

Next-Generation Firewall with Palo Alto Networks



PALO ALTO NETWORKS NEXT-GENERATION SECURITY PLATFORM

What's Changed?

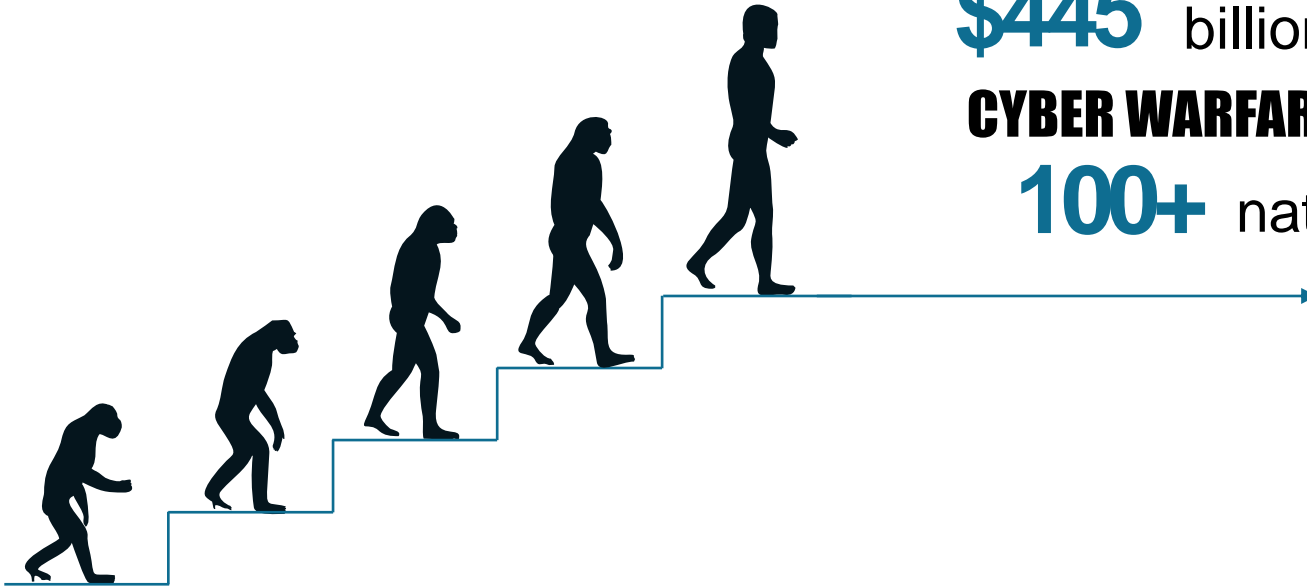
THE EVOLUTION OF THE ATTACKER

CYBERCRIME NOW

\$445 billion industry

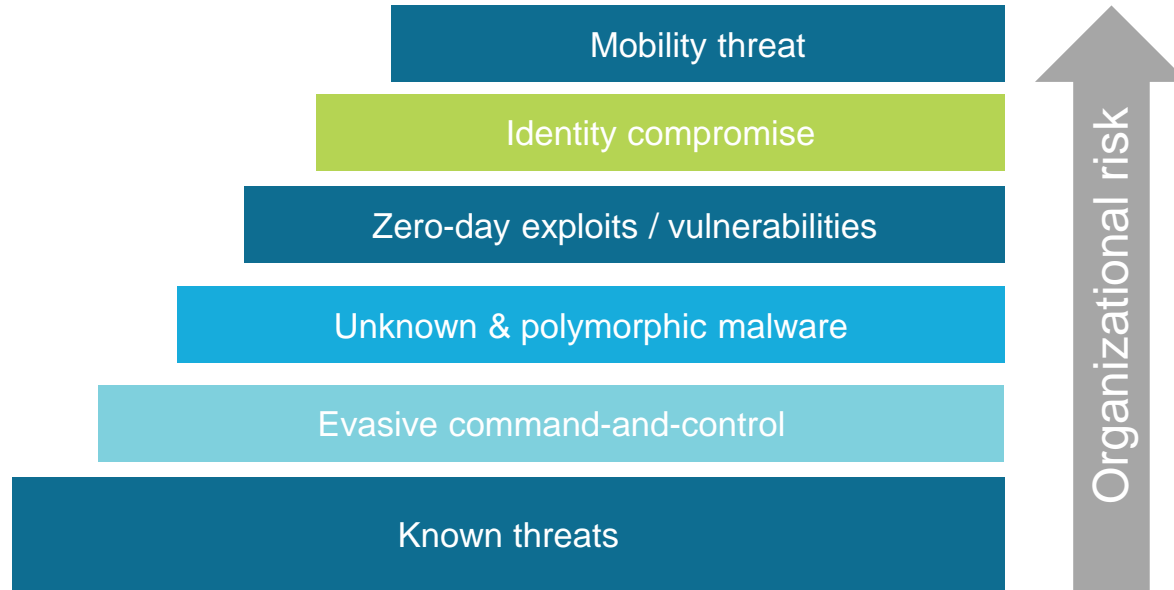
CYBER WARFARE

100+ nations

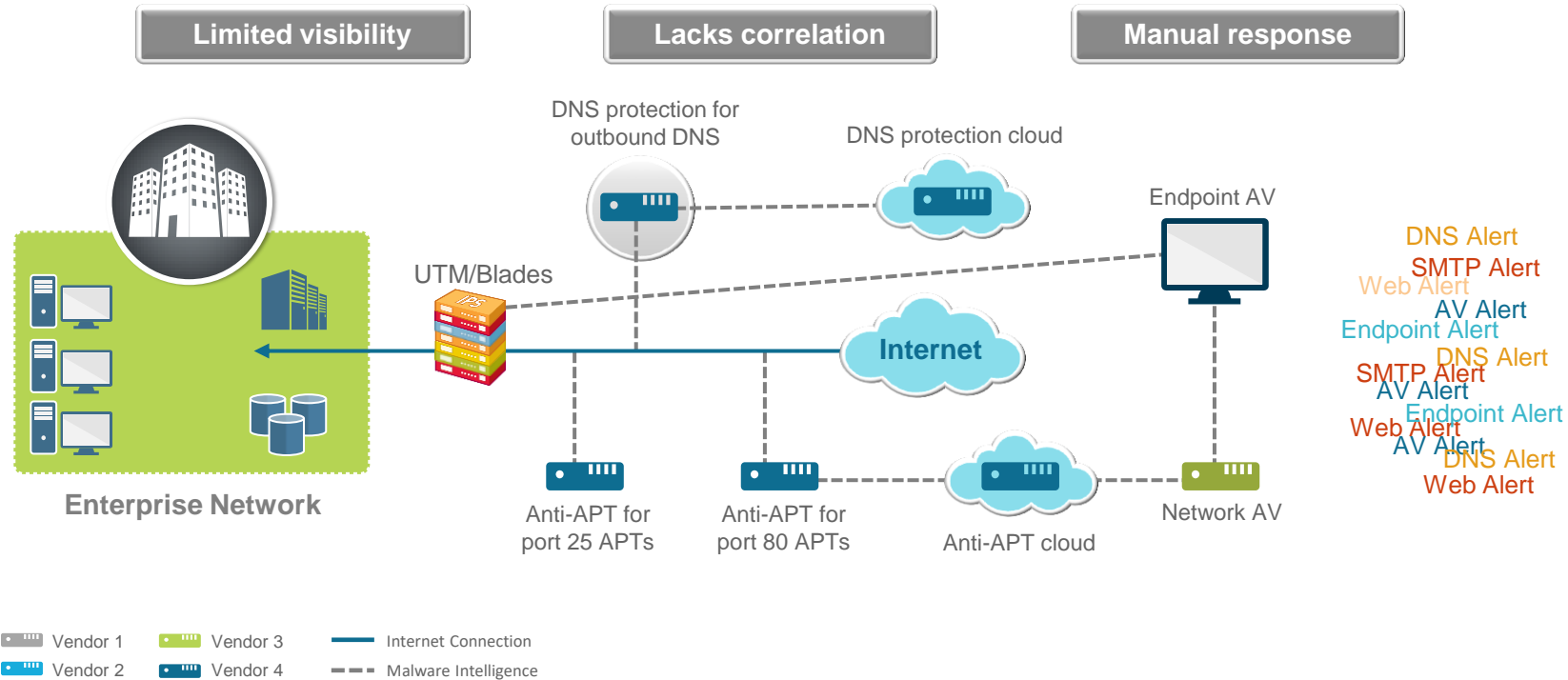


What's Changed?

