Preventing Attacks On the Endpoint

Introducing Traps™

Patrick Reischl, CISSP

Specialist System Engineer – Traps - Nordics, Baltics and Eastern Europe

Is Real-Time, Automatic Prevention of Attacks that use Unknowns and Zero-Days Possible?

Attackers Leverage Weak Malware Coverage and Software Bugs to Compromise Endpoints

Attack Sequence

Conduct Reconnaissance

Compromise Endpoint

Establish Control Channel

Pursue Objectives

Delivery

- Web-Based Exploitation
- Malware Download
- Email Attachments

Malicious Action

- Exploit Good Applications
- Run Malware
- Run Scripts
- Run MS Office Macros
- Exploit Operating System
- Escalate Privileges

paloalto NETWORKS

Exploits

Weaponized Data Files & Content

Subvert Normal Applications

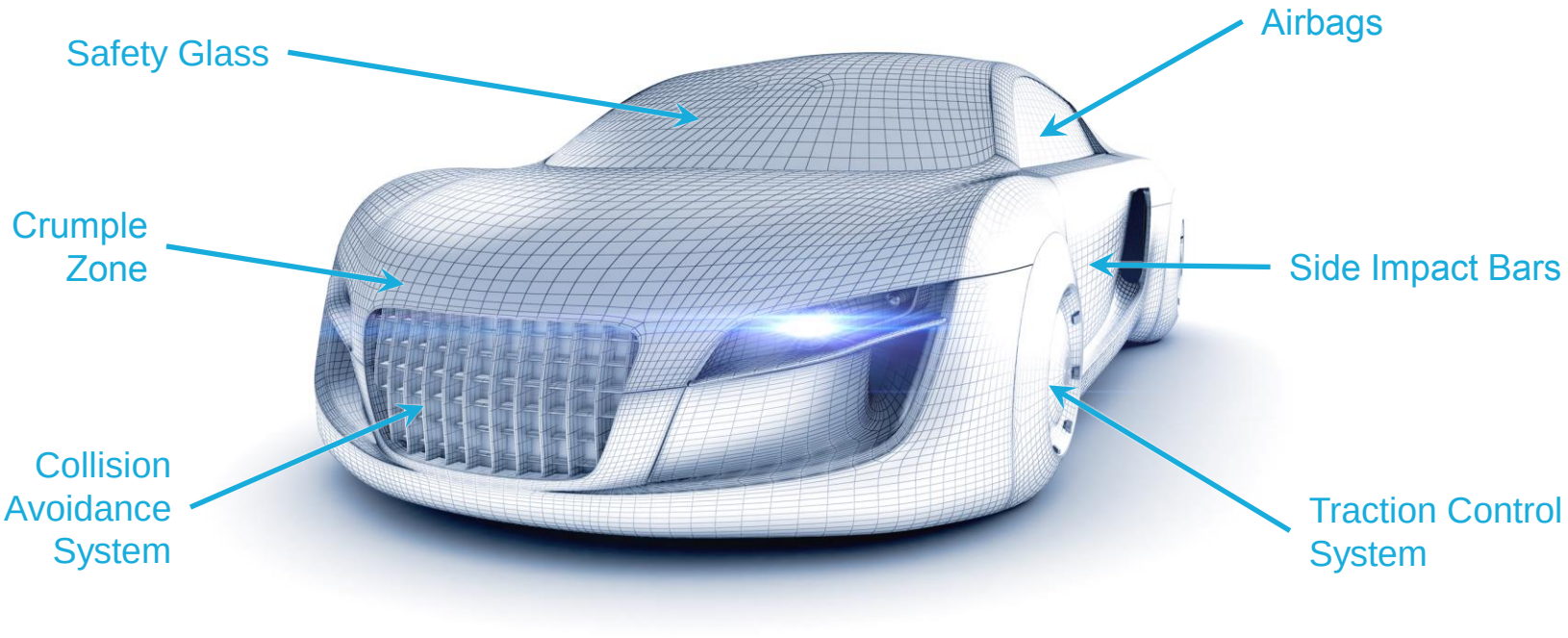
≠

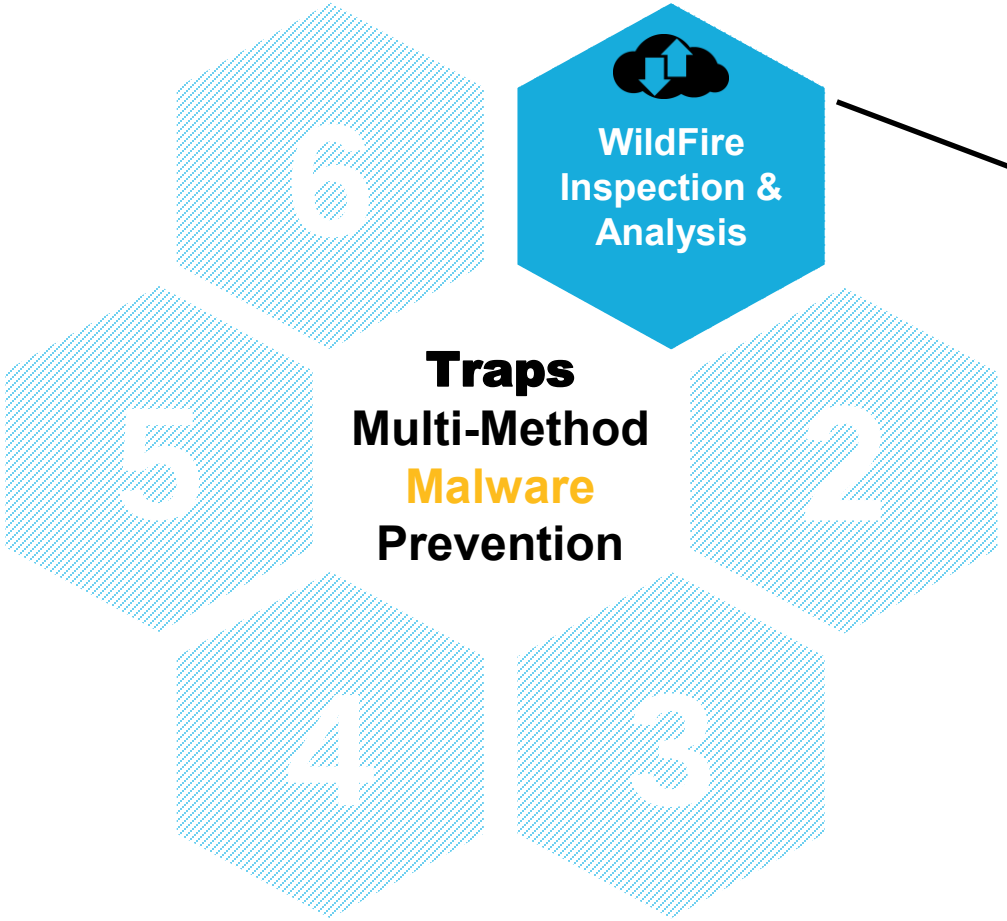
Malware

Executable Programs

Carry Out Malicious Activity

Prevention Requires a Combination of Multiple Purpose-built Methods





Traps Leverages the Power of WildFire to Prevent Known Malware and to Detect Unknown Malware

