The Bad guys Never had it Easier, but Prevention is Possible.

Traps

Andreas Persson, CSSR

Patrick Reischl, CSS SE

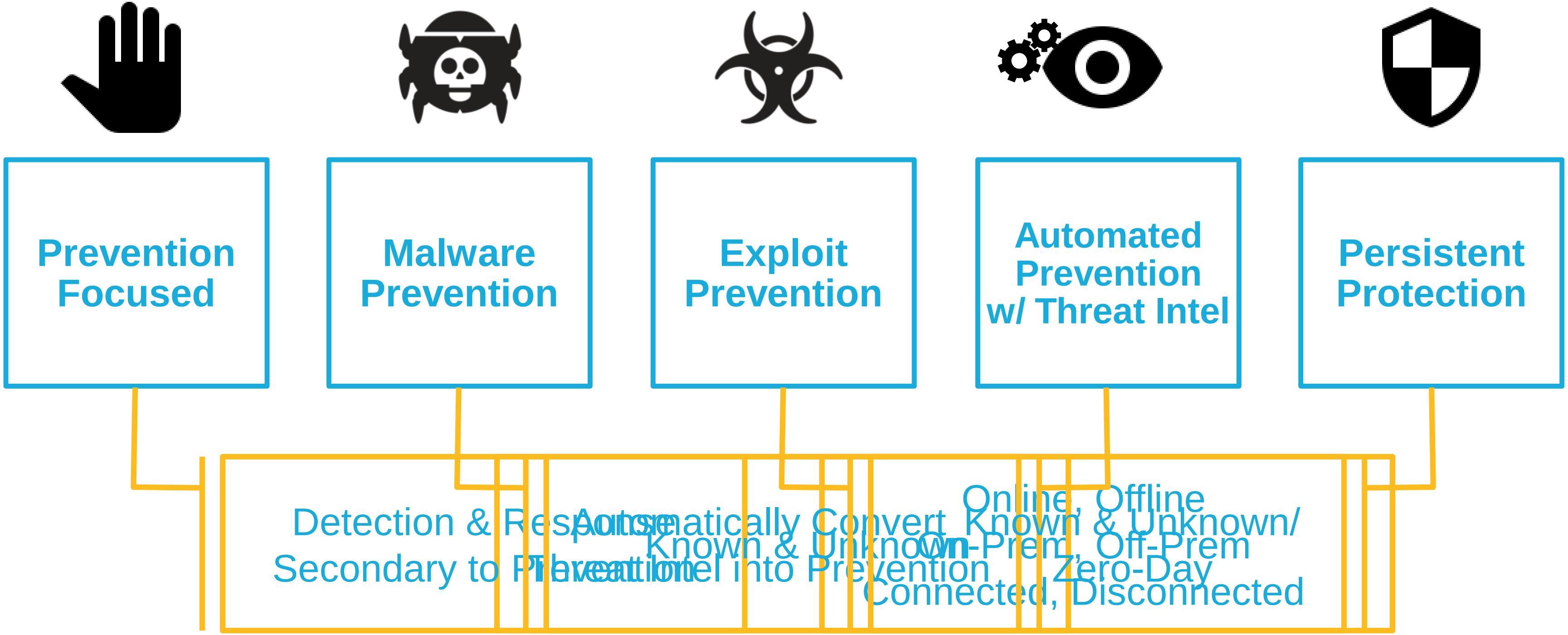
Mini-Survey

Are you using **Anti-Virus** in your organization today?

Traditional AV is Not the Solution to Endpoint Protection.

It's the Problem!