THE EVOLUTION OF THE ATTACK



Failure of Legacy Security Architectures

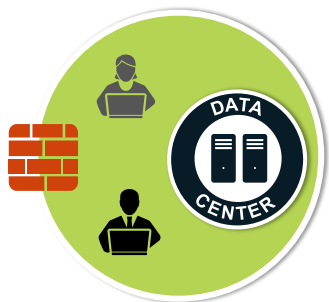


Requirements For The Future

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

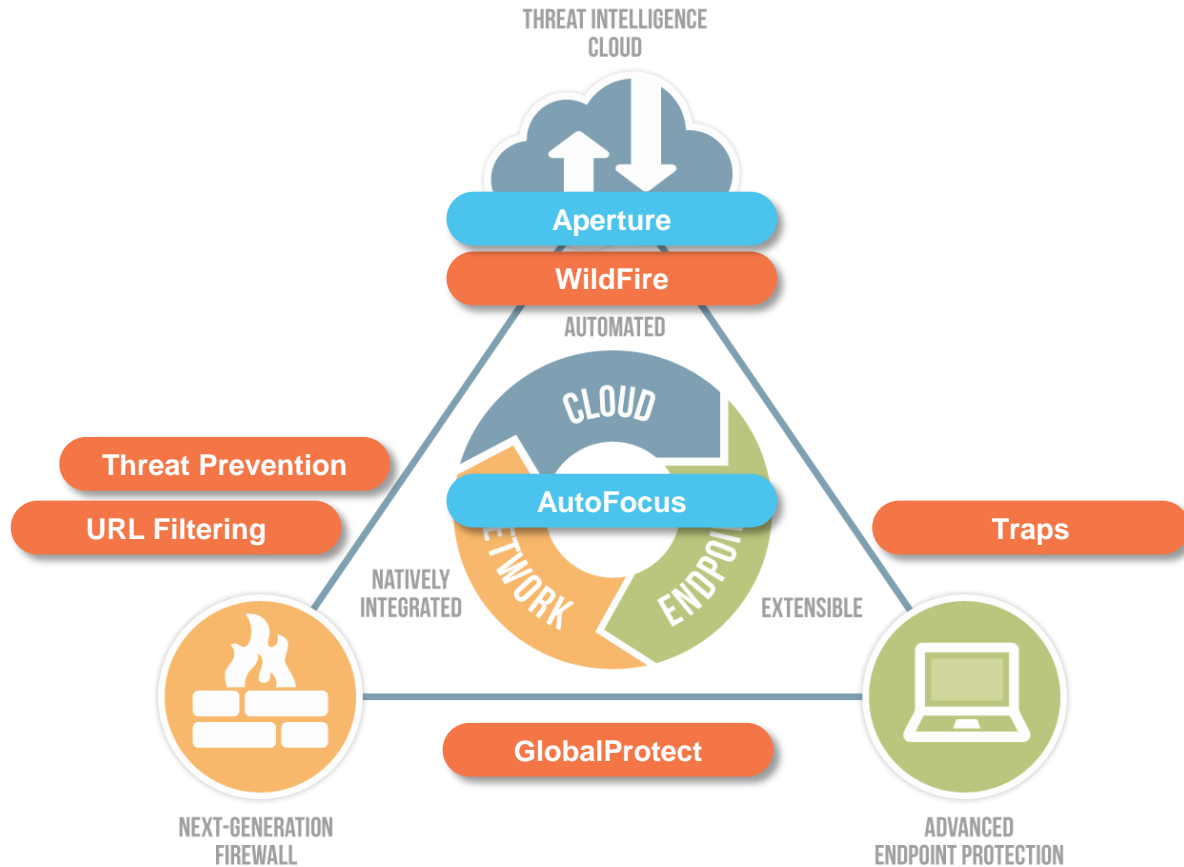


At the data center edge, and between VM's



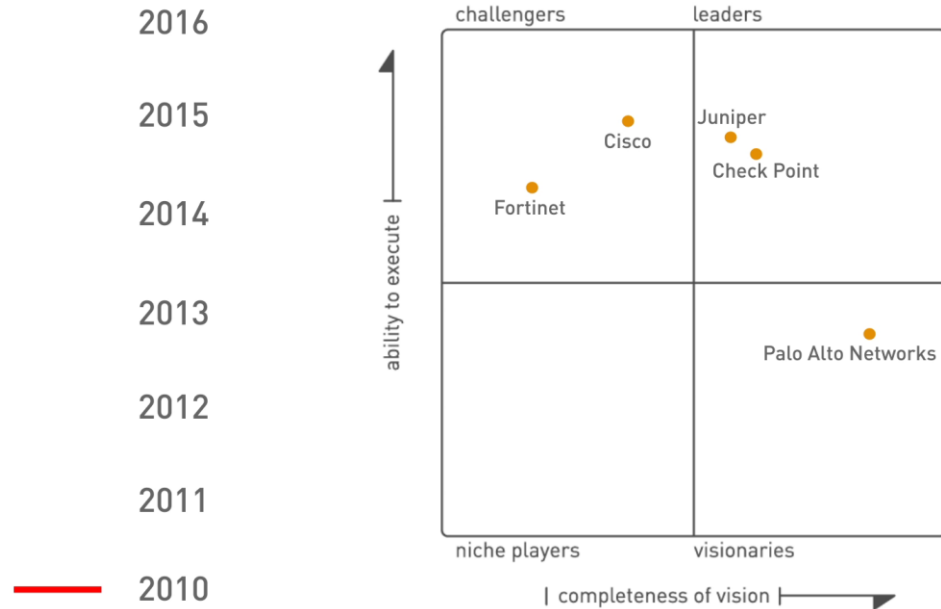
Within private, public and hybrid clouds

Delivering Continuous Innovation



Palo Alto Networks is positioned as a Leader in the Gartner Magic Quadrant for enterprise network firewalls.*

Palo Alto Networks is highest in execution and a visionary within the Leaders Quadrant.



*Gartner Magic Quadrant for Enterprise Network Firewalls, Adam Hils, Greg Young, Jeremy D’Hoinne, and Rajpreet Kaur, May 2016.

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner’s research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Palo Alto Networks Recognized by J.D. Power & Associates and TSIA for Delivering "An Outstanding Customer Support Experience"



2015 & 2016 J.D. Power Certified Assisted Technical Support Program –

Palo Alto Networks, Inc. has been recognized by J.D. Power for two consecutive years for providing “An Outstanding Customer Service Experience” for its Assisted Technical Support.

2015 & 2016 TSIA Global Rated Outstanding Assisted Certification

— TSIA certification recognizes that Palo Alto Networks has achieved Global Rated Outstanding Assisted Support for a second consecutive year. Customers can purchase Palo Alto Networks products with confidence knowing that Palo Alto Networks meets the highest industry support standards.



ASSISTED SUPPORT
GLOBAL | PALO ALTO NETWORKS

2014 TSIA Star Award for Innovation in the Delivery of Support Services –

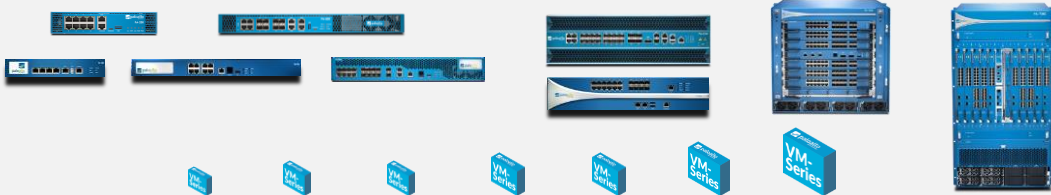

This award recognizes the company that has embraced innovation in people, process and technology to increase agent productivity, service levels or customer satisfaction; increase problem avoidance; or effectively handle more interactions using unassisted channels.



J.D. Power 2016 Certified Assisted Technical Support Program, developed in conjunction with TSIA. Based on successful completion of an audit and exceeding a customer satisfaction benchmark for assisted support operations. For more information, visit www.jdpower.com or www.tsia.com.

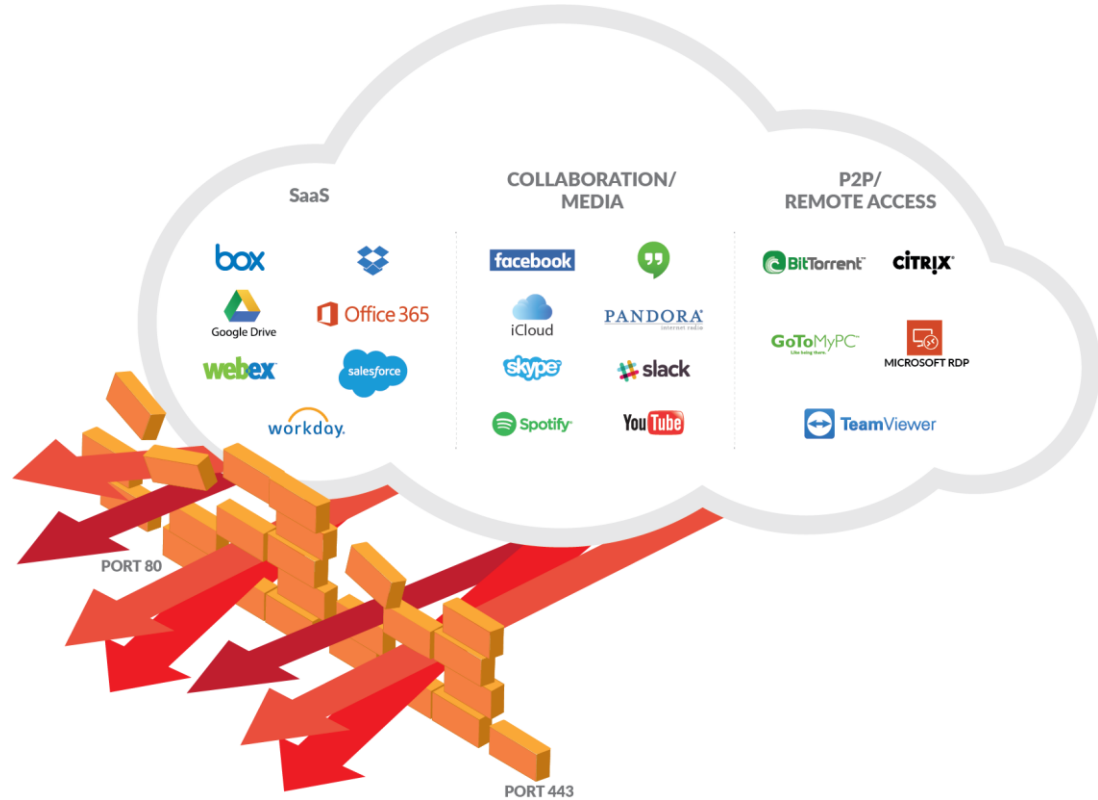


Covering the Entire Enterprise

Locations	Branch Office	Enterprise Perimeter	Endpoints / Mobile	Data Center	Private & Public Cloud	SaaS
Next-Generation Firewalls	<p><u>Physical</u>: PA-200, PA-220, PA-500, PA-800 Series, PA-3000 Series, PA-5000 Series, PA-5200 Series, PA-7000 Series</p> 					
	<p><u>Virtual</u>: VM-Series for ESXi, NSX, Hyper-V, AWS, Azure, KVM and Citrix</p>  <p>VM-50 VM-100 VM-200 VM-300 VM-1000-HV VM-500 VM-700</p>					
Subscriptions	Threat Prevention					
	WildFire™					
	AutoFocus					
	URL Filtering					
	GlobalProtect™					
	Aperture (SaaS Security)					
Traps (Endpoint)						
Management	<u>Panorama</u> : Virtual, M-100, M-500 appliances					
Use Cases	Securing Internet Gateway	Network Segmentation / Zero Trust	Securing Private & Public Clouds	Enabling Secure SaaS Adoption	Protecting Distributed Organizations	

