Next Generation Threat Prevention

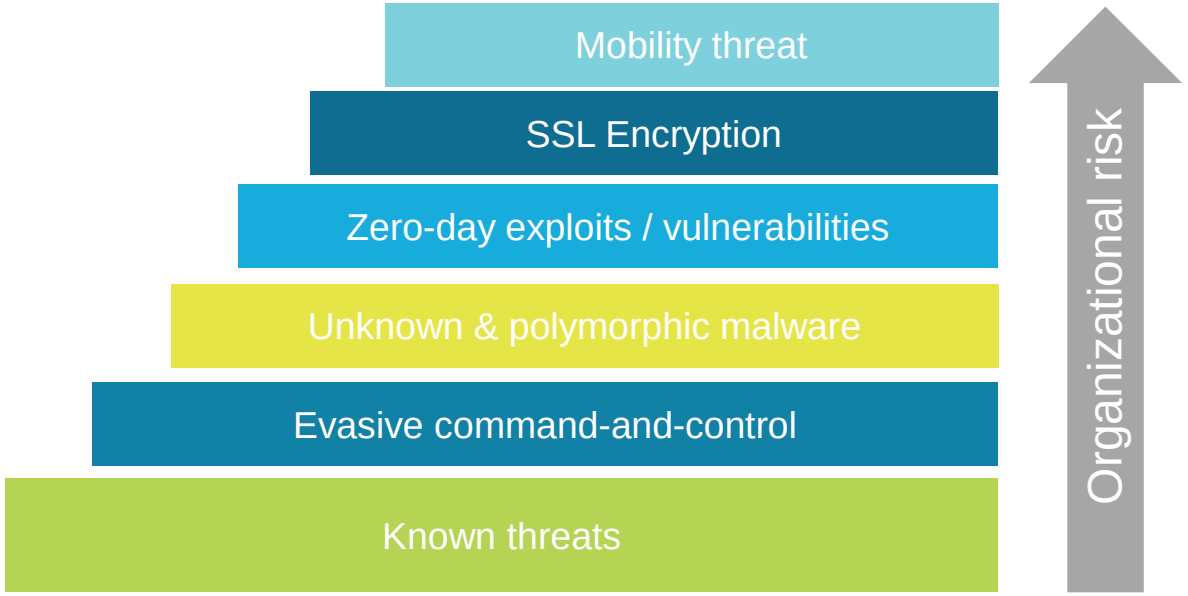
Samer Shbeeb CISSP, CISA, CCIE, CEH, CHFI

Security Solution Architect

sshbeeb@paloaltonetworks.com

WHAT'S CHANGED?

THE EVOLUTION OF THE **ATTACK**

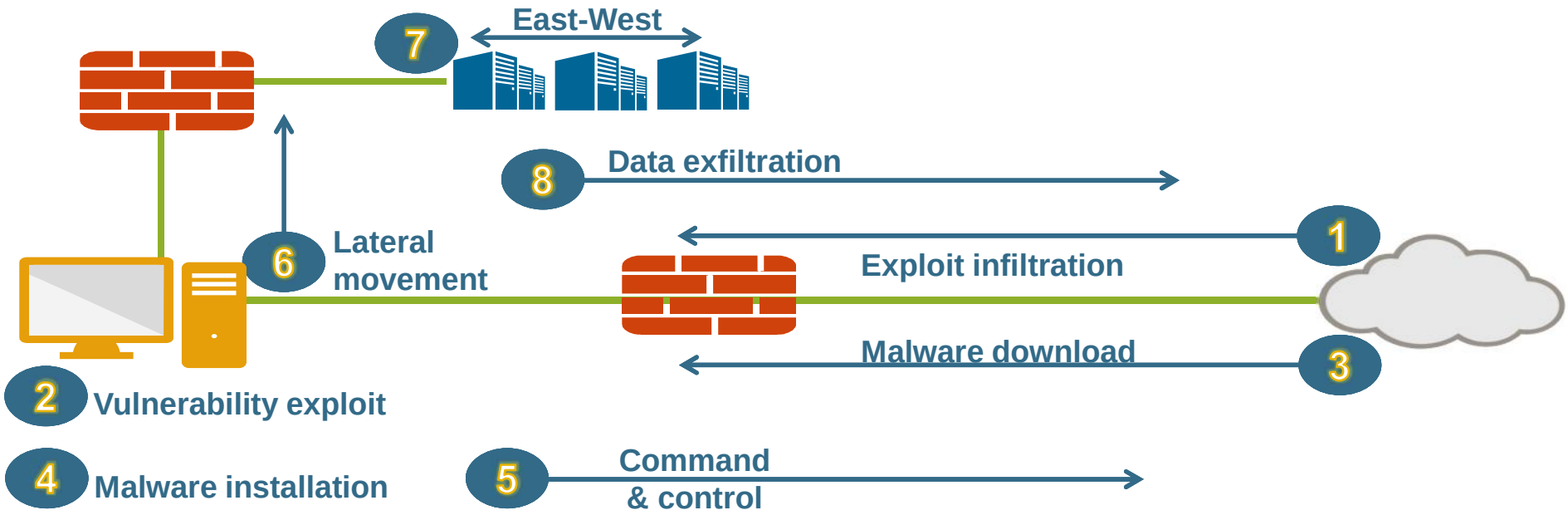


TYPICAL CYBER ATTACK LIFECYCLE

Gather Intelligence	Leverage Exploit	Execute Malware	Control Channel	Steal Data
Plan the Attack	Silent Infection	Malicious File Executed	Malware Communicates with Attacker	Data Theft, Sabotage, Destruction

Preventive Controls **Reactive Controls**

The prevention opportunity in the attack lifecycle



Cyber Security

Cyber Security

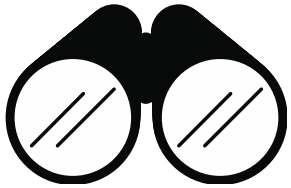
10 Years Ago

paloalto NETWORKS

Cyber Security

Cyber Security

Philosophy for prevention



COMPLETE VISIBILITY

REDUCE ATTACK SURFACE

PREVENT KNOWN THREATS

PREVENT UNKNOWN THREATS

Preventing attacks

Complete visibility	Reduce attack surface area	Prevent all known threats	Detect & prevent new threats
• Network & endpoint (different views) • All applications, inc. cloud & SaaS • All users & devices, inc. all locations • Encrypted traffic	• Enable business apps • Block “bad” apps • Limit app functions • Limit high risk websites and content • Require multi-factor authentication	• Exploits • Malware • Command & control • Malicious & phishing websites • Bad domains	• Unknown malware • Zero-day exploits • Custom attack behavior

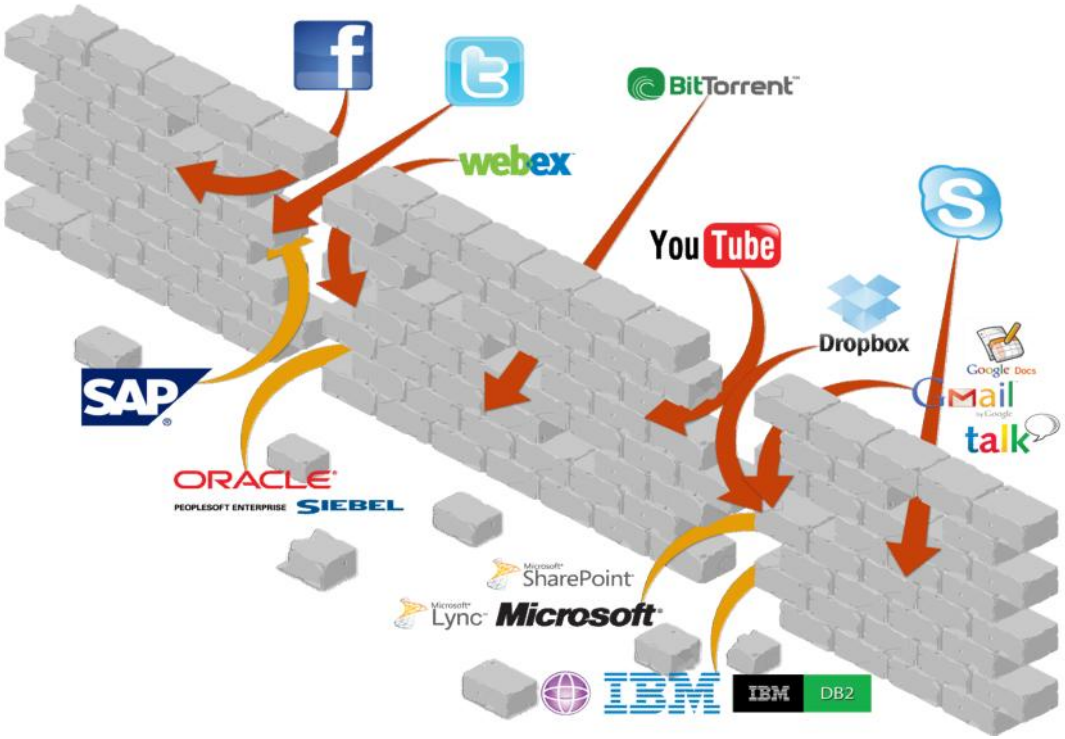
A Different Way of thinking when it comes to security...

"Security as a business enabler vs. a business inhibitor."

