

'Traditional firewalls and endpoint solutions are waste of money against ransomware - what's needed?'

Jari Hemminki
Major Account Manager
jhemminki@paloaltonetworks.com

@Stallion 911



History of Ransomware

Dear Customer:

It is time to pay for your software lease from PC Cyborg Corporation. Complete the INVOICE and attach payment for the lease option of your choice. If you don't use the printed INVOICE, then be sure to refer to the important reference numbers below in all correspondence. In return you will receive:

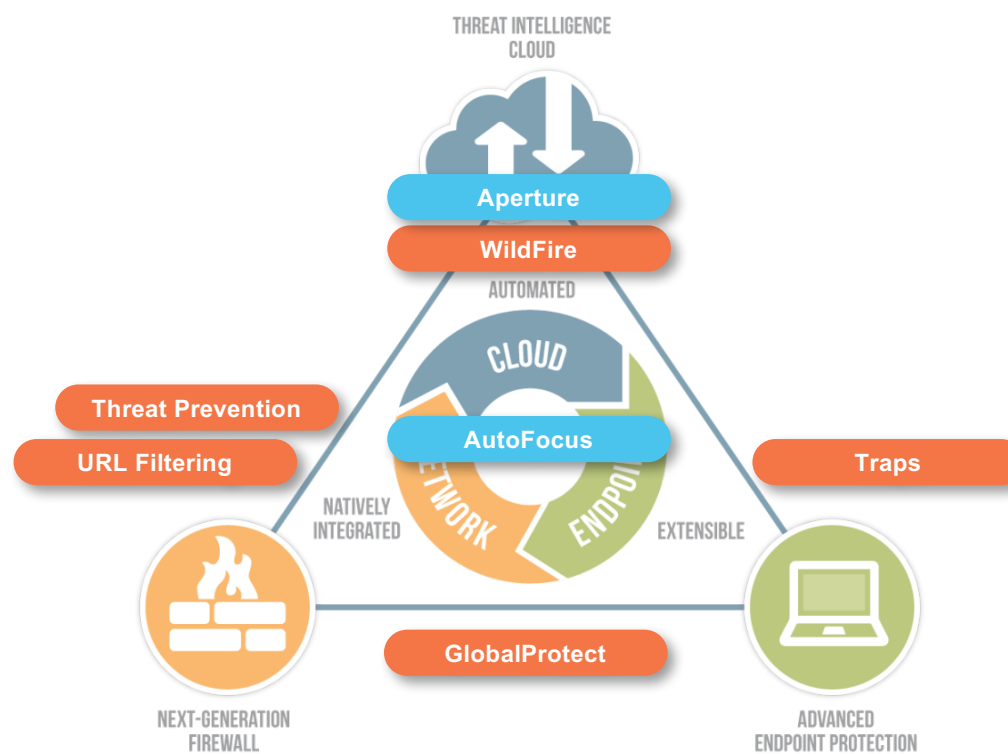
- a renewal software package with easy-to-follow, complete instructions;
- an automatic, self-installing diskette that anyone can apply in minutes.

Important reference numbers: A5599796-2695577-

The price of 365 user applications is US\$189. The price of a lease for the lifetime of your hard disk is US\$378. You must enclose a bankers draft, cashier's check or international money order payable to PC CYBORG CORPORATION for the full amount of \$189 or \$378 with your order. Include your name, company, address, city, state, country, zip or postal code. Mail your order to PC Cyborg Corporation, P.O. Box 87-17-44, Panama 7, Panama.

Press ENTER to continue

Next Gen Security Platform Approach= State of the Art



User picks up the email from junk email

Kuriren Har Inte levererat Paketet

Vi har fått ditt paket **CT8380159SE** på **2016/01/29**. Courier inte leverera detta paket till dig.