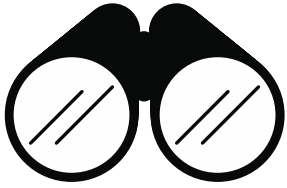
Security Starts With The Firewall, But It's Broken...

- The firewall is the right place to enforce policy control
 - Sees all traffic
 - Defines trust boundary
 - Enables access via positive control
- BUT...applications have changed
 - Ports \neq Applications
 - IP Addresses \neq Users
 - Packets \neq Content



Need to restore visibility and control in the firewall

Palo Alto Networks Approach For Preventing Attacks



Complete visibility

- Network & endpoint (different views)
- All applications, inc. cloud & SaaS
- All users & devices, inc. all locations
- Encrypted traffic



Reduce attack surface area

- Enable business apps
- Block “bad” apps
- Limit app functions
- Limit high risk websites and content
- Require multi-factor authentication



Prevent all known threats

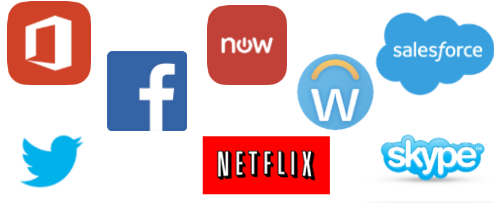
- Exploits
- Malware
- Command & control
- Malicious & phishing websites
- Bad domains



Detect & prevent new threats

- Unknown malware
- Zero-day exploits
- Custom attack behavior

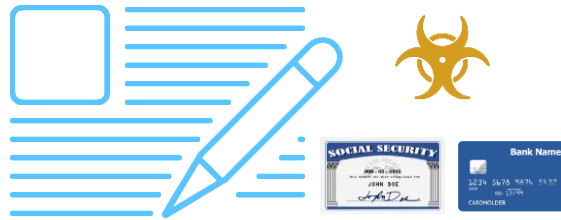
Palo Alto Networks Next-Generation Firewall: Built Right



All traffic, always
classified by application

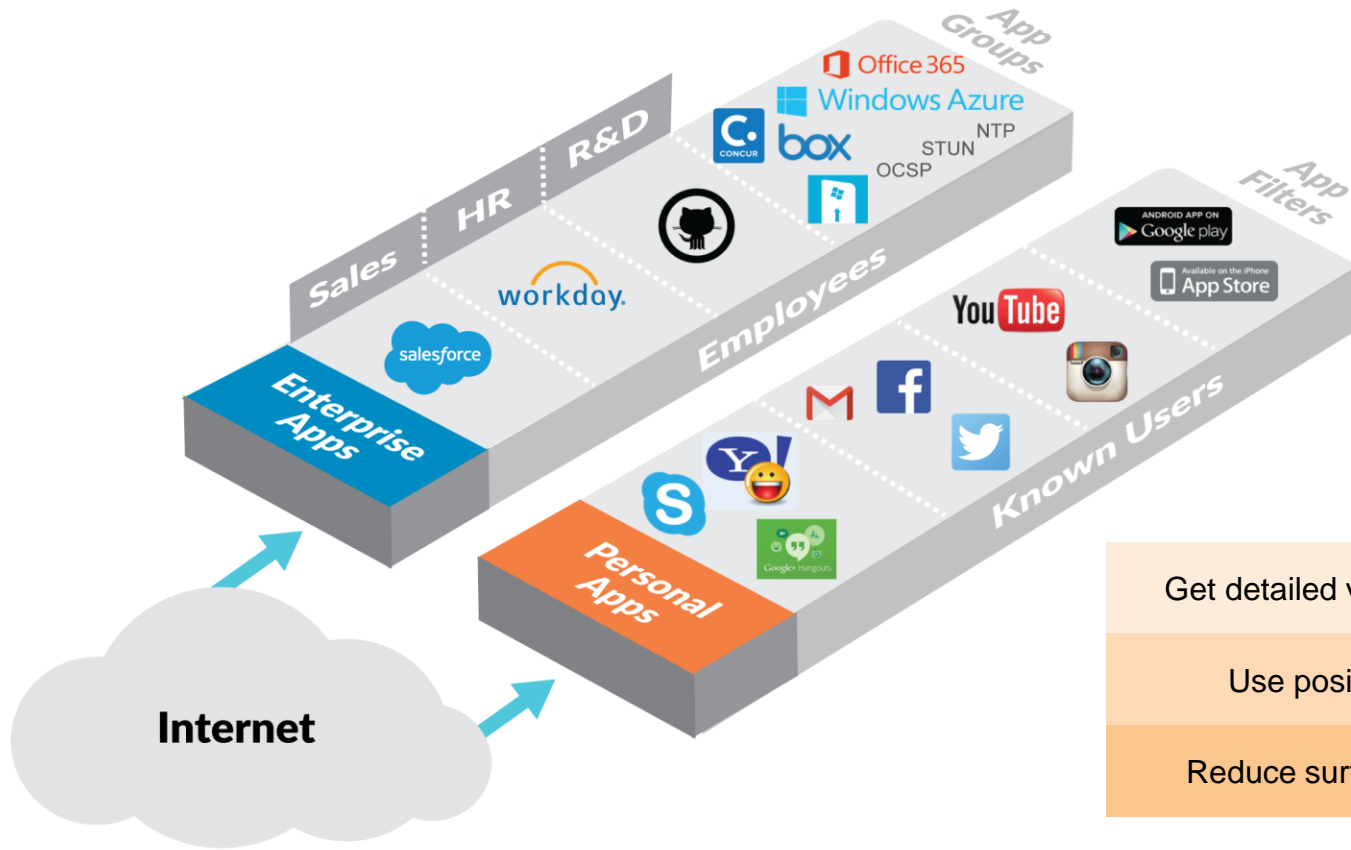


Users and devices identified
regardless of location



Content scanned and protected against
all threats, both known and unknown

App-ID: Safely Enable Applications



Get detailed visibility and granular control

Use positive enforcement model

Reduce surface area for cyber attacks

SaaS Application Usage Report



box.net
Sanctioned SaaS
5101 users
100 files · 6TB

Wildfire submissions: **321**
Benign: **318** Malicious: **3**

TOP 10 USERS BY DATA MOVEMENT

paloaltonetworks\skumar
paloaltonetworks\jcole
paloaltonetworks\shiwani
paloaltonetworks\lduran
paloaltonetworks\mwana
paloaltonetworks\rdavid
paloaltonetworks\rcruz
paloaltonetworks\rfraise
paloaltonetworks\esmith
paloaltonetworks\janeegan

TOP 10 BLOCKED OR ALERTED FILE TYPES

flash	454
ms-office	123
pdf	99

TOP 10 THREATS

[32356] Micros...	1534
[34243] PNG Fi...	123
[32326] Adobe ...	111
[32002] Micros...	12
[32282] Micros...	9
[34239] Adobe ...	8
[30520]HTTP O...	7
[1270088]Viru...	7
[33456]Macrom...	4



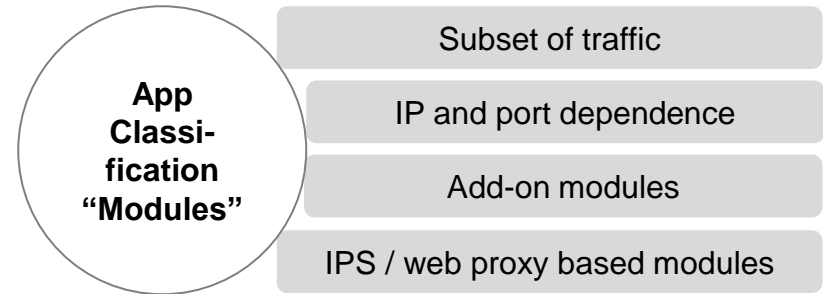
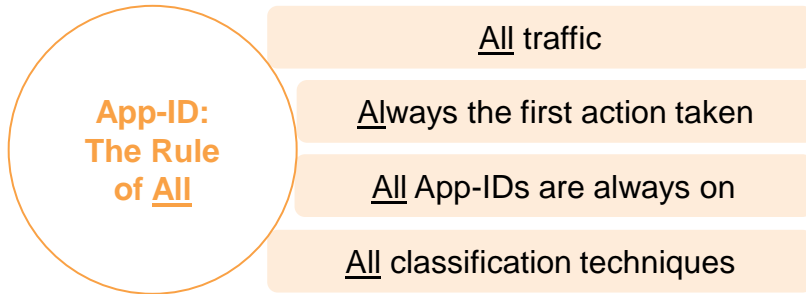
Sanctioned and unsanctioned SaaS apps

Detailed breakdown by user and file type

Top threats seen in SaaS traffic



Don't All FWs Classify Applications?



