TRAPS
PROTECT YOURSELF FROM ANTIVIRUS

WildFire Demonstrates the Shortcomings of Legacy AV

71.9M — All Files

5.3M — Malicious

2.0M — Detected by AV
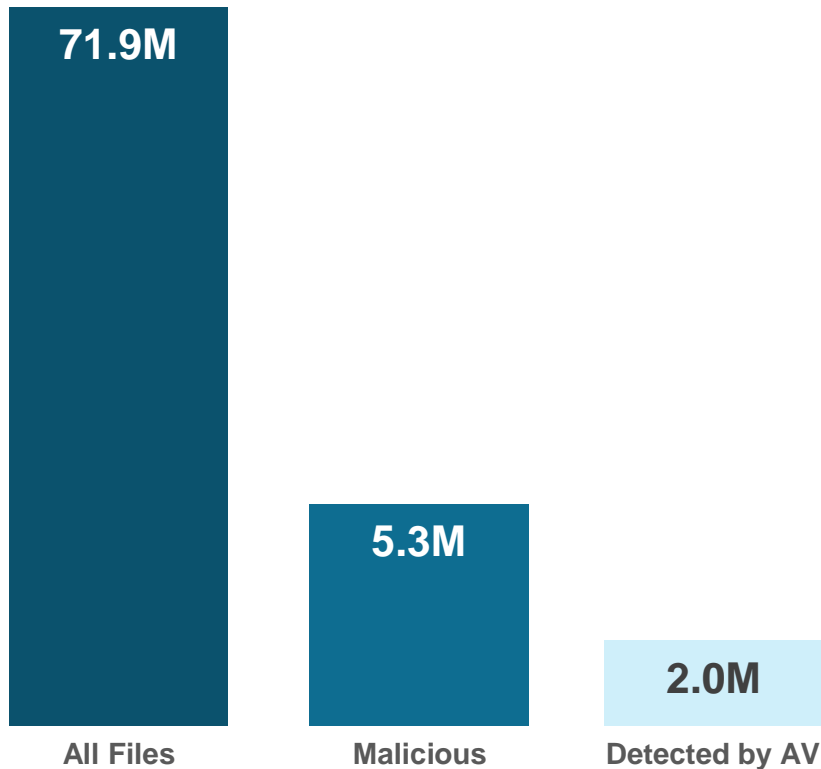
37.5%

Of the malware files seen by WildFire each month are detected by the top 6 enterprise AV vendors[*].

*Average monthly values as of January 2016. Source: Palo Alto Networks WildFire and Multi-Scanner