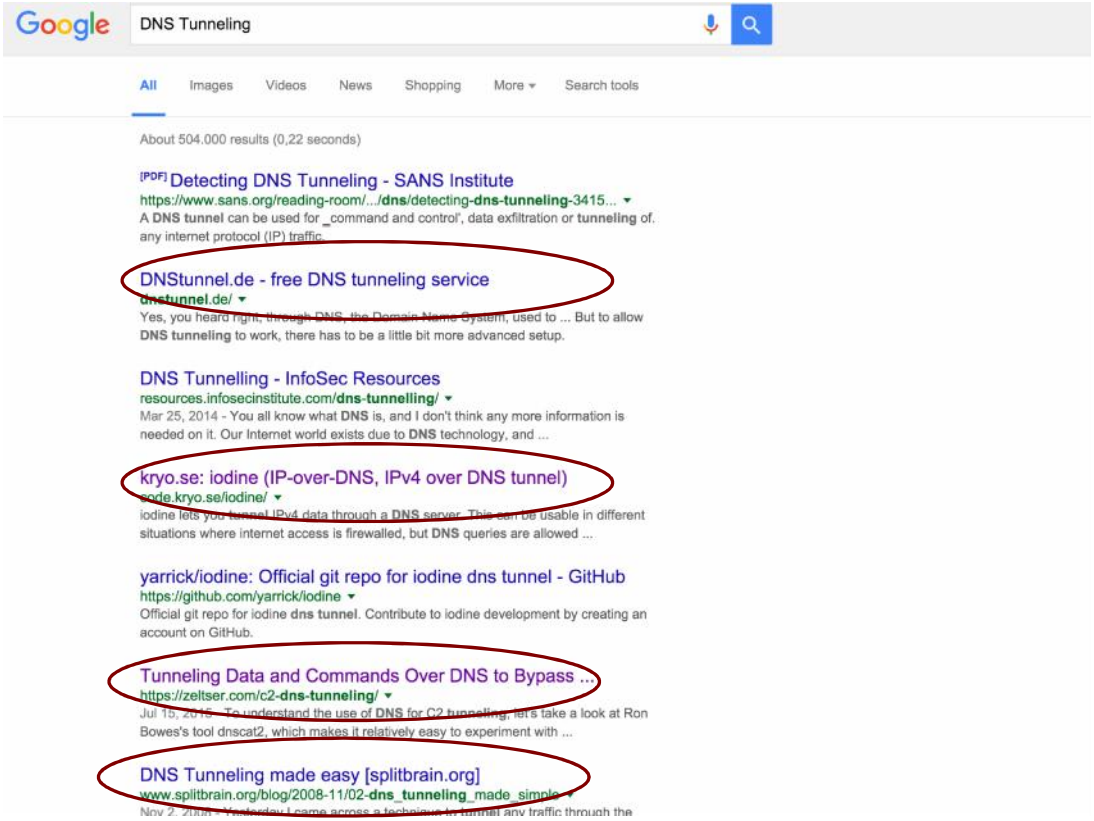
Application **Enablement** ensures full business benefits while minimizing the security risks.

Application **Prevention** forces organizations to either completely block or unsafely allow modern applications

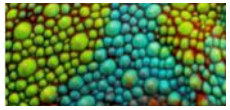
Ports and protocols have lost their meaning



DNS Tunneling



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

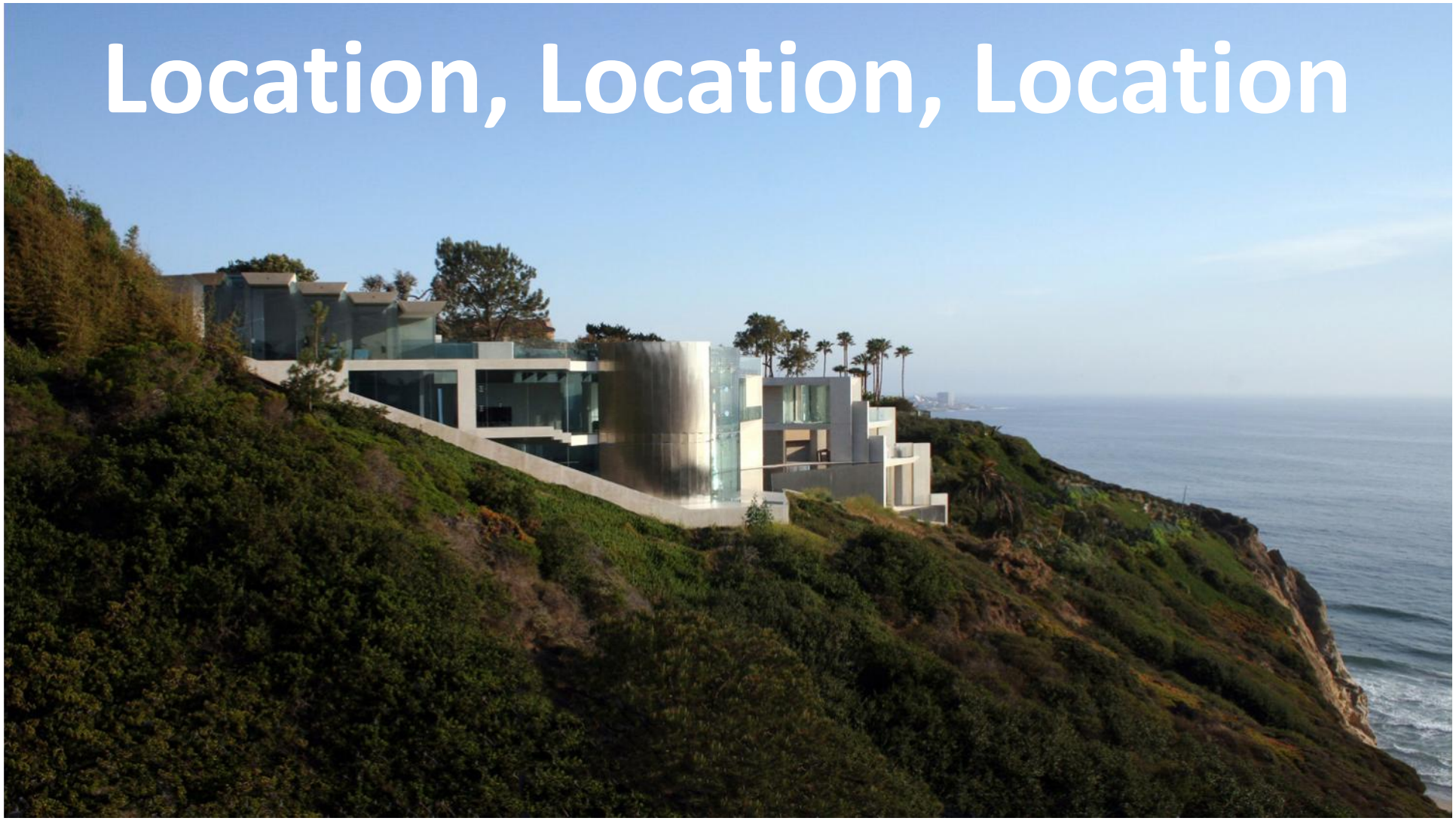
or

Allow, **but**:

scan for threats
block files
per schedule
etc.

(Enables)

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

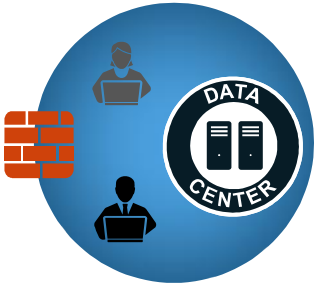

Location, Location, Location

Location, Location, Location

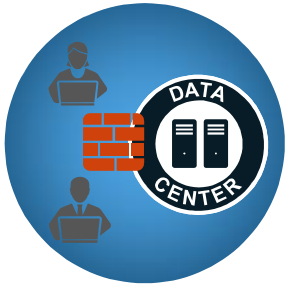
REQUIREMENTS FOR THE FUTURE

- **DETECT AND PREVENT** THREATS AT EVERY POINT ACROSS THE ORGANIZATION

At the (mobile) device



At the internet edge



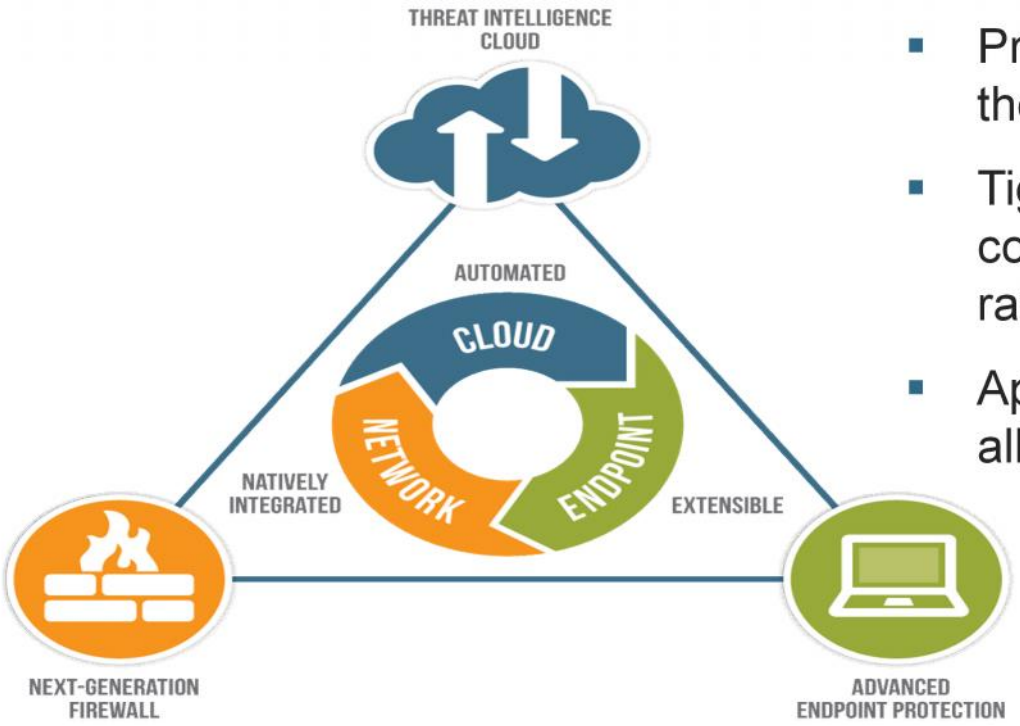
Between employees and devices within the LAN

At the data center edge, and between VM's

Within private, public and hybrid clouds

paloalto NETWORKS

Security platform for all stages of the attack lifecycle



- Prevention-focused at all stages of the attack lifecycle
- Tightly integrated and automated to continuously increase prevention rates
- Applies to all applications, all users, all devices, all of the time

