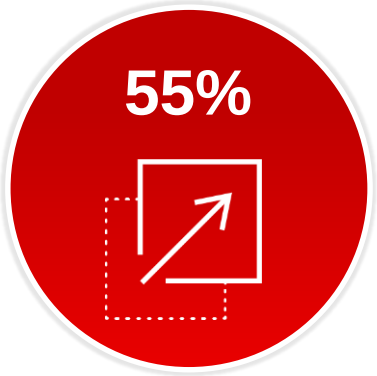
Traps
Advanced Endpoint Protection

Timo Laue

SE EMEA

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

 © 2018, Palo Alto Networks. All Rights Reserved.

INSUFFICIENT ENDPOINT OPTIONS

Traditional EPP

Heavy Footprint & Insufficient

Next-Gen AV

Inconsistent Prevention

EDR

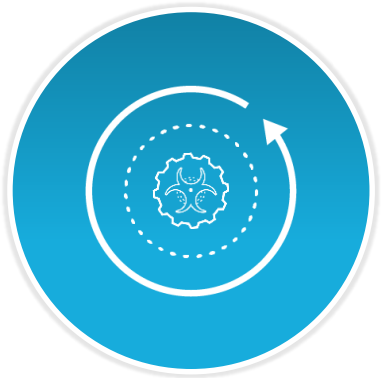
Detection overwhelming without great prevention

 © 2018, Palo Alto Networks. All Rights Reserved.

REQUIREMENTS FOR A NEW APPROACH…

Accurate Prevention: Known *and* Unknown Threats

On all endpoints



Protection Across Attack Techniques

Prevention First Approach

Rapid Detection and Response to Sophisticated Attacks

Integration with the right tools

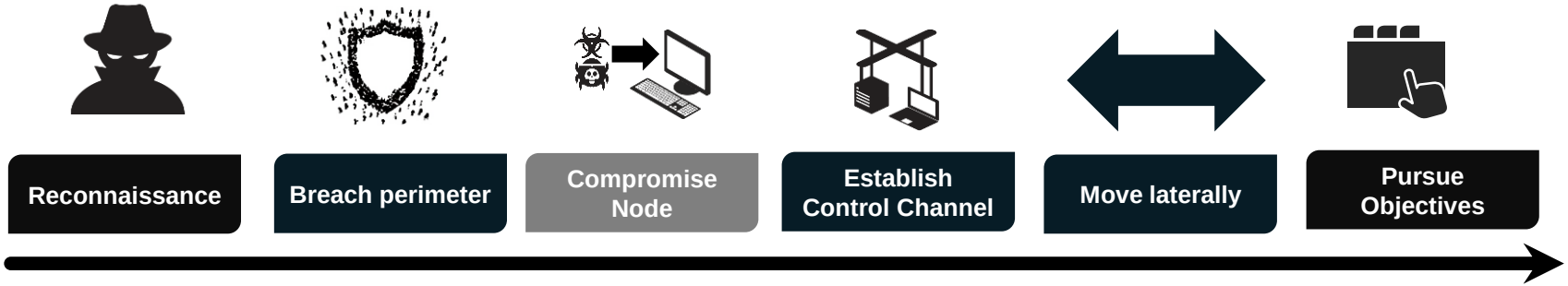
 © 2018, Palo Alto Networks. All Rights Reserved.

A PREVENTION FIRST APPROACH THAT LETS YOU…

Block Malware and Ransomware

Block Exploits and Fileless Threats

Stop Sophisticated Attacks



Attack Life Cycle

 © 2018, Palo Alto Networks. All Rights Reserved.

MALWARE PREVENTION

Block Malware and Ransomware

Block known malware using WildFire threat intelligence

Block Exploits and Fileless Threats

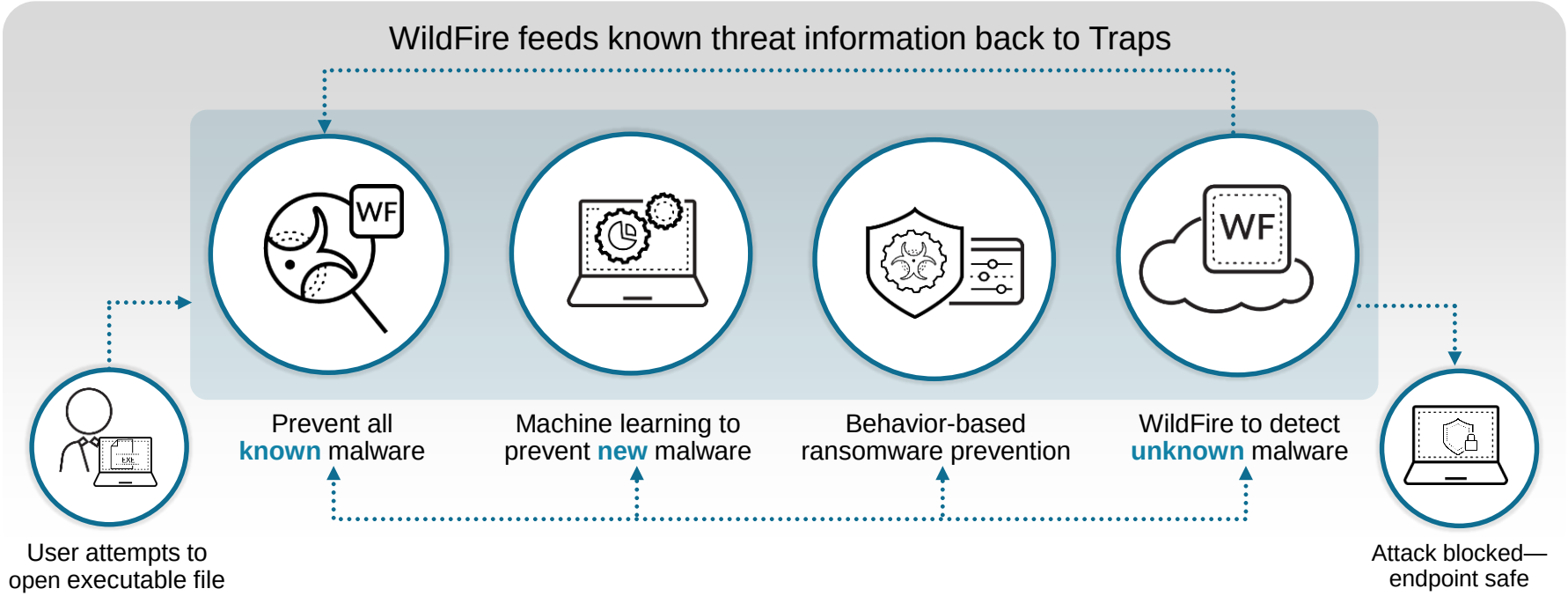
Block unknown malware with local *machine learning* and *behavior-based* analysis

Stop Sophisticated Attacks

Analyze unknown files with industry leading WildFire cloud service

 © 2018, Palo Alto Networks. All Rights Reserved.

