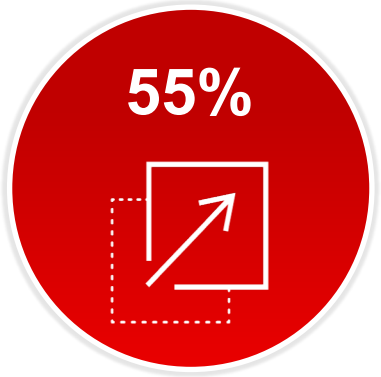
Giving your endpoints the protection they deserve.

Eirik Valderhaug

Systems Engineer Specialist - CSS – Nordics, Baltics & Eastern Europe

paloalto NETWORKS®

THREAT LANDSCAPE CONTINUES TO EVOLVE



Volume of Attacks

Increase in
new malware

Severity of Attacks

35% increase in
fileless attacks

More Sophisticated

Targeted and
multi-vector

ATTACKERS NEED TO CONTROL THE ENDPOINT

Attackers objectives require leveraging the endpoint

Malicious email

Exploit software vulnerabilities

Execute malware

Rapidly changing malware

Targeted malware

Macros, scripts, etc

Diving deeper into exploits

Exploit

Usually requires a software vulnerability
In some cases, the vulnerability is known, while in others – it isn't (a zero day)

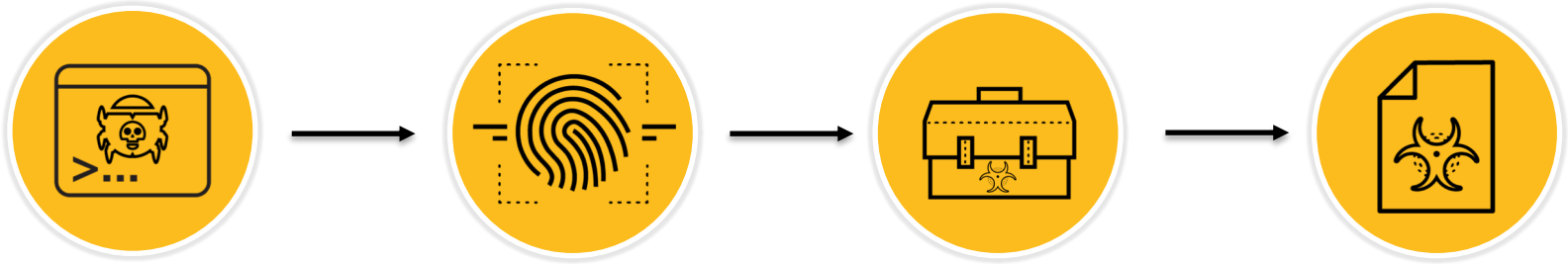
Can be delivered using any input the vulnerable software receives
Web traffic or web pages, PDF documents, SWF files, etc.

To exploit a vulnerability, attackers must follow critical steps
Such as writing code into the memory and getting that code to run

Source: https://www.paloaltonetworks.com/cyberpedia/what-is-an-exploit-kit

What are exploit Kits?

Exploit kits are automated threats that utilize compromised websites to divert web traffic, scan for vulnerable browser-based applications, and run malware.



Landing page
Malicious advertisement or a compromised web server

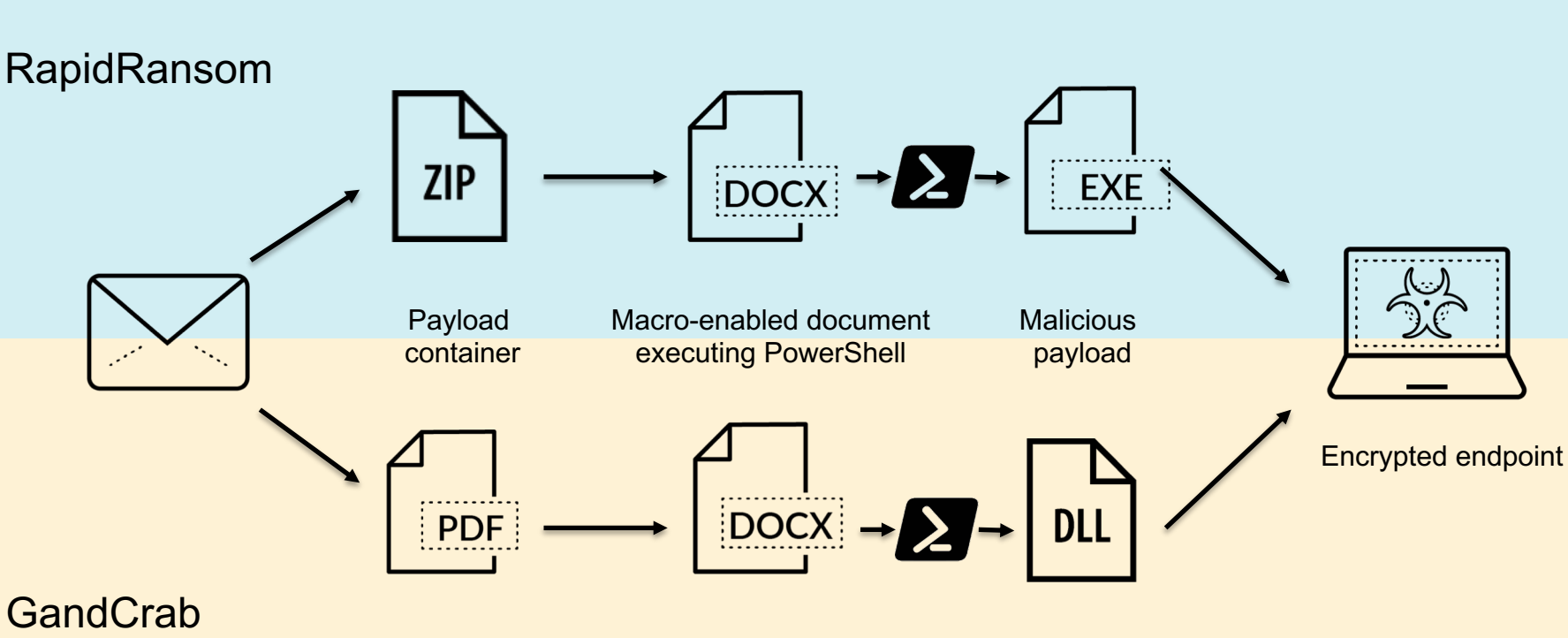
Performs initial fingerprinting

Exploit
A file or crafted web traffic, targeted to attack specific applications or web browsers