WildFire Detects Malware Using Multiple Methods & Techniques

Static Analysis

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

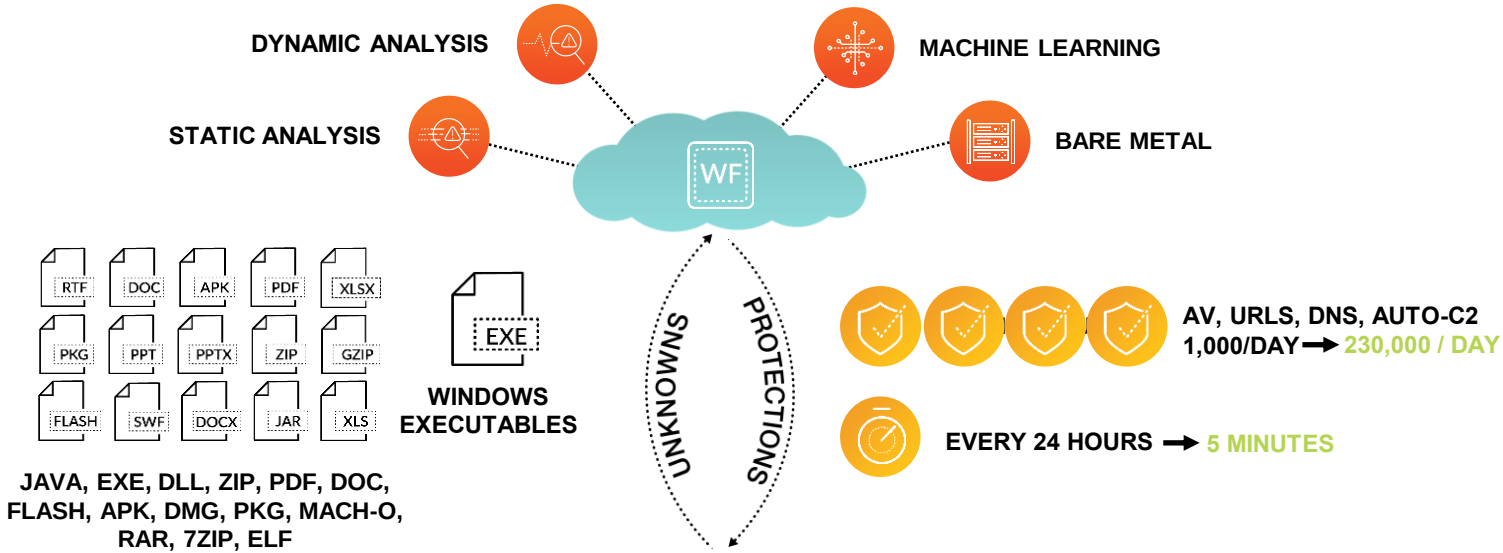
Dynamic Analysis

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

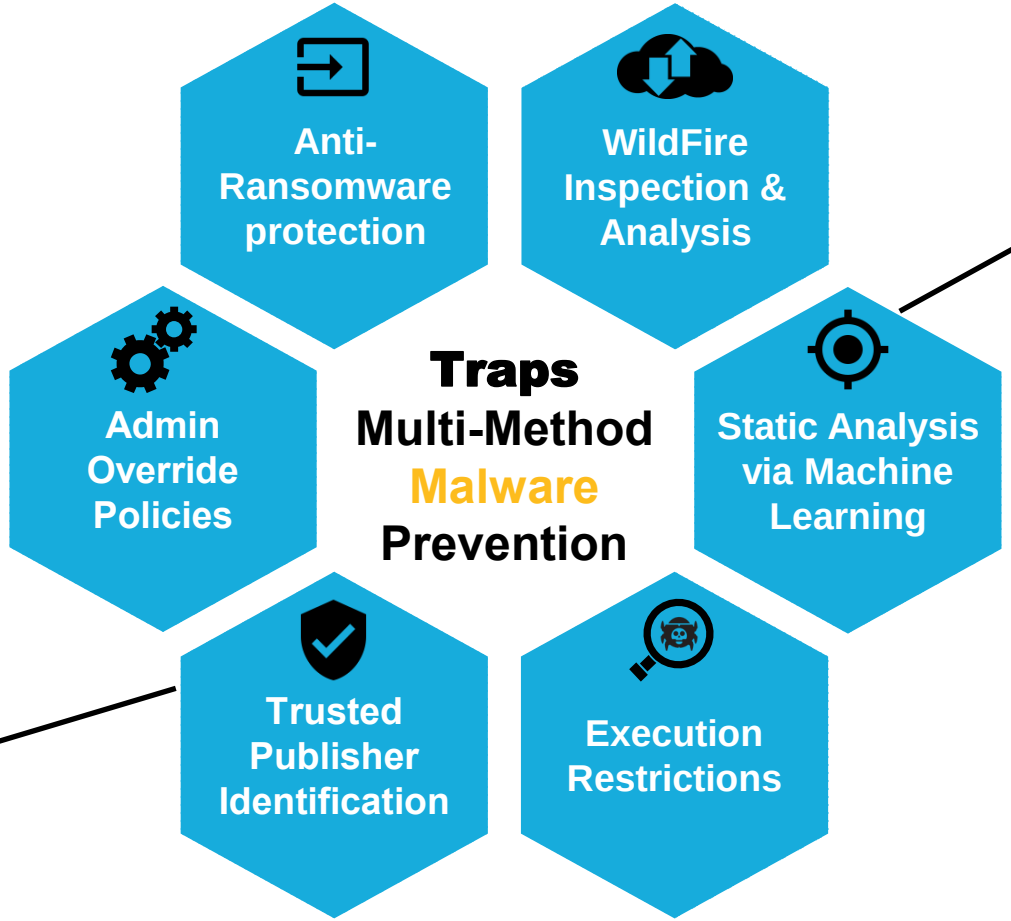
WildFire Turns the *Unknown* into the *Known* in About 5 Minutes

paloalto NETWORKS

COMPREHENSIVE ANALYSIS AND DETECTION VIA WILDFIRE

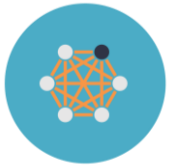


Identifies and Allows New Executable Files that are Digitally Signed by Trusted Software Publishers to Run without Unnecessary Analysis



Static Analysis Prevents Malware Variants that Have Never Been Seen Before

Anti-Ransomware Protection



Behavior based prevention module

Identifies ransomware-like behavior, by identifying applications that access and modify user and OS files on the endpoint

Provides an **additional layer** of prevention

An independent layer, that examines different properties of the application than what is currently examined

Doesn’t rely on signatures or known samples

Only relies on the fact that the ransomware will try to encrypt files!