paloalto NETWORKS®

Five Fundamental Capabilities Any AV Replacement Must Deliver

Prevention Focused

Malware Prevention
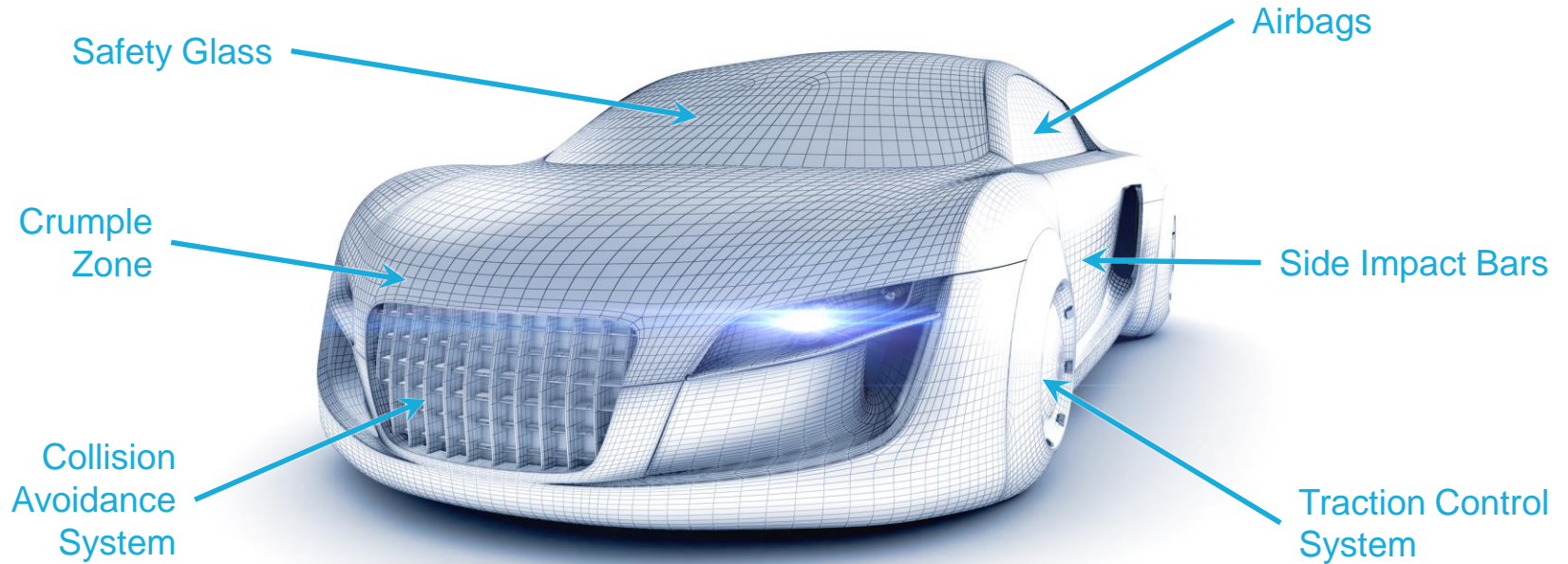
Exploit Prevention

Automated Prevention w/ Threat Intel

Persistent Protection

Detection & Response Secondary to Prevention

Automatically Convert Threat Intel into Prevention

Known & Unknown

Known & Unknown/ Zero-Day

Online, Offline On-Prem, Off-Prem Connected, Disconnected

paloalto
NETWORKS®

Prevention Requires a Combination of Multiple Purpose-built Methods

Safety Glass

Airbags

Crumple Zone

Side Impact Bars