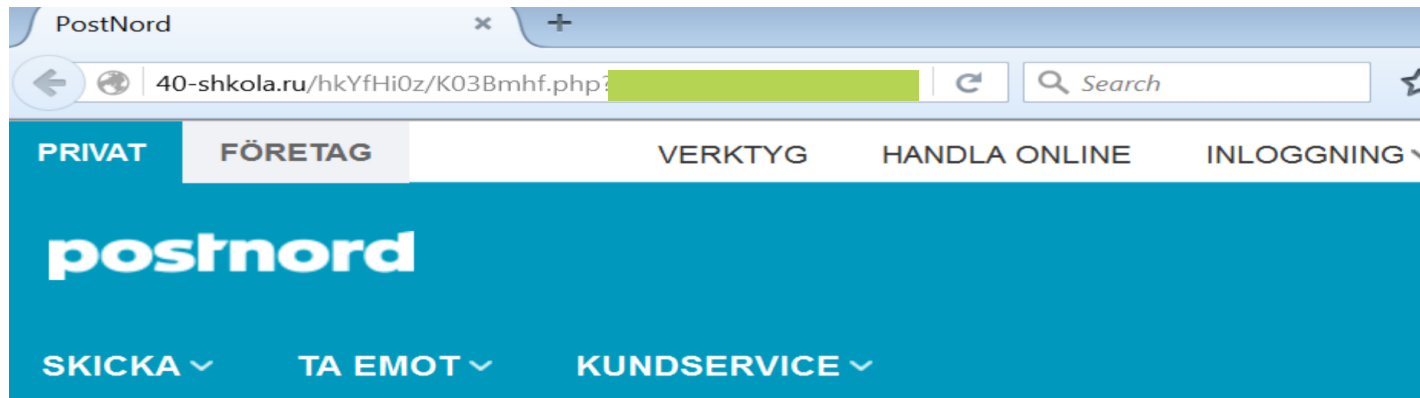
Skriv ut fraktetikett och visa den på närmaste postkontor för att få ditt paket.

Få fraktetikett

Om paketet inte kommer att tas emot inom 16 arbetsdagar, har Postnord rätt att kräva ersättning från dig - 64 kronor för varje dag för paketet lagring. Du kan hitta information om förfarandet och villkoren för paketet lagring i närmaste kontor.

Detta är ett automatiskt meddelande. [Klicka här](#) för att avregistrera.

Behind the link is “captcha”