Malicious payload

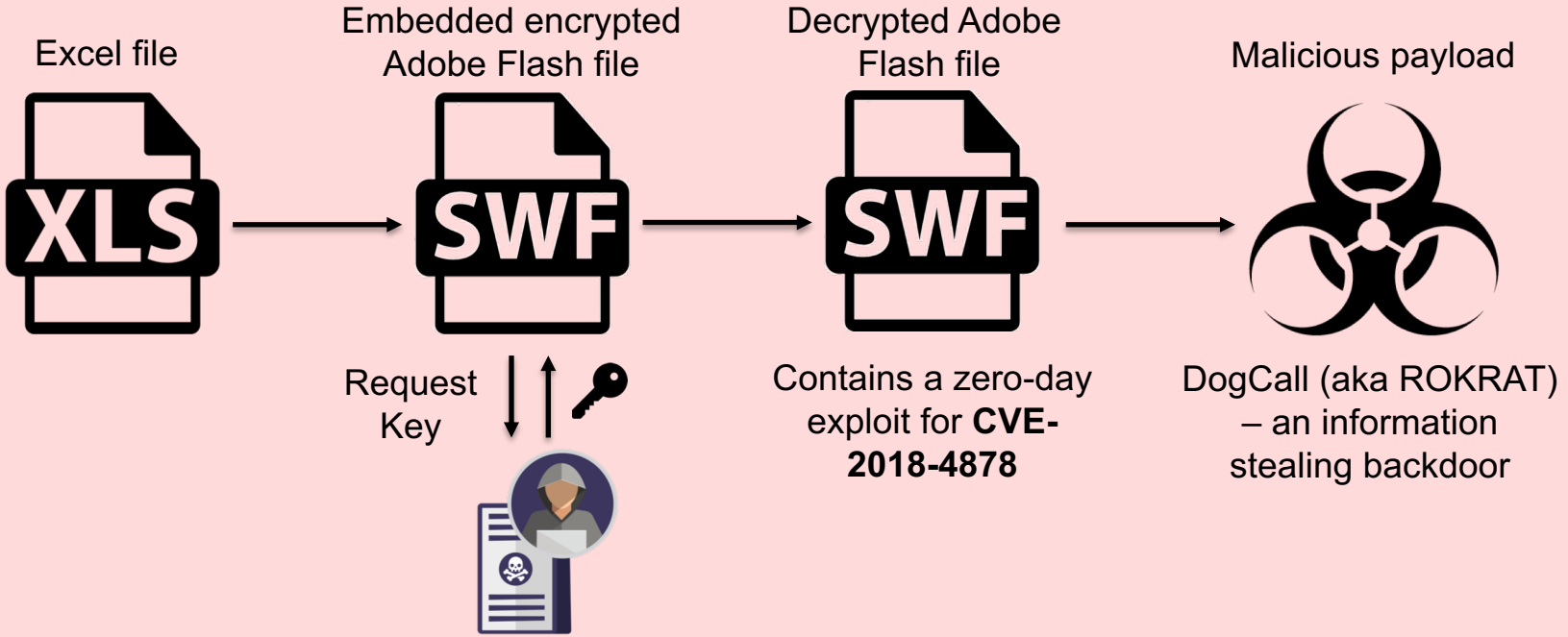
Source: https://www.paloaltonetworks.com/cyberpedia/what-is-an-exploit-kit

DIFFERENT ATTACKS - SIMILAR ATTACK CHAIN



Sources: https://myonlinesecurity.co.uk/please-note-irs-urgent-message-164-malspam-delivers-rapid-ransomware/
https://isc.sans.edu/forums/diary/GandCrab+Ransomware+Now+Coming+From+Malspam/23321/

ZERO-DAY EXPLOIT ATTACK



Source: https://researchcenter.paloaltonetworks.com/2018/02/unit42-traps-prevents-adobe-flash-player-zero-day/

INSUFFICIENT ENDPOINT OPTIONS

Traditional EPP

Cumbersome & Insufficient

Next-Gen AV

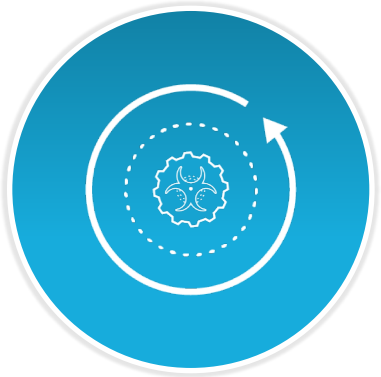
Inconsistent Prevention

EDR

Detection overwhelming without great prevention

REQUIREMENTS FOR A NEW APPROACH…

Accurate Prevention:
Known *and* Unknown
Threats



Protection Across
Attack Techniques

Rapid Detection
and Response to
Sophisticated Attacks

Across all platforms and environments

A PREVENTION FIRST APPROACH THAT LETS YOU…

Block Malware and Ransomware

Block Exploits and Fileless Threats

Stop Sophisticated Attacks

Traps 5.0

WHAT'S NEW IN TRAPS 5.0

Cloud Delivered Service

Management as a cloud service, connected to Application Framework

Reimagined Interface

Complete UI overhaul, logical groupings, simplified workflows, focus on event management

Platform Expansion

Linux support and protection; relevant in data center and cloud workloads

TRAPS MANAGEMENT SERVICE

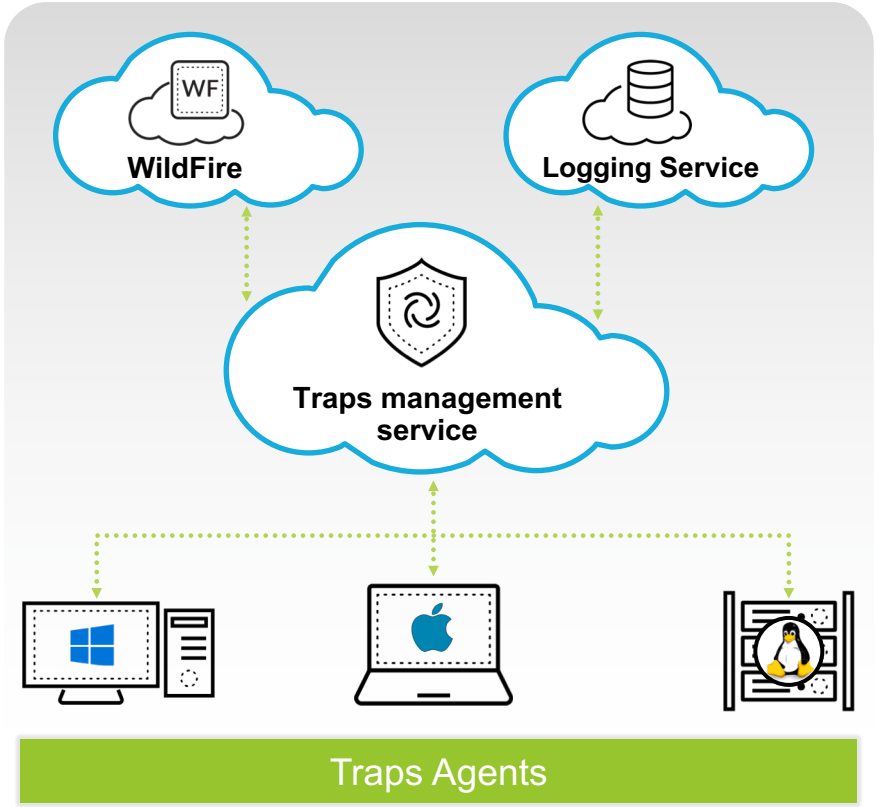
Cloud-delivered Service

- Moves Traps management into the cloud
- Eliminates operational overhead of on-prem server(s)
- New interface for more intuitive experience