PREVENT KNOWN AND UNKNOWN MALWARE



Multiple methods of prevention improve accuracy and coverage

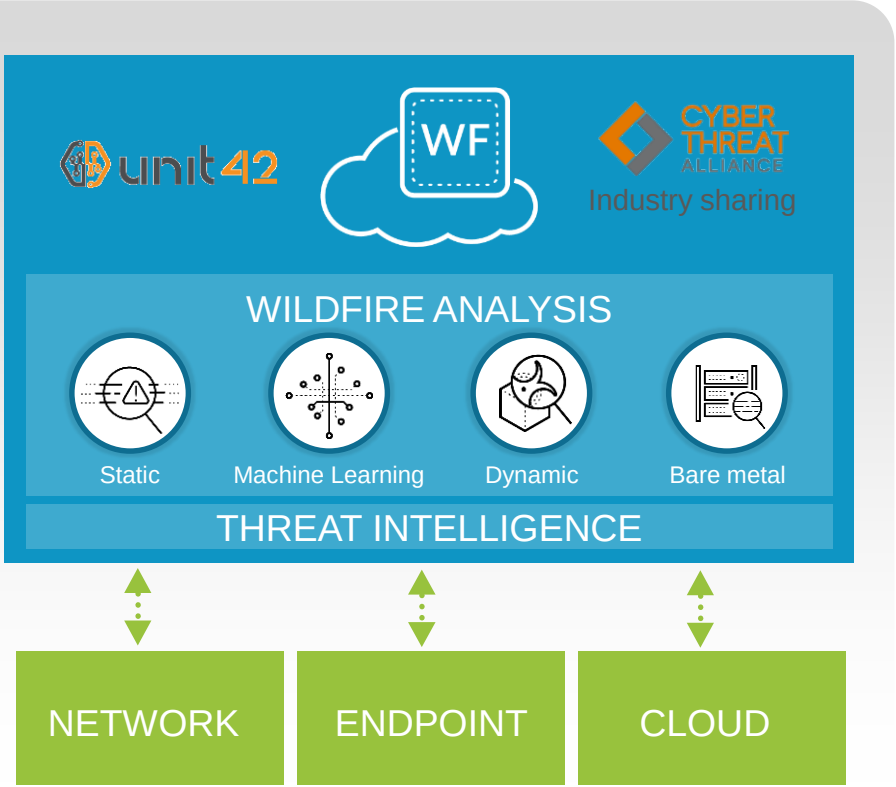
 © 2018, Palo Alto Networks. All Rights Reserved.

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, and cloud



 © 2018, Palo Alto Networks. All Rights Reserved.

EXPLOT PREVENTION

Block Malware and Ransomware

Block Exploits and Fileless Threats

Stop Sophisticated Attacks

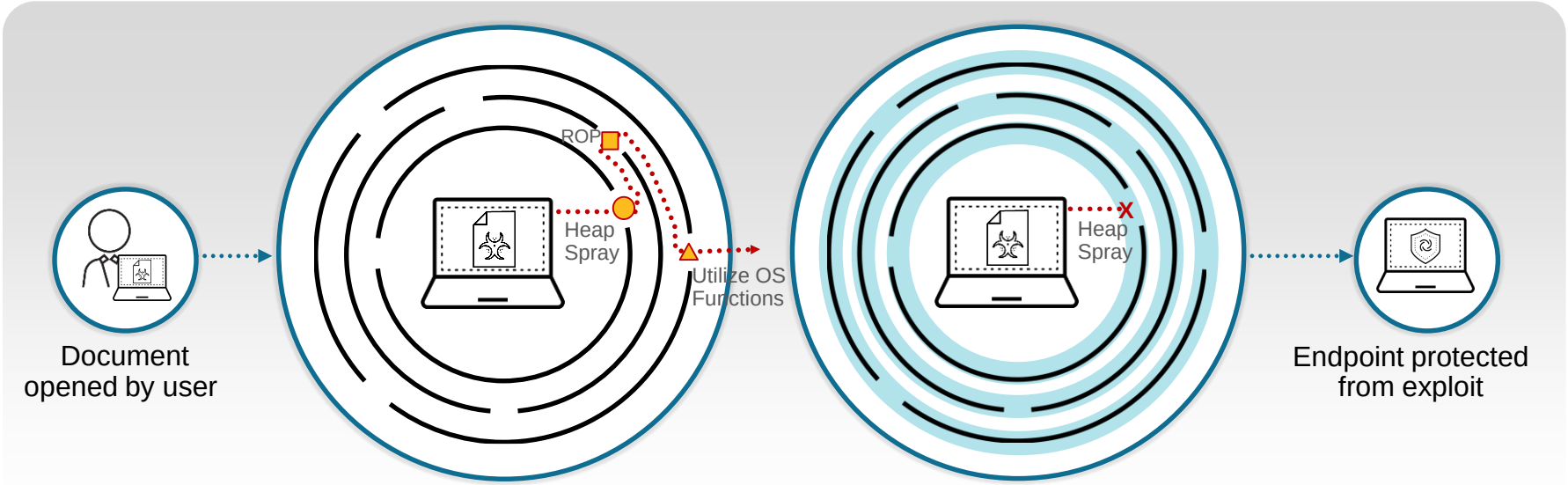
Reduce opportunities for attack on endpoint with policy and restrictions

Prevent exploits by technique, not the exploits

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

 © 2018, Palo Alto Networks. All Rights Reserved.

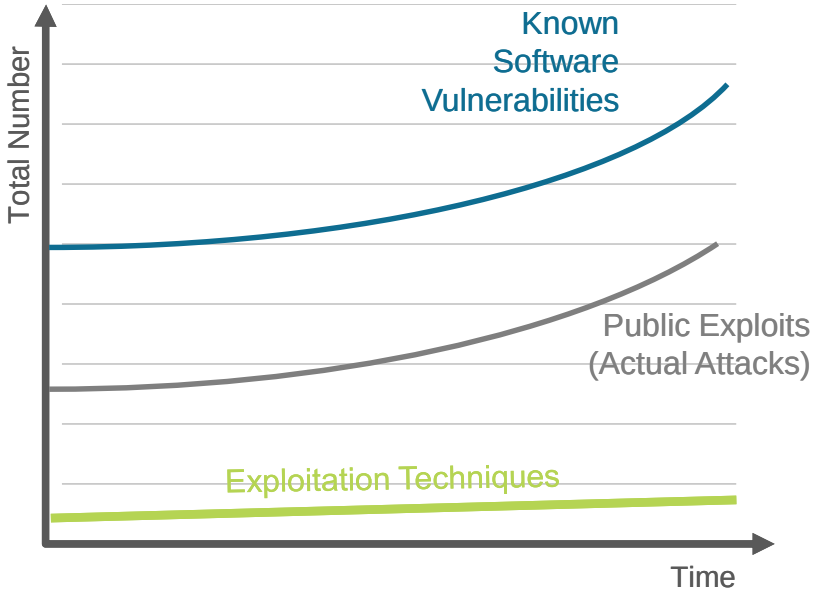
EXPLOIT PROTECTION FOCUSES ON TECHNIQUE



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

 © 2018, Palo Alto Networks. All Rights Reserved.