Collision Avoidance System

Traction Control System

paloalto
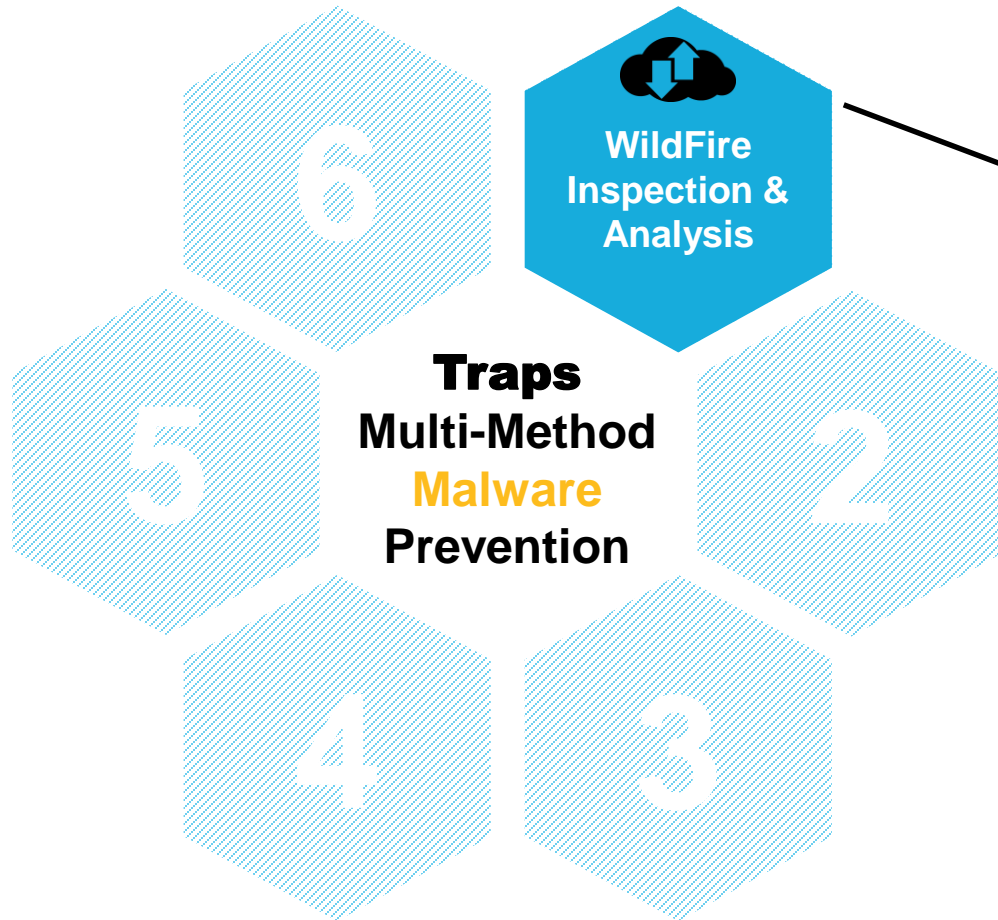NETWORKS®

Traps *Multi-Method* Approach to Prevention

Combines Multiple Prevention Methods

Multiple Purpose-built Techniques per Method

Maximum Coverage
for Each Attack Type

Maximum Accuracy
from Purpose-Built Techniques

Methods Tuned
for Their Strengths

paloalto
NETWORKS®

WildFire Inspection & Analysis

6

5

2

4

3

Traps
Multi-Method
Malware
Prevention

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

paloalto
NETWORKS®

WildFire Detects *Malware* Using Multiple Methods & Techniques