Application Framework Integration

- Detailed event information stored in Logging Service
- Enables correlation of endpoint, network, and cloud
- Allows for easy adoption of new capabilities (e.g. Magnifier)

NOTE: ESM still available for customers who are unable to take advantage of the cloud



REIMAGINED USER EXPERIENCE

Intuitive Web-based Interface

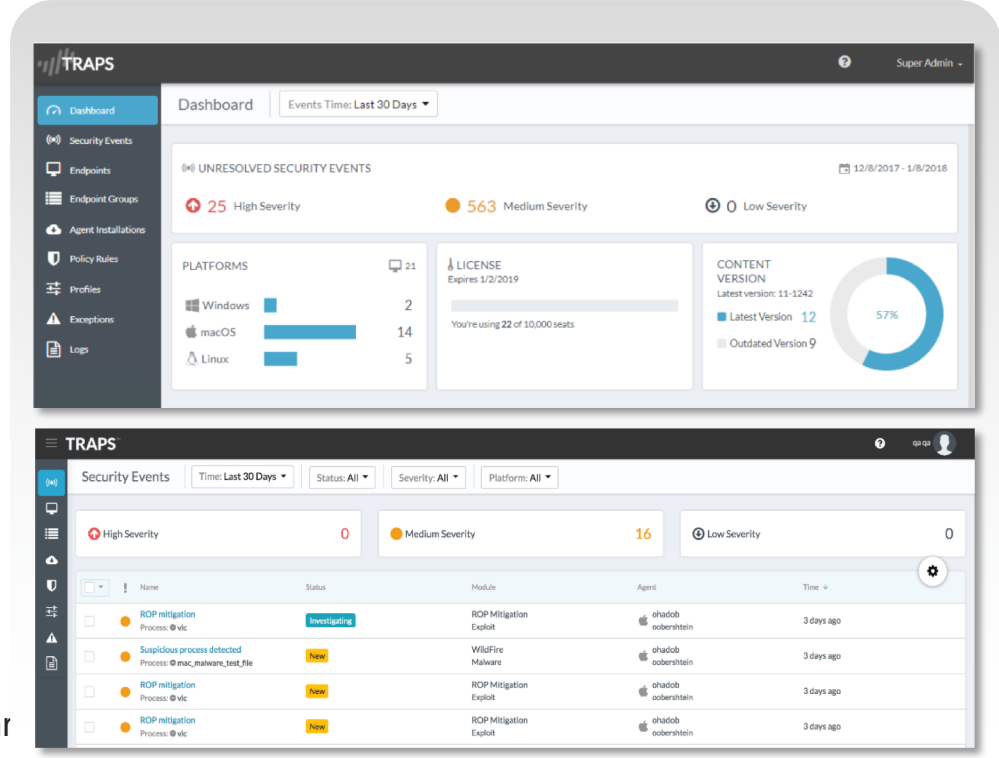
- Minimizes operational challenges
- Consistent policy management
- Dynamic endpoint grouping

Simplified Event Management

- At-a-glance events dashboard
- Threat assessment for faster triage
- Event investigation status tracking

Integrated WildFire Threat Reports

- Quick drill-down into threats
- Display information about:
  - Targeted users
  - Application that delivered threat
  - URLs involved in the delivery of thr
- Observed behavior of the threat



ALL MAJOR OS PLATFORMS SUPPORTED

Introducing LINUX Support

- Out of the box protection for common services
- Provides exploit protection tailored for Linux-based servers
- Immediate protection – does not require restart upon installation

Protection for Data Center & Cloud

- Lightweight Agent and best security for Linux
- Real-time exploit protection
- Protects unpatched workloads

Supported Distributions

- RedHat (RHEL) – 6.x and 7.x
- CentOS – 6.x and 7.x
- Ubuntu Server – 12.x, 14.x, 16.x
- SUSE – 12.1, 12.2

PROACTIVE THREAT SCANNING

Scanning Endpoints for Malware

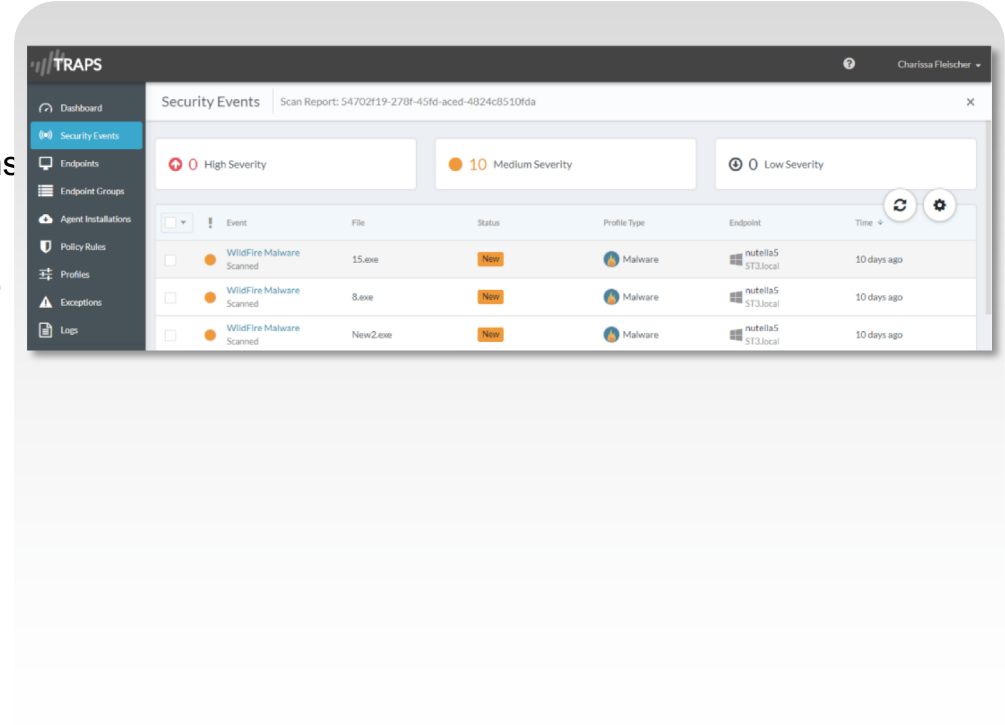
- Identifies dormant malware before execution
- On-demand or scheduled file system scans
- WildFire threat intelligence for known files