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

 © 2018, Palo Alto Networks. All Rights Reserved.

SIX YEARS OF EXPLOIT PROTECTION INNOVATION

TRAPS ADVANCED ENDPOINT PROTECTION

NEW

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

EXPLOIT PREVENTION MODULES

 © 2018, Palo Alto Networks. All Rights Reserved.

SPEED DETECTION AND RESPONSE TO SOPHISTICATED ATTACKS

Block Malware and Ransomware

Block Exploits and Fileless Threats

Stop Sophisticated Attacks

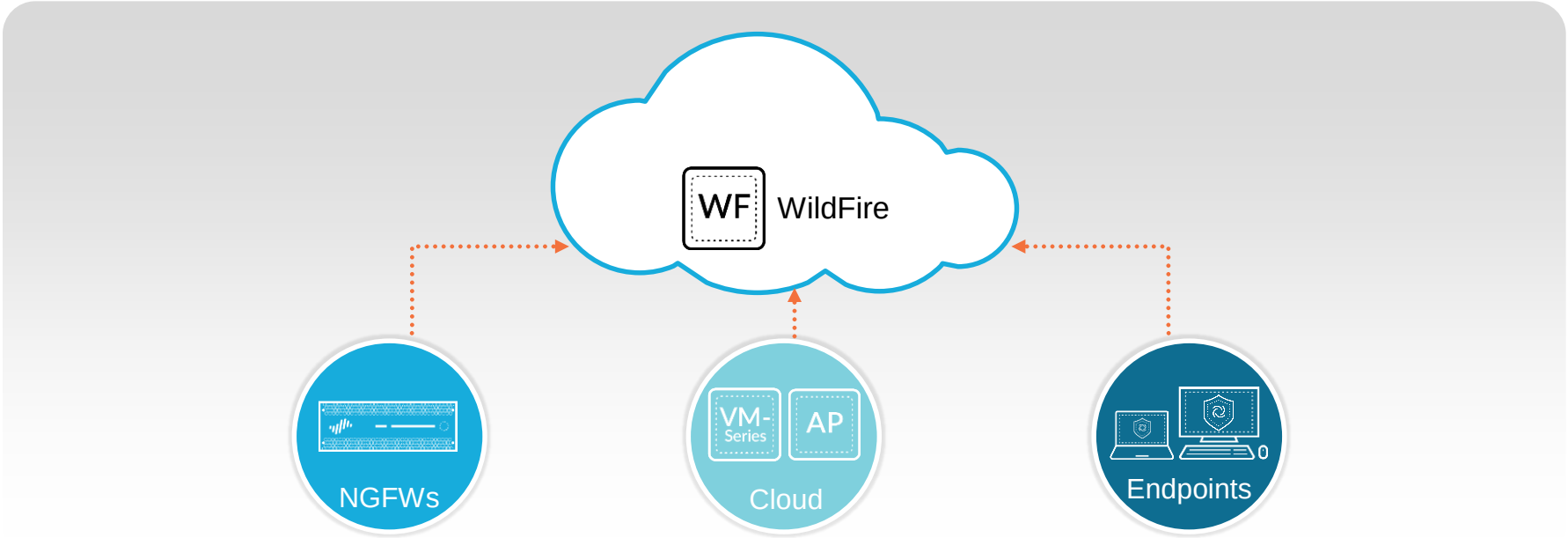
Coordinate enforcement across network, endpoint, and cloud

Accelerate investigation with analytics, context, and classification

Rapidly consume innovative detection and response capabilities

 © 2018, Palo Alto Networks. All Rights Reserved.

SHARED THREAT INTELLIGENCE ACROSS LOCATIONS

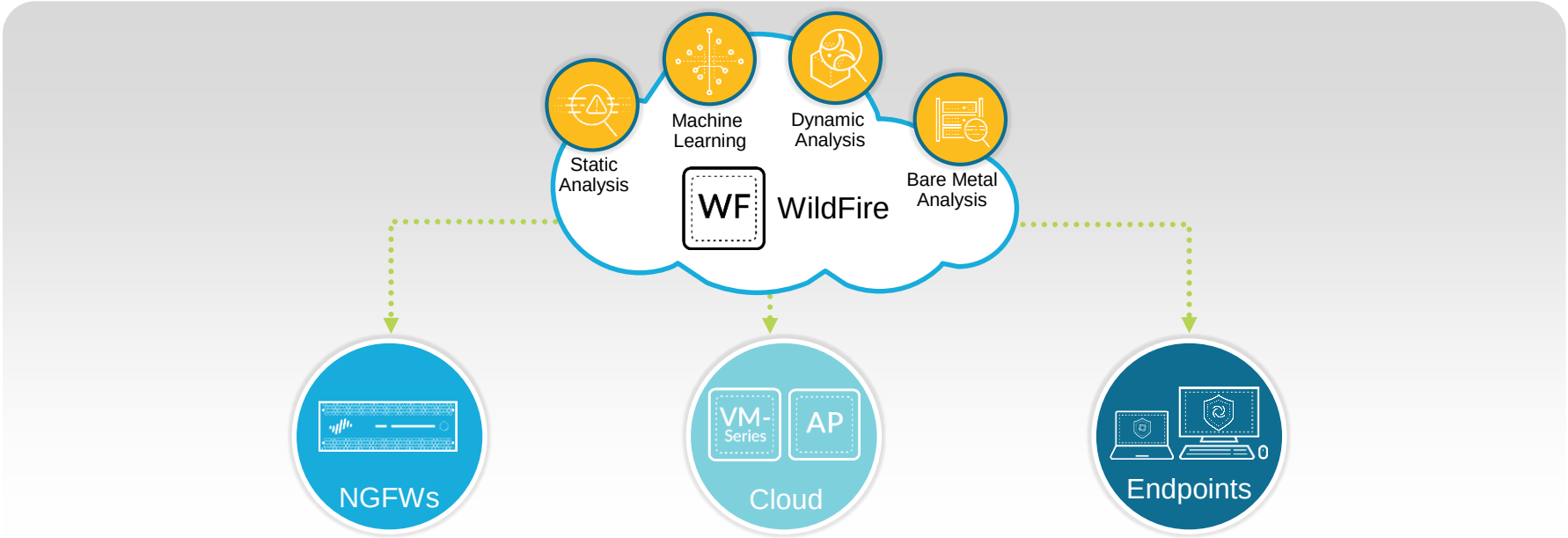


1

NGFWs, Aperture, and Traps send unknowns or suspicious files and links to WildFire

 © 2018, Palo Alto Networks. All Rights Reserved.