What You Get With Palo Alto Networks NGFW

Complete visibility: All traffic is classified

Complete control: App-ID controls all traffic regardless of port and protocol

Simple and secure: Single policy with App-ID, Users, Threats, URL...

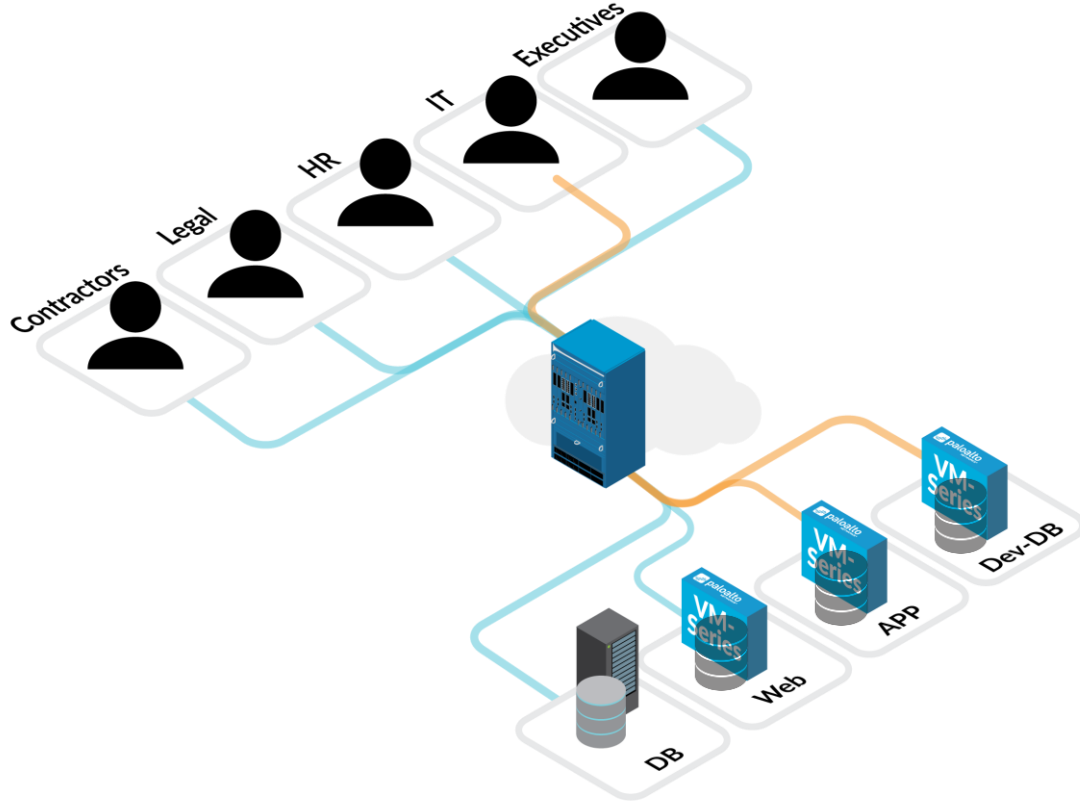
What You Get With Other “NGFWs”