Static Analysis

File Anomaly Detection

Static Signatures

String & Code Block Detection

Machine Learning &
Static Analysis

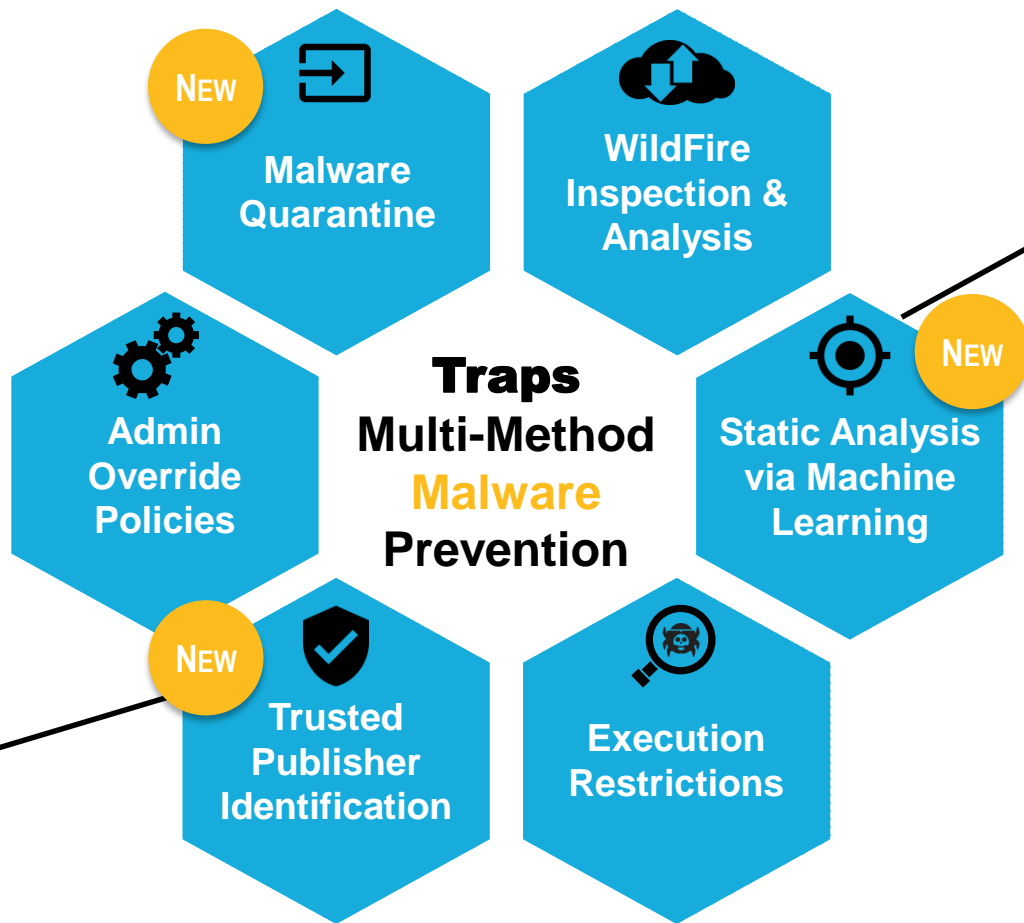## Dynamic Analysis

Full Execution Analysis

Multi-version
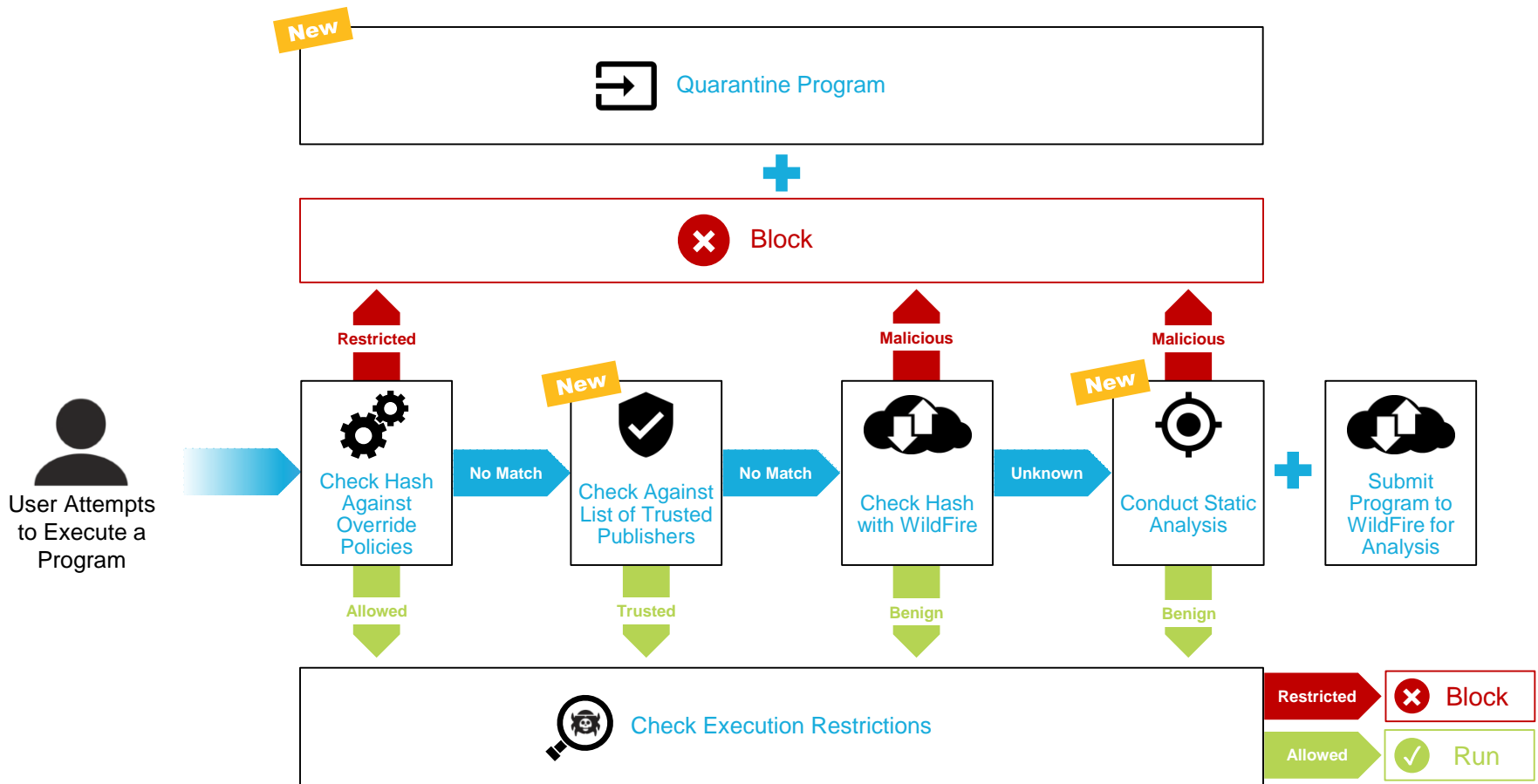Execution Environment

Multi-dimensional Scoring

Network
Traffic Analysis

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

paloalto
NETWORKS®

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

NEW
Malware Quarantine

WildFire Inspection & Analysis

Admin Override Policies

Traps
Multi-Method
Malware
Prevention

NEW