Five Fundamental Capabilities of Any Endpoint Product



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

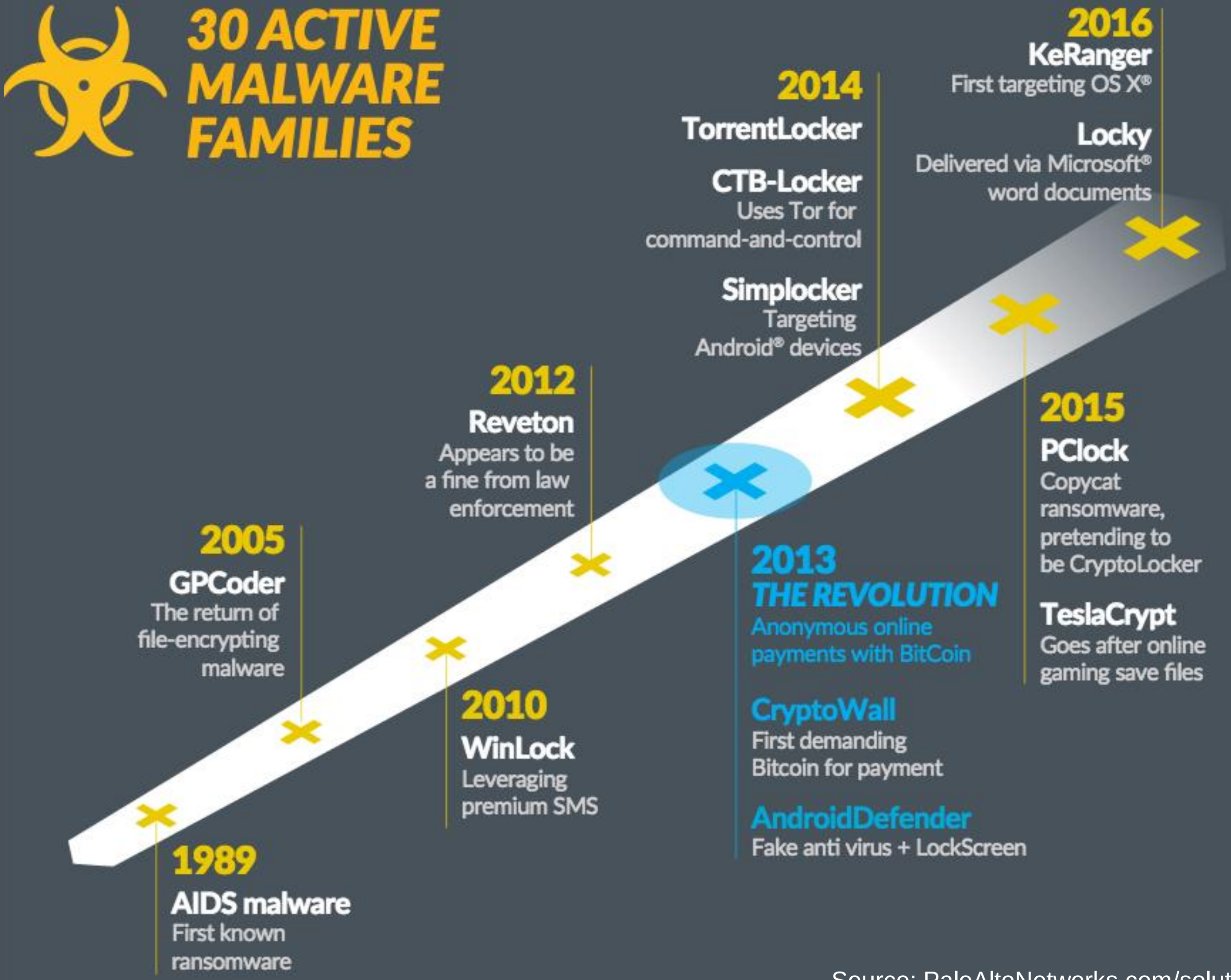
Known & Unknown/
Zero-Day

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

Mini-Survey

Do you know what **Ransomware** is?