Traps Multi-Method Malware Prevention

Threat Intelligence

Local Analysis

Enhanced in 4.1

Dynamic Analysis

Enhanced in 4.1

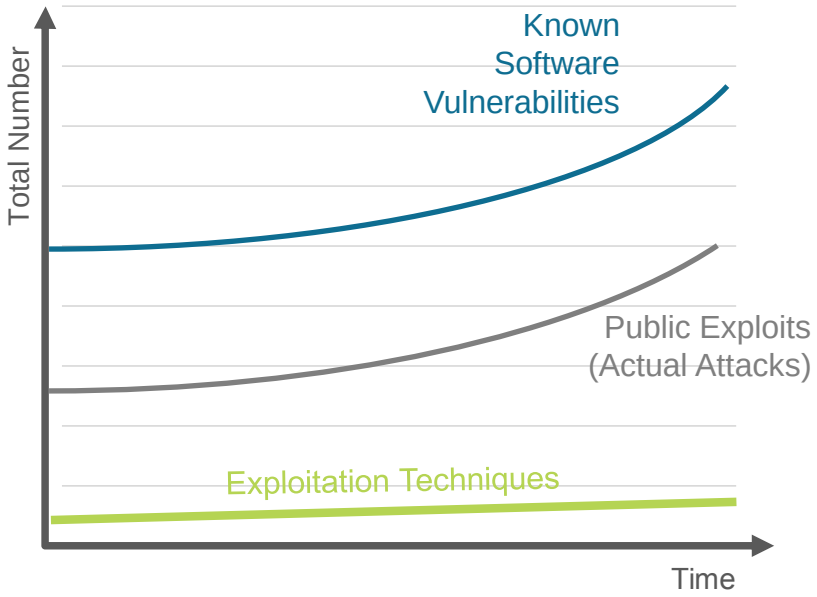
Malicious Process Prevention

Enhanced in 4.1

Ransomware Protection

New in 4.1

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

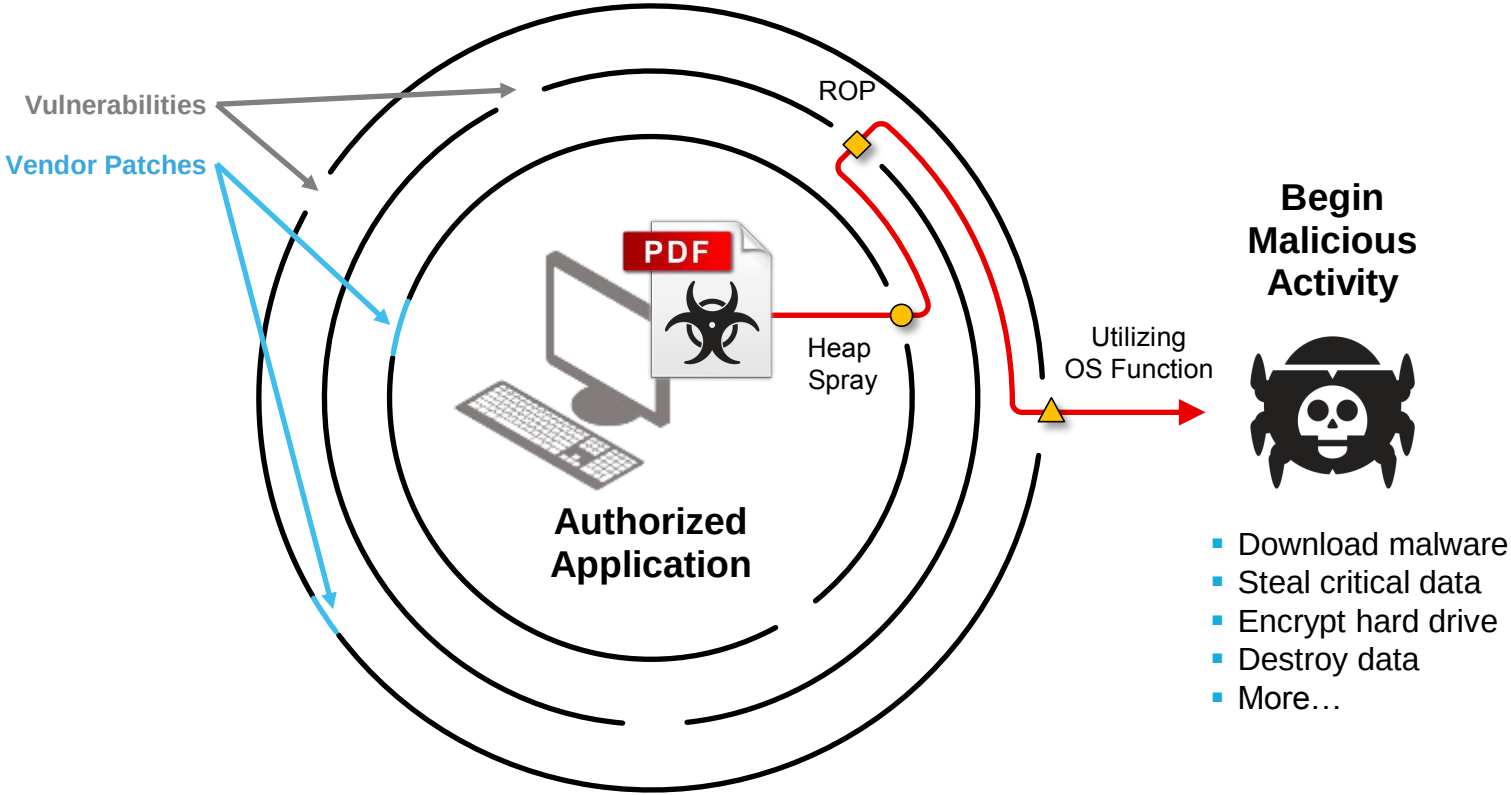
Traps Multi-Method Exploit Prevention

Memory Corruption Prevention

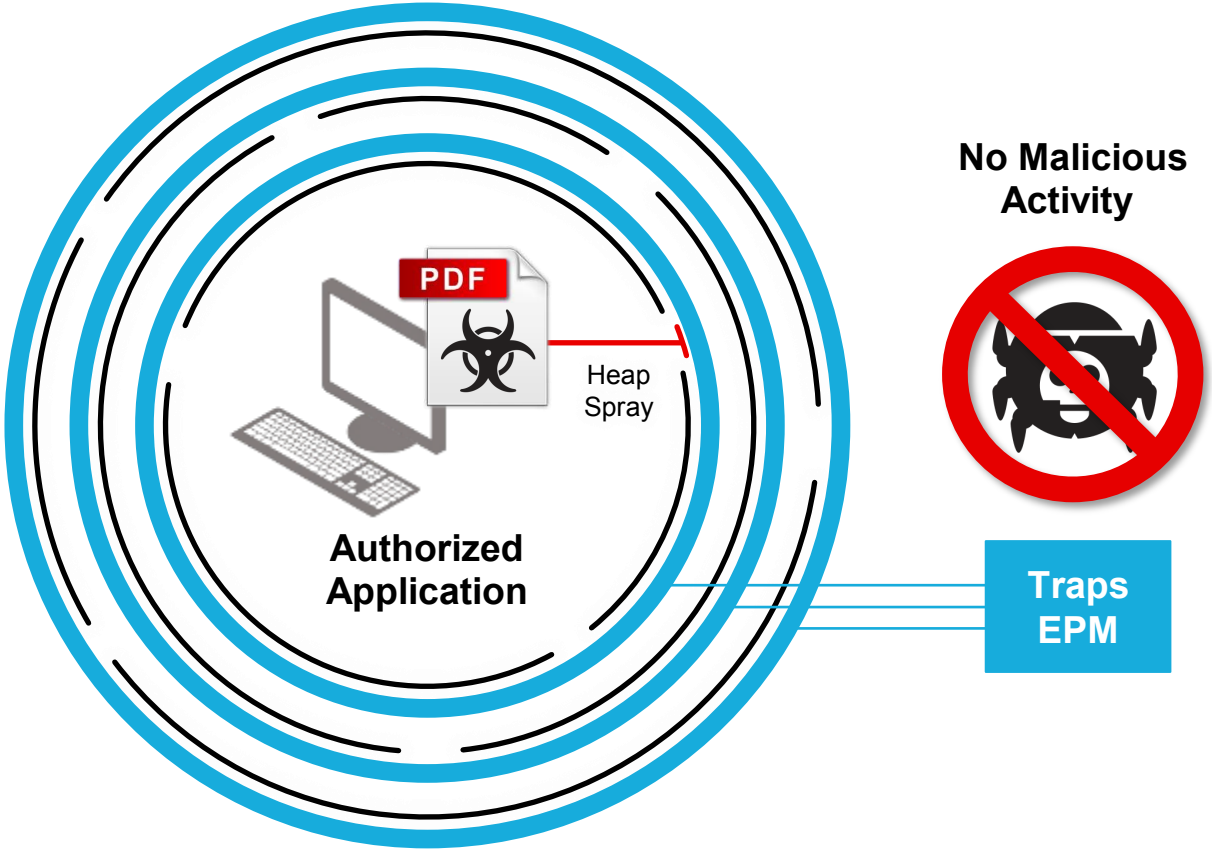
Logic Flaw Prevention

Malicious Code Execution Prevention

Exploits Subvert Authorized Applications

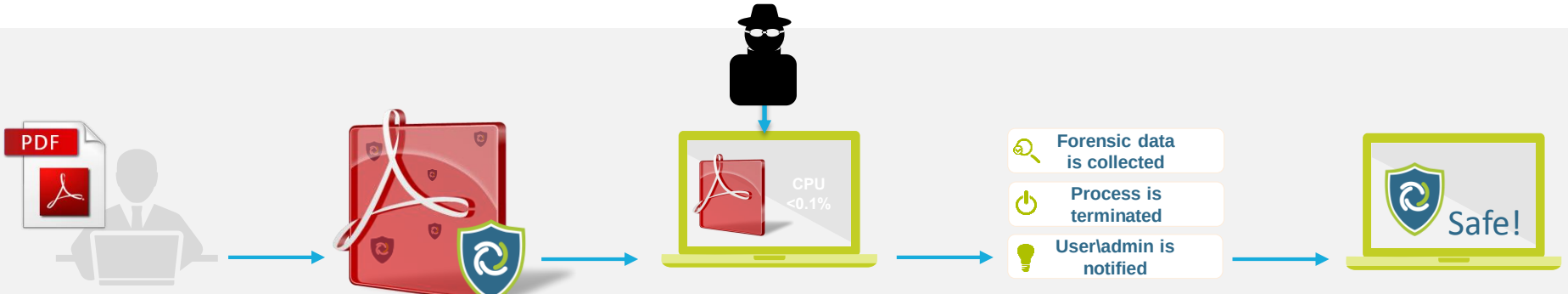


Traps Blocks Exploit Techniques



Exploit technique prevention

In case of exploitation attempt, the exploit hits a "trap" and fails before any malicious activity initiation