No visibility into traffic filtered out by stateful inspection

Cumbersome to control evasive applications due to dependence on ports

Multiple layered policies: difficult to maintain, open up security holes

User-ID: Connect Users to Assets Securely

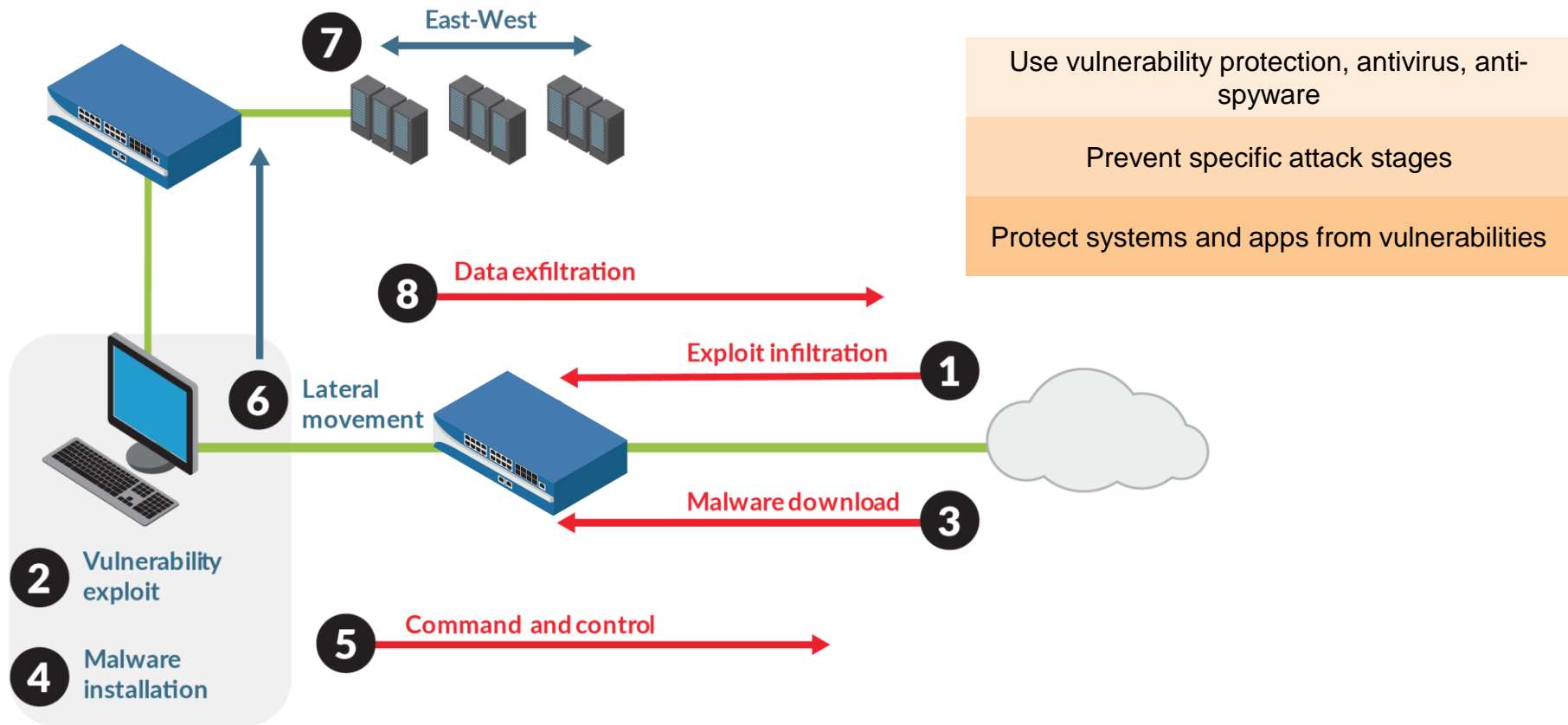


Leverage multiple sources of user identity

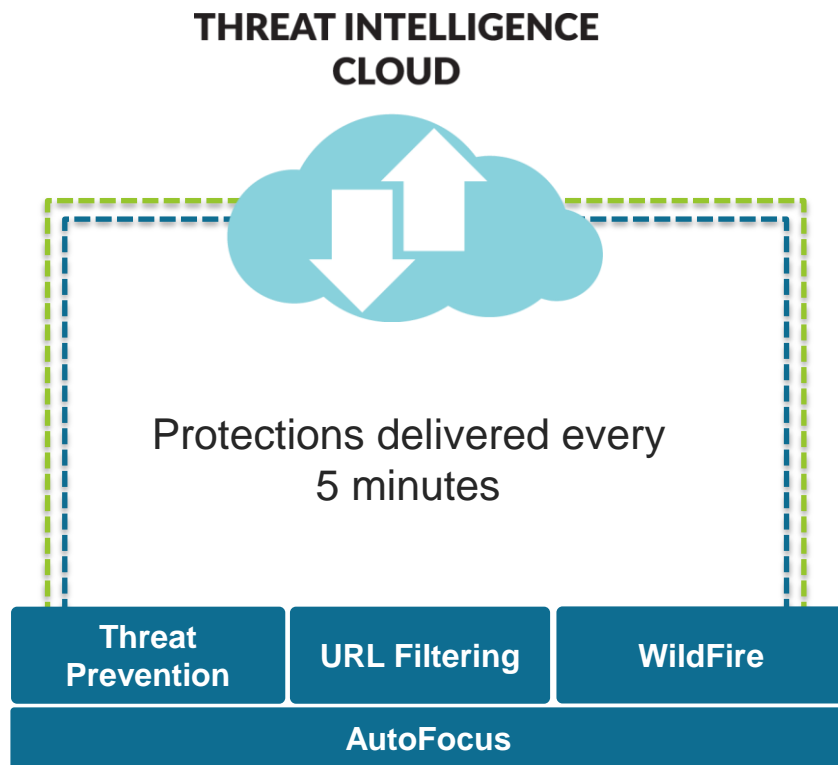
Enable employees, partners, contractors

Control data exfiltration with reliable User-ID

Content-ID: Prevent Threats



Threat Intelligence Cloud: Automate Protection

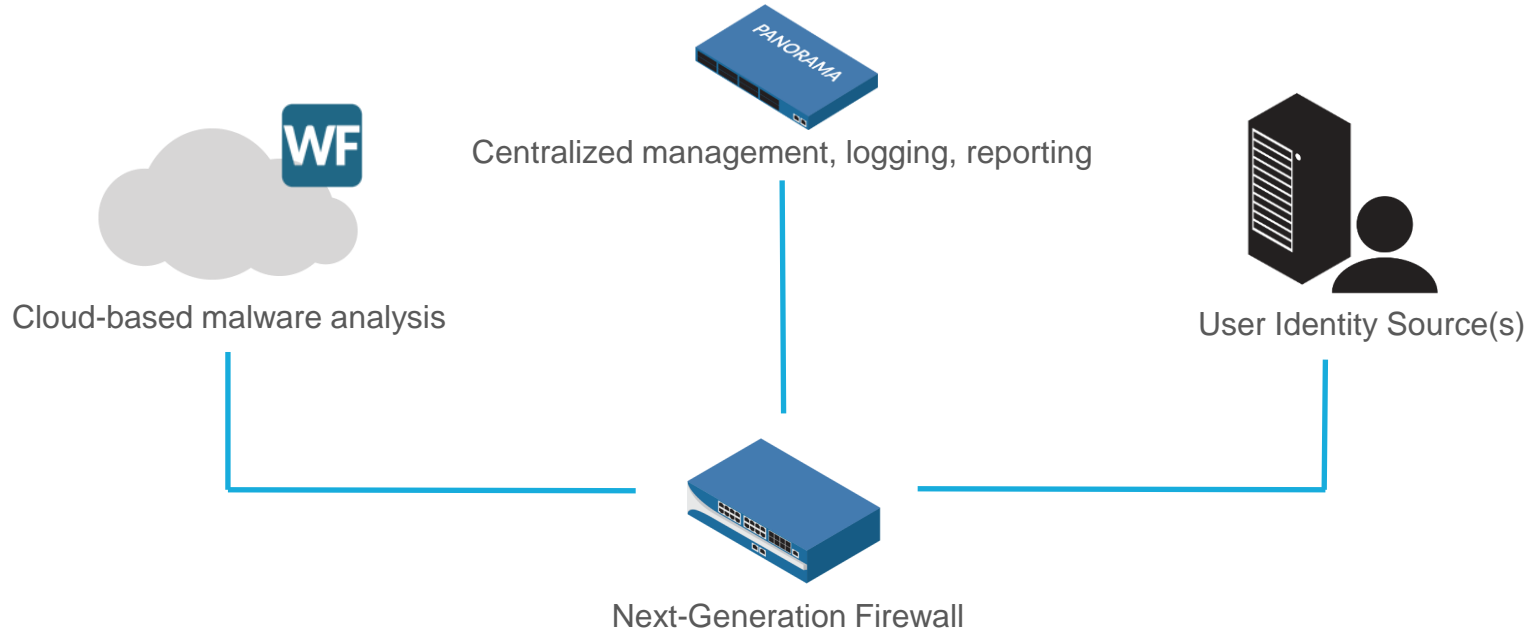


3-5 million new samples per day

1.5 billion samples analyzed

1.5 billion sessions captured