Not all firewalls are created equal

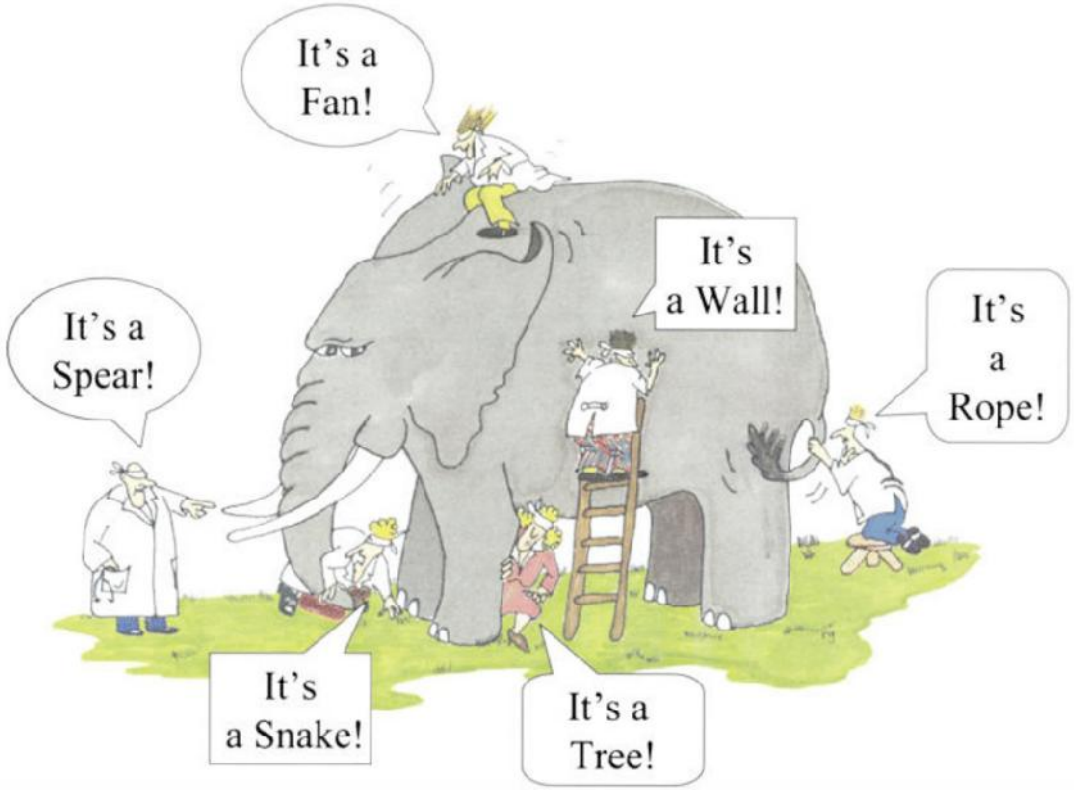
Perception

paloalto NETWORKS

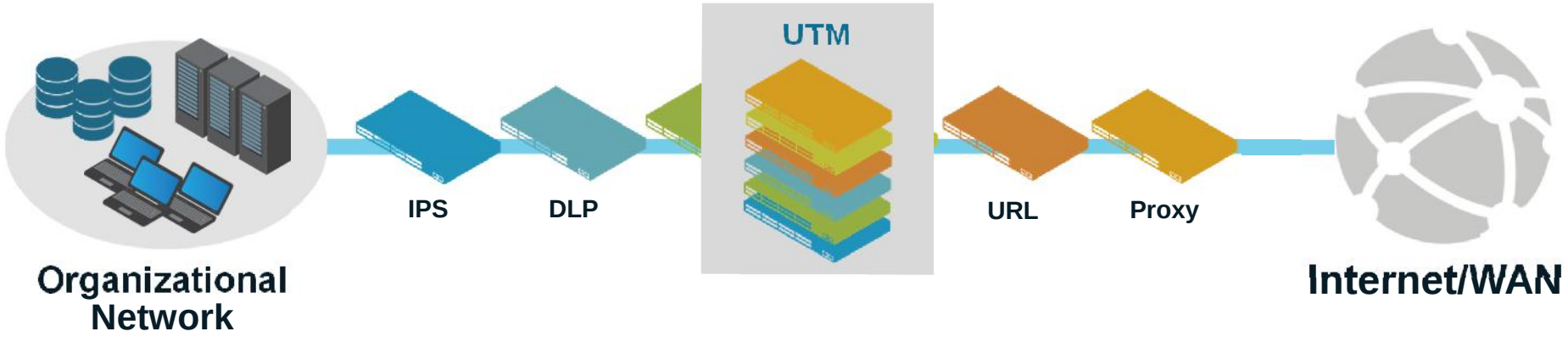
Not all firewalls are created equal

Reality

Partial visibility - broader context = flawed conclusions

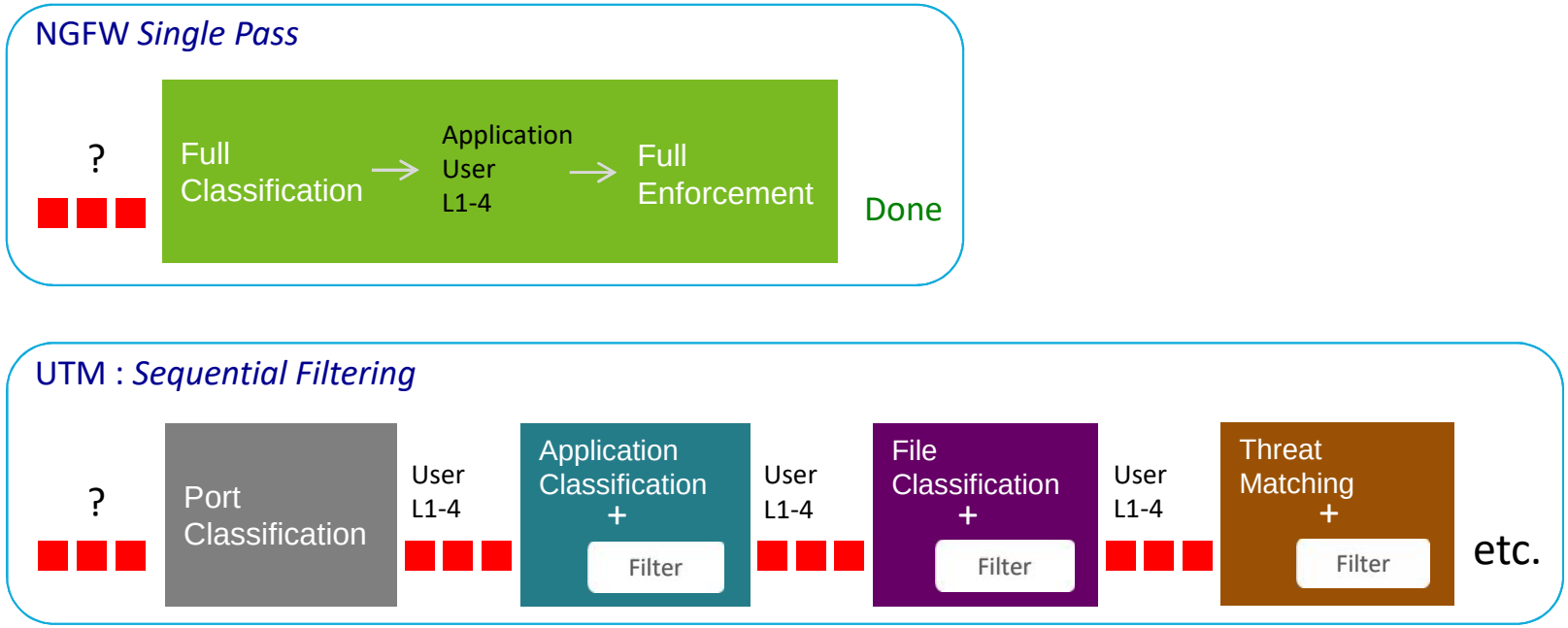


SECURITY EVOLUTION TO-DATE



An Accidental Architecture

A fundamentally different architecture



Safe Applications Enablement – control each application independently

Web-browsing

Block all file types

Cloud Backup

Allow all file types