Helps Incident Response & Compliance

- Run scans after security event
- Satisfies compliance requirements
- Last checkbox for legacy cutover

Leverages Existing Infrastructure

- Analyzes files not seen in previous scans
- Analyzes unknown files prior to execution
- Scans in background to maintain low footprint



NOTE: Supported on Windows operating systems

MINIMIZE ENDPOINT INFECTIONS

Block Malware and Ransomware

Block Exploits and Fileless Threats

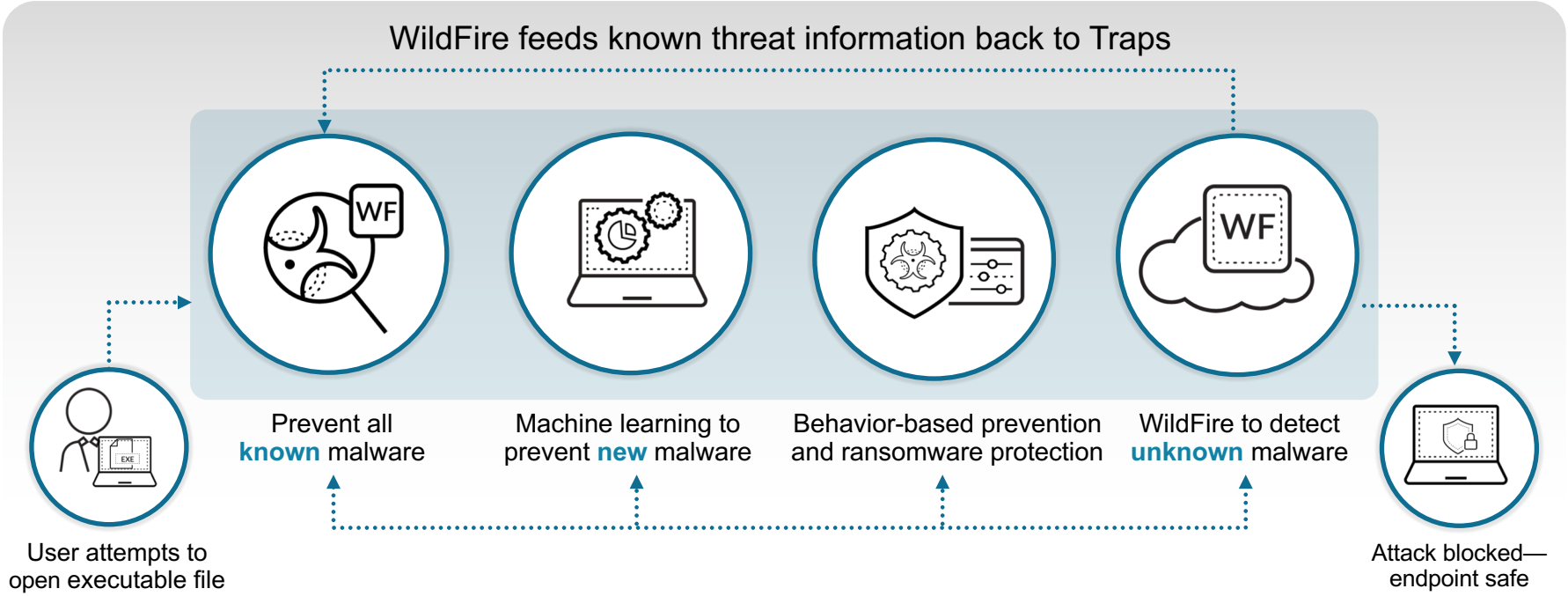
Stop Sophisticated Attacks

Block known malware using WildFire threat intelligence

Block unknown malware with local *machine learning* and *behavior-based* analysis

Analyze unknown files with industry leading WildFire cloud service

PREVENT KNOWN AND UNKNOWN MALWARE



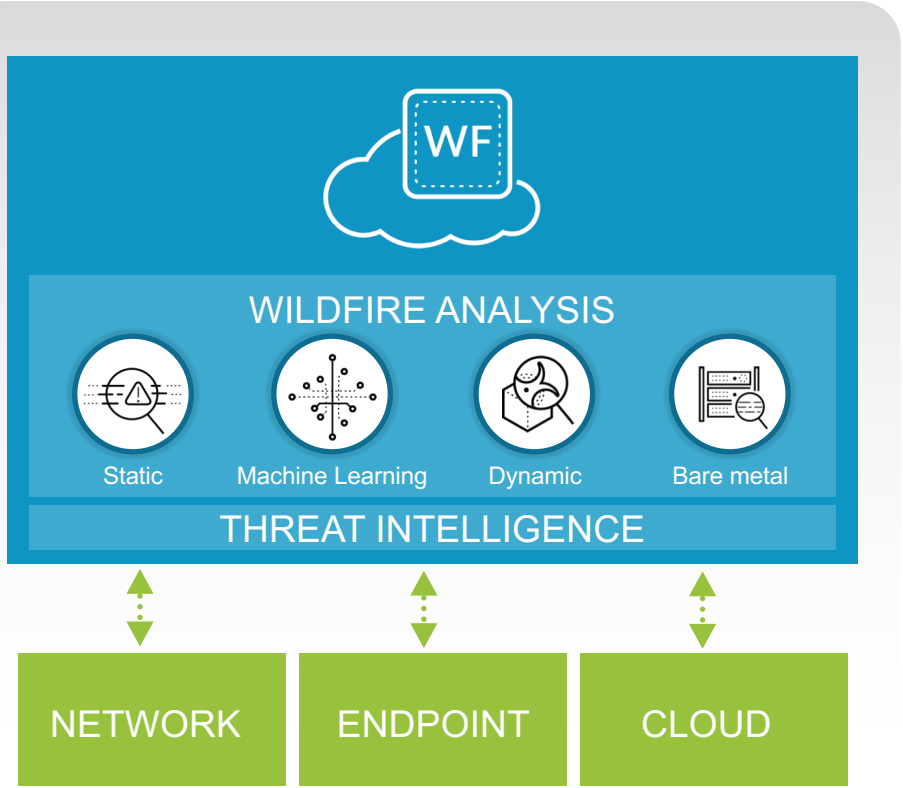
Multiple methods of prevention improve accuracy and coverage

WILDFIRE INCREASES TRAPS ACCURACY AND COVERAGE

300M New malware samples detected by WildFire monthly

45% Malware detected by WildFire is never seen by Virus Total

Threat intelligence shared across endpoint, network, cloud & cyber threat alliance