30 ACTIVE MALWARE FAMILIES



1989
AIDS malware
First known ransomware

2005
GPCoder
The return of file-encrypting malware

2010
WinLock
Leveraging premium SMS

2012
Reveton
Appears to be a fine from law enforcement

2013
THE REVOLUTION
Anonymous online payments with BitCoin

CryptoWall
First demanding Bitcoin for payment

AndroidDefender
Fake anti virus + LockScreen

2014
TorrentLocker

CTB-Locker
Uses Tor for command-and-control

Simplocker
Targeting Android® devices

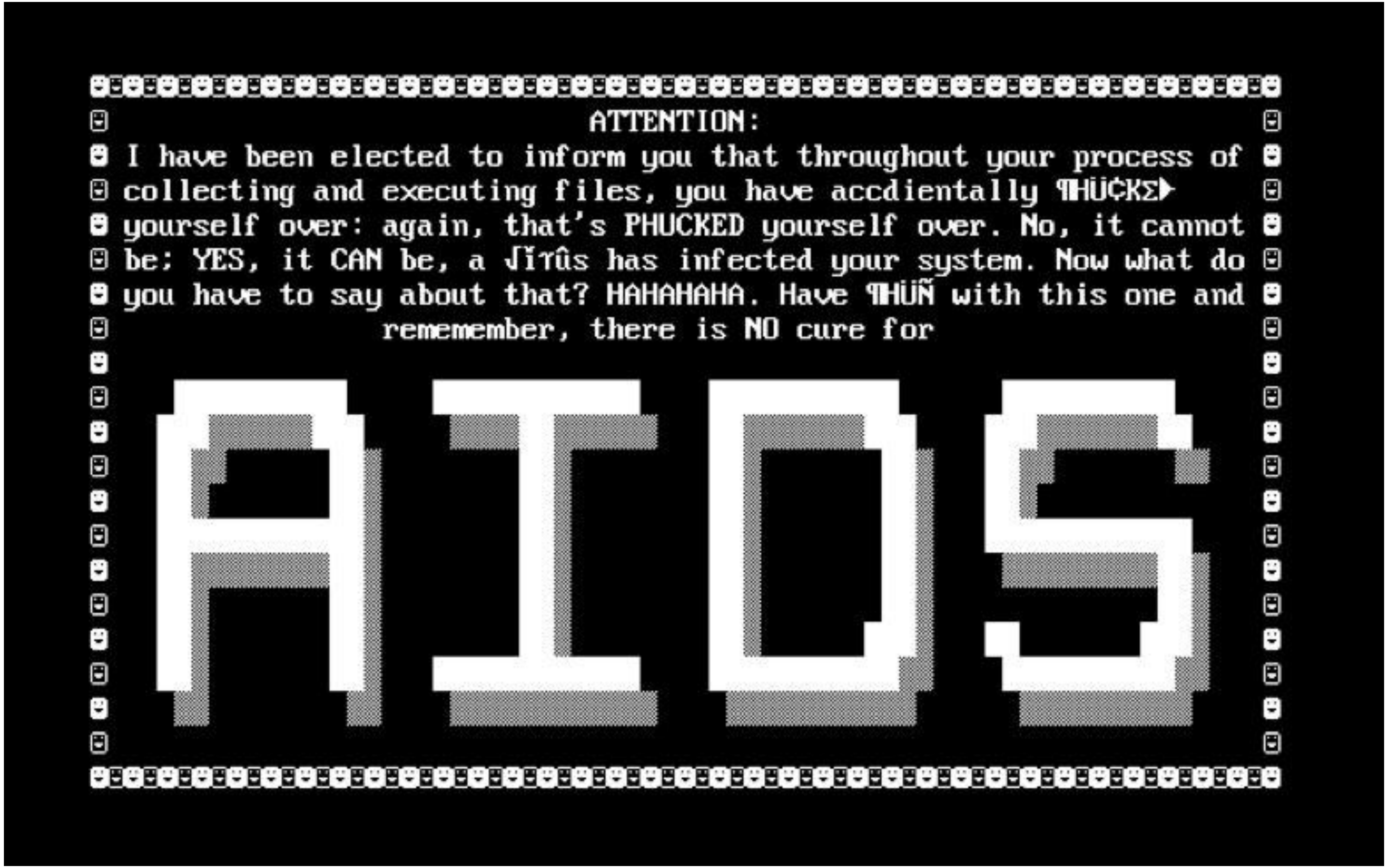
2015
PClock
Copycat ransomware, pretending to be CryptoLocker