SHARED THREAT INTELLIGENCE



1

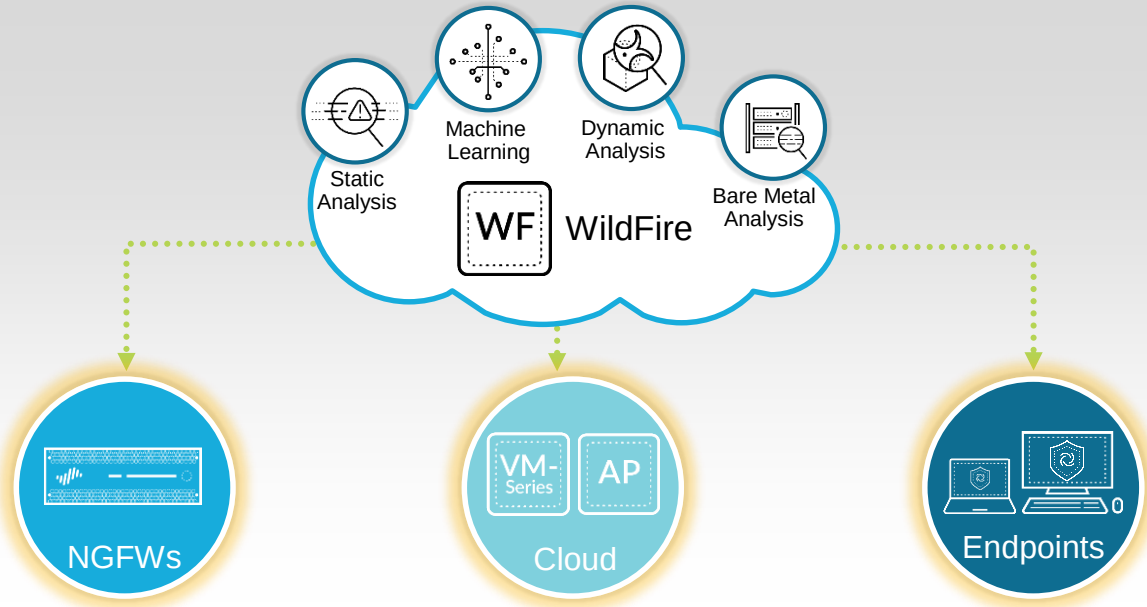
NGFWs, Aperture, and Traps send unknowns or suspicious files and links to WildFire

2

WildFire analyzes the unknown, renders a verdict, and shares threat intelligence

 © 2018, Palo Alto Networks. All Rights Reserved.

SHARED THREAT INTELLIGENCE



1. NGFWs, Aperture, and 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 protect against new threat

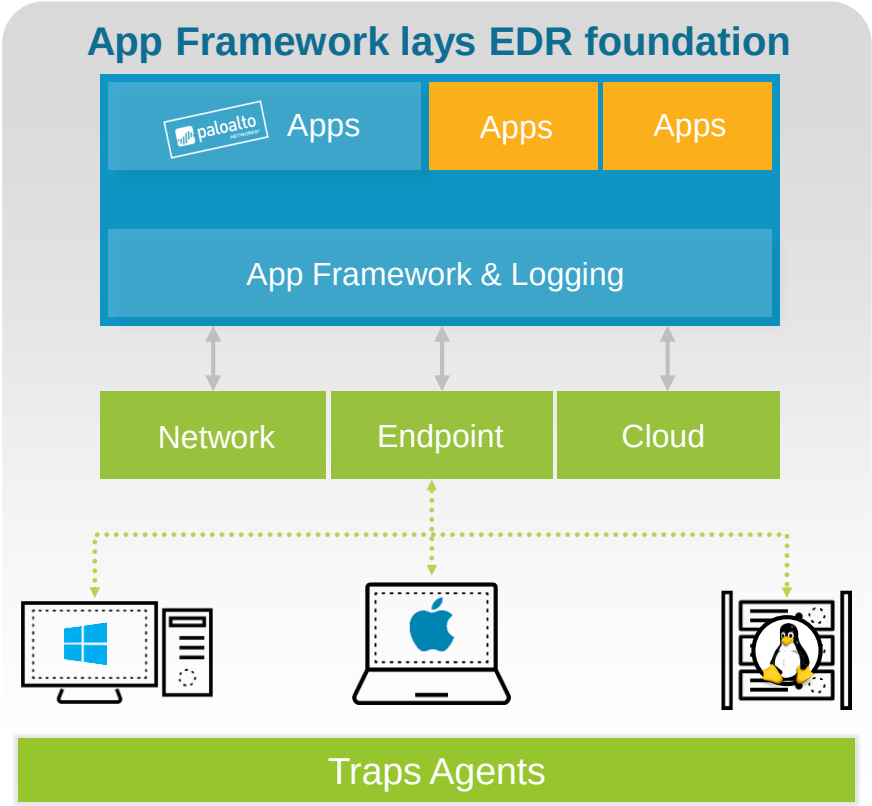
 © 2018, Palo Alto Networks. All Rights Reserved.