A document is opened by user

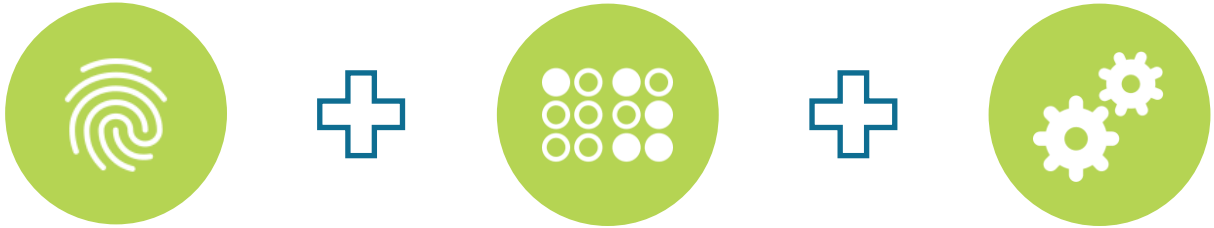
Traps engines seamlessly inject traps to the software that opens the file

Process is protected. Traps perform NO scanning and NO monitoring

Traps triggers immediate actions

Attack is blocked before any malicious activity initiation

Traps Multi-Method Exploit Prevention



Pre-Exploitation Protection

Automatic Prevention of Vulnerability Profiling Used by Exploit Kits

Technique-Based Exploitation Prevention

Blocking of Exploitation Techniques Attackers Use to Manipulate Good Applications

Kernel Exploit Protection

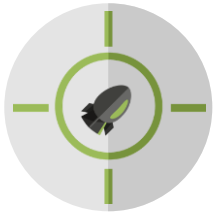
Protection Against the Exploitation of the Operating System Kernel