Ladda ner och skriva ut fraktsedel

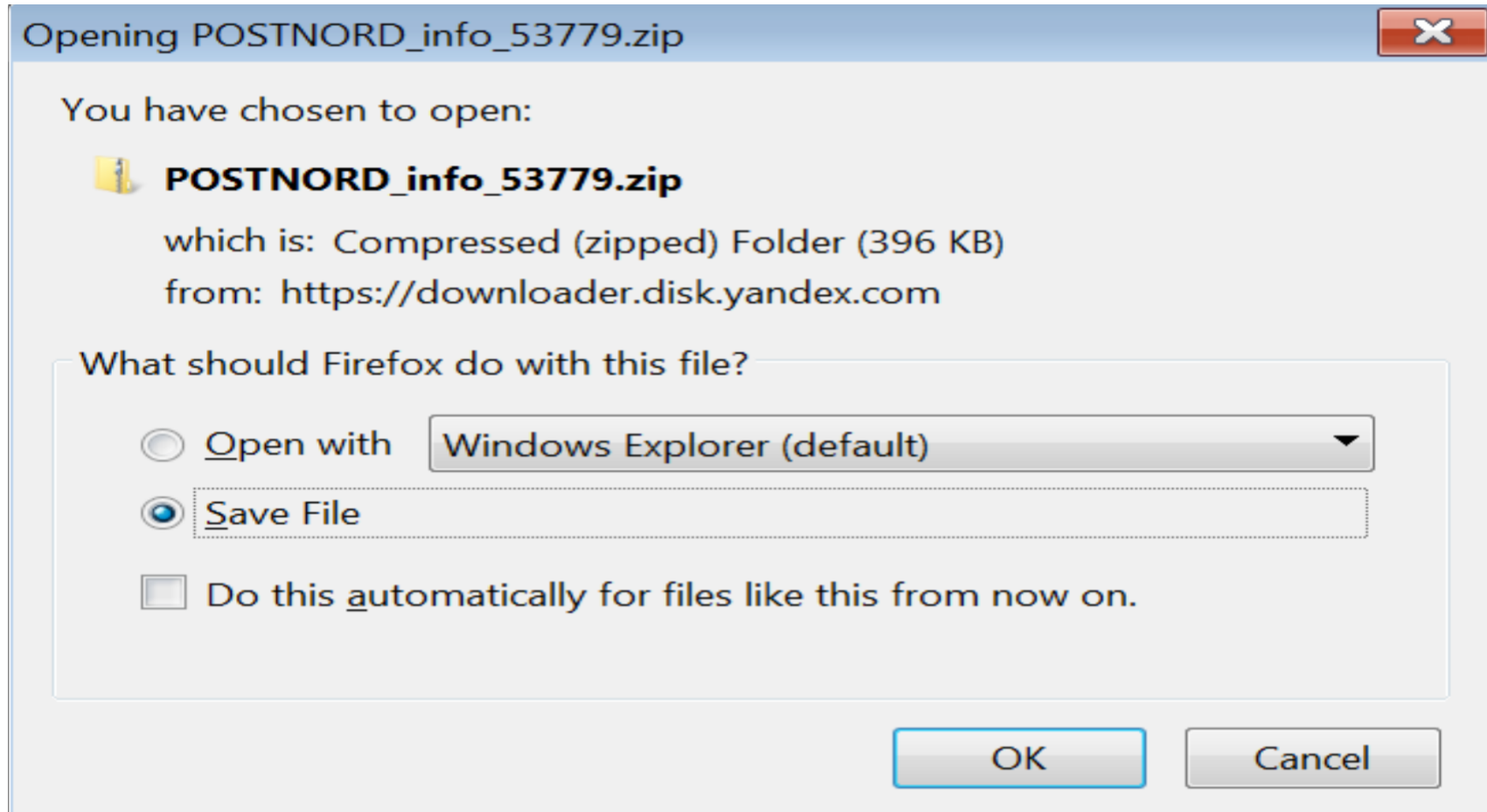


Ladda ner och skriva ut fraktsedel (PDF) och visa den på närmaste postkontor för att få paketet.


764674

HÄMTA FRAKTSEDEL

Download a .zip



Which contains a “pdf” looking document

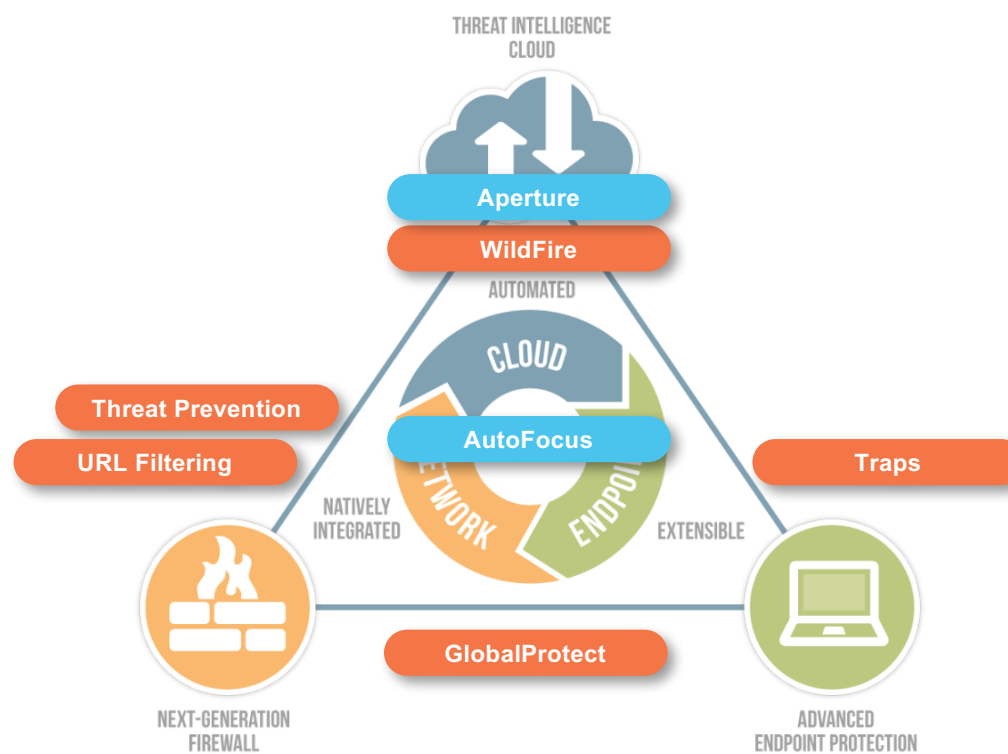
Name	Date modified	Type	Size
 POSTNORD_info_53779	2/4/2016 1:38 PM	Application	524 k