ACCELERATE DETECTION AND RESPONSE

Send endpoint events into logging service

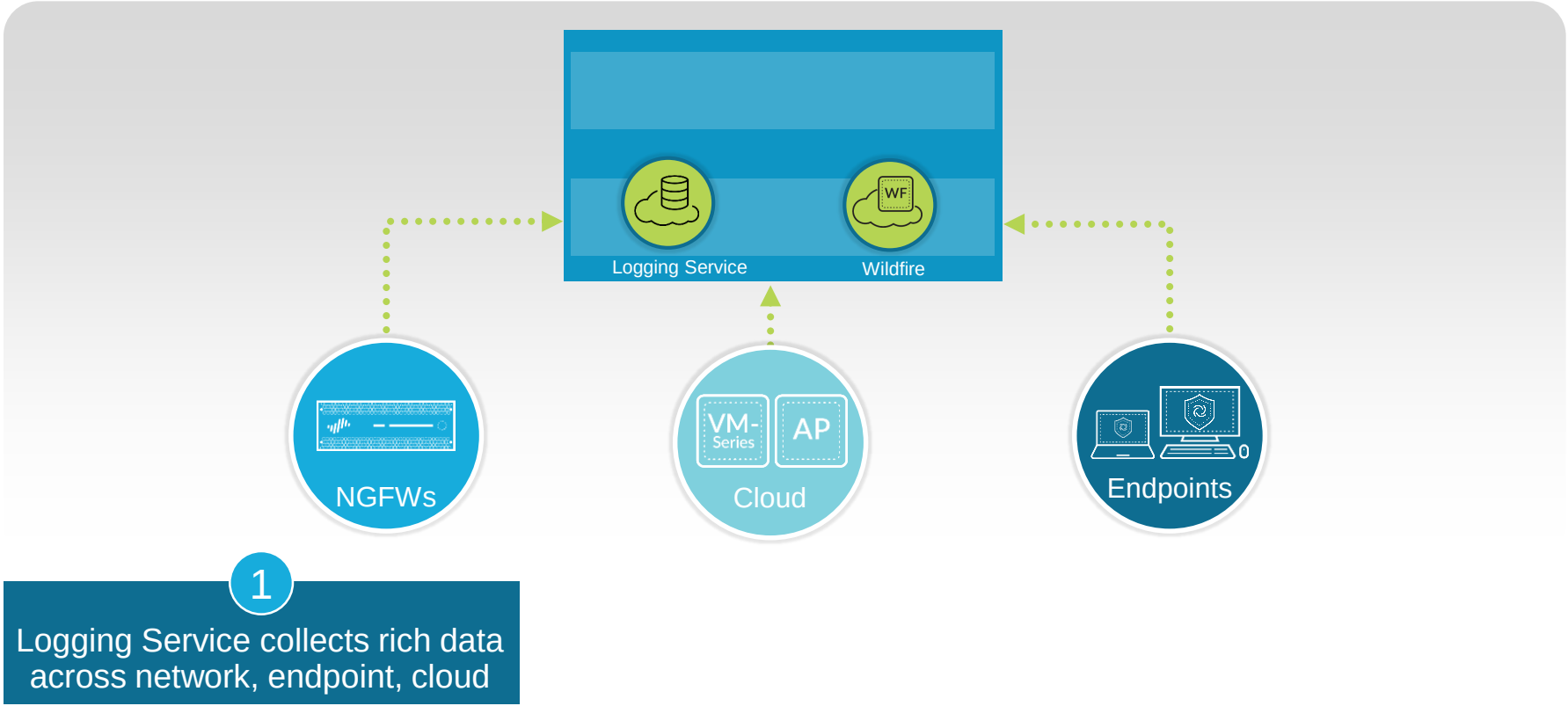
Organize data for analytics

Rapidly adopt new capabilities to stop attacks



 © 2018, Palo Alto Networks. All Rights Reserved.

QUICKLY DETECT AND RESPOND TO ATTACKS

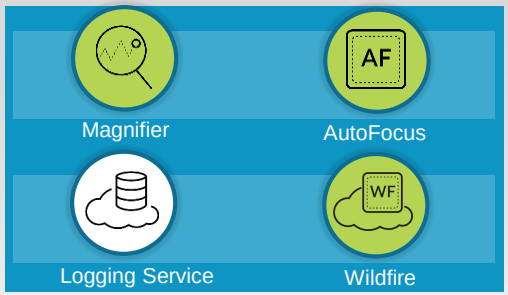


1

Logging Service collects rich data across network, endpoint, cloud

 © 2018, Palo Alto Networks. All Rights Reserved.

QUICKLY DETECT AND RESPOND TO ATTACKS



1

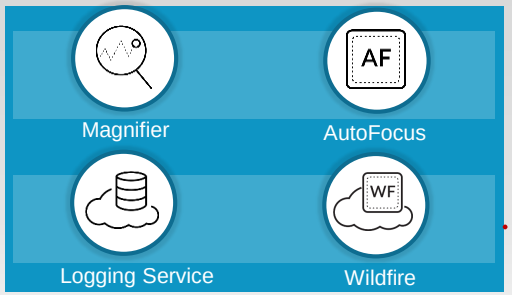
Logging Service collects rich data across network, endpoint, cloud

2

Detect attacks using threat and intelligence behavioral analytics

 © 2018, Palo Alto Networks. All Rights Reserved.

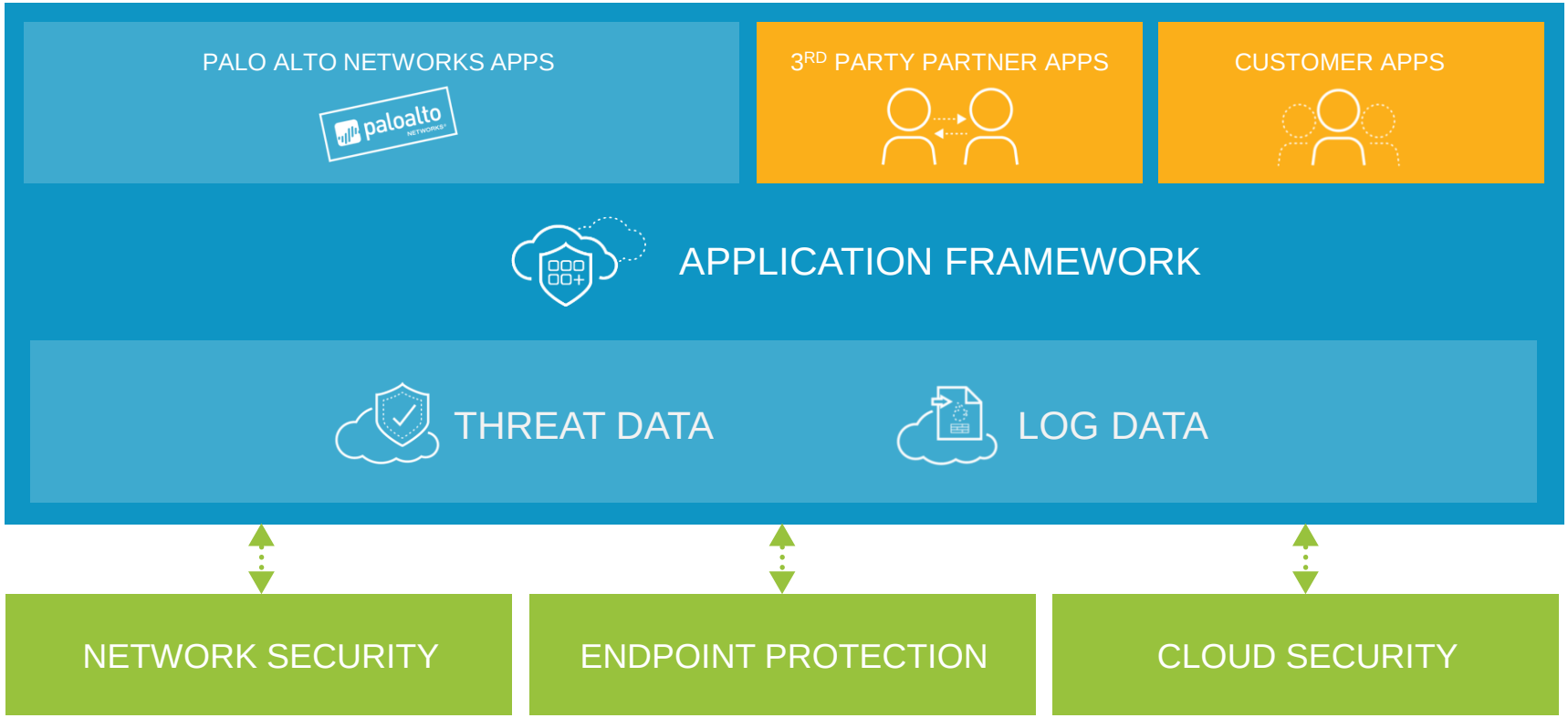
QUICKLY DETECT AND RESPOND TO ATTACKS



1. Logging Service collects rich data across network, endpoint, cloud
2. Detect attacks using threat and intelligence behavioral analytics
3. Isolate attack and contain infected endpoint

 © 2018, Palo Alto Networks. All Rights Reserved.