Enhanced in 4.1

Kernel APC Protection

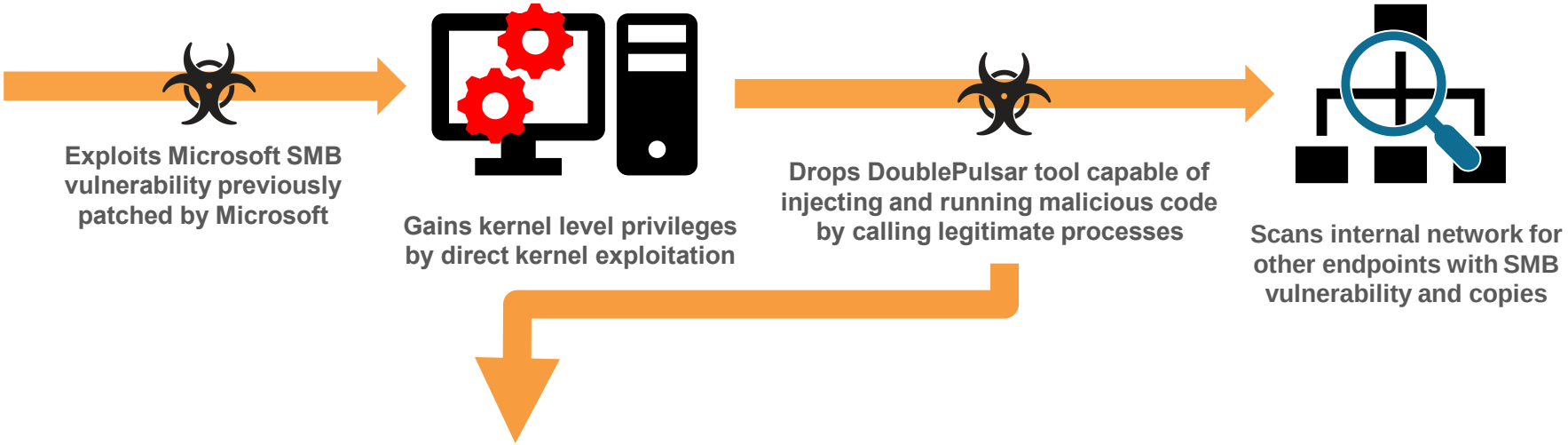
With this technique, the attacker redirects a legitimate process call to a **malicious injected shellcode**

The new module protects against this technique by **preventing it from accessing the shellcode**

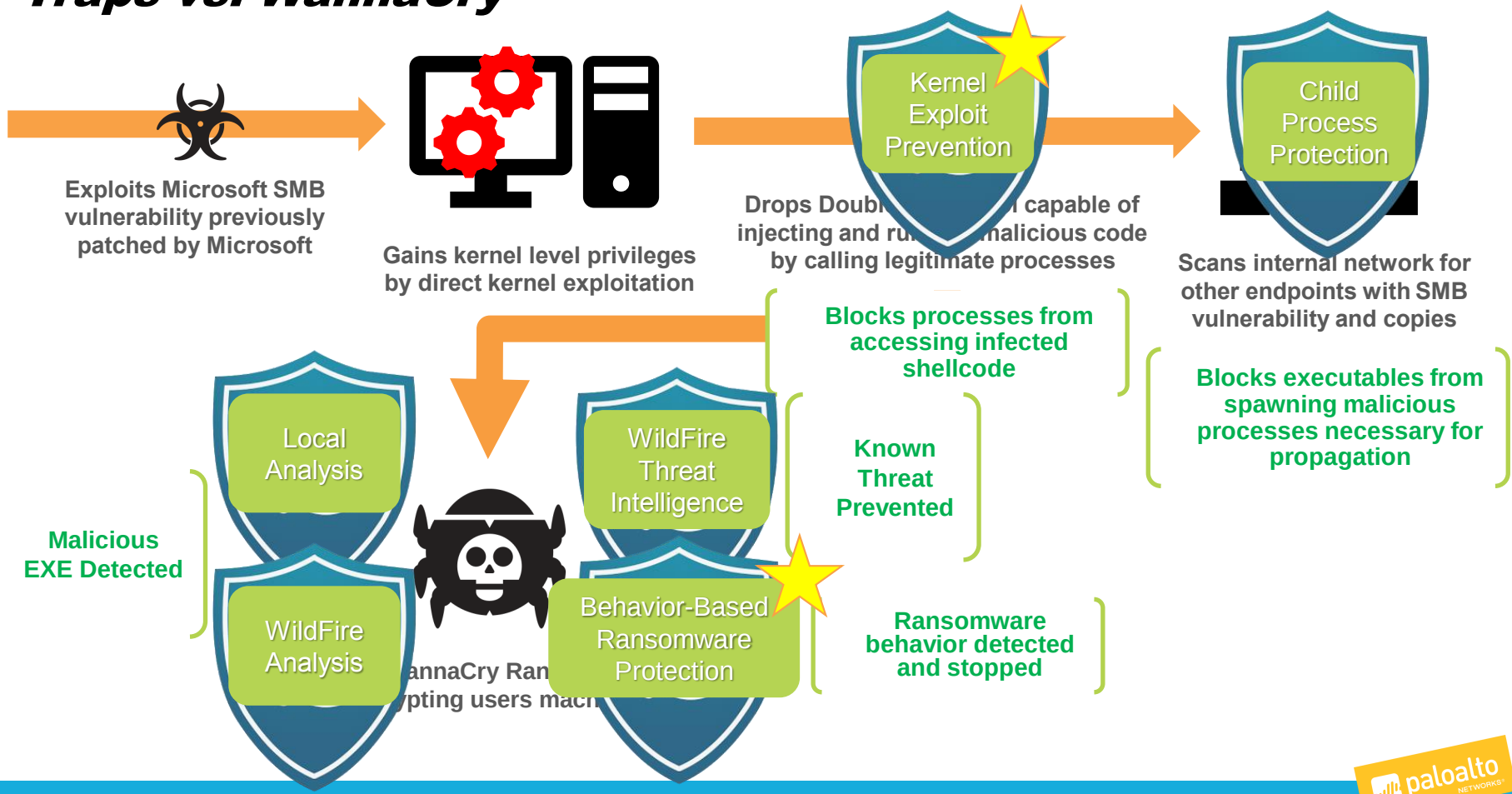


Prevents the exploitation phase of advanced attacks, like **WannaCry** and **Petya\NotPetya**

