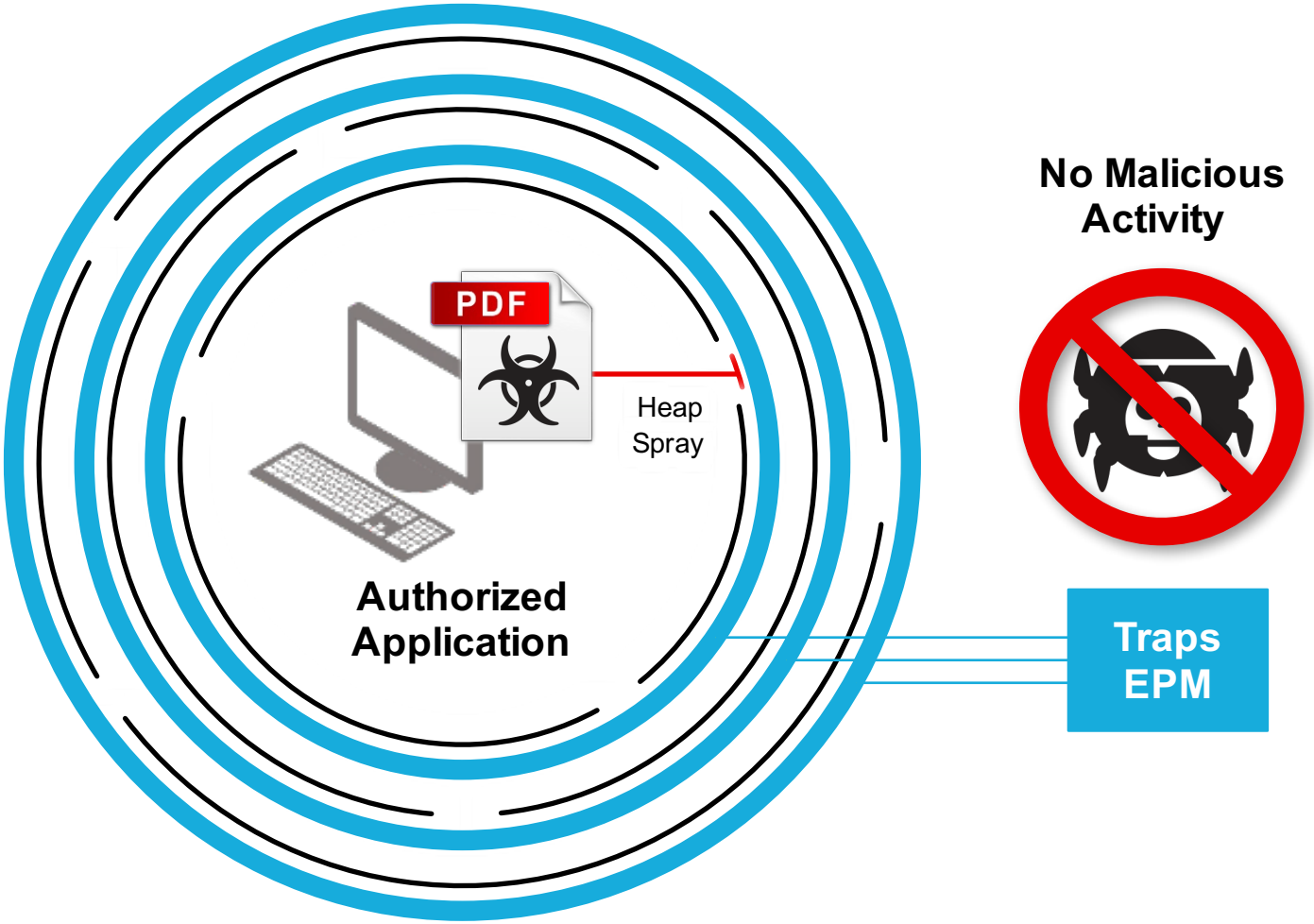
Traps Prevents Zero-day and Unknown Exploits That Have Yet to be Discovered