Static Analysis via Machine Learning

NEW
Trusted Publisher Identification

Execution Restrictions

Static Analysis Prevents Malware Variants that Have Never Been Seen Before

paloalto
NETWORKS®

Memory
Corruption
Prevention

Traps
Multi-Method
Exploit
Prevention

Logic
Flaw
Prevention

Code
Execution
Prevention
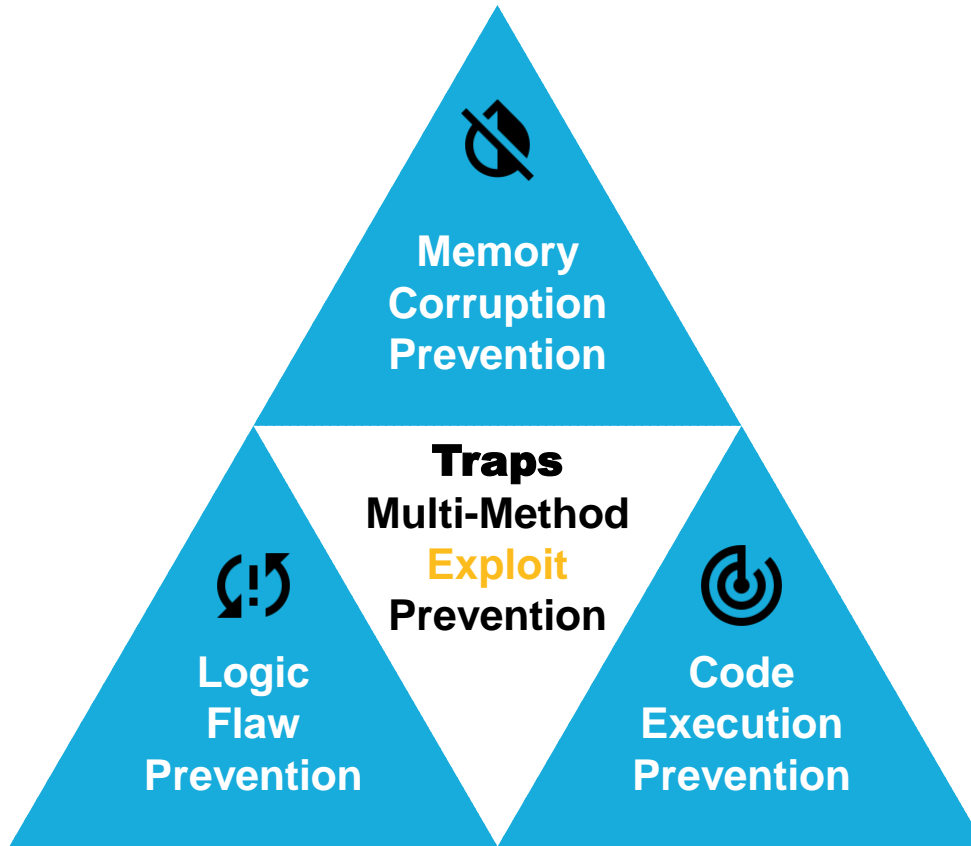
Traps Prevents Exploits At Their Core

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**

Chart labels:
- Total Number (y-axis)
- Time (x-axis)
- Known Software Vulnerabilities
- Public Exploits (Actual Attacks)
- Exploitation Techniques