EK = Exploit Kit = “malware delivery platform”

- Angler
- Rig
- Sweet-Orange
- Magnitude
- Nuclear
- Hanjuan
- Neutrino
- Fiesta
- Hunter
- Kaixin
- ...

So what? The user doesn't have to do anything wrong

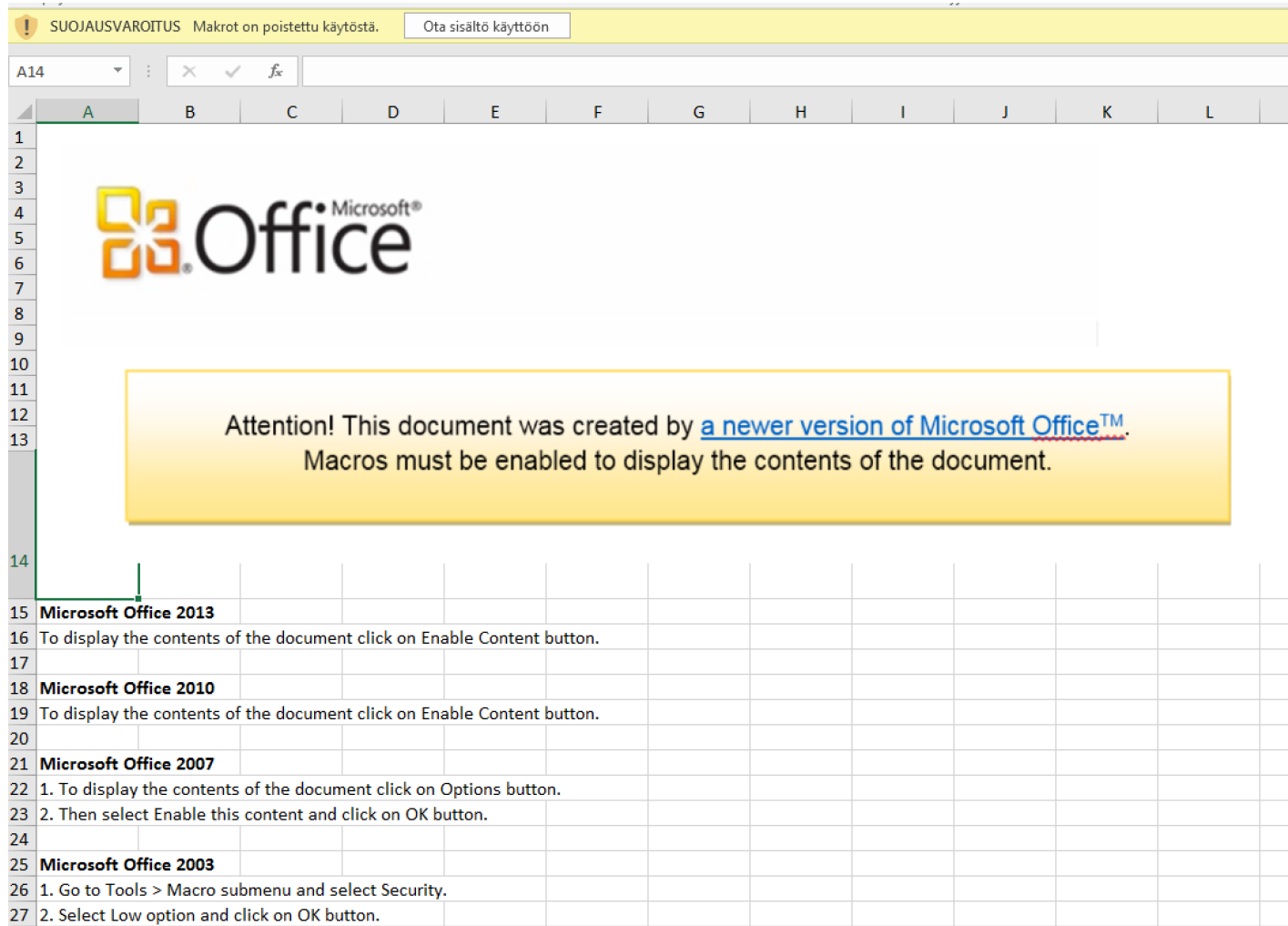
Next Gen Security Platform Approach= State of the Art