TeslaCrypt
Goes after online gaming save files

2016
KeRanger
First targeting OS X®

Locky
Delivered via Microsoft® word documents

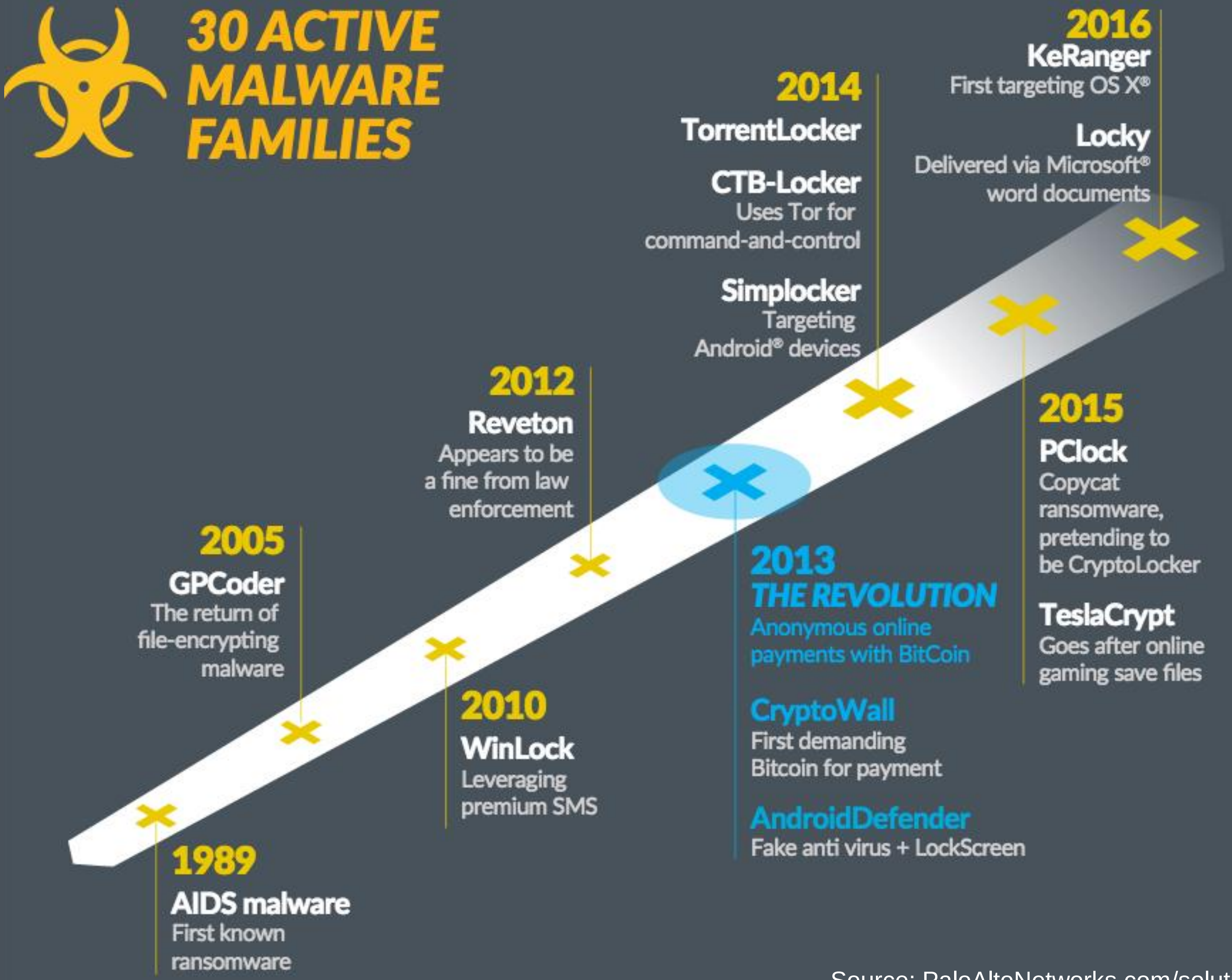
Source: PaloAltoNetworks.com/solutions/initiatives/ransomware



```
                             ATTENTION:
I have been elected to inform you that throughout your process of
collecting and executing files, you have accdientally ¶HÜ¢KΣ►
yourself over: again, that's PHUCKED yourself over. No, it cannot
be; YES, it CAN be, a √ïτûs has infected your system. Now what do
you have to say about that? HAHAHAHA. Have ¶HÜÑ with this one and
               rememember, there is NO cure for

                           AIDS
```