Palo Alto Networks: Simple, Efficient, Effective



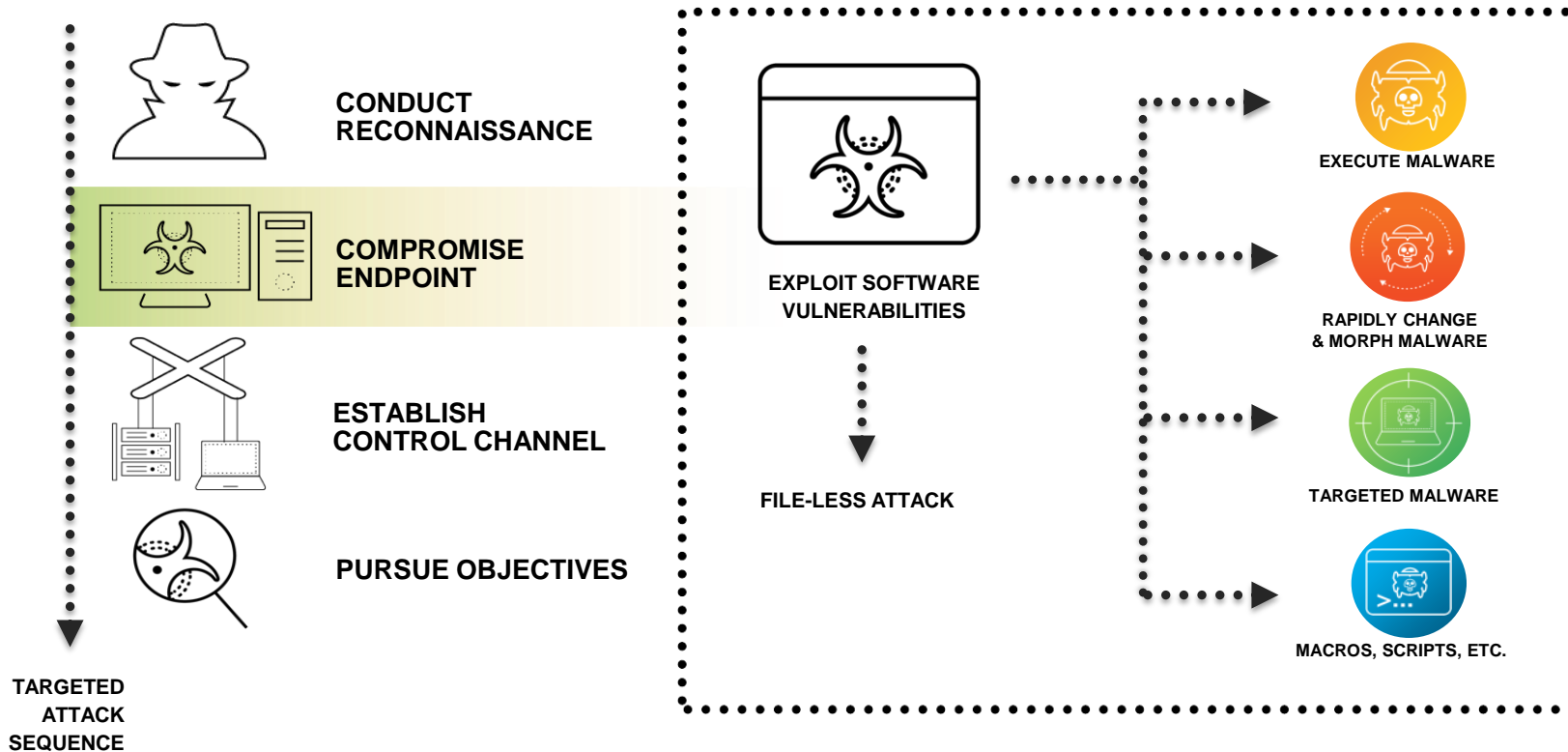
TRAPS

ADVANCED ENDPOINT

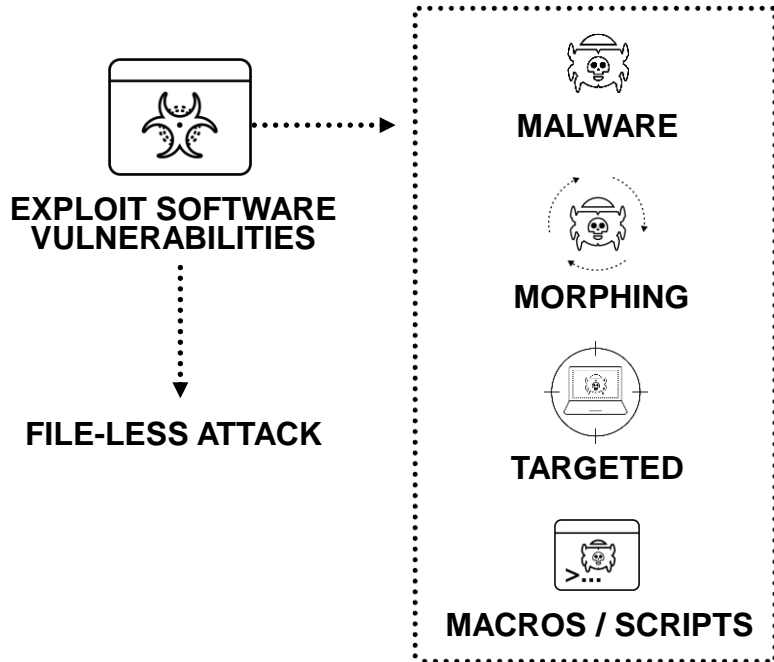
PROTECTION



The Need For A Multi-Method Prevention Approach



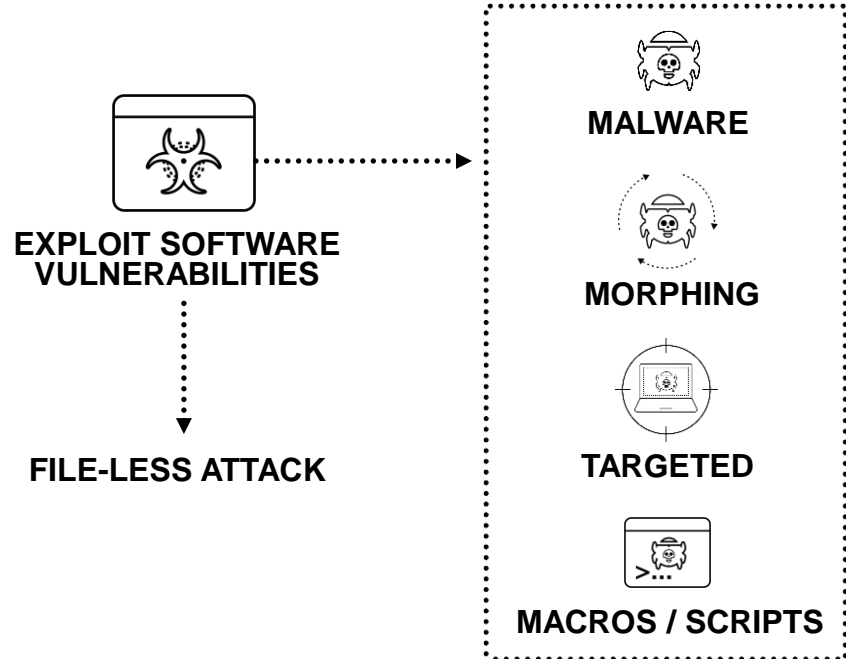
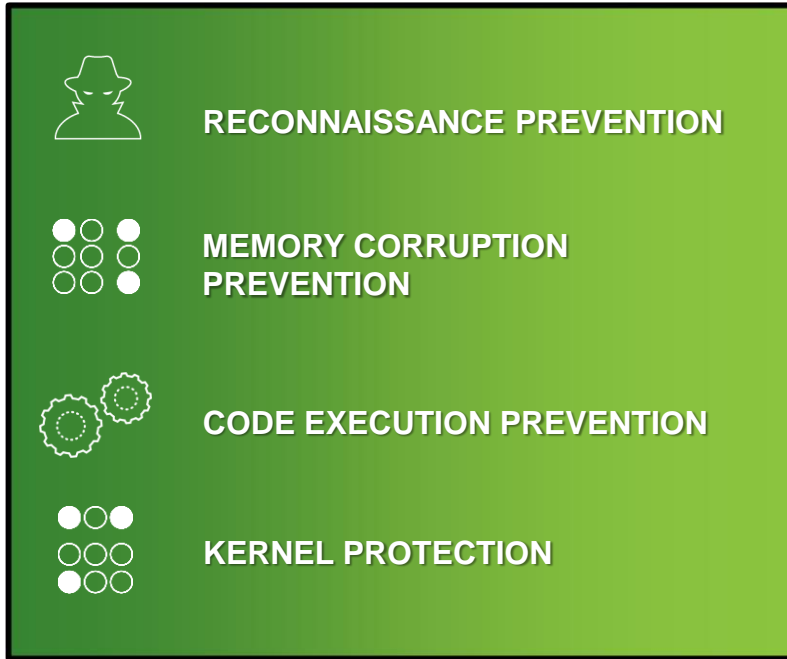
Multi-Method Malware Prevention



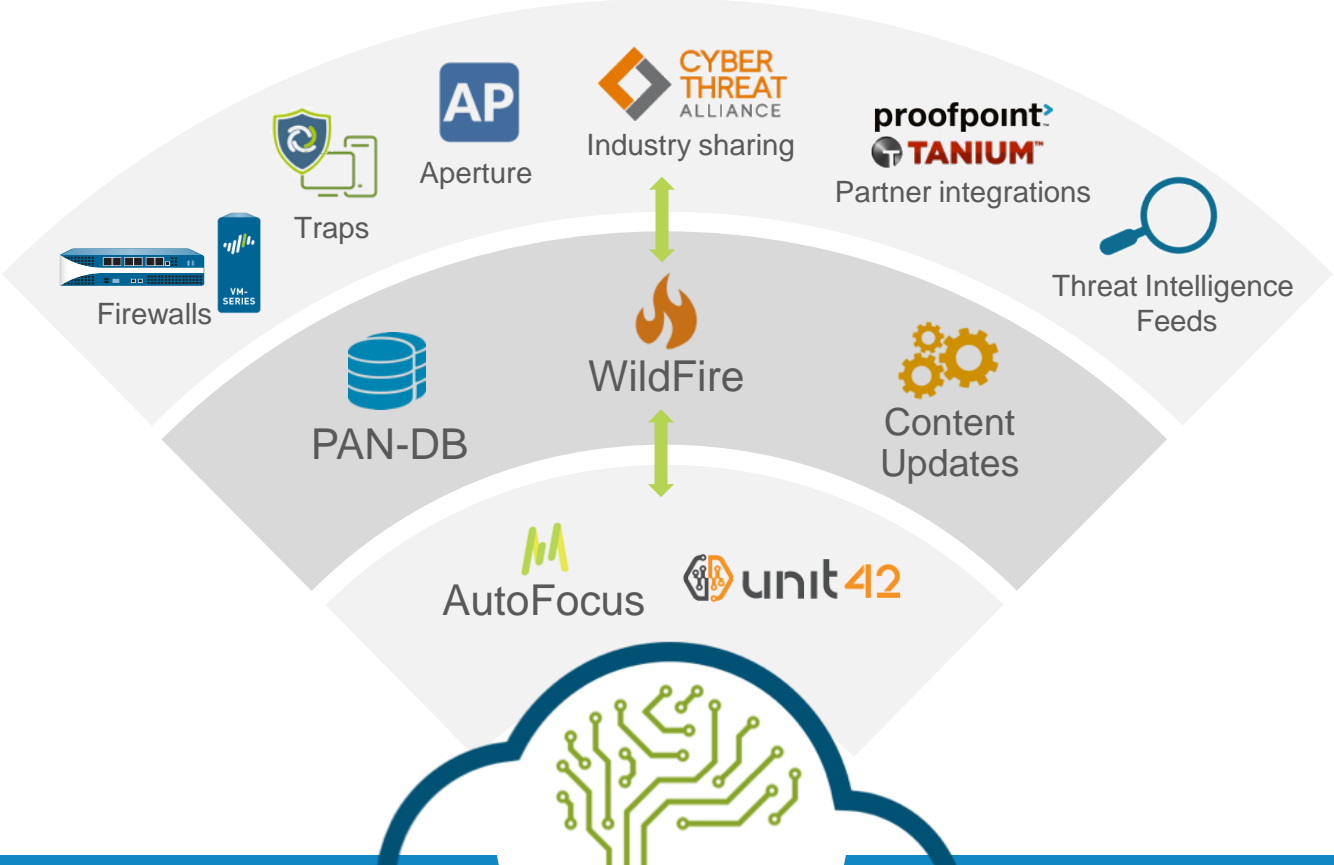
The green box contains four prevention methods, each with an icon and a description:

- REDUCE THE ATTACK SURFACE**
Policy Controls, Child Processes, Execution Restrictions
- PREVENT KNOWN MALWARE**
WildFire Threat Intelligence
- PREVENT UNKNOWN MALWARE**
Local Analysis via Machine Learning
- DETECT ADVANCED THREATS**
WildFire Inspection & Analysis