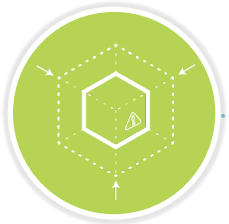


MINIMIZE ENDPOINT INFECTIONS

Block Malware and Ransomware

Block Exploits and Fileless Threats

Stop Sophisticated Attacks

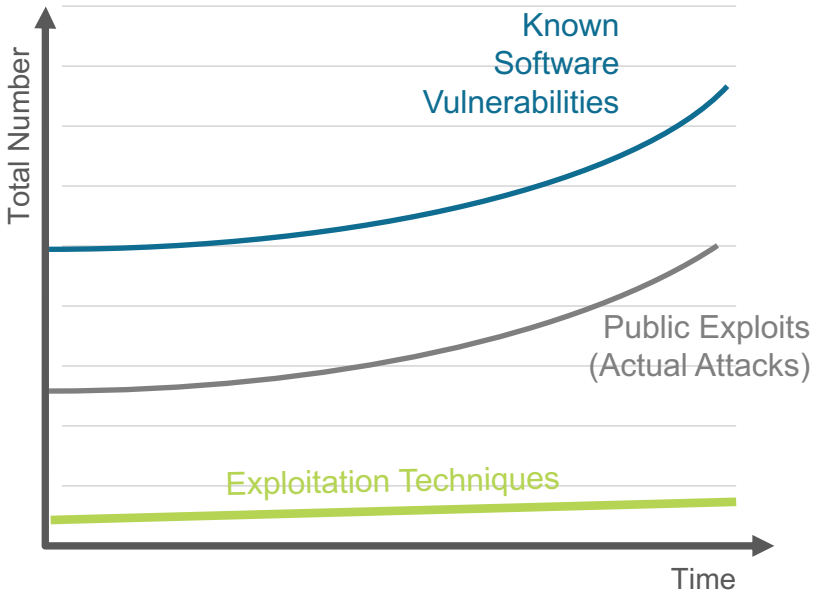


Reduce opportunities for attack on endpoint with policy and restrictions

Prevent exploits by technique, not the exploits

Block in-memory fileless threats that don't write to disk

Blocking Exploitation Techniques Is the Most Effective Approach

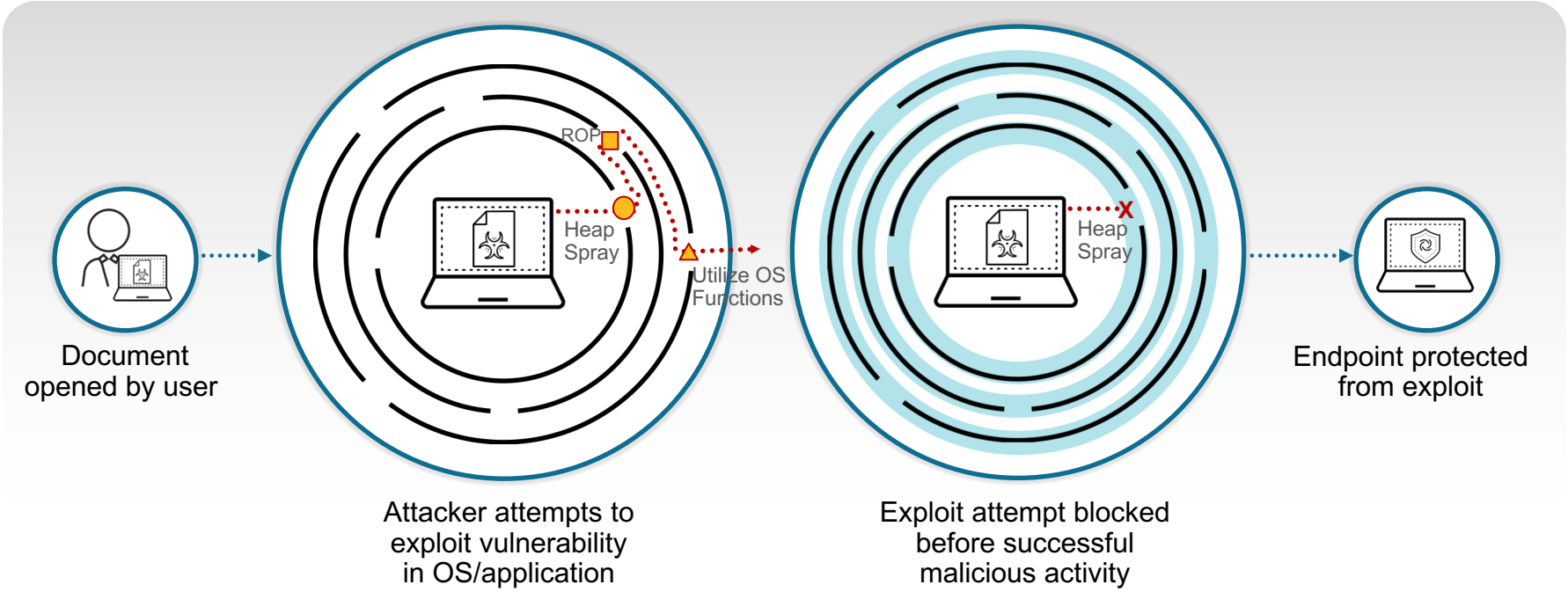


Patching — Requires Prior Knowledge, Proactive Application

Signature / Behavior — Requires Prior Knowledge of Weaponized Exploits

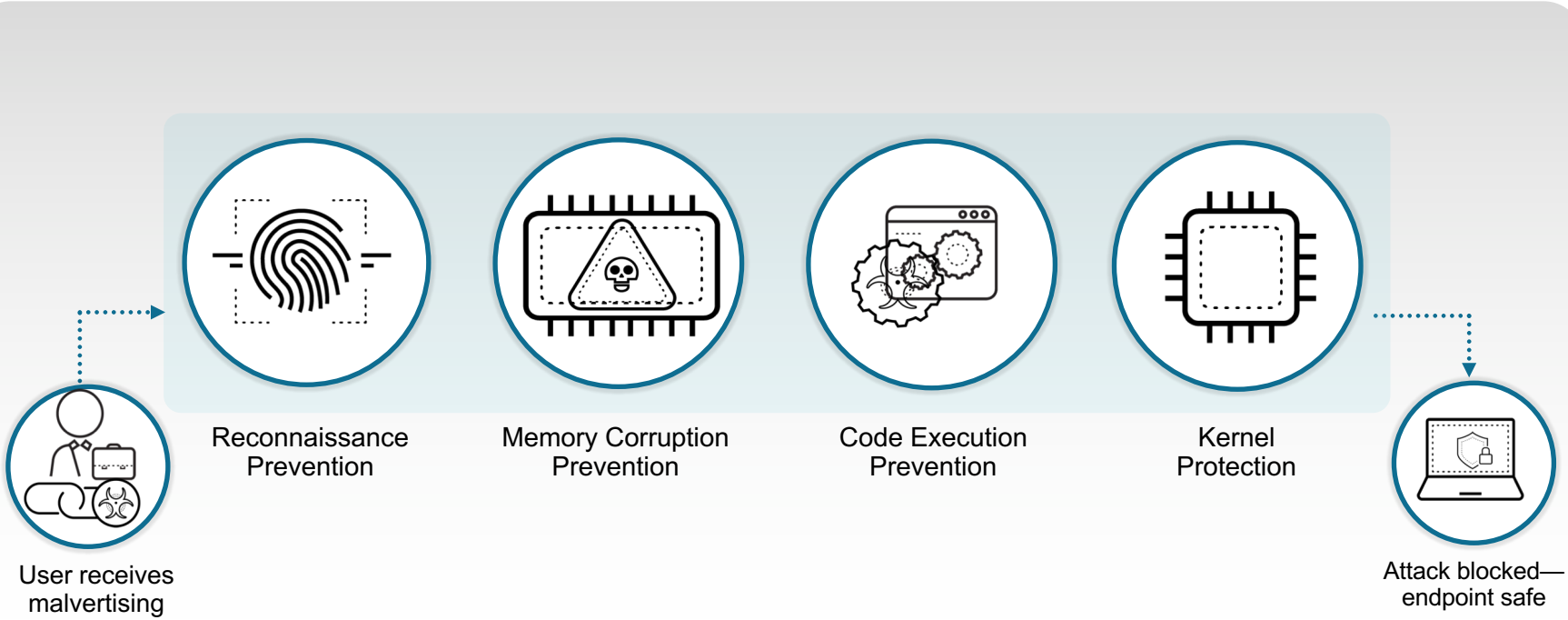
Traps — Requires No Patching, No Prior Knowledge of Vulnerabilities, and No Signatures