30 ACTIVE MALWARE FAMILIES



1989
AIDS malware
First known ransomware

2005
GPCoder
The return of file-encrypting malware

2010
WinLock
Leveraging premium SMS

2012
Reveton
Appears to be a fine from law enforcement

2013
THE REVOLUTION
Anonymous online payments with BitCoin

CryptoWall
First demanding Bitcoin for payment

AndroidDefender
Fake anti virus + LockScreen

2014
TorrentLocker

CTB-Locker
Uses Tor for command-and-control

Simplocker
Targeting Android® devices

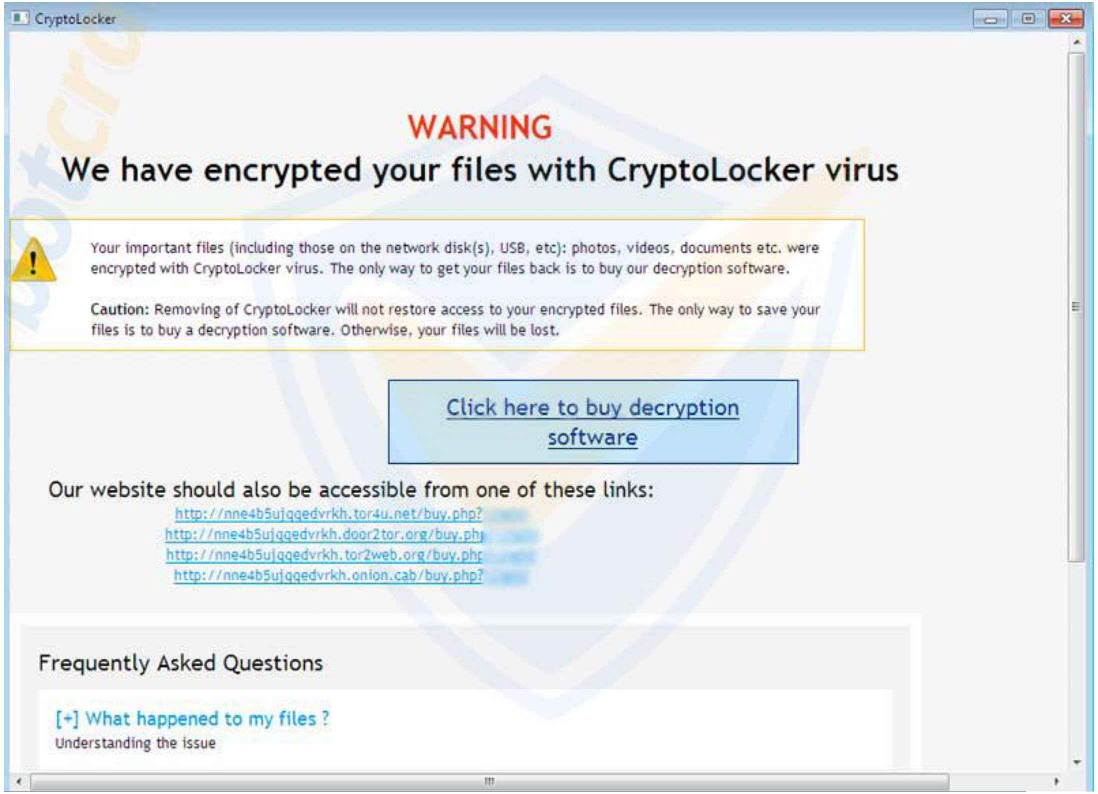
2015
PClock
Copycat ransomware, pretending to be CryptoLocker

TeslaCrypt
Goes after online gaming save files

2016
KeRanger
First targeting OS X®

Locky
Delivered via Microsoft® word documents

Source: PaloAltoNetworks.com/solutions/initiatives/ransomware



WARNING

We have encrypted your files with CryptoLocker virus

Your important files (including those on the network disk(s), USB, etc): photos, videos, documents etc. were encrypted with CryptoLocker virus. The only way to get your files back is to buy our decryption software.

Caution: Removing of CryptoLocker will not restore access to your encrypted files. The only way to save your files is to buy a decryption software. Otherwise, your files will be lost.