Exploits Subvert Authorized Applications

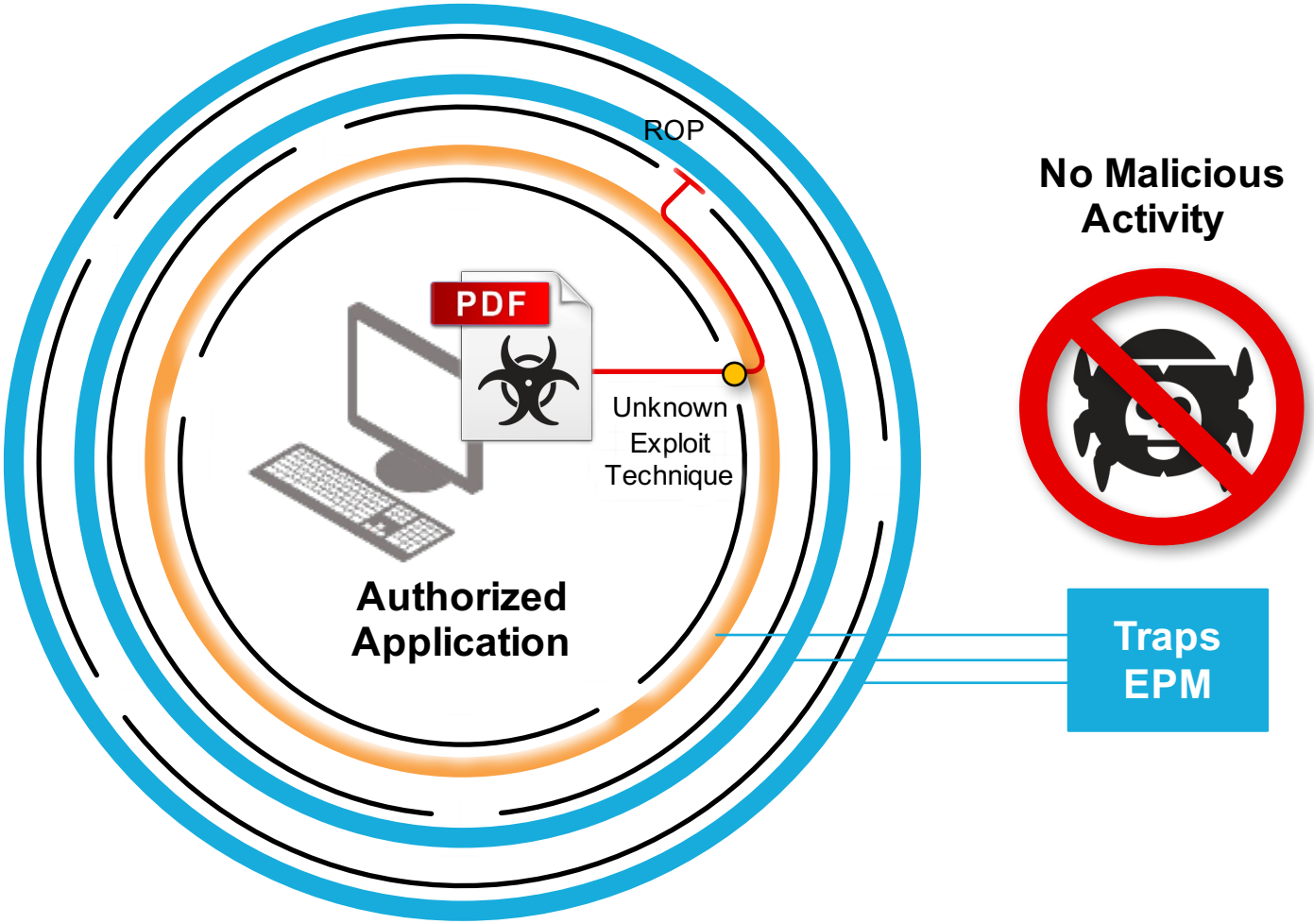



Vendor Patch
ROP
PDF
Heap
Spray
Authorized
Application
Utilizing
OS Function
Begin
Malicious
Activity
Activate key logger
Steal critical data
Encrypt hard drive
Destroy data
More…

Traps Blocks Exploit Techniques



Traps Blocks Exploits That Use Unknown Techniques



Traps

The right way to deal with advanced cyber threats

Prevent Exploits
Including zero-day Exploits

Prevent Advanced Malware
Including unknown malware

Collect Attempted-Attack Forensics
For further analysis

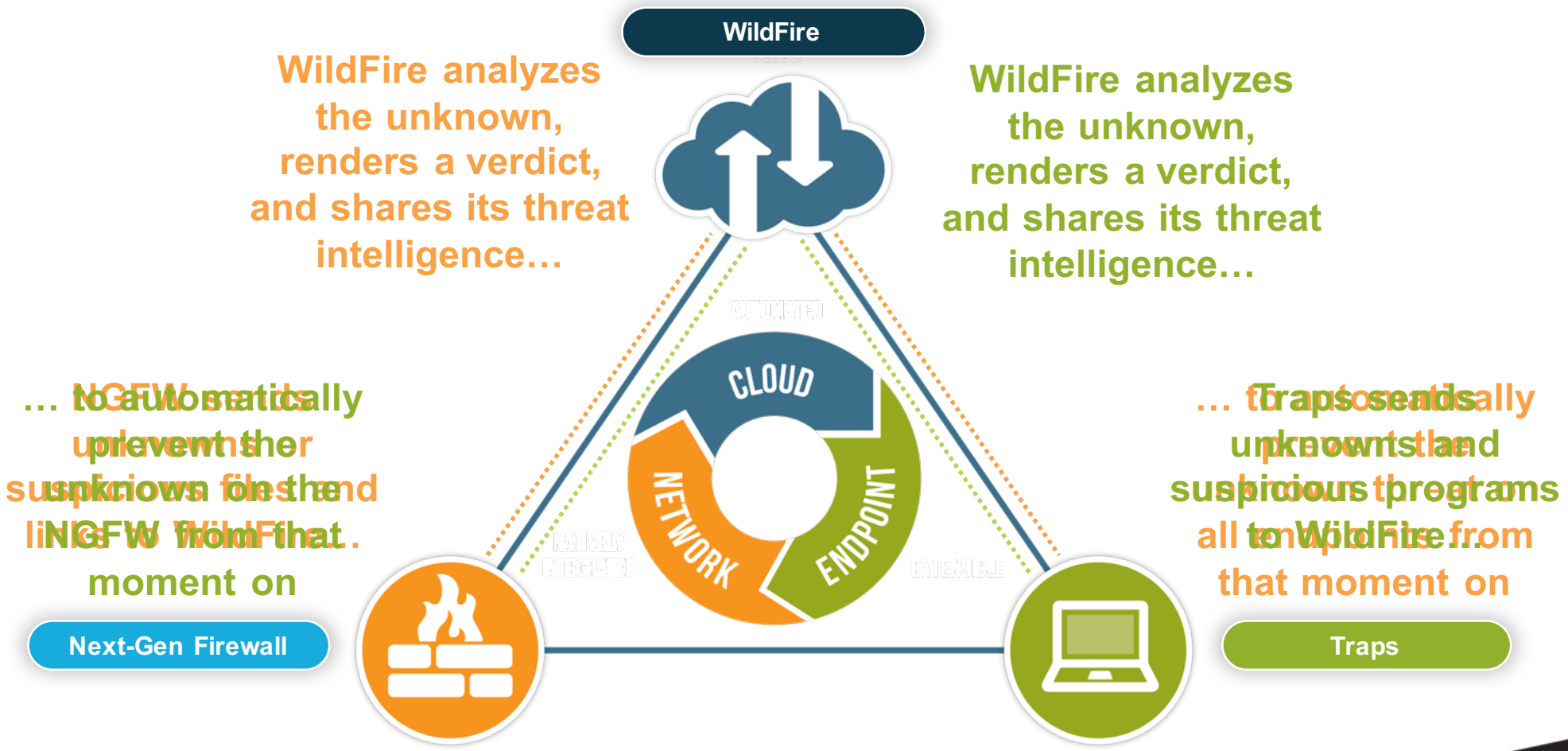
Lightweight, Scalable, User Friendly
Must cover complete enterprise

Integrate with Network and Cloud Security
For data exchange and crossed-organization protection