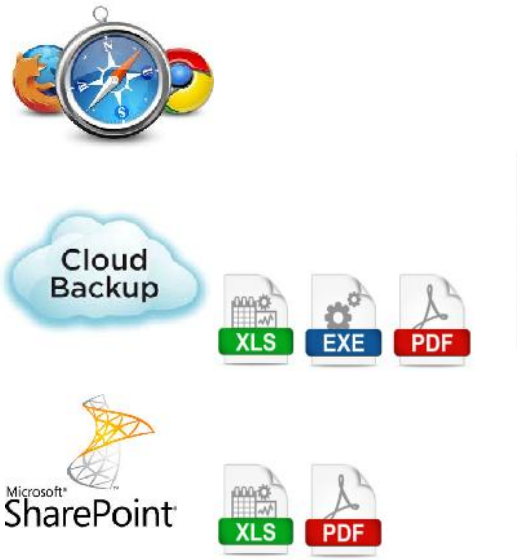
Web Mail

Block all web mail like applications

Ms SharePoint

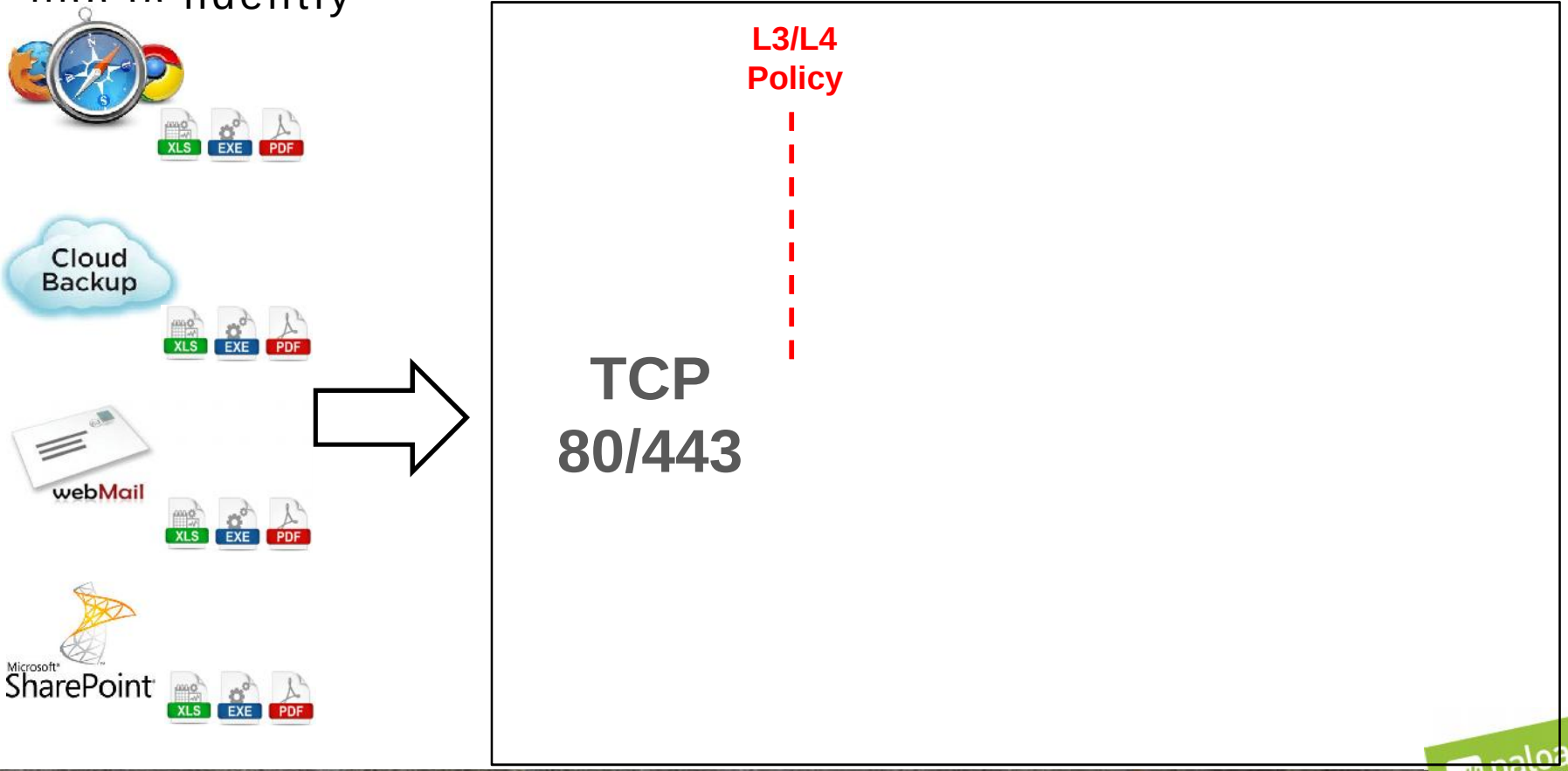
Block only EXE files

Safe Applications Enablement – control each application independently

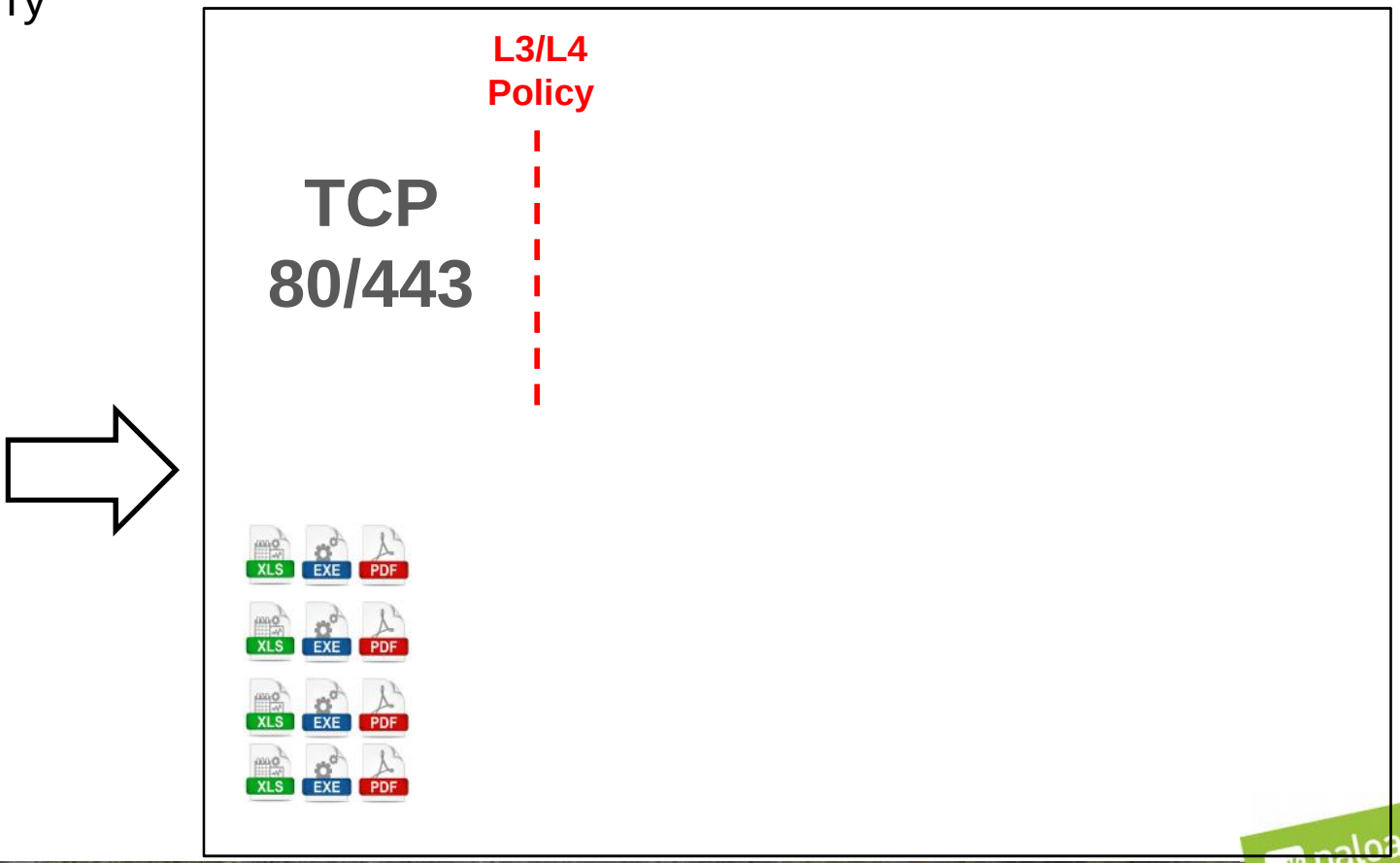


Let's check if we can get the same configuration and how easy it is to setup such requirements using UTM or L4 base firewalls

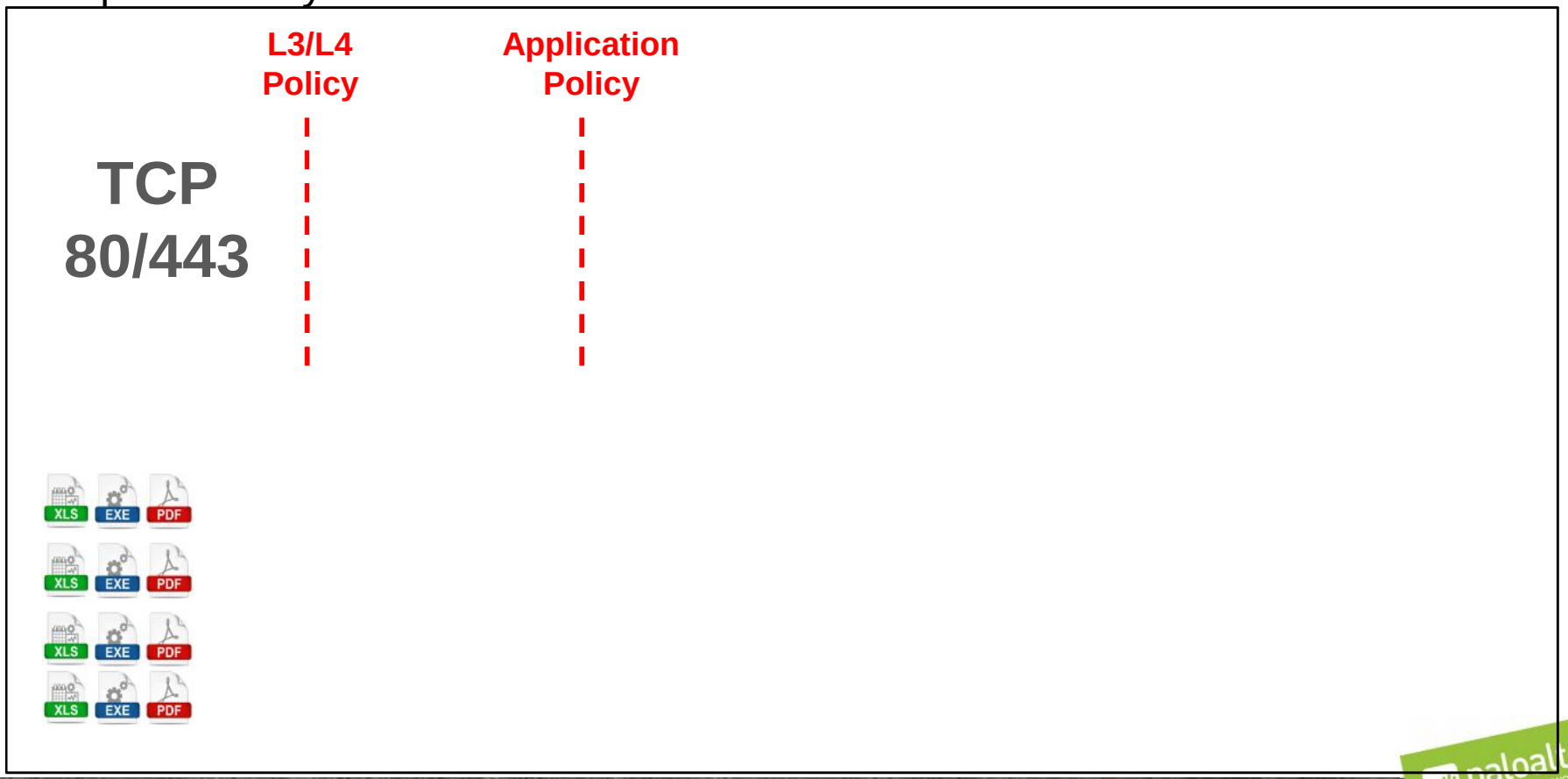
Safe Applications Enablement – control each application independently