PALO ALTO NETWORKS NEXT GENERATION SECURITY PLATFORM



 © 2018, Palo Alto Networks. All Rights Reserved.

A PREVENTION FIRST APPROACH THAT LETS YOU…

Block Malware and Ransomware

Best protection against malware and ransomware

Block Exploits and Fileless Threats

Best protection against exploits and fileless attacks

Stop Sophisticated Attacks

Accelerate incident response and automate containment

 © 2018, Palo Alto Networks. All Rights Reserved.

Traps 5.0
What's New Slides

TRAPS MANAGEMENT SERVICE

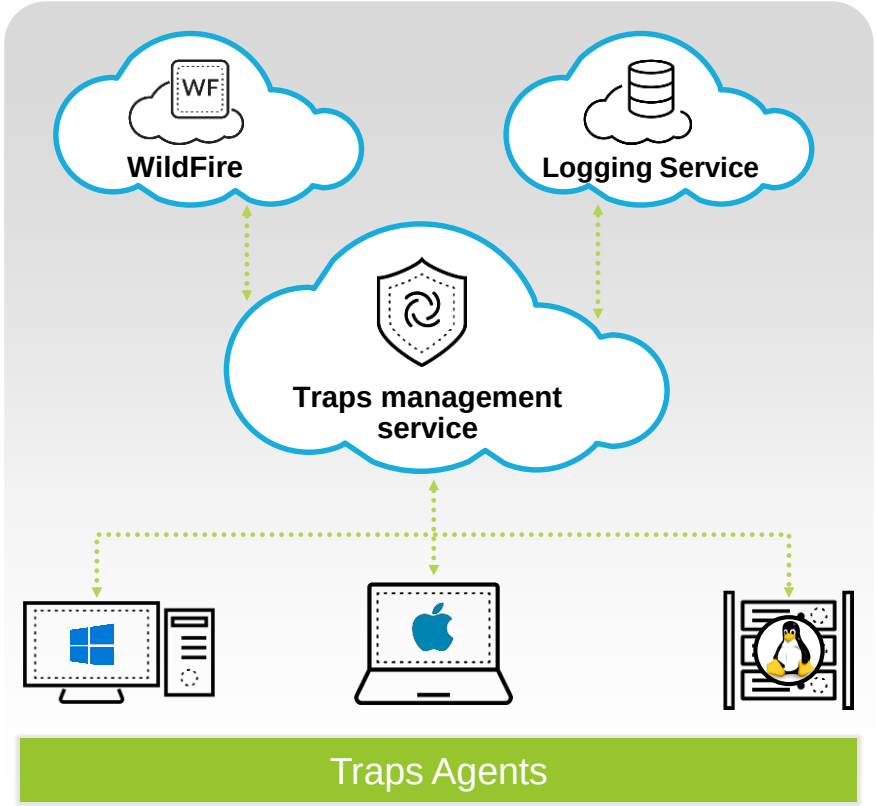
Cloud-delivered Service

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

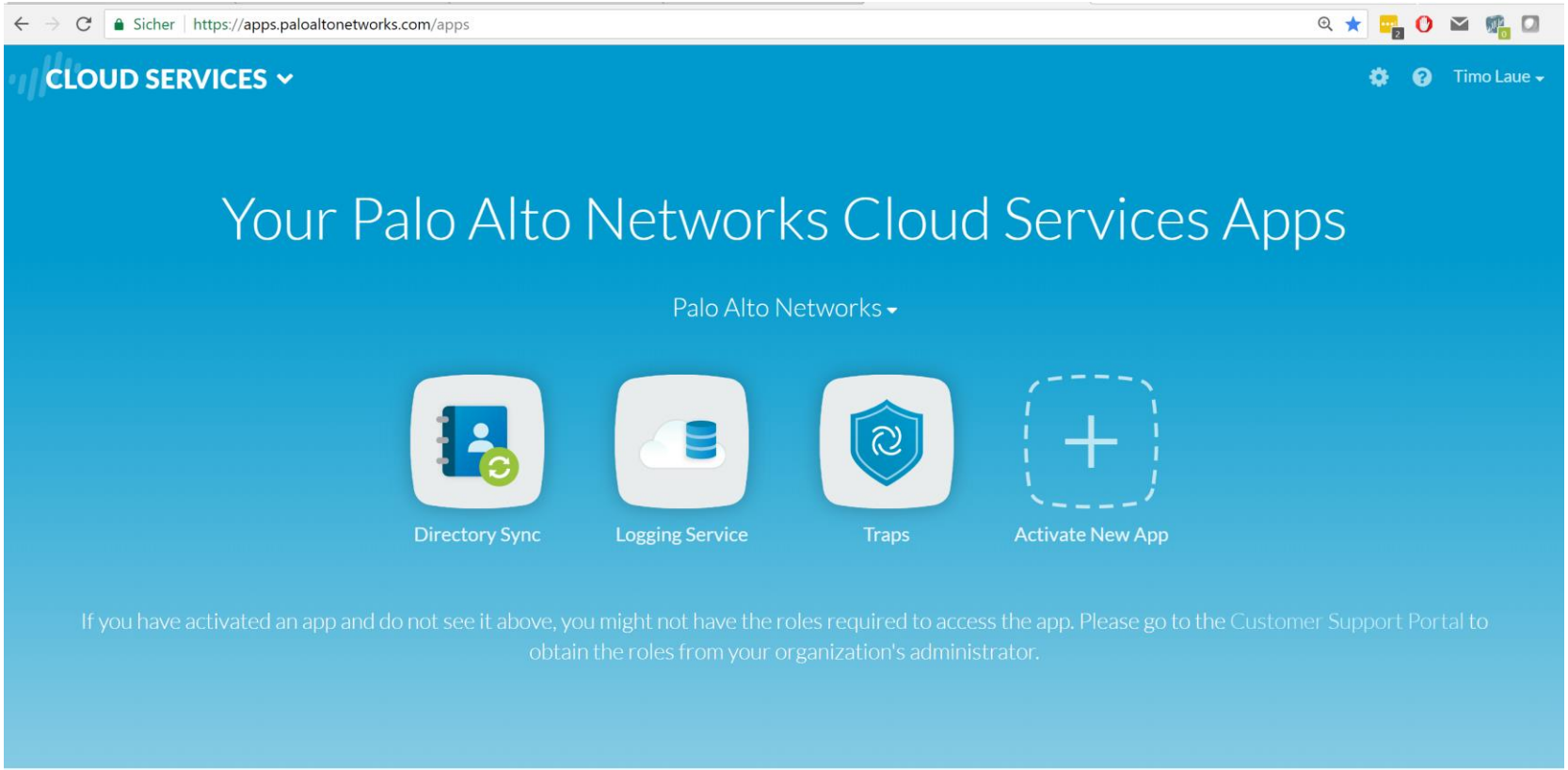
Application Framework Integration

- 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



TRAPS MANAGEMENT SERVICE



REIMAGINED USER EXPERIENCE

Intuitive Web-based Interface

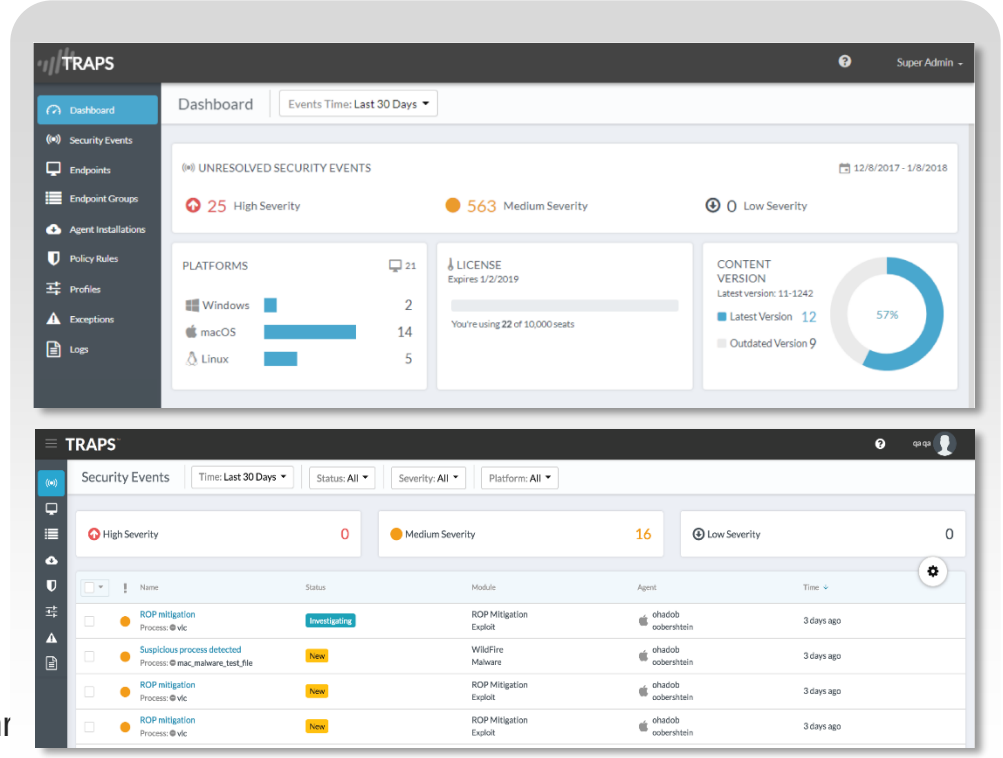
- Minimizes operational challenges
- Consistent policy management
- Dynamic endpoint grouping