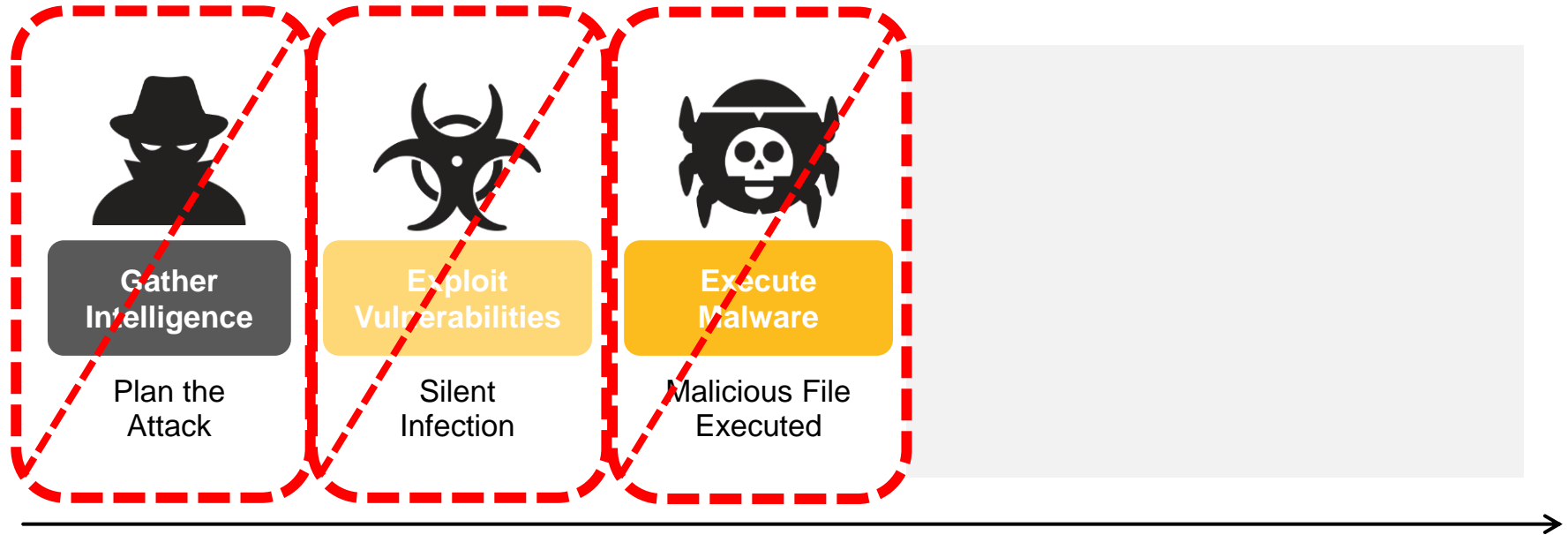
Multi-Method Exploit Prevention



Threat Intelligence Cloud

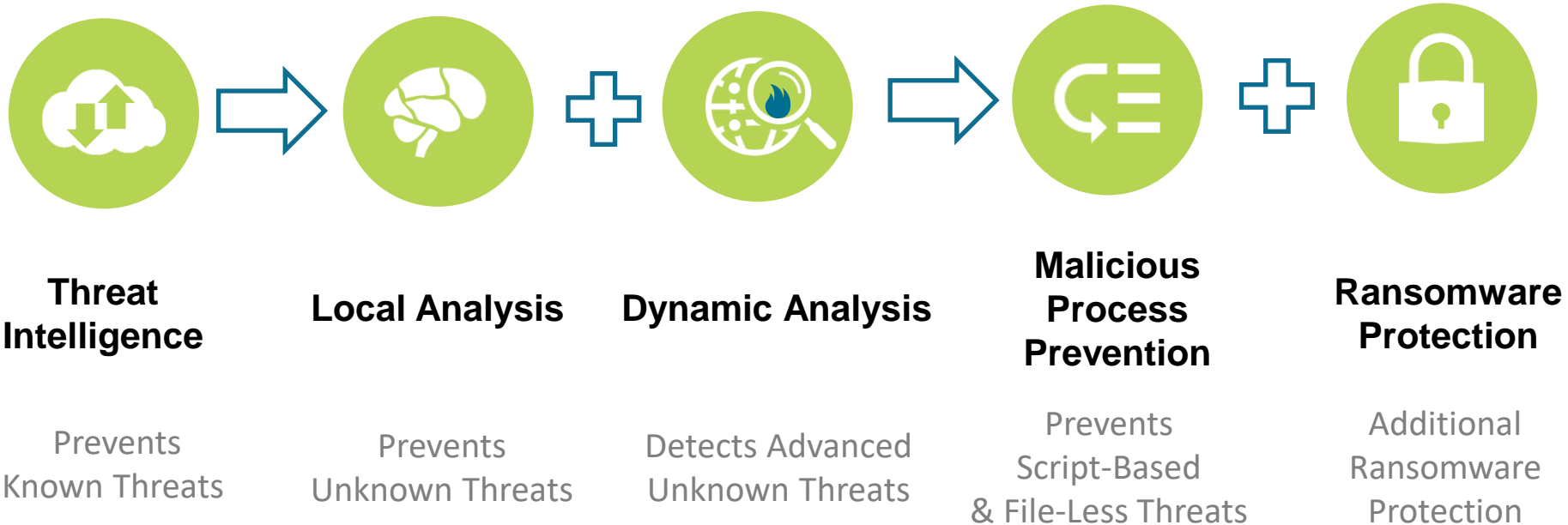


Stop One Building Block, Stop the Attack



Traps Can Block the Attack at Multiple Points
Before it Can Initiate any Malicious Activity

Traps Multi-Method Malware Prevention



Traps Multi-Method Exploit Prevention



Reconnaissance Protection

Automatic Prevention of Vulnerability Profiling Used by Exploit Kits



Technique-Based Exploit Prevention

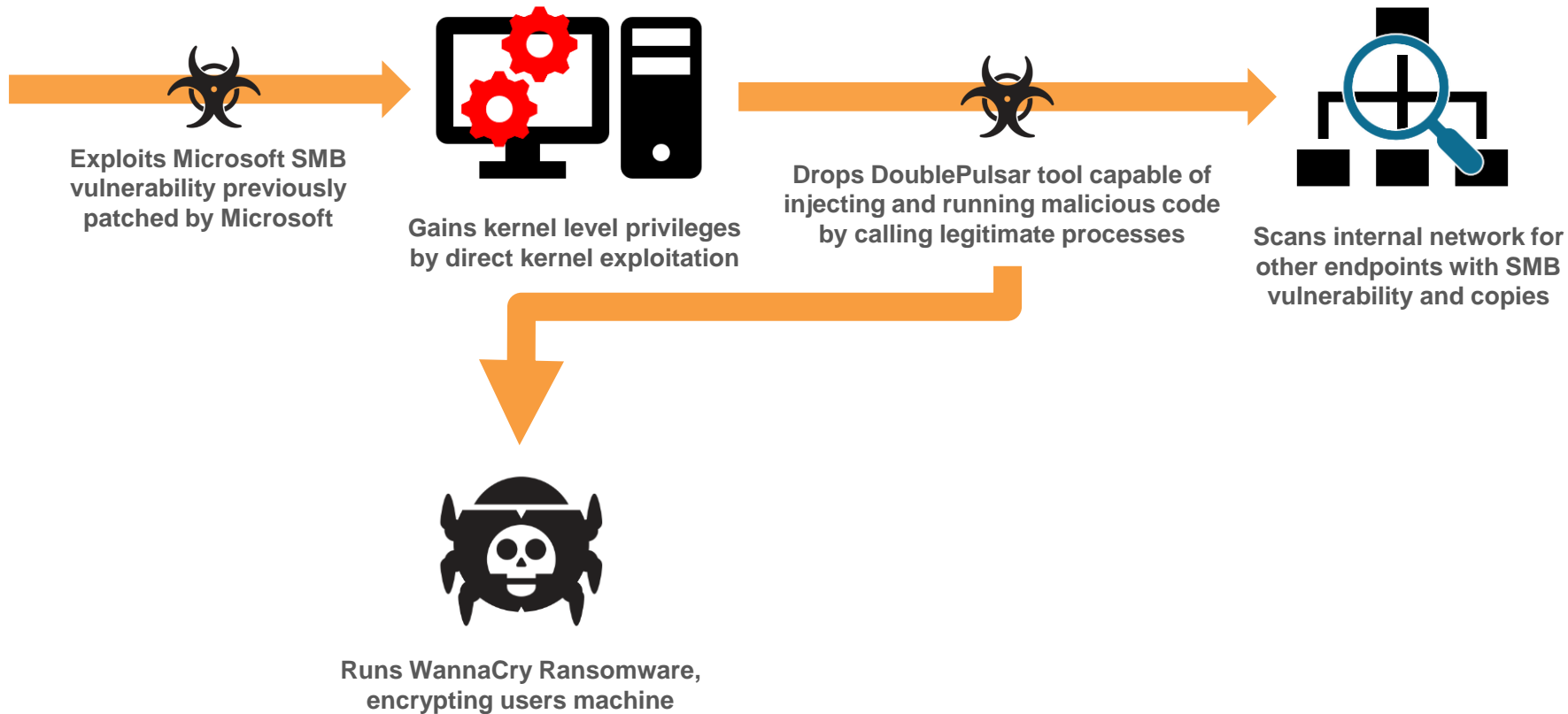
Blocking of Exploit Techniques Used to Manipulate Good Applications