Click here to buy decryption software

Our website should also be accessible from one of these links:

http://nne4b5ujqqedvrkh.tor4u.net/buy.php?[redacted]
http://nne4b5ujqqedvrkh.door2tor.org/buy.php[redacted]
http://nne4b5ujqqedvrkh.tor2web.org/buy.php[redacted]
http://nne4b5ujqqedvrkh.onion.cab/buy.php?[redacted]

Frequently Asked Questions

[+] What happened to my files ?
Understanding the issue

CYBER THREAT ALLIANCE

CryptoWall v3 Investigation

Co-Founded by

Palo Alto Networks

Intel Security

Symantec

Fortinet

$325M

Estimated Damages Across the Globe

44%

Victims Paid Up

30.7%

Exploit Delivery

Source: http://go.paloaltonetworks.com/cryptowall

Mini-Survey

Do you think your Anti-Virus product can **prevent** Ransomware attacks?

To Prevent Ransomware:

1. **Attack Vectors**
2. **Delivery Methods**

1. Attack Vectors

Exploits

Macros

Exec

2. Delivery Methods

Exploit Kits

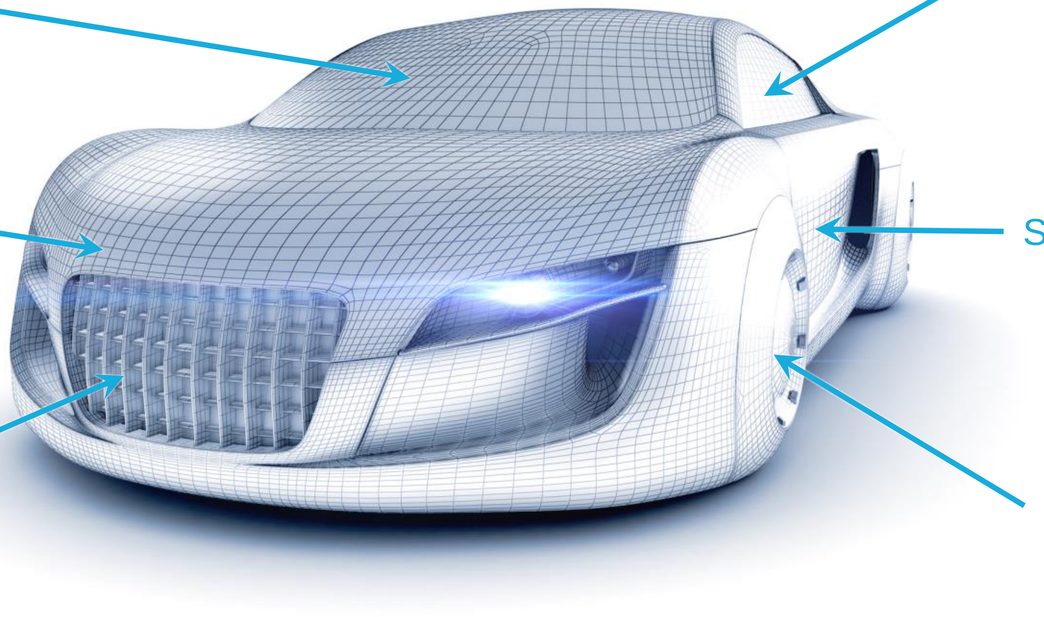
Email Attachments

Drive-by Downloads

Mini-Survey

Do you think your Anti-Virus product can block **unknown malware** and **unknown exploits**?