Traps

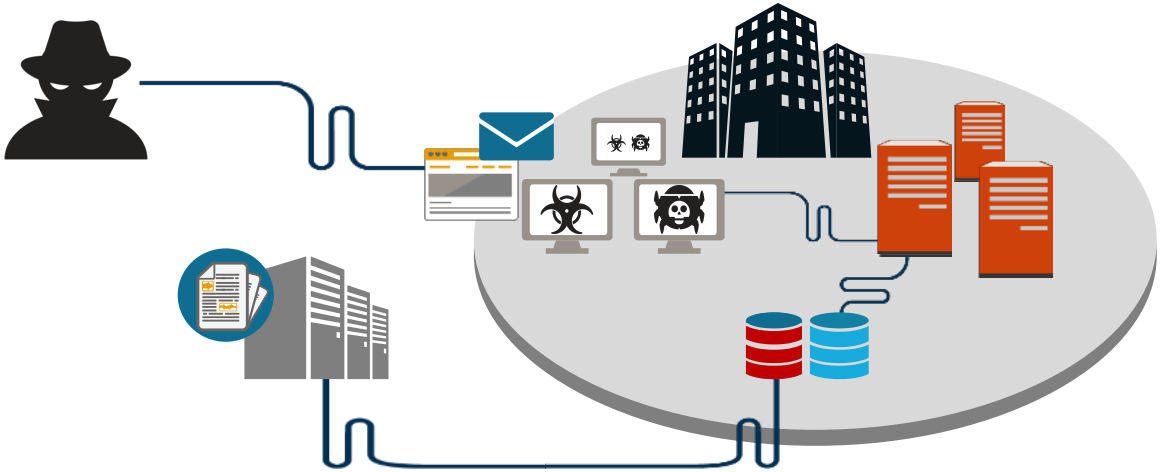
Advanced Endpoint Protection

Traps Integrates into Palo Alto Networks Security Platform

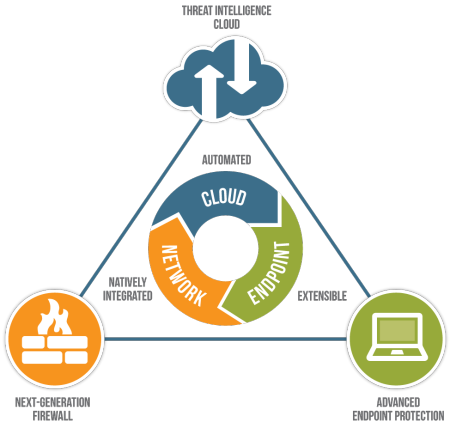


Preventing Security Breaches at Every Stage

Breach the Perimeter	Compromise Endpoints	Move Laterally	Exfiltrate Data
Next-Generation Firewall / GlobalProtect	Traps / WildFire	Next-Generation Firewall / GlobalProtect	Threat Prevention
Threat Prevention		WildFire	URL Filtering
URL Filtering			
WildFire			

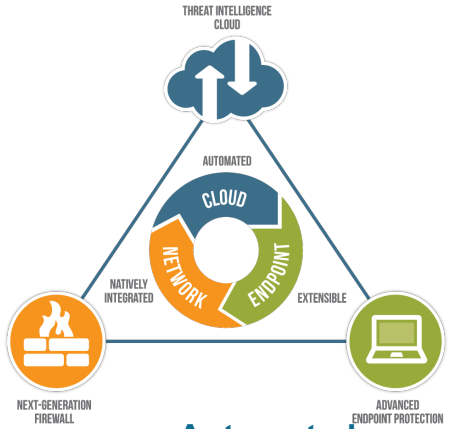


CLOSED LOOP: DETECTION TO PREVENTION



Suspicious Files & Links

Third-Party Data
Unit42
Community Sharing



Automated Protection

Third-Party Data
Unit42
Community Sharing

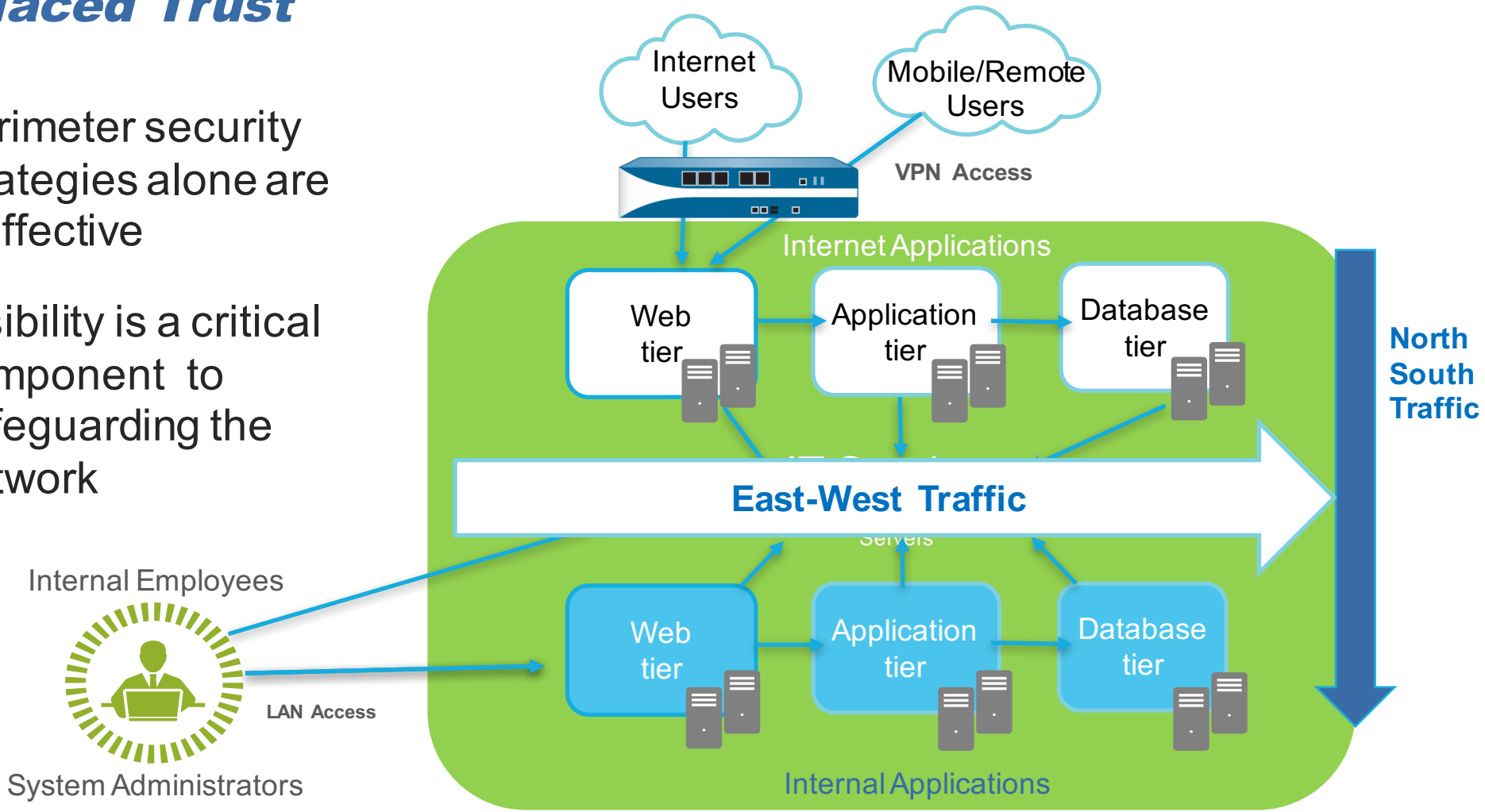
Automated Protection Delivered In As Little As 5 Minutes