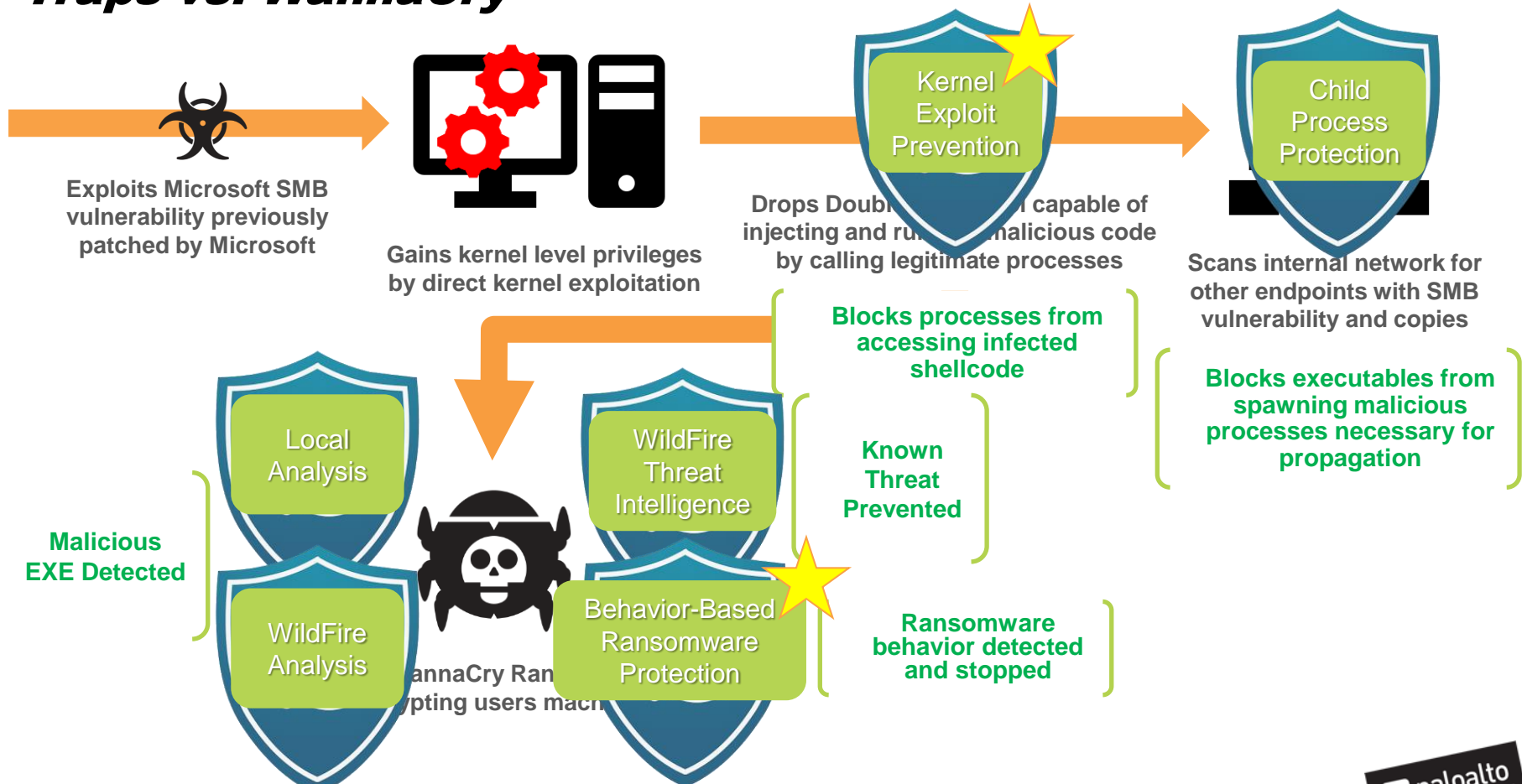
Kernel Protection

Protection Against Exploits Targeting or Originating from the Kernel

Traps vs. WannaCry



Traps vs. WannaCry



Preventing Known Threats



WildFire Threat Intelligence

- Delivers over 230,000 new protections daily in 5min intervals
- A 2-way street across 19,500 customers and millions of sensors
 - *Enterprises*
 - *Governments*
 - *Tech Partners*
 - *3rd Party Intel Feeds*
 - *Human Analysis from Unit 42*
 - *Other Palo Alto Networks components*
- **Continuously analyzed and utilized by the entire Next-Gen Security Platform of Palo Alto Networks**

Preventing Unknown Threats



Local Analysis

- Windows and Mac, for online or offline users
- No signatures or scanning and invisible to end users
- Based on Machine-Learning trained from WildFire



WildFire Analysis

- Runs in the cloud enabling significant computing power without affecting users
 - Static Analysis via Machine Learning
 - Dynamic Analysis
 - Bare-Metal Analysis
- Acts as a secondary check to reduce potential FPs

Preventing Unknown Threats



Granular Child Process Protection

- Customizable protection against script-based and file-less attacks
- Delivered out-of-the-box and automatically updated based on new threat intelligence without user action



Behavior-Based Ransomware Protection

- An additional layer of prevention to pre-existing malware and exploit prevention capabilities
- Not reliant on signatures or known samples
- Able to discern between good and malicious encryption

Traps Multi-Method Exploit Prevention



Reconnaissance Protection

- **Protection against “Fingerprinting”**
- **Attackers learn what you’re running to determine the best exploit and attack to run against you**
- **Prevent an attack before it starts**
- **Enabled for Internet Explorer and Edge Browsers**

Exploit Technique Preventions

Control Panel Protection	Data Execution Prevention	UASLR	DLL-Hijacking Protection
Exception Heap Spray Check	Exploit Kit Fingerprinting Protection	SysExit	Hot Patch Protection
Just-in-Time (JIT) Mitigation	Kernel Privilege Escalation Protection	Library Pre-allocation	Memory Limit Heap Spray Check
Null Dereference Protection	ROP Mitigation	Structured Exception Handler Protection	Shellcode Pre-allocation

Traps Multi-Method Exploit Prevention



Kernel Protection

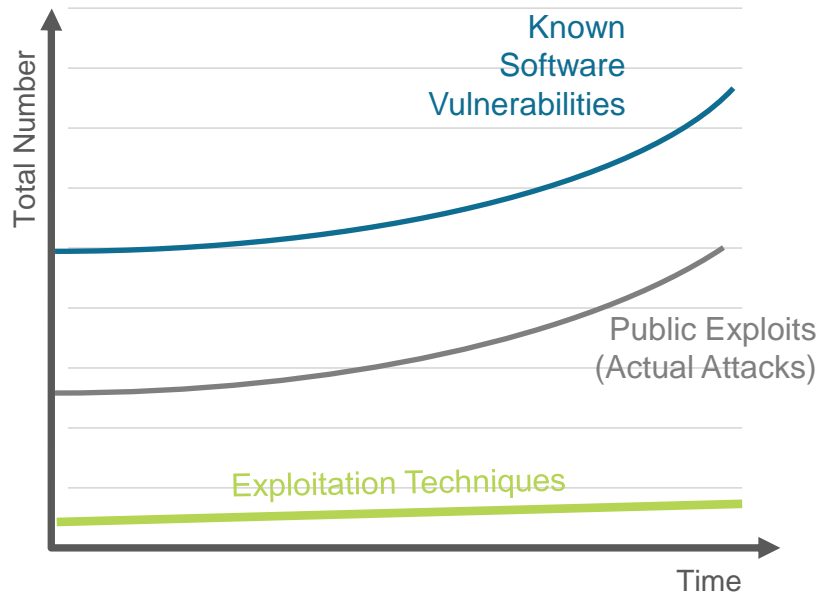
Escalation Protection

- Prevents using privilege information of another process to run with system permissions
- Ability to Whitelist if necessary

DoublePulsar Prevention

- New technique utilized in WannaCry and NotPetya
- Prevents legitimate processes from calling malicious shellcode injected from the kernel
- Legitimate processes continue to run unaffected

Blocking Exploitation Techniques Is the Most Effective Approach



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

Continued Validation from AV-TEST

Further validation
Traps can replace
legacy AV

100% detection of
real-world samples
(no signatures)

Maximum
performance score
(no slowdown)

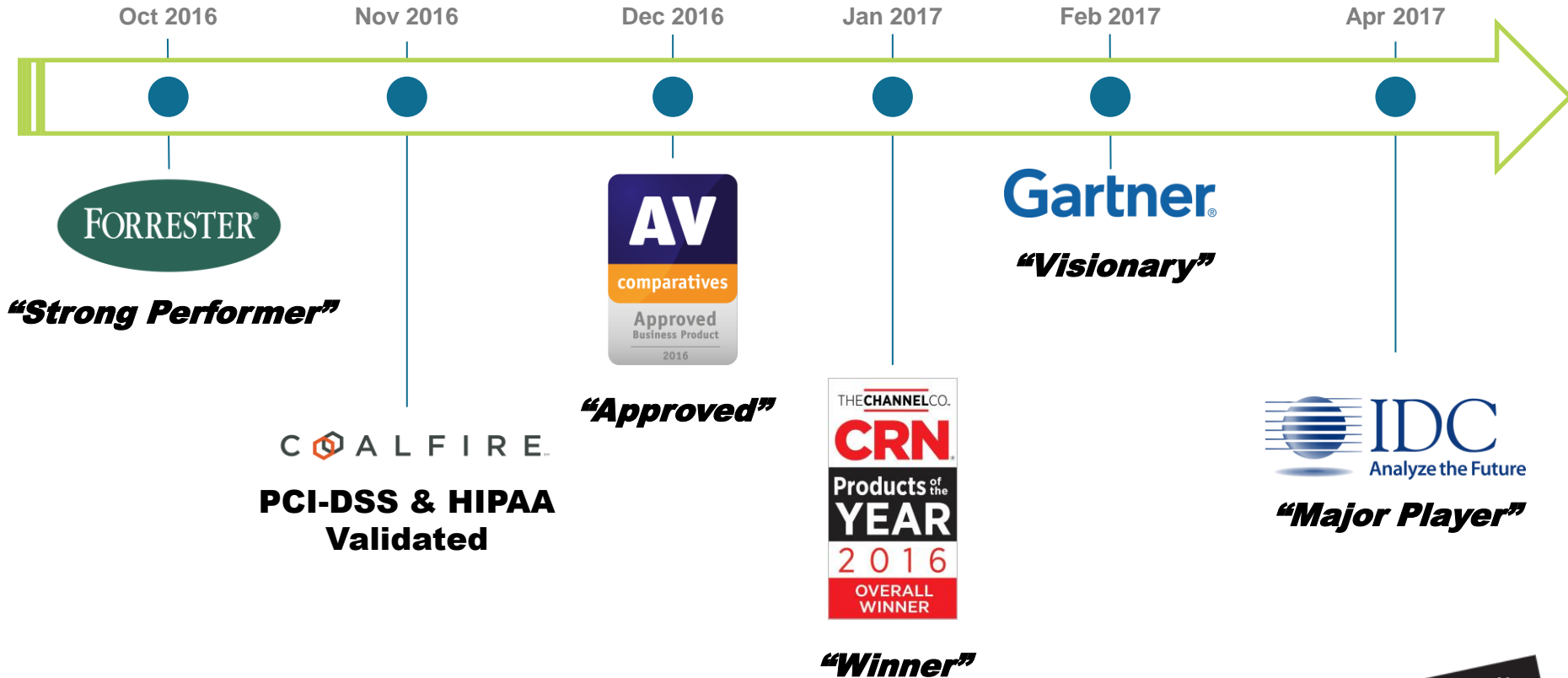
Combined score
higher than average
of incumbents

Only next-generation
endpoint protection
offering tested by AV-
TEST in 2017.



**Based on 4.0
Q3, 2017**

Traps: Award-Winning, Compliance-Ready, Industry-Recognized



Thank You



UpGreat
we know-how to do IT

The Palo Alto Networks logo, which includes a white icon of a network diagram (a square with four vertical bars of increasing height) on a yellow background.

paloalto
NETWORKS®