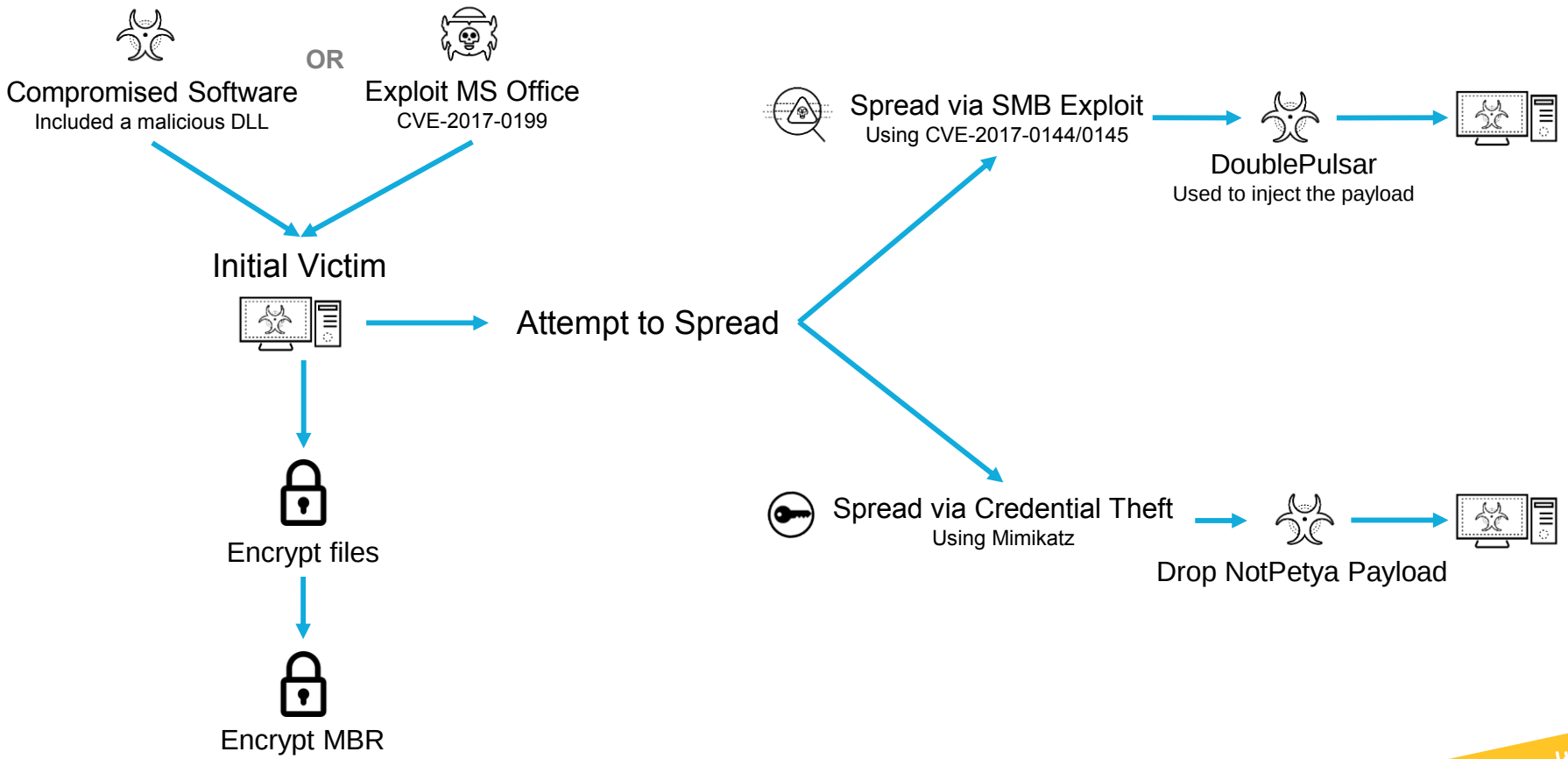
Traps vs. WannaCry



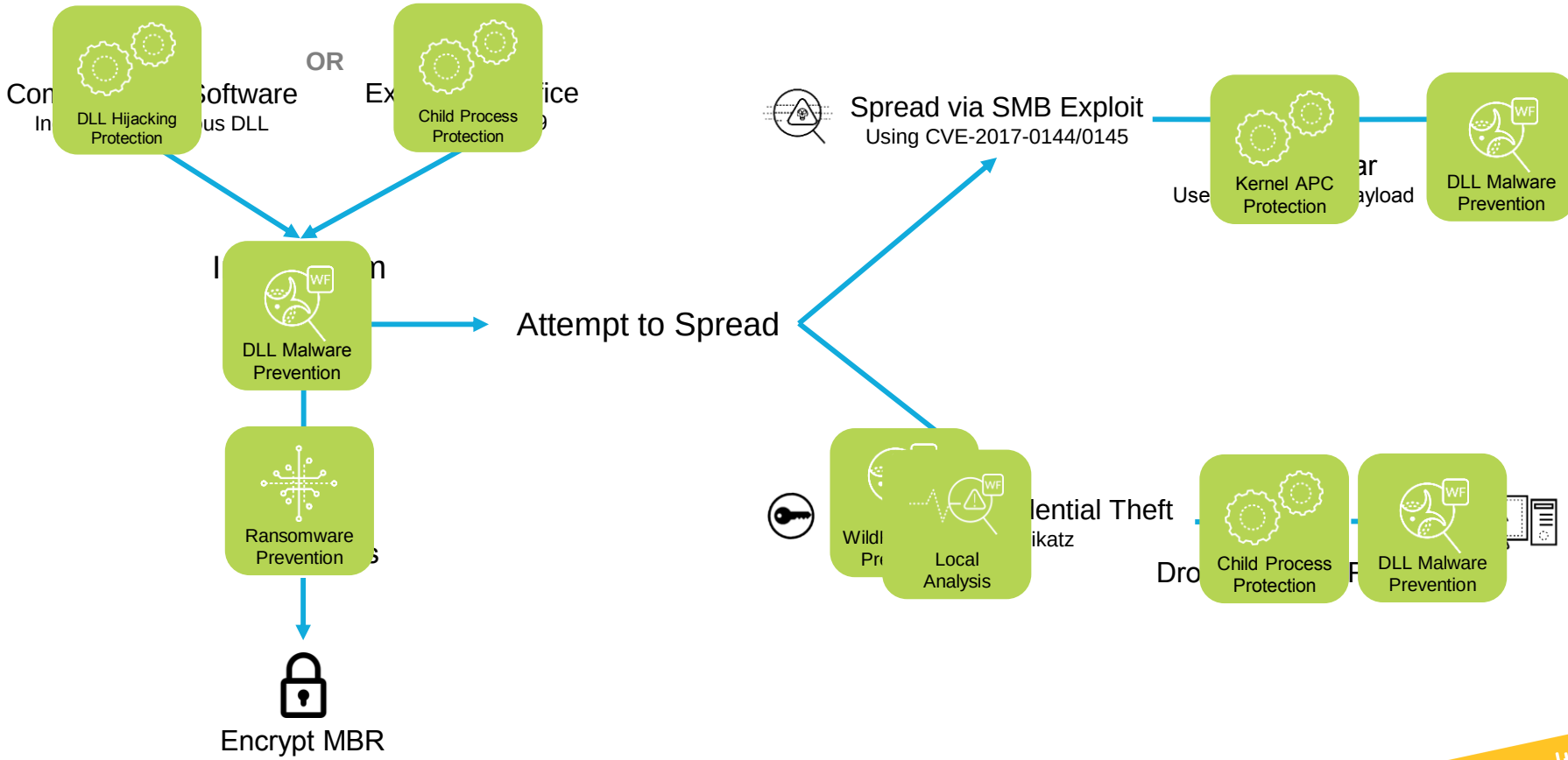
Traps vs. WannaCry



NotPetya attack flow



Prevention opportunities with traps



Traps Delivers Flexible Platform Coverage

Workstations

- Windows XP* (32-bit, SP3 or later)
- Windows Vista (32-bit, 64-bit, SP1 or later; FIPS mode)
- Windows 7 (32-bit, 64-bit, RTM and SP1; FIPS mode; all editions except Home)
- Windows Embedded 7 (Standard and POSReady)
- Windows 8* (32-bit, 64-bit)
- Windows 8.1 (32-bit, 64-bit; FIPS mode)
- Windows Embedded 8.1 Pro
- Windows 10 Pro (32-bit and 64-bit, CB and CBB)
- Windows 10 Enterprise LTSB
- OS X 10.10 (Yosemite)
- OS X 10.11 (El Capitan)
- macOS 10.12 (Sierra)
- macOS 10.13 (High Sierra)