paloalto NETWORKS

Zero Trust Network

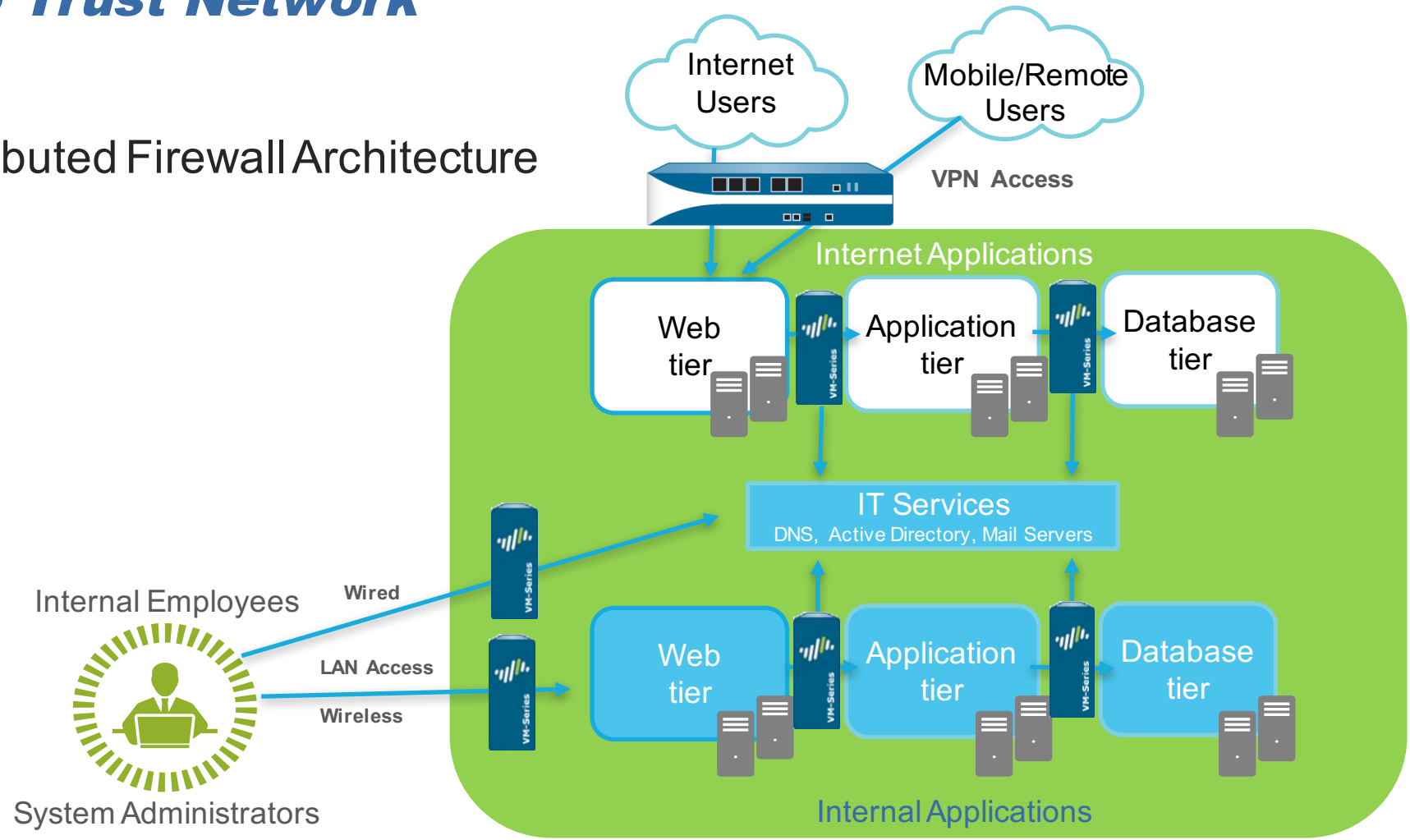
Misplaced Trust

- Perimeter security strategies alone are ineffective
- Visibility is a critical component to safeguarding the network