paloalto NETWORKS®

Value of Technique-based Exploit Prevention

Mar 2014

Apr 2015

Oct 2015

TIMELINE

**Traps
Version 2.3.6
Released**

**Vulnerability
Discovered in
Adobe Flash Player**
(CVE-2015-0359)

**Attackers Attempted to
Exploit Vulnerability.**

**Traps Blocked the
Attempt.**

Traps v2.3.6

No Updates or
Patches
Since Installation
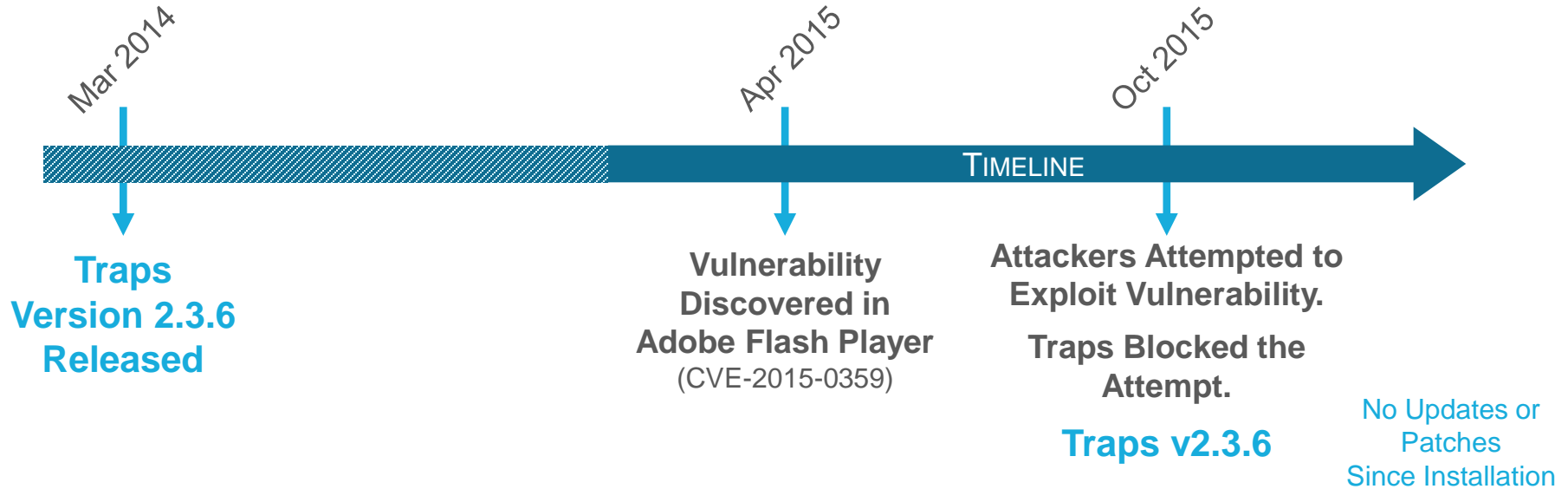
Traps Prevents Zero-day and Unknown
Exploits That Have Yet to be Discovered

Traps vs. Top 10 Zero-Day Exploits of 2015

Discovery Date	Application	Exploit Identifier	Did Traps Block Zero-Day Exploit?
January 23, 2015	Flash	CVE-2015-0311	✓
March 13, 2015	Flash	CVE-2015-0336	✓
April 14, 2015	Flash	CVE-2015-3043	✓
June 23, 2015	Flash	CVE-2015-3113	✓
July 8, 2015	Flash	CVE-2015-5119	✓
July 14, 2015	Office	CVE-2015-2424	✓
July 14, 2015	Flash	CVE-2015-5122	✓
September 8, 2015	Office	CVE-2015-2545	✓
October 15, 2015	Flash	CVE-2015-7645	✓
December 28, 2015	Flash	CVE-2015-8651	✓

paloalto NETWORKS

Next-Generation *Preventive* *Endpoint Protection*

Replaces Legacy Approach to Antivirus with Next-generation Multi-Method Prevention

Leverages Multiple Purpose-built Techniques for Maximum Accuracy in Preventing Malware

Adds Most Complete Multi-Method Exploit Prevention Available

Requires the Smallest Footprint Possible

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

WILDFIRE THREAT INTELLIGENCE CLOUD

AUTOMATED

CLOUD

NETWORK

ENDPOINT

NATIVELY INTEGRATED

EXTENSIBLE

INTELLIGENCE COLLECTION

PREVENTION CAPABILITIES

NEXT-GENERATION FIREWALL

TRAPS ADVANCED ENDPOINT PROTECTION

paloalto
NETWORKS®