Servers

- Windows Server 2003* (32-bit, SP2 or later)
- Windows Server 2003 R2 (32-bit, SP2 or later)
- Windows Server 2008 (32-bit, 64-bit; FIPS mode)
- Windows Server 2008 R2 (32-bit, 64-bit; FIPS mode)
- Windows Server 2012 (all editions; FIPS mode)
- Windows Server 2012 R2 (all editions; FIPS mode)
- Windows Server 2016 (Standard edition)

Virtual Environments

- VMware ESX, Horizon View
- Citrix XenServer, XenDesktop, XenApp
- Oracle Virtualbox
- Microsoft Hyper-V

* Microsoft no longer supports this operating system.

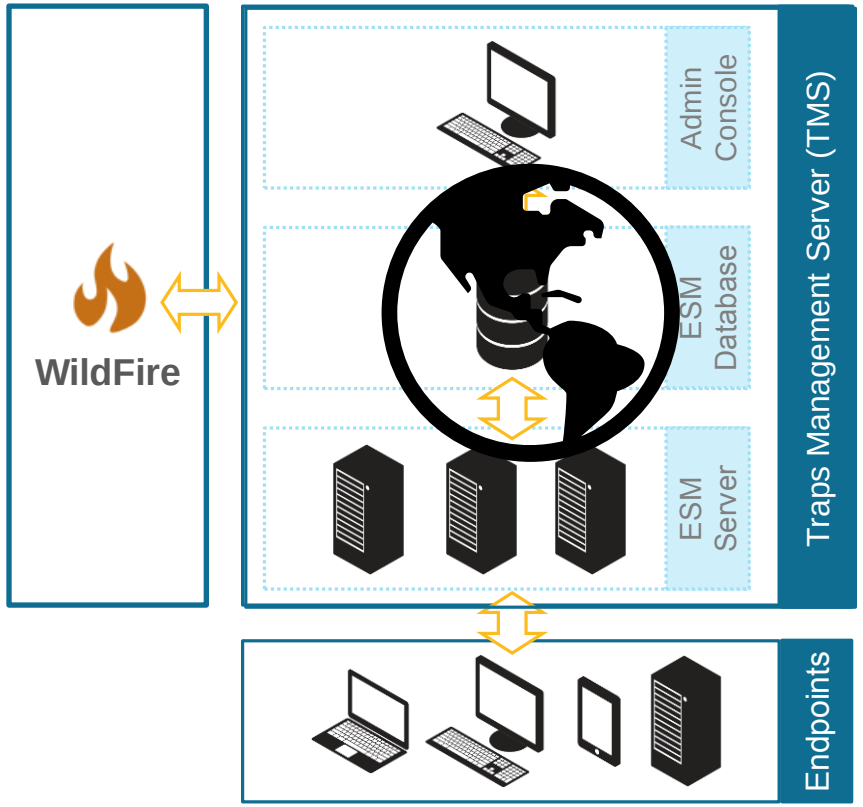
Flexible and Scalable, With Minimal Footprint

Flexible

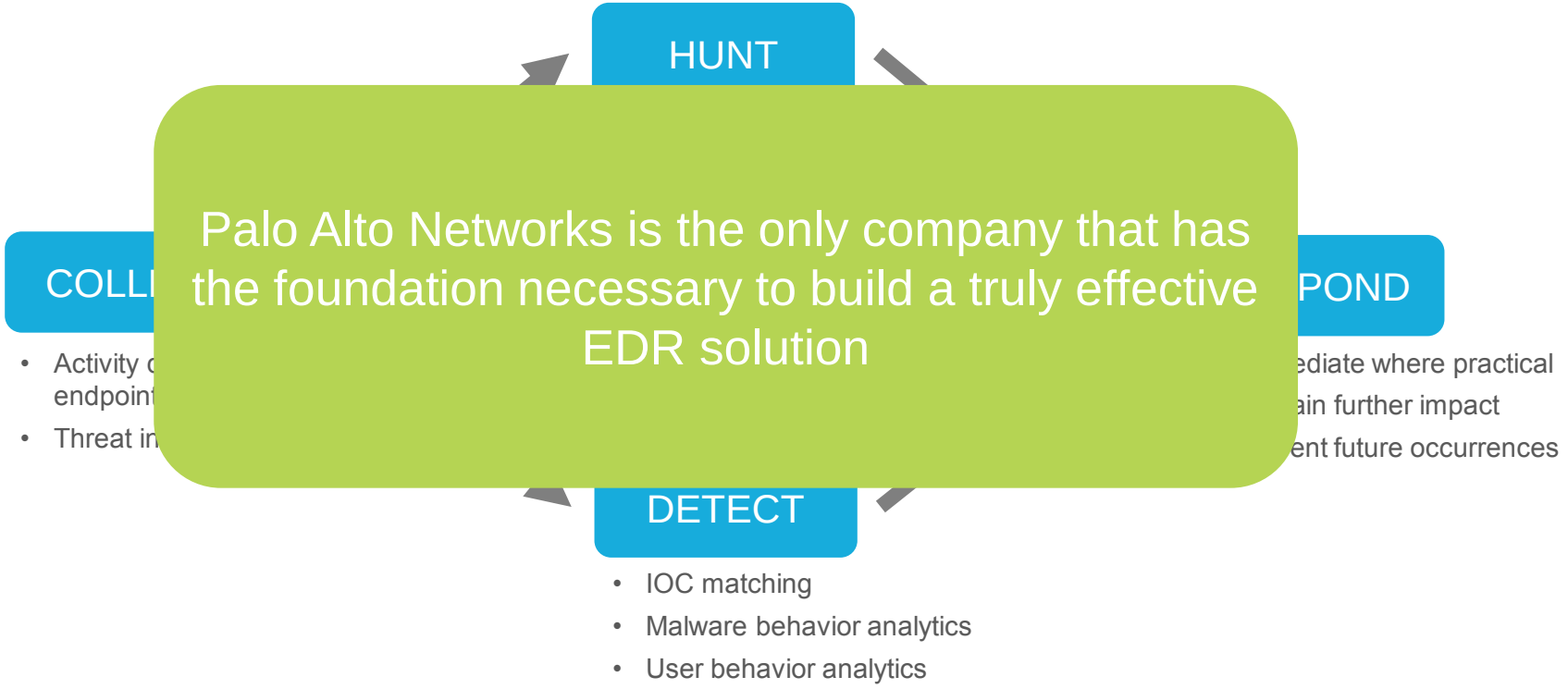
- Supports physical & virtual systems
- Supports Windows & Mac (Linux)