Simplified Event Management

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

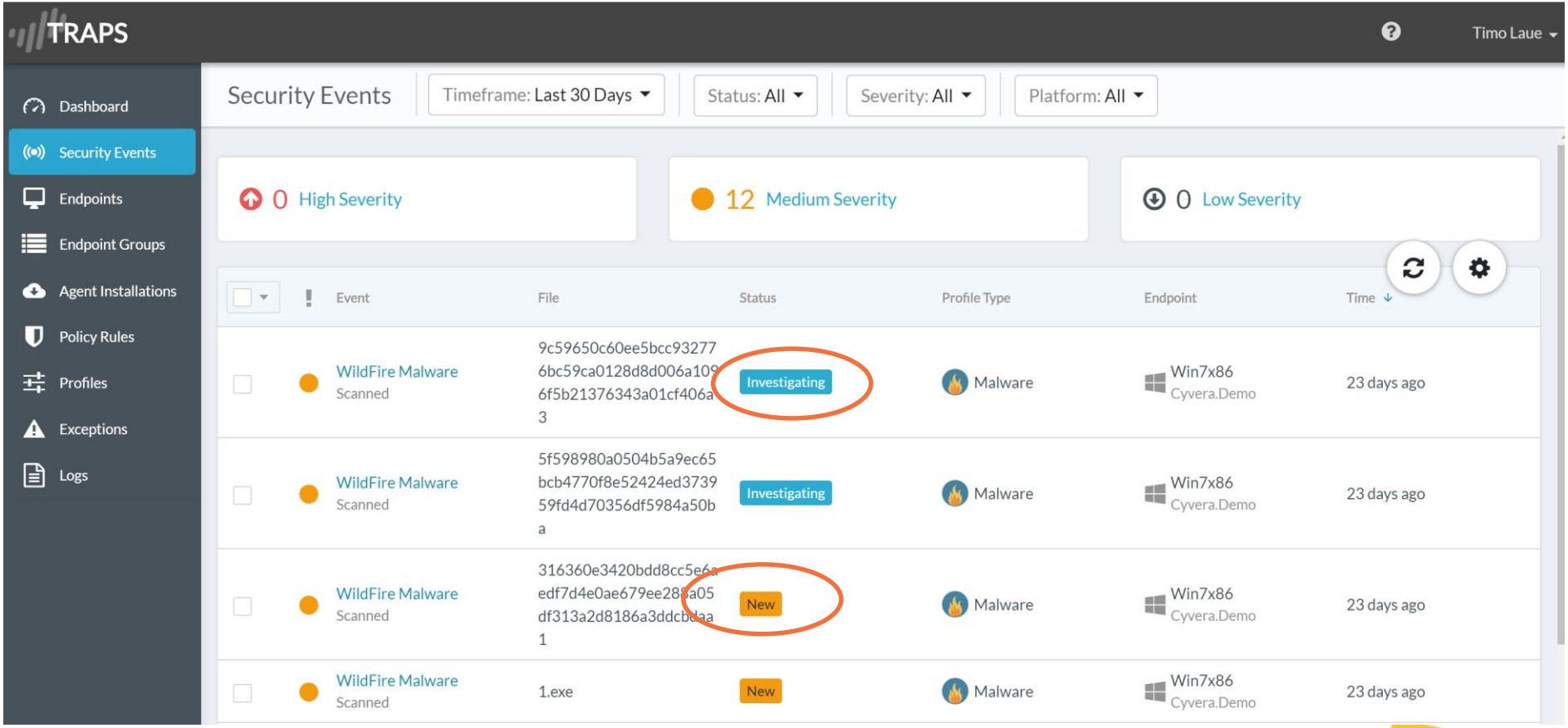
Integrated WildFire Threat Reports

- 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

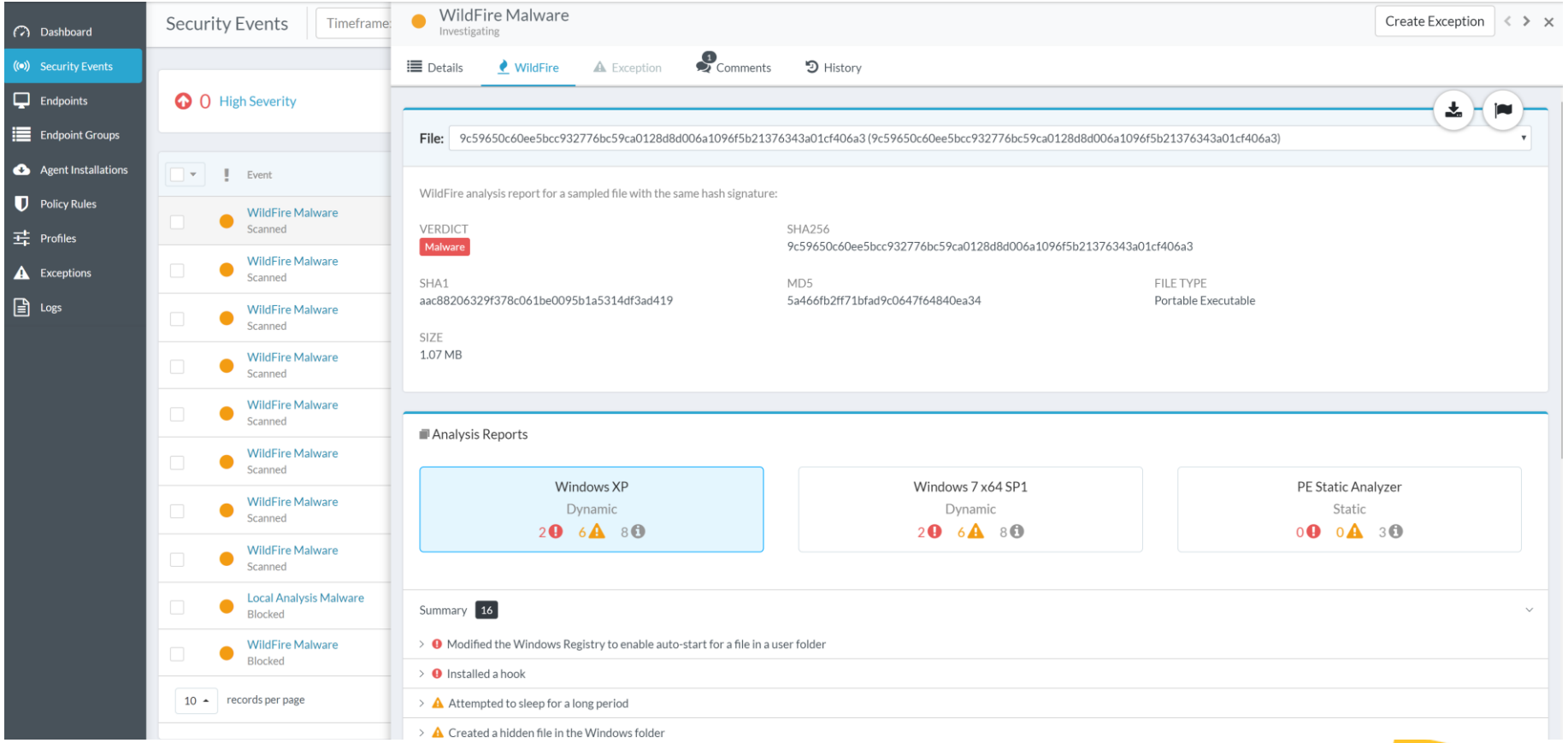


 © 2015, Palo Alto Networks. Confidential and Proprietary.

TRAPS MANAGEMENT SERVICE



TRAPS MANAGEMENT SERVICE



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