EXPLOIT PROTECTION FOCUSES ON TECHNIQUE



Traps focuses on exploit techniques *rather than the exploit itself*

EXPLOIT PREVENTION FOCUSED ON TECHNIQUE



Multiple methods of prevention stop zero day attacks

SIX YEARS OF EXPLOIT PROTECTION INNOVATION

TRAPS ADVANCED ENDPOINT PROTECTION

NEW

2012/13	2014	2015	2016	2017	2018
JAVA	SEH Protection	Hot Patch Protection	Enhanced DLL Security	DLL File Protection	Local Privilege Escalation Protection
DEP	T01 Compatibility	Shellcode & Library Preallocation	Enhanced JIT Protection	Child Process Protection	Brute Force Protection
UASLR	Null Dereference Protection	Null Dereference Protection	JIT Mitigation	Kernel APC Protection	ROP Mitigation (Linux)
Heap Spray Checks	Font Protection	ShellLink Protection	CPL Protection	Gatekeeper Enhancement	
	Heap Spray Mitigation		SysExit	Dylib-Hijacking Protection	
	Heap Corruption Mitigation		GS Cookie	Kernel Privilege Escalation	
	ROP Mitigation			Exploit Kit Fingerprinting	
	DLL Hijacking			Child Process Protection	
	DLL Security				
	Packed DLLs				

EXPLOIT PREVENTION MODULES

SPEED DETECTION AND RESPONSE TO SOPHISTICATED ATTACKS

Block Malware and Ransomware

Block Exploits and Fileless Threats

Stop Sophisticated Attacks

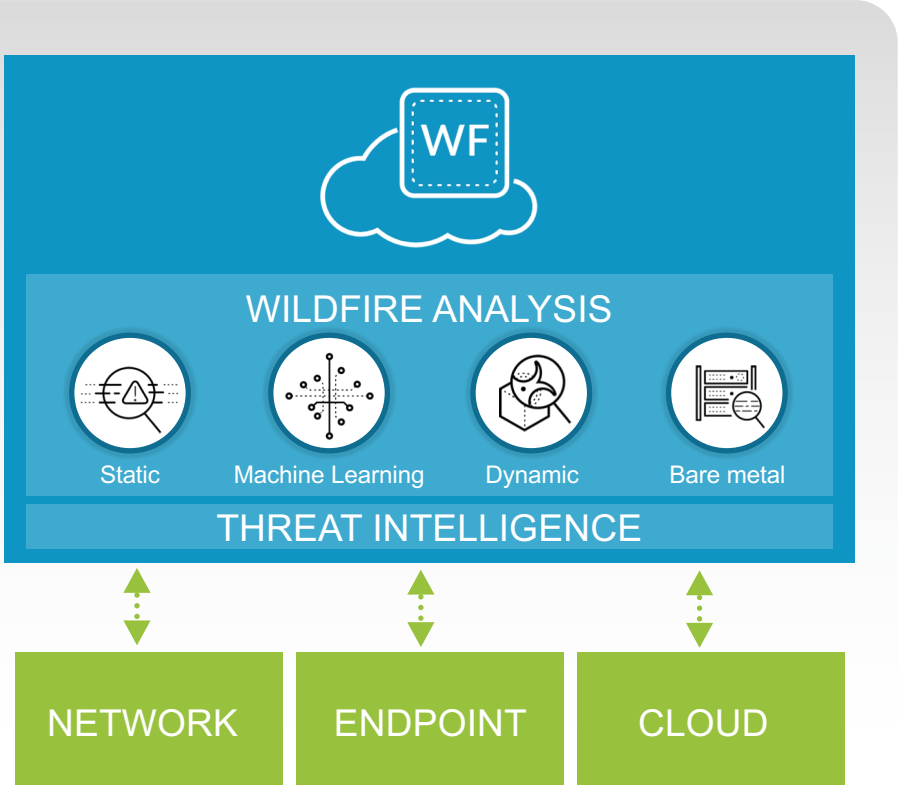
Coordinate enforcement across network, endpoint, and cloud

Accelerate investigation with analytics, context, and classification

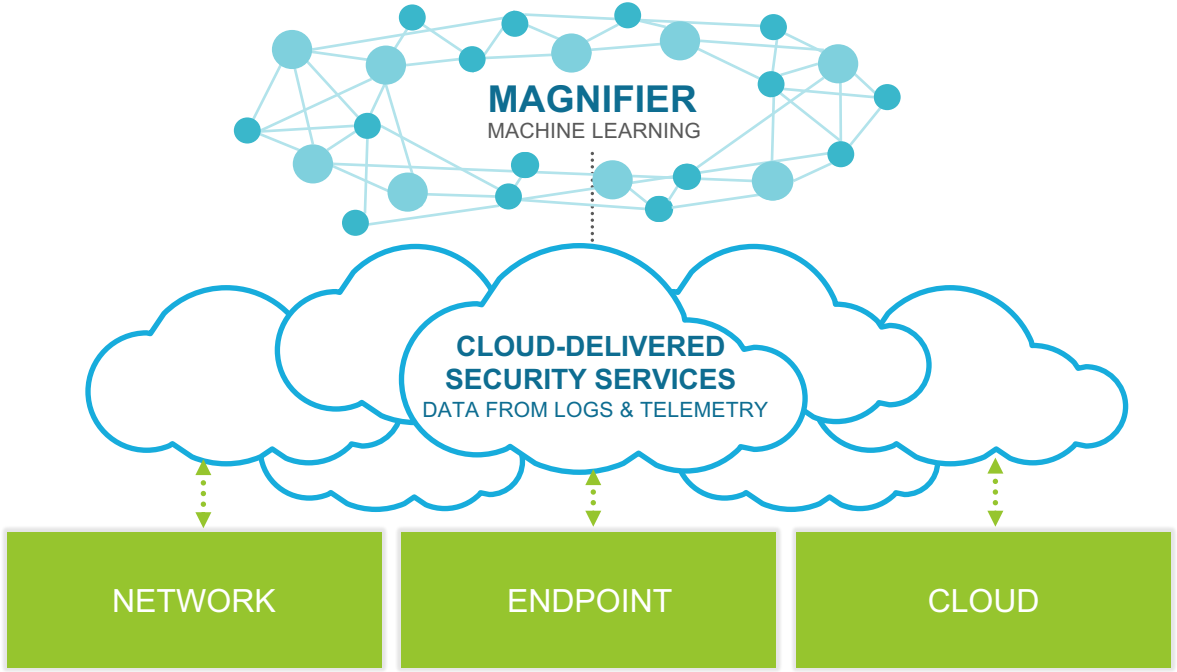
Rapidly consume innovative detection and response capabilities