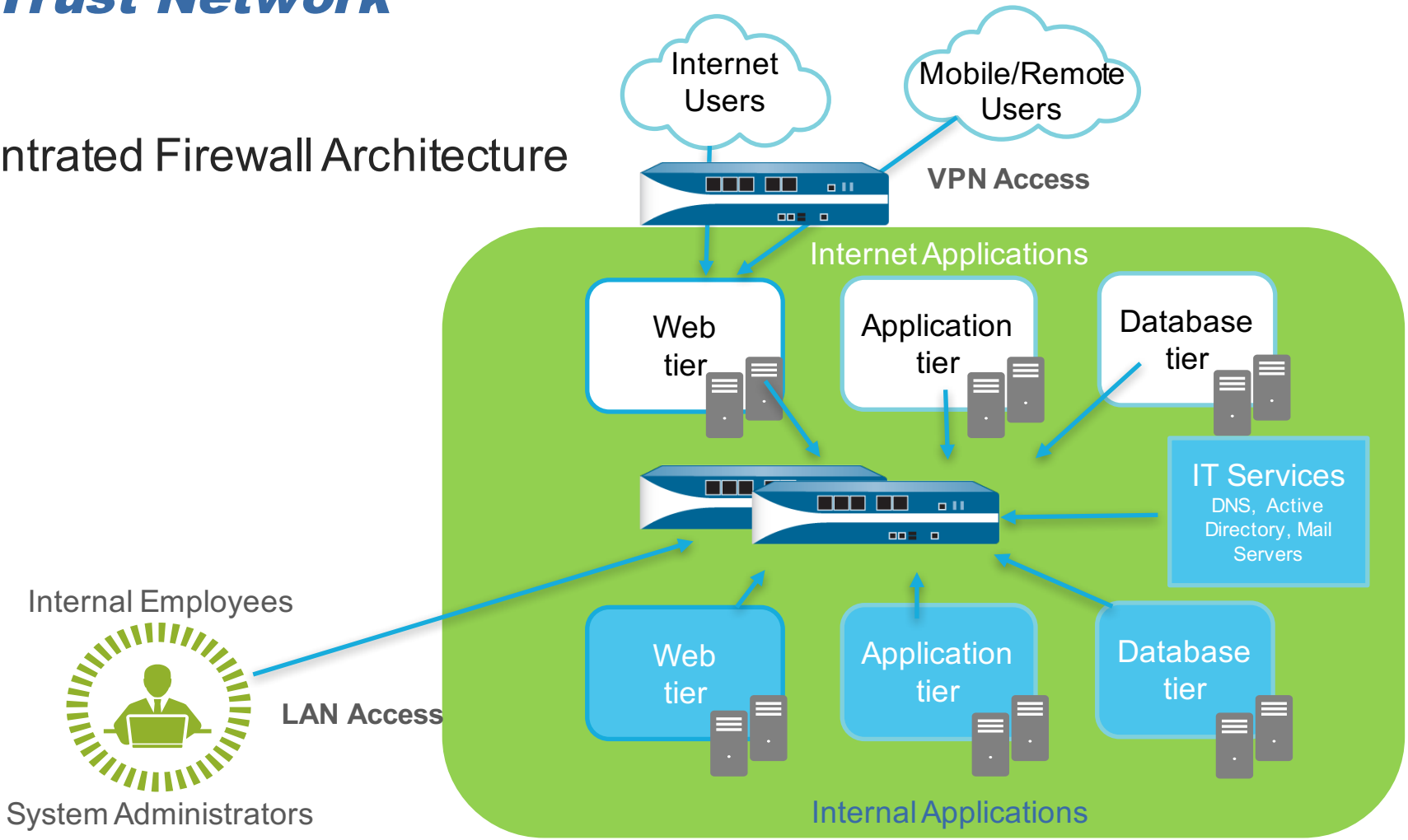
Zero Trust Network

Distributed Firewall Architecture



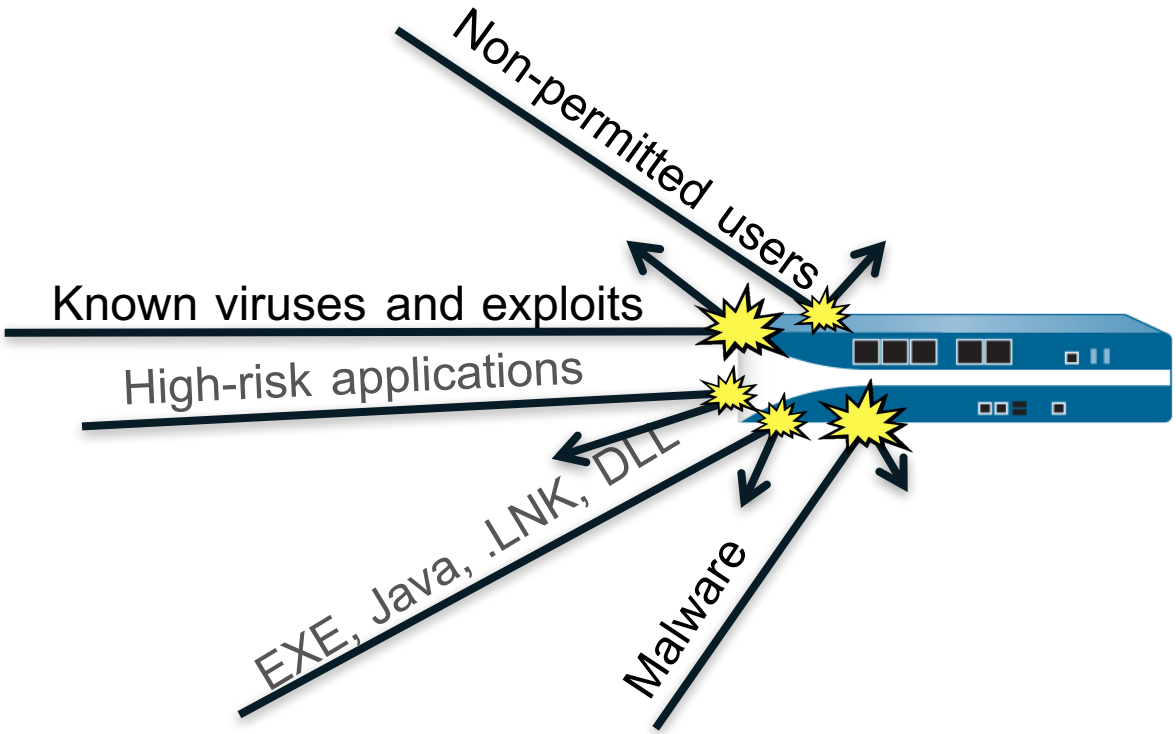
Zero Trust Network

Concentrated Firewall Architecture



Conclusion: Multi-Layered Prevention Approach

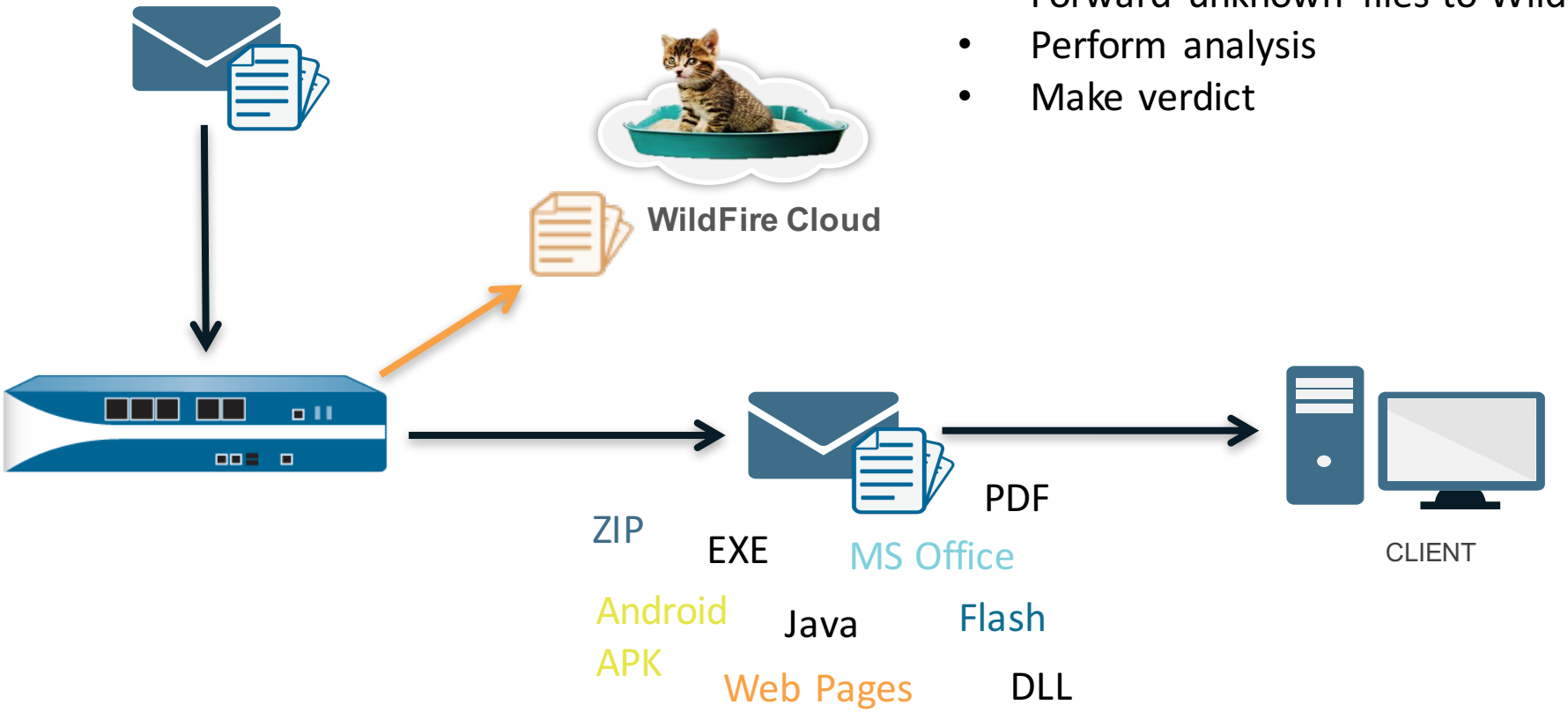
Our Multi-Layered Prevention Approach (1)



1. Reduce Attack Surface with Positive Security Model