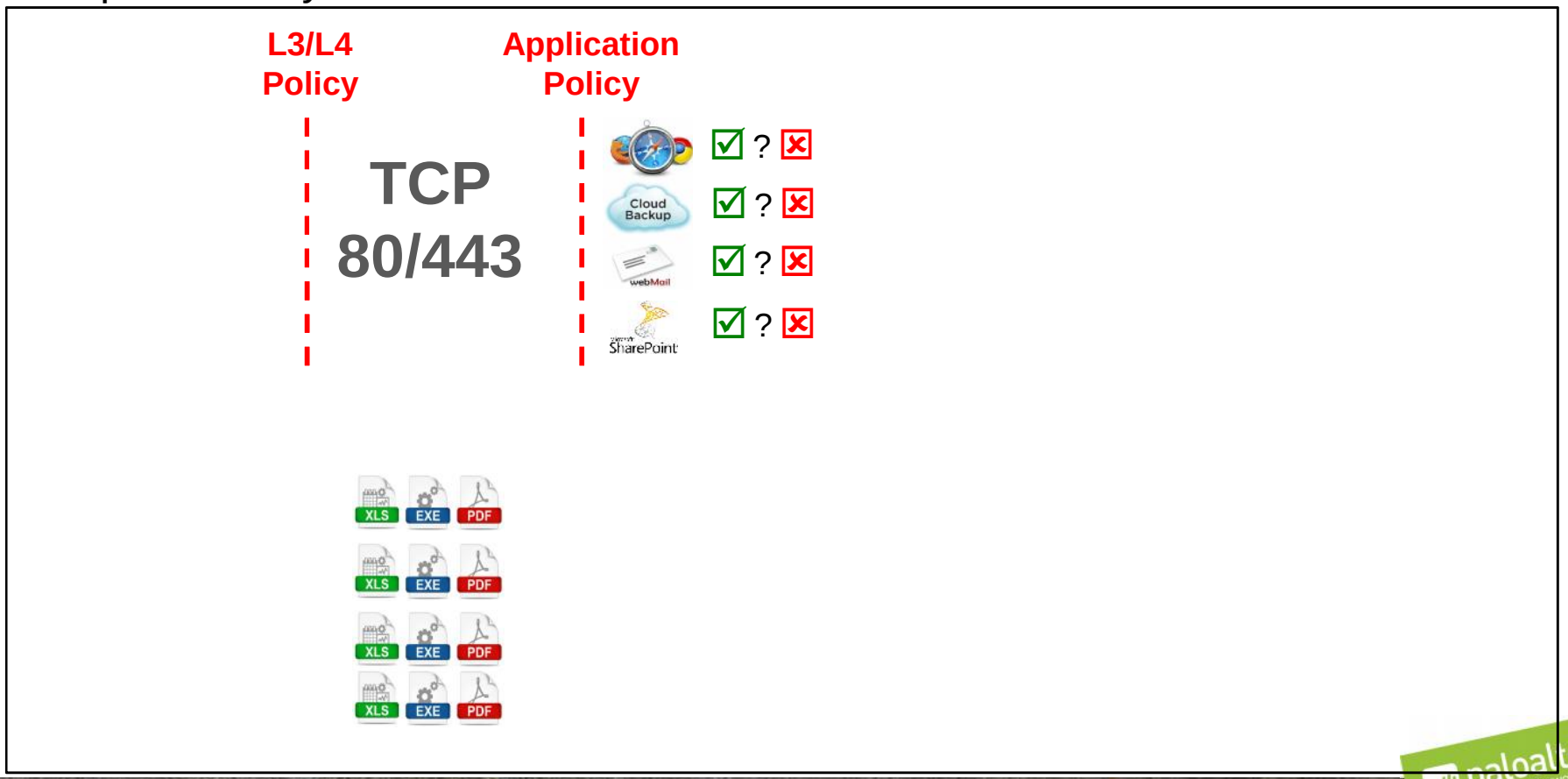
Safe Applications Enablement – control each application independently



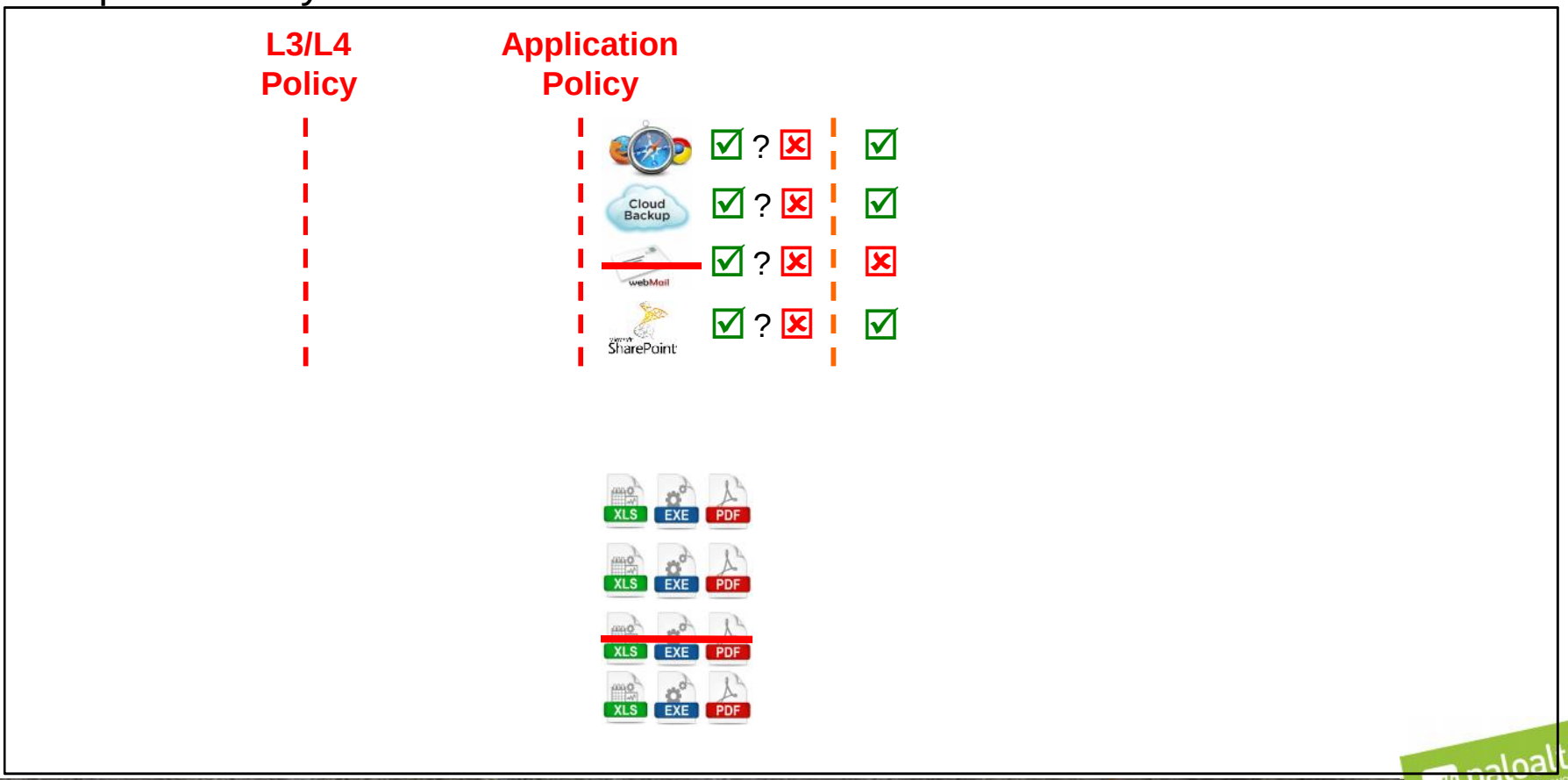
Safe Applications Enablement – control each application independently