COORDINATED ENFORCEMENT

1. NGFWs & Traps send unknowns or suspicious files and links to WildFire
2. WildFire analyzes the unknown renders a verdict and shares threat intelligence
3. Automatically reprogram NGFW and endpoints to contain and prevent any new attack



MAGNIFIER BEHAVIORAL ANALYTICS

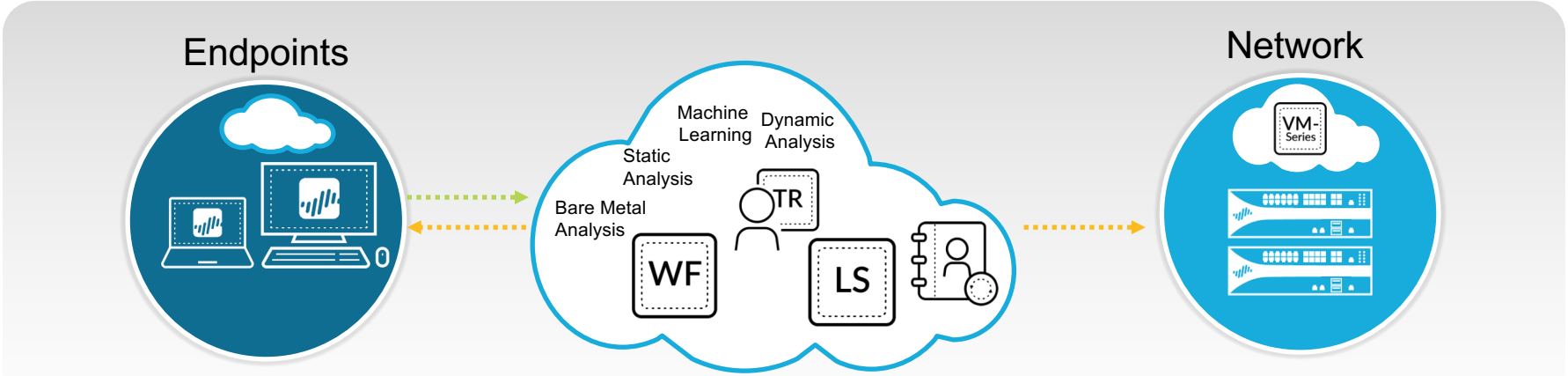


Analyze rich network, endpoint and cloud data with machine learning

Accelerate investigations with endpoint analysis

Gain scalability, agility and ease of deployment as a cloud-delivered app

PREVENTION FIRST WITH TRAPS



1

- Prevention of known and unknown exploits & malware
- Offline & online protection
- Protection for unpatched devices
- Support for cloud & Linux

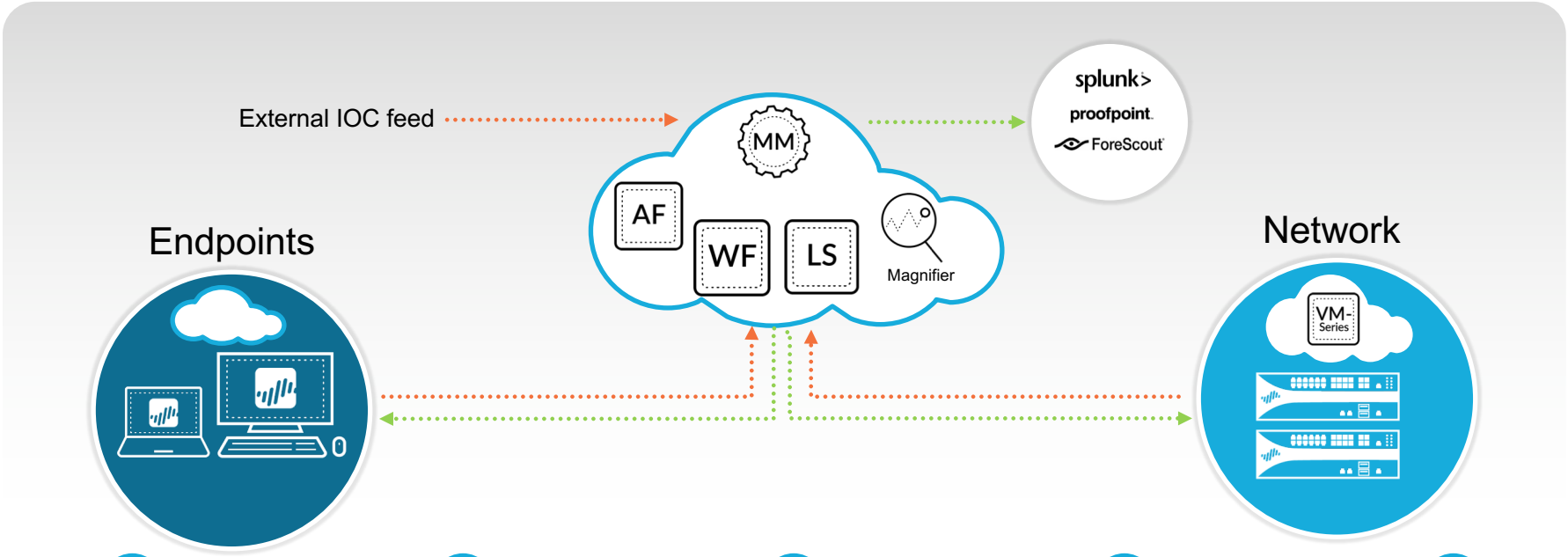
2

- Wildfire analyzes the unknown renders a verdict and shares threat intelligence with NGFW
- Scanning to detect dormant malware

3

- Cloud based or on premise management
- Directory integration to create groups
- Logging service to enrich data