 © 2016, Palo Alto Networks. Confidential and Proprietary.

PROACTIVE THREAT SCANNING

Scanning Endpoints for Malware

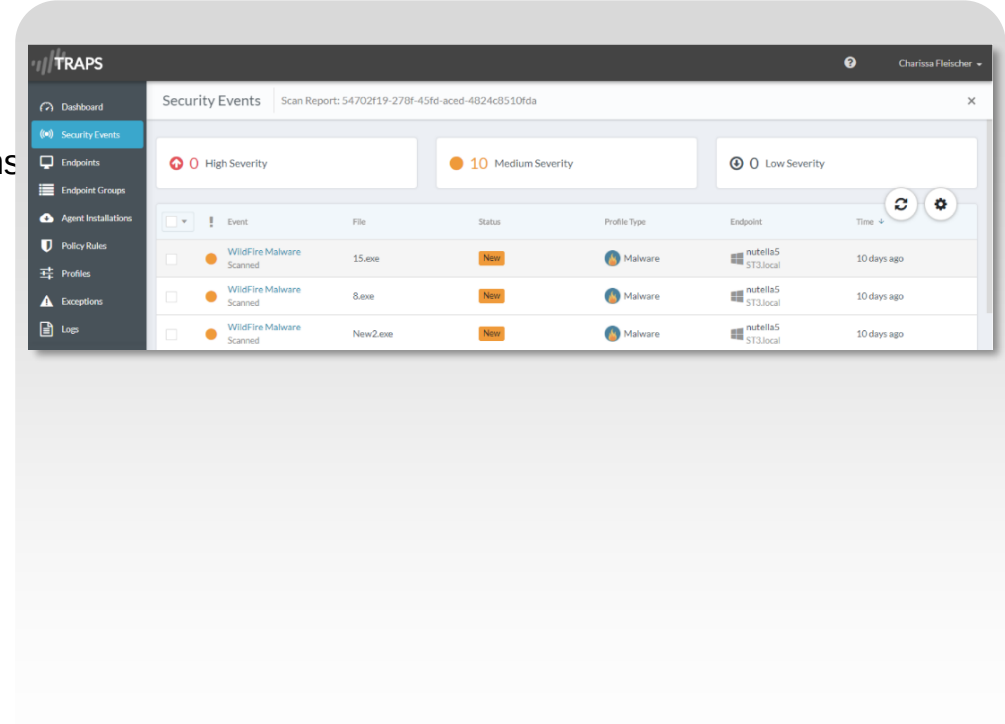
- Identifies dormant malware before execution
- On-demand or scheduled file system scans
- WildFire threat intelligence for known files

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

 © 2015, Palo Alto Networks. Confidential and Proprietary.

THANK YOU

Email: tlaue@paloaltonetworks.com Twitter: @PaloAltoNtwks