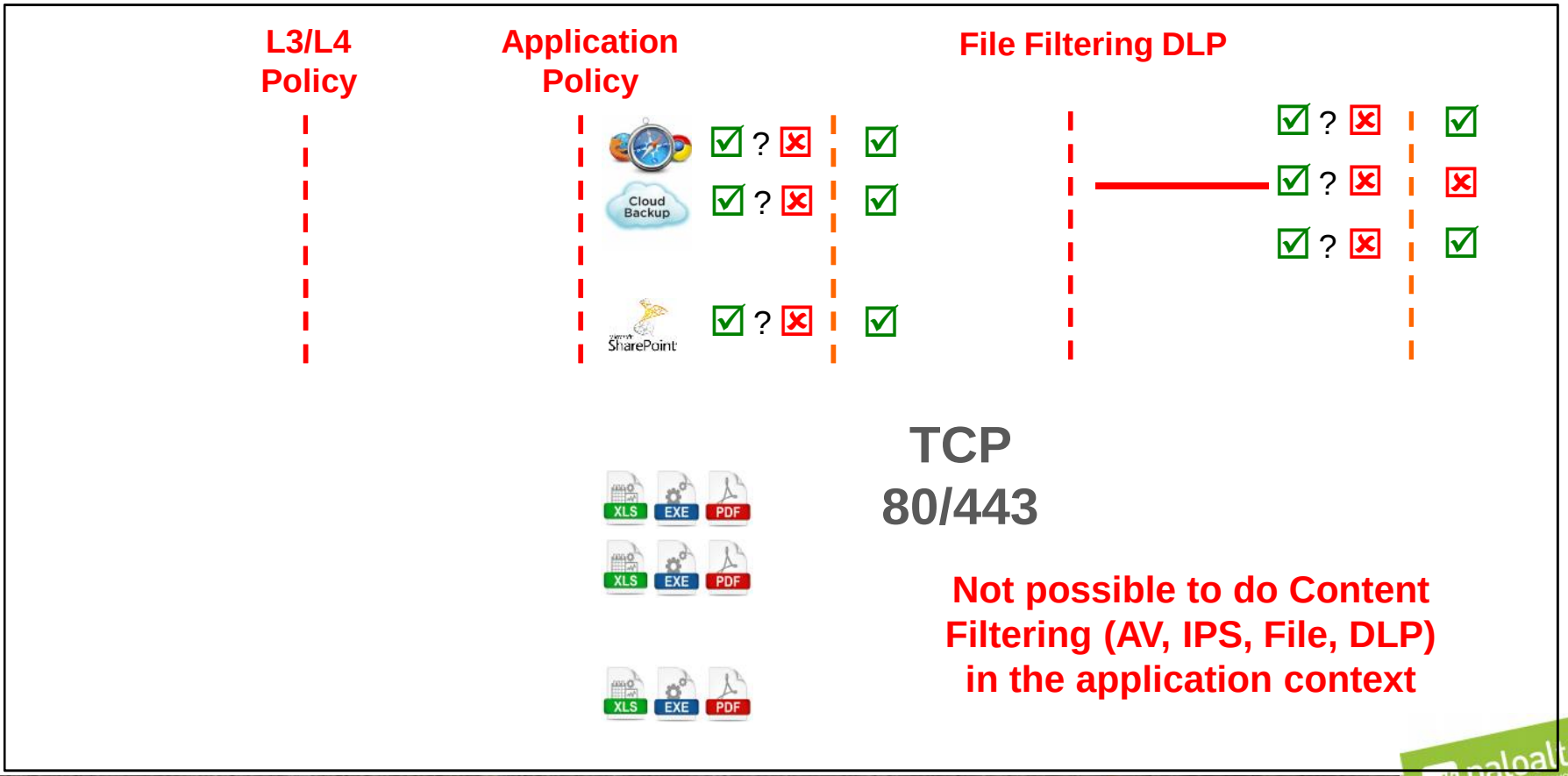
Safe Applications Enablement – control each application independently



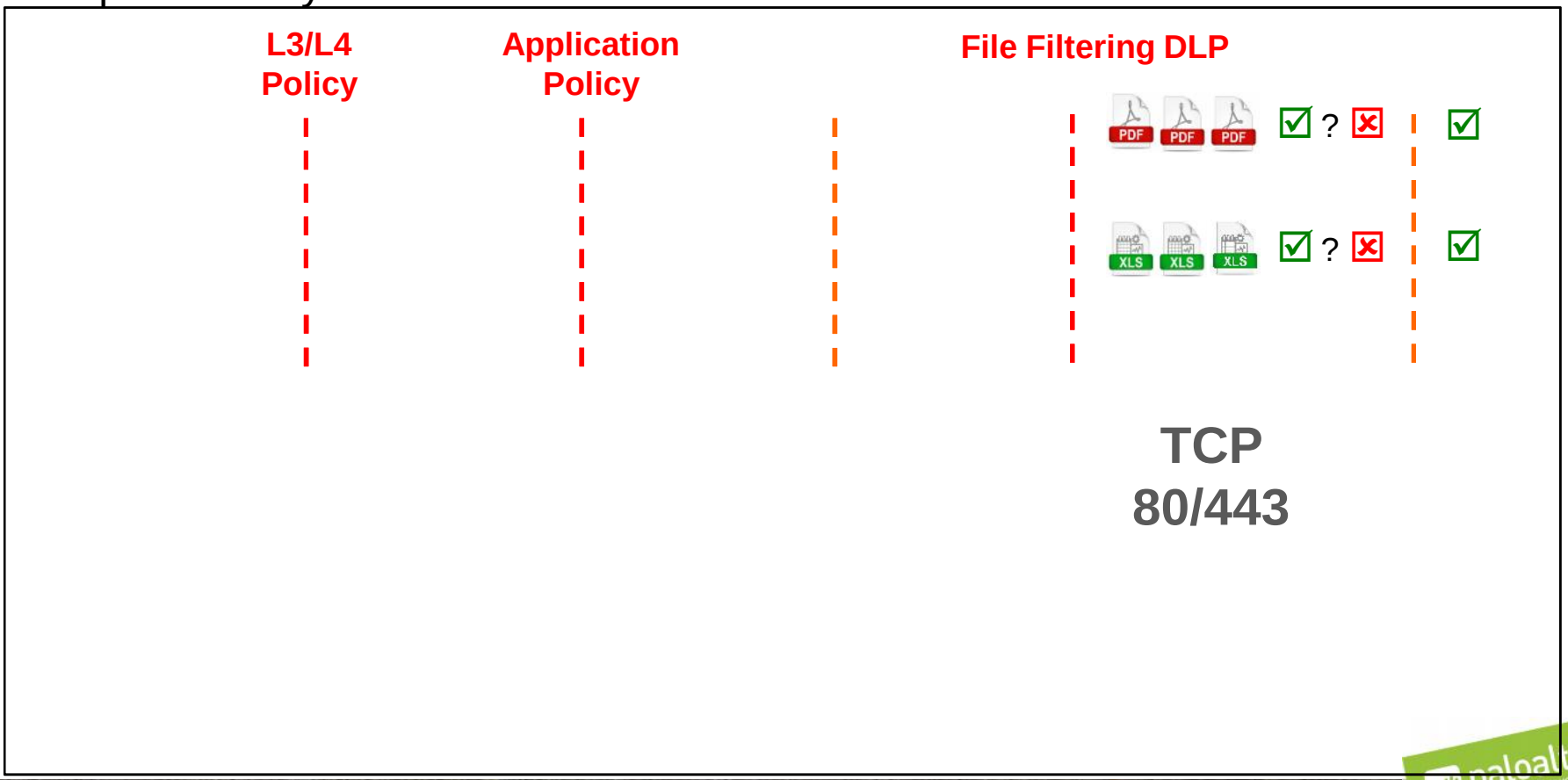
Safe Applications Enablement – control each application independently



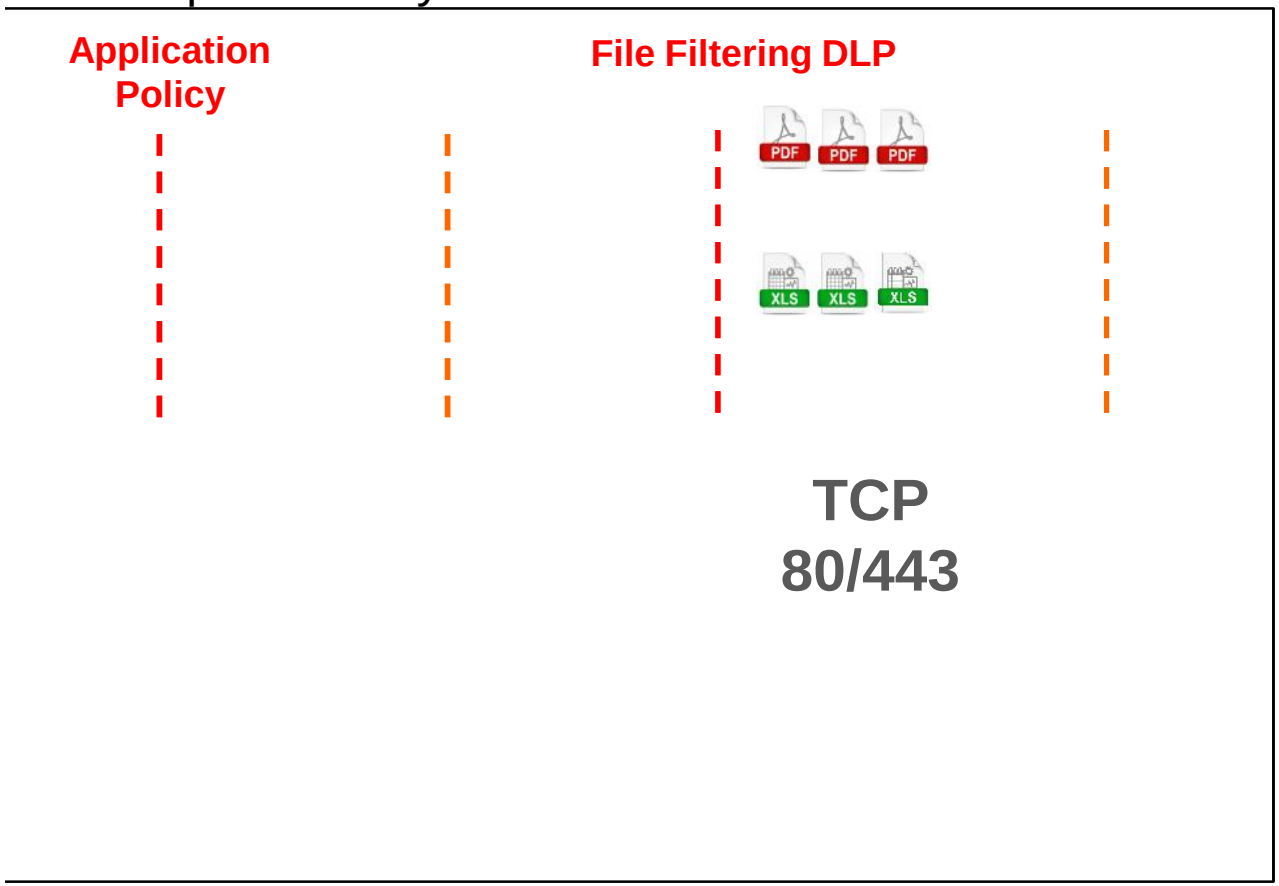
Safe Applications Enablement – control each application independently