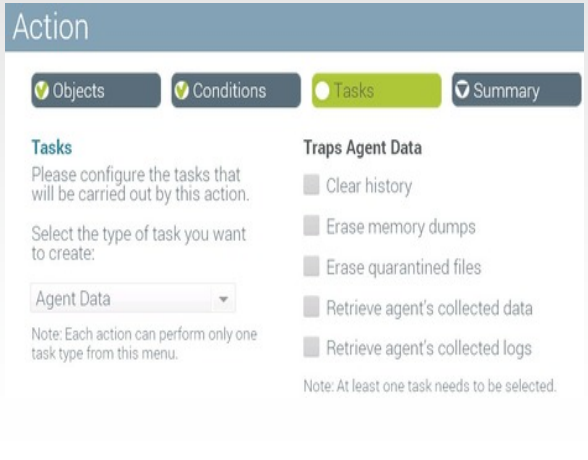
DETECT & AUTOMATICALLY RESPOND TO ADVANCED ATTACKS



1	2	3	4	5
Rich network, endpoint and cloud data sent to logging service	Run behavioral anomaly detection to identify latent & advanced threats	Identify additional locations of threat or attack activity including potential threats	Import external threat intelligence to match IOCs against 3rd parties	Automated remediation & reporting directly & via 3rd party solutions

USE CASE: GAIN ADDITIONAL CONTEXT ON MALWARE ATTACKS

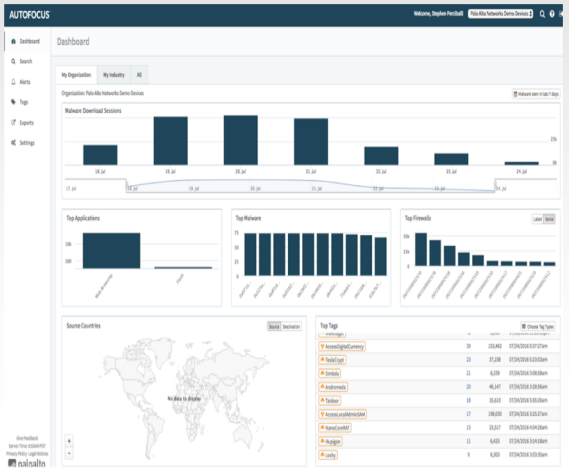
Traps



1

Detect attacks based on rich network, endpoint and cloud data sent to logging service

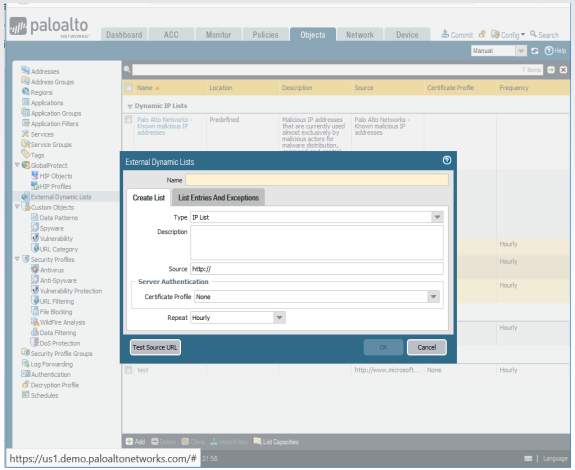
AutoFocus



2

Learn the actors behind the malware and the type of malware

Firewall

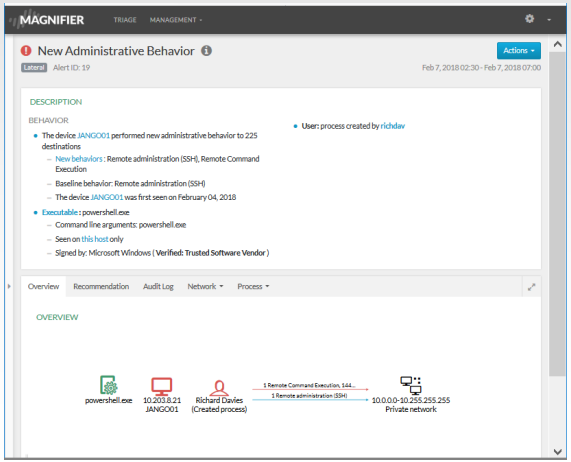


3

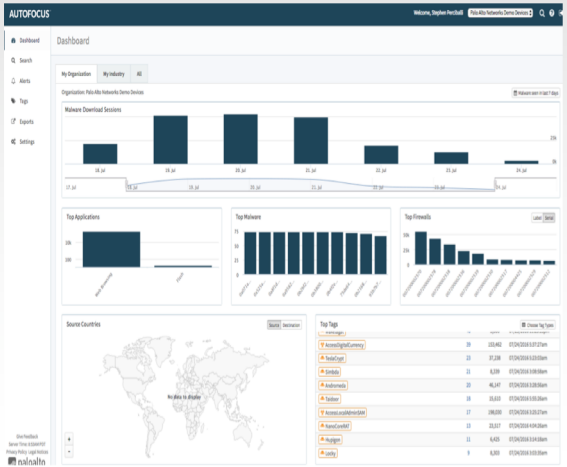
Identify additional locations of threat or attack activity and neutralize

USE CASE: DETECT AND RESPOND TO NETWORK ATTACKS

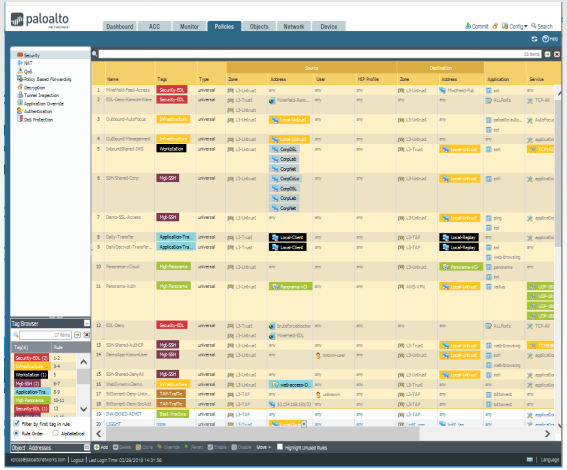
Magnifier



AutoFocus



Firewall



1. Detect attacks based on rich network, endpoint and cloud data sent to logging service

2. Gain additional context by examining IP addresses or file hashes in AutoFocus to confirm attacks

3. Create policies in the firewall to isolate compromised machines or block access to C2 servers

Questions?

Common Questions

- Is Traps 5.0 available?
- How do I get access to 5.0?
- Is Logging service part of Traps?
- What about Android support?
- I bought Traps before 5.0, can I migrate to 5.0?
- How frequently do I need to upgrade Traps?
- What is the footprint of Traps?
- Where can I find more information on malware, exploits or attacks?
- …

THANK YOU

Email: preischl@paloaltonetworks.com I Twitter: @PaloAltoNtwks