   - App-ID:
     - Safely enable business apps
   - User-ID:
     - Grant privileges to users
   - Content-ID
     - URL Policy
     - File-blocking
   - Intrusion Prevention
     - Block known exploits
     - Block known bad C2
   - Anti-Virus
     - Scan files for known malware

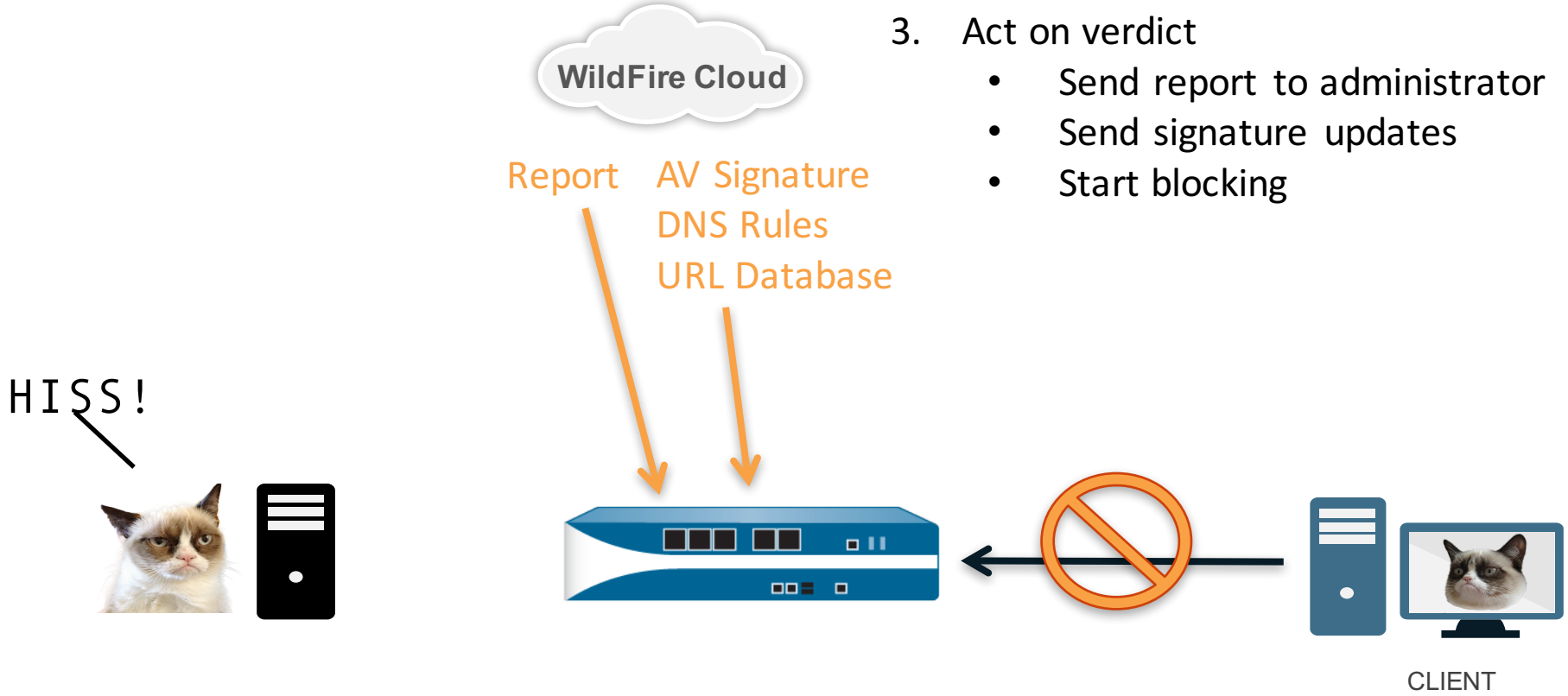
Our Multi-Layered Prevention Approach (2)