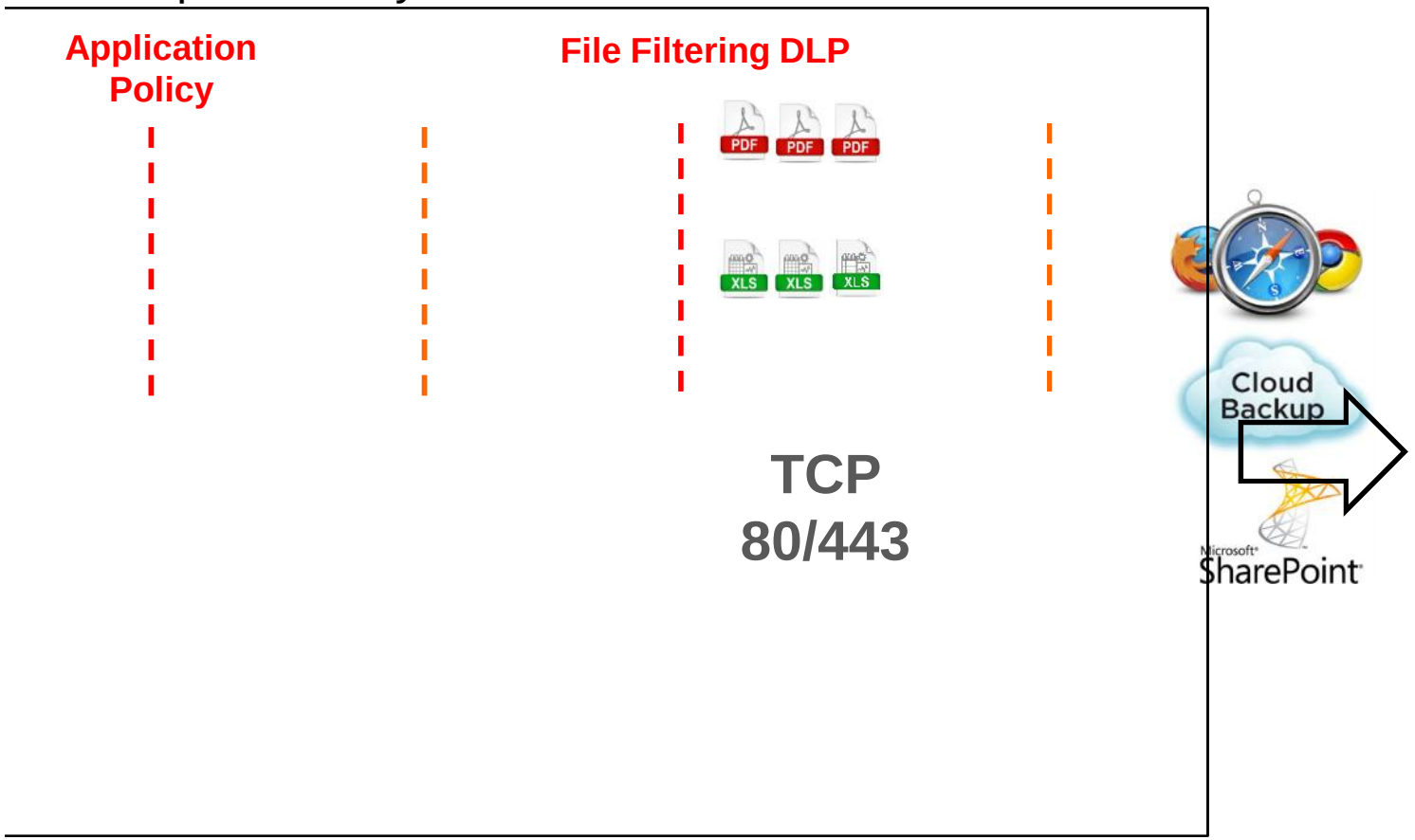
Safe Applications Enablement – control each application independently



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, zero-day attacks protection

Unconventional attack vectors

Beware of keystroke loggers disguised as USB phone chargers, FBI warns

Private industry notification comes 15 months after debut of KeySweeper.