Prevention Requires a Combination of Multiple Purpose-built Methods



Safety Glass

Airbags

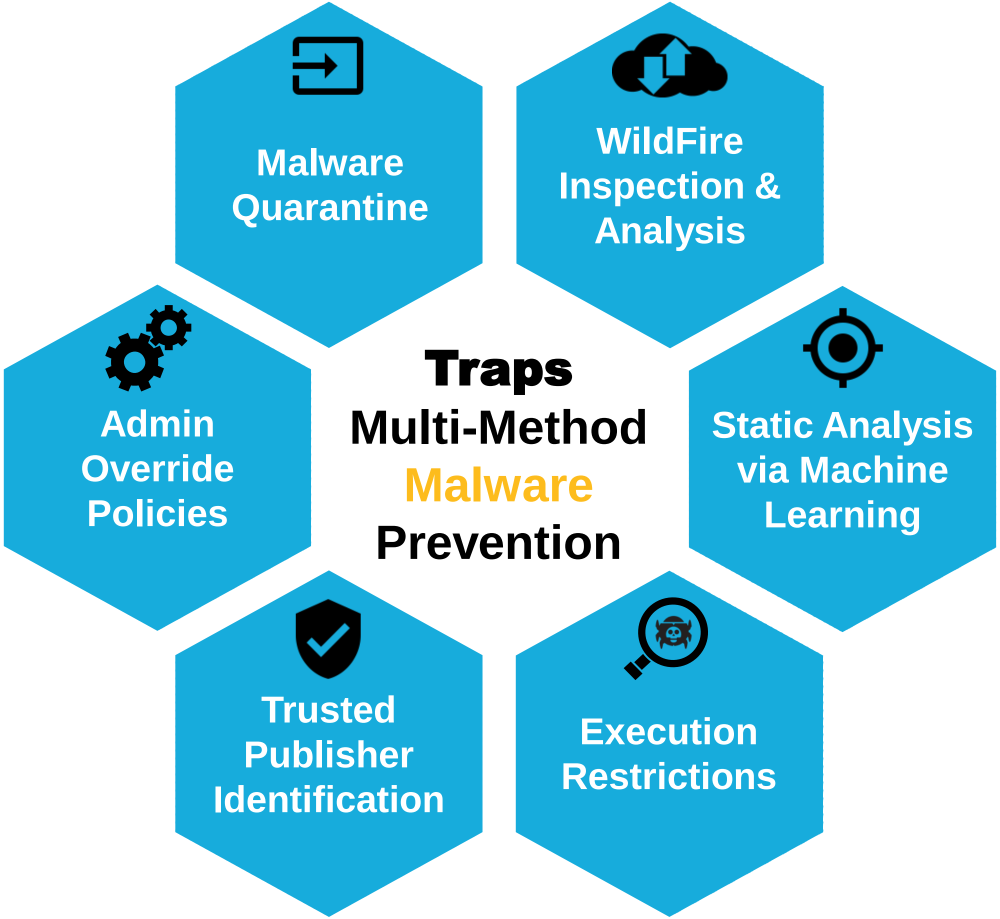
Crumple Zone

Side Impact Bars

Collision Avoidance System

Traction Control System

Traps Multi-Method Malware Prevention



Traps Multi-Method Malware Prevention

Malware Quarantine

WildFire Inspection & Analysis

Static Analysis via Machine Learning

Execution Restrictions

Trusted Publisher Identification

Admin Override Policies

Traps Multi-Method Exploit Prevention

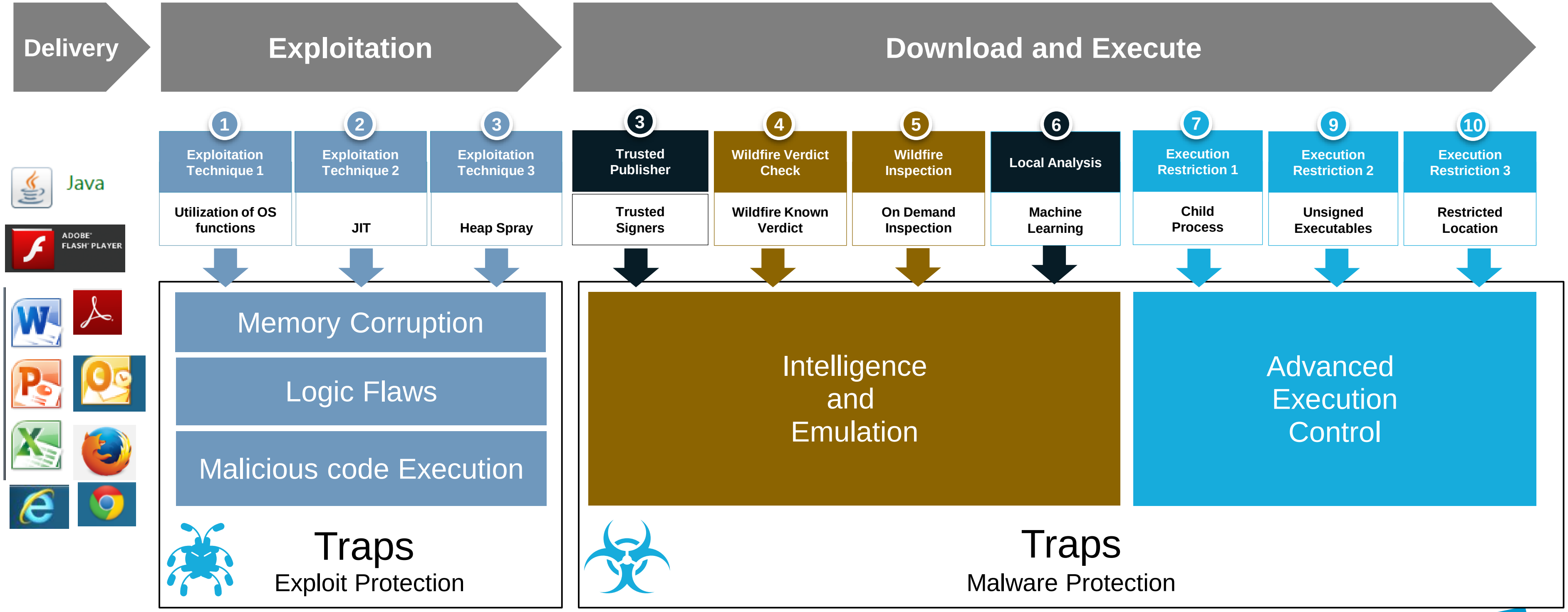
Memory Corruption Prevention

Logic Flaw Prevention

Malicious Code Execution Prevention

Demo

Traps Kill-Points Through the Attack Life Cycle



Delivery → Exploitation → Download and Execute

	Exploitation			Download and Execute						
	1	2	3	3	4	5	6	7	9	10