2. Turn Unknown into Known
   - Forward unknown files to Wildfire
   - Perform analysis
   - Make verdict



Our Multi-Layered Prevention Approach (3)

3. Act on verdict
   - Send report to administrator
   - Send signature updates
   - Start blocking



Palo Alto Networks: Delivering continuous innovation

Unique platform offering

Consistency	Cloud	Datacenter	Enterprise perimeter	Distributed/BYOD	Endpoint
Products	AutoFocus Aperture™	 Physical: *PA-200, PA-500, PA-3000 Series, PA-5000 Series, PA-7050, PA-7080* WildFire: *WF-500* Virtual: *VM-Series for NSX, AWS, and KVM*			Traps™
Subscriptions	Threat Prevention				
	URL Filtering				
	GlobalProtect™				
	WildFire™				
Use cases	Next-Generation Firewall	Cybersecurity: IDS / IPS / APT	Web gateway	VPN	Mobile security
Management system	Panorama, M-100 & M-500 appliances				
Operating system	PAN-OS™				

Case Study

Security Infrastructure Refresh

CSU The California State University

Background

- 23 Campuses
- 460,000 students
- 47,000 faculty staff members
- Juniper for network security
- Aruba Networks for wireless
- Alcatel-Lucent for switching and routing
- NEED: re-evaluate network security tools and deployment in the presence of cyber threats

CSU The California State University

ALPHA
Gathering Requirements
Apply test campuses
Collect lessons learned
Refine process

BETA
Process improvements
Verification
Applying lessons learned
Configuration migration

PHASE I
Like for like migration
Cut-over window
Monitoring

PHASE II
Applying next-generation features
- App-ID
- User-ID
- Threat reports

PHASE III
Clean up
Threat review
App-ID review
Commit configurations

CSU The California State University

Phase 1

- Involved a “like for like” replacement of Juniper firewalls with Palo Alto Networks next-generation firewalls, using existing security rules with the aid of Palo Alto Networks Migration Tool.
- During a 60-day proving period, the Palo Alto Networks next-generation firewalls logged application data, which was used to build application-based rules.
- In addition, Palo Alto Networks Threat Prevention service was enabled in “alert only” mode.

Phase 2

- cloning of legacy security rules plus adding application information
- traffic filtering only based on new application-based rule, legacy rule retained for verification
- User-ID enabled to identify end users by name rather than only their IP address
- Threat Prevention fully enabled
- Environment ran for 60 days

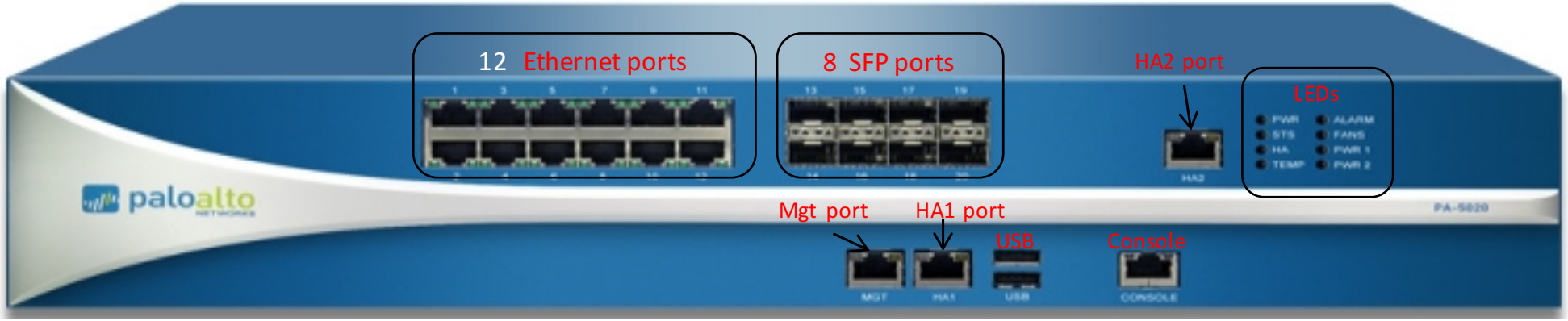
CSU The California State University

Phase 3

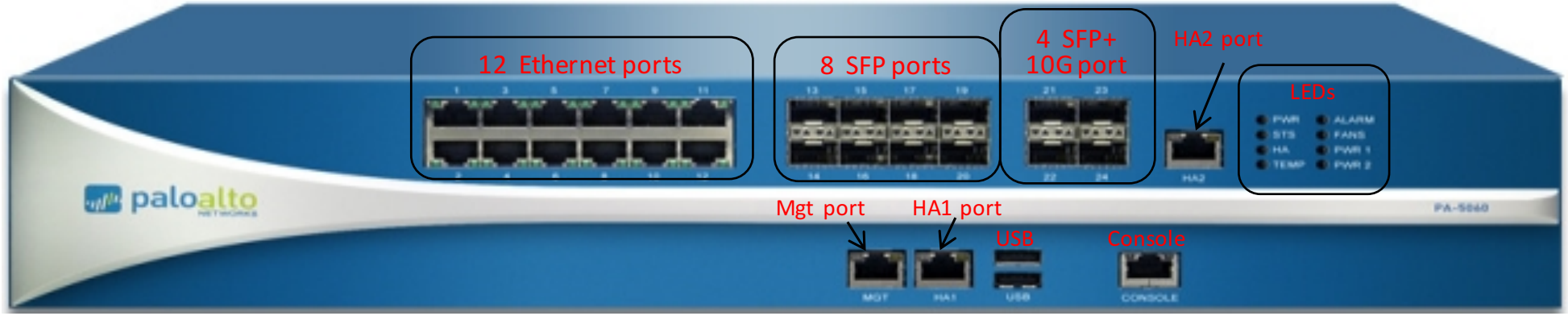
- Planned 18 month Migration-Phase from Juniper to Palo Alto Networks for all campuses/sites
- Based on the following variables
  - *number of students,*
  - *number of concurrent sessions,*
  - *WAN traffic plus projected growth over four years*
  - *percentage of SSL decryption*