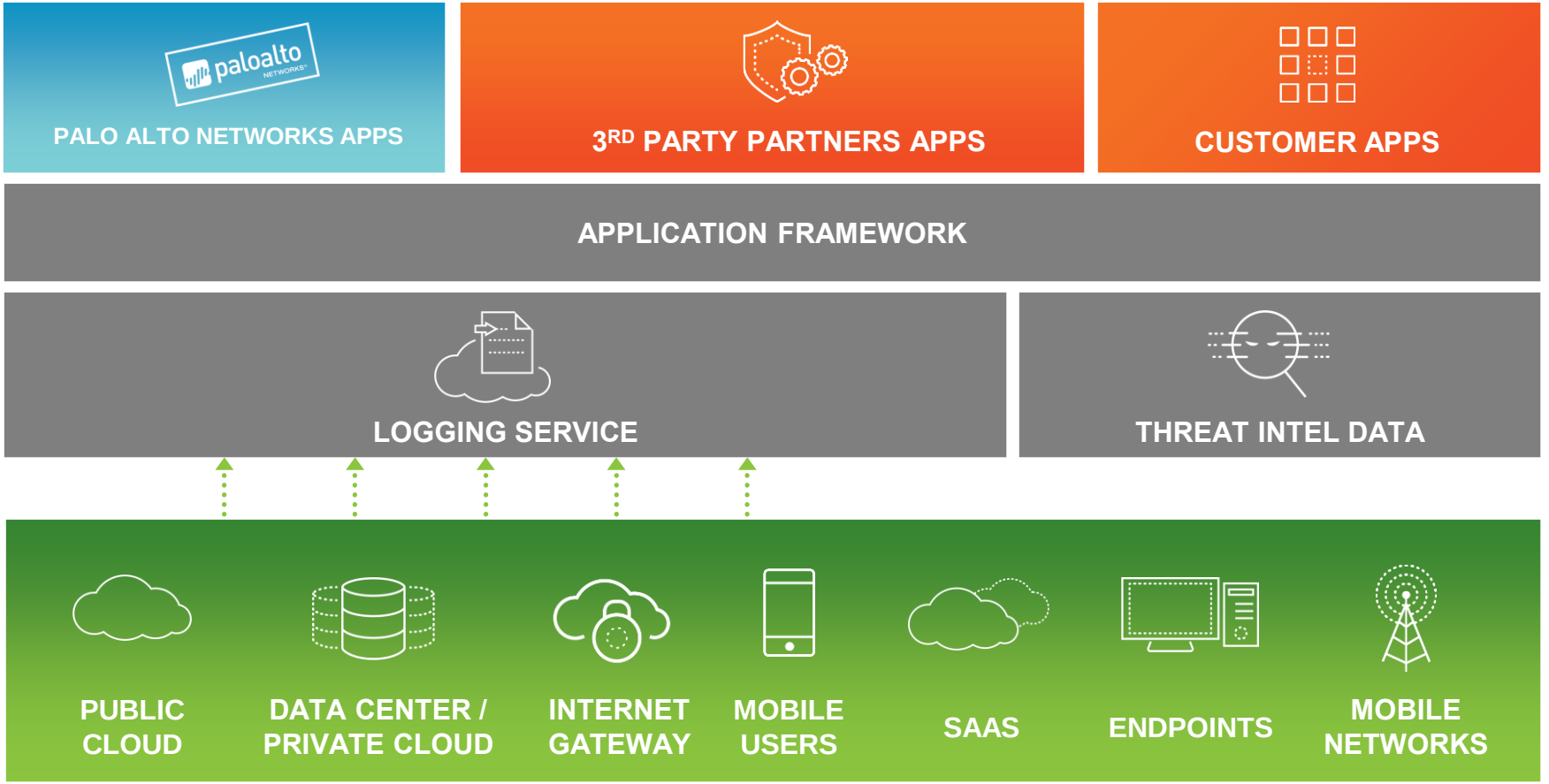
Minimal Footprint

- 0.1% CPU Load
- 50 MB RAM
- 200 MB HD
- No scanning
- No virus-signature databases



Essential components of effective EDR




PALO ALTO NETWORKS APPS
3RD PARTY PARTNERS APPS
CUSTOMER APPS
APPLICATION FRAMEWORK
LOGGING SERVICE
THREAT INTEL DATA
PUBLIC CLOUD
DATA CENTER / PRIVATE CLOUD
INTERNET GATEWAY
MOBILE USERS
SAAS
ENDPOINTS
MOBILE NETWORKS

MAGNIFIER (LIGHTCYBER)

MINEMELD

APPLICATION FRAMEWORK

LOGGING SERVICE

Collecting detailed network activity from firewalls and endpoint activity from Pathfinder

THREAT INTEL DATA

PUBLIC CLOUD

DATA CENTER / PRIVATE CLOUD

INTERNET GATEWAY

MOBILE USERS

SAAS

ENDPOINTS

MOBILE NETWORKS

TRAPS MANAGEMENT SERVICE (HOGWARTS)

MAGNIFIER (LIGHTCYBER)

MINEMELD

APPLICATION FRAMEWORK

LOGGING SERVICE

Addition of endpoint activity from Traps and cloud activity from Aperture

THREAT INTEL DATA

PUBLIC CLOUD

DATA CENTER / PRIVATE CLOUD

INTERNET GATEWAY

MOBILE USERS

SAAS

ENDPOINTS

MOBILE NETWORKS

Q&A

Next-Gen Security Platform Converts Intelligence into Prevention, Automatically!