	Exploitation Technique 1	Exploitation Technique 2	Exploitation Technique 3	Trusted Publisher	Wildfire Verdict Check	Wildfire Inspection	Local Analysis	Execution Restriction 1	Execution Restriction 2	Execution Restriction 3
	Utilization of OS functions	JIT	Heap Spray	Trusted Signers	Wildfire Known Verdict	On Demand Inspection	Machine Learning	Child Process	Unsigned Executables	Restricted Location

Memory Corruption

Logic Flaws

Malicious code Execution

Traps
Exploit Protection

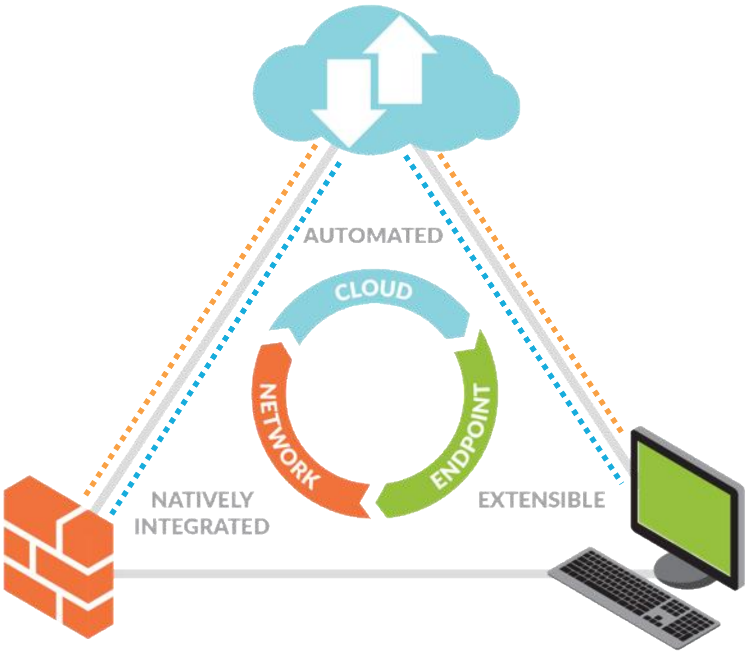
Intelligence
and
Emulation

Advanced
Execution
Control

Traps
Malware Protection

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

WildFire Threat
Intelligence Cloud



Next-Generation
Firewall

Traps Advanced
Endpoint Protection

······ Intelligence Collection

······ Prevention Capabilities

THANK YOU

paloalto NETWORKS®