  decision was made for
  - PA-5050 as the baseline edge firewall for medium-sized campuses
  - PA-5060 as the baseline edge firewall for large campuses
  - PA-5060 for any data center firewall deployments
- In total the CSU will deploy over 100 firewalls in 30 locations until end of 2017

PA-5000 Series (Hawk)



PA-5020



PA-5050/PA-5060

PA-5000 Series Specs

PA-5020

- 5 Gbps FW
- 2 Gbps threat prevention
- 2 Gbps IPSec VPN
- 5,000 SSL VPN Users
- 1,000,000 sessions
- Up to 20 VSYS
- (8) SFP (1 Gig) I/O
- (12) 10/100/1000
- DP0, DP1

PA-5050

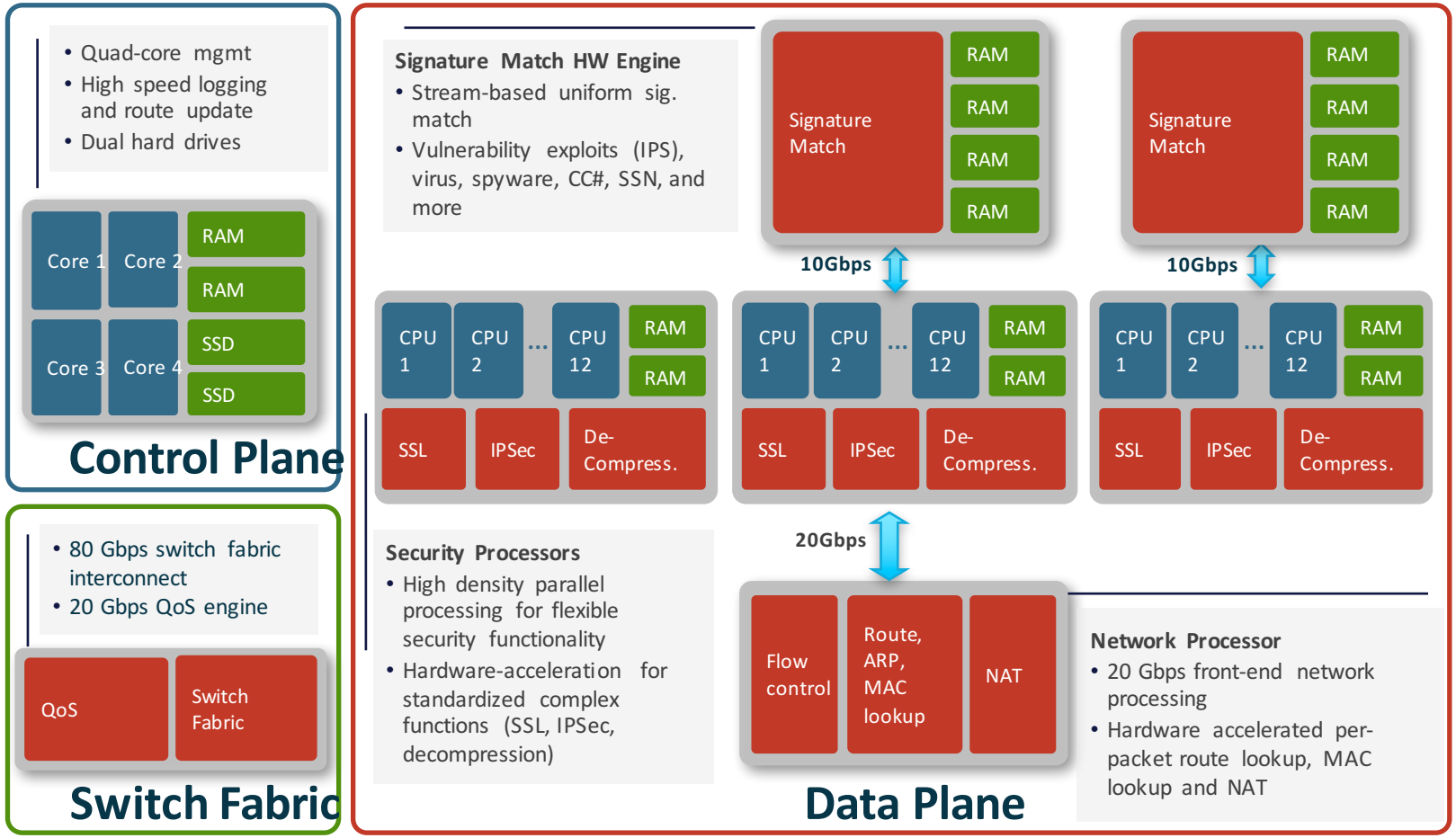
- 10 Gbps FW
- 5 Gbps threat prevention
- 4 Gbps IPSec VPN
- 10,000 SSL VPN Users
- 2,000,000 sessions
- Up to 125 VSYS
- (4) SFP+ (10 Gig) I/O
- (8) SFP (1 Gig) I/O
- (12) 10/100/1000
- DP0, DP1

PA-5060

- 20 Gbps FW
- 10 Gbps threat prevention
- 4 Gbps IPSec VPN
- 20,000 SSL VPN Users
- 4,000,000 sessions
- Up to 225 VSYS
- (4) SFP+ (10 Gig) I/O
- (8) SFP (1 Gig) I/O
- (12) 10/100/1000
- DP0, DP1, DP2

- Hot swappable fans, power supplies
- Dual, solid state hard drives (SSD), field replaceable (not hot swap)
- Dedicated HA and management interfaces
- 2U standard rack mount form factor
- PAN-OS 4.0 and later

PA-5000 Series Architecture



Questions?