E-Cigarette Found To Have Malware Hard Coded Into Its USB Charger

Chameleon: the Wi-Fi Virus That Hides in Plain Sight and Spreads Like a Cold

"USBdriveby" Emulates Mouse and Keyboard to Hijack Computers

Exploit

Executable

Exploits

Weaponized Data Files & Content

Subvert Normal Applications

≠

Malware

Executable Programs

Carry Out Malicious Activity

paloalto NETWORKS

Block the Core Techniques – Not the Individual Attacks

Number of New Variants Each Year

Individual Attacks

1,000s

Software Vulnerability Exploits

Thousands of new vulnerabilities and exploits

Core Techniques

2-4

Exploitation Techniques

Only two to four new exploit techniques

1,000,000s

Malware

Millions of new malware variations

~10s

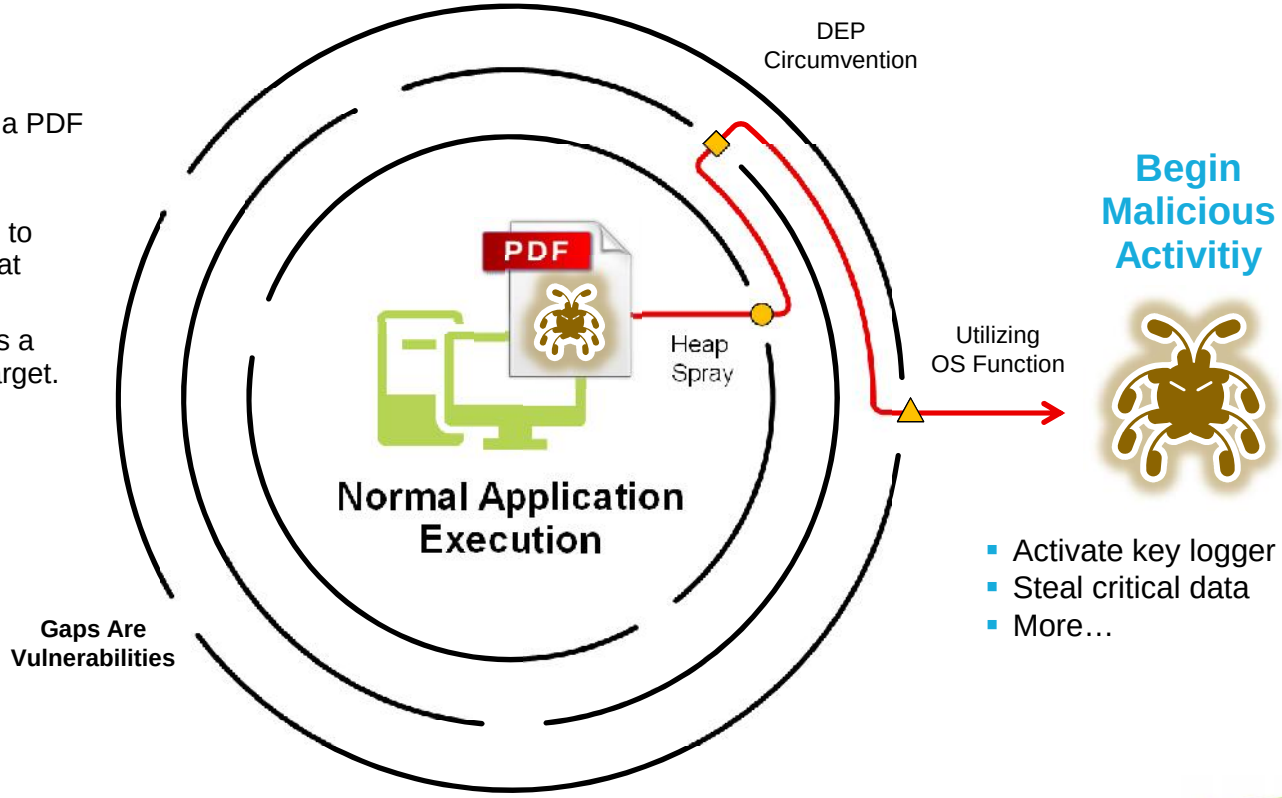
Malware Techniques

Tens of new malware sub-techniques

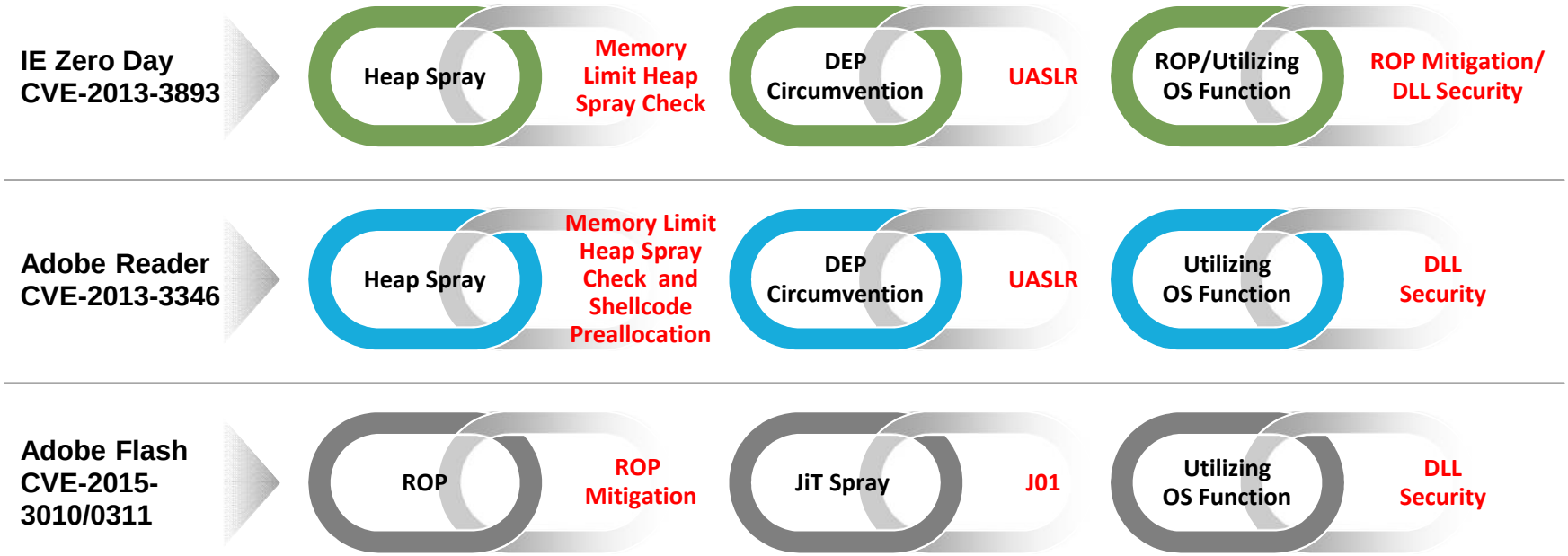
Exploit Techniques

Exploit Attack

1. Exploit attempt contained in a PDF sent by “known” entity.
2. PDF is opened and exploit techniques are set in motion to exploit vulnerability in Acrobat Reader.
3. Exploit evades AV and drops a malware payload onto the target.
4. Malware evades AV, runs in memory.



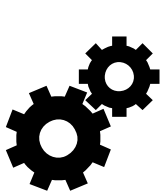
Exploit Prevention Case Study
Unknown Exploits Utilize Known Techniques



Prevention of One Technique in the Chain will Block the Entire Attack

paloalto NETWORKS

Multi-Method Malware Prevention



Admin Override Policies

Trusted Publisher

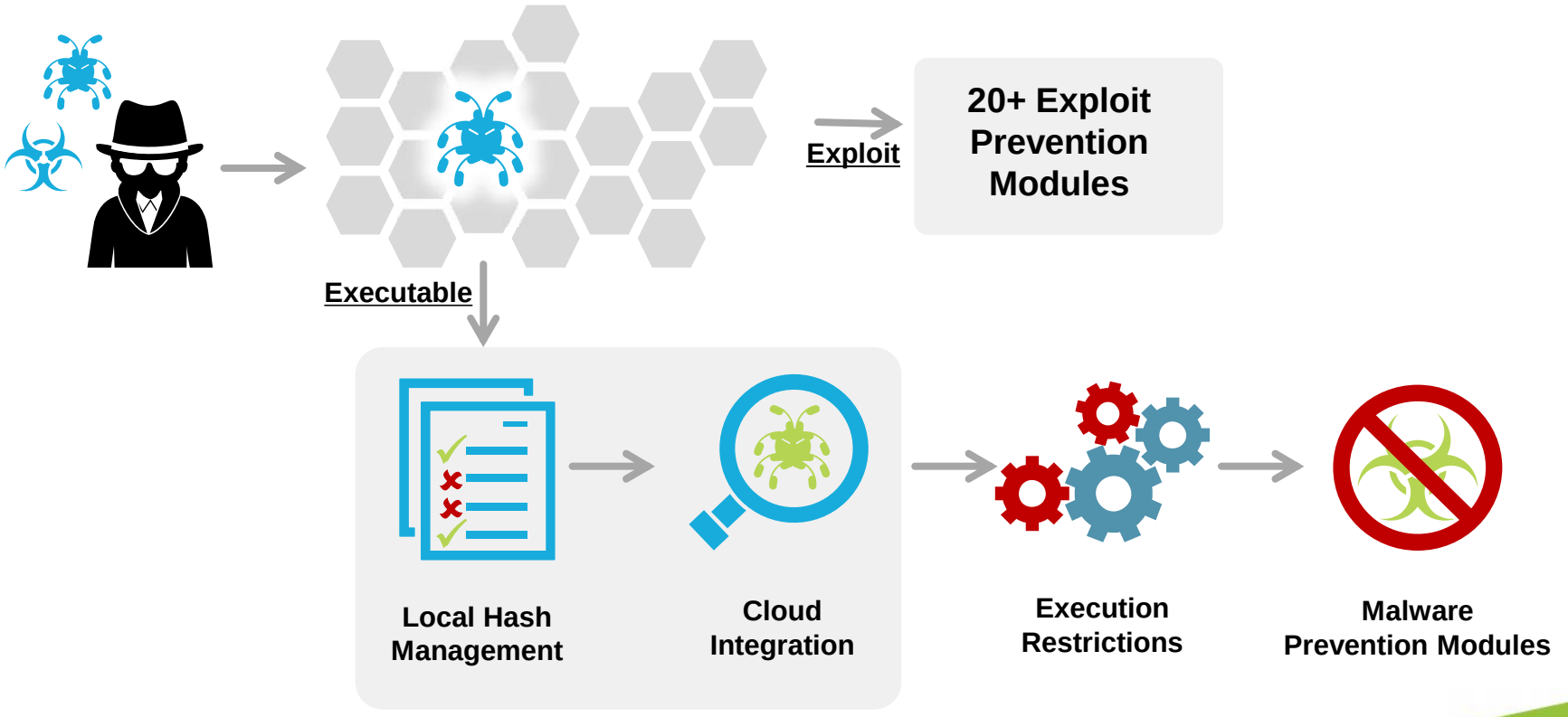
Cloud Inspection & Analysis

Static Analysis via Machine Learning

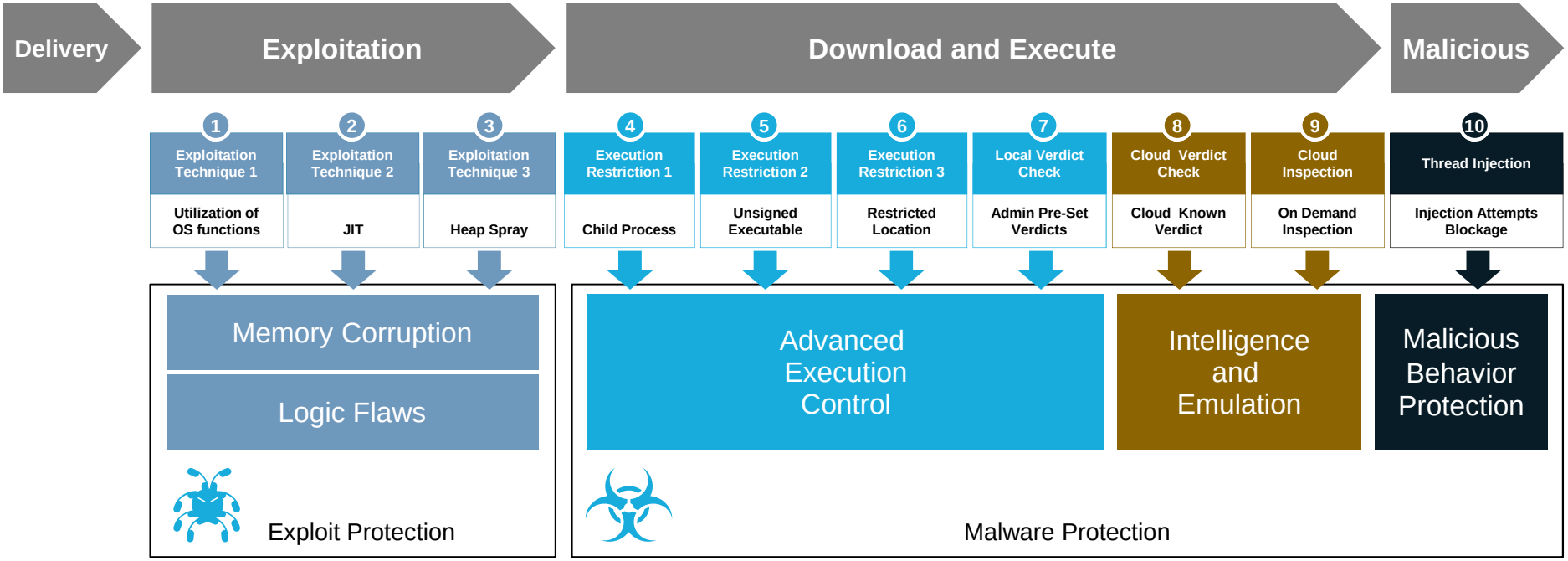
Execution Restrictions

Static Analysis Prevents Malware Variants that Have Never Been Seen Before

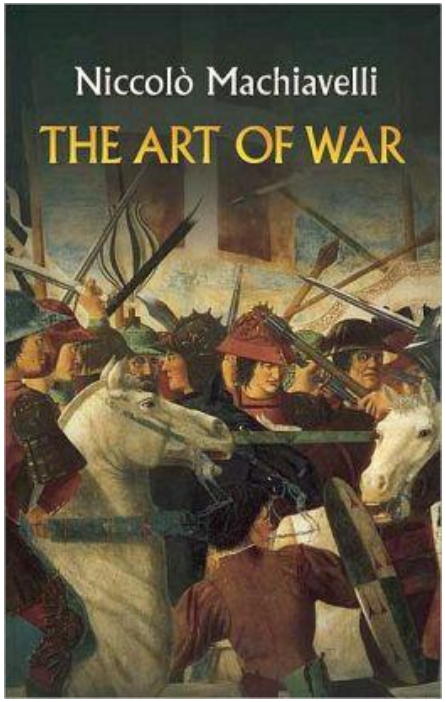
The Most Comprehensive Approach to Endpoint Protection



Endpoint Kill-Points Through the Attack Life Cycle



Expect the unexpected



There is nothing as likely **to succeed** as what the enemy believes you cannot attempt.

Niccolò Machiavelli- The Art of War

Questions ?


Thank You
paloalto
NETWORKS®