Quick check list for firewalling

- Do You decrypt SSL?
- Do You scan all the traffic for malware, C&C, and exploits?
- Do You scan all the traffic for applications? Are You blocking unwanted applications (such as ToR)?
- Are You warning users about PE downloads happening in the back?
- Are You blocking executable (and script) downloads from at least dyn-dns, or unknown URLs?

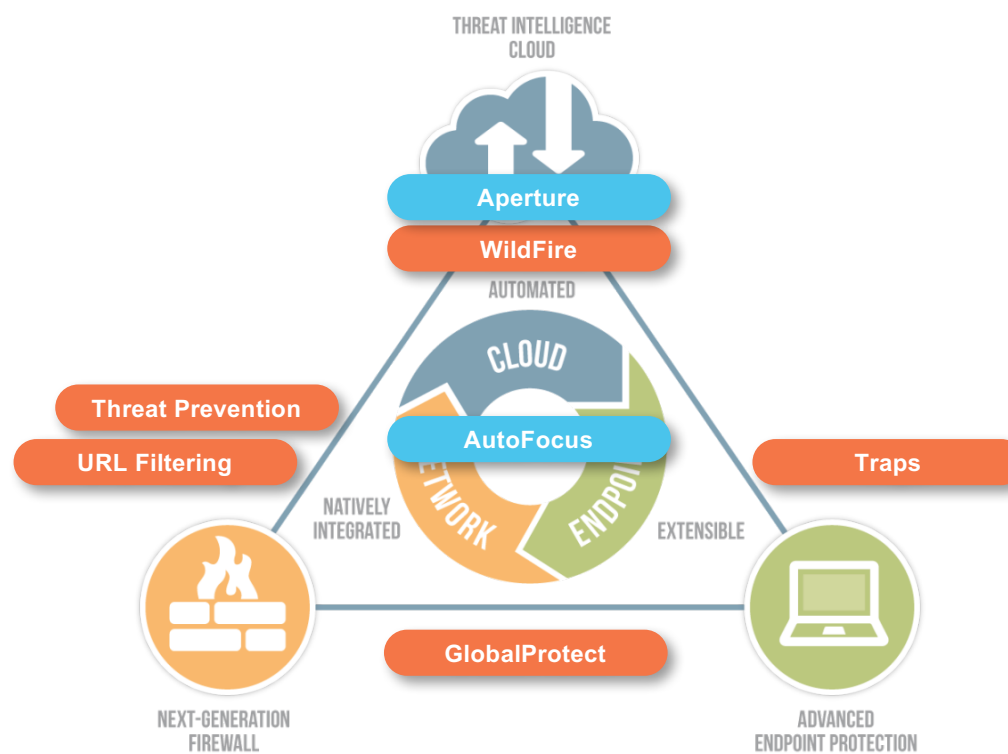
Macro based delivery



How to bypass sandboxes and other network level threat prevention systems

- ACME corp. employee receives an excel spreadsheet from a seemingly trusted source
- Against instructions he enables macros “to see full content”
- Macro runs and downloads a script to the computer
- Script starts and downloads obfuscated malware and helper files
 - Uses the helper files to de-obfuscate the malware
- The revealed exe starts and checks the internet for a specific web page to be up.
 - If the site is down or the page at site is wrong (hash) the malware will start to poll the site periodically.
 - If the site is up and the hash is correct the malware will then connect to the C&C infrastructure.

Next Gen Security Platform Approach= State of the Art



Exploits vs. Malicious Executables

A Critical Distinction

Exploit

- Malformed data file
- Processed by a legitimate application
- Exploits a vulnerability in the legitimate application to allow the attacker to execute code



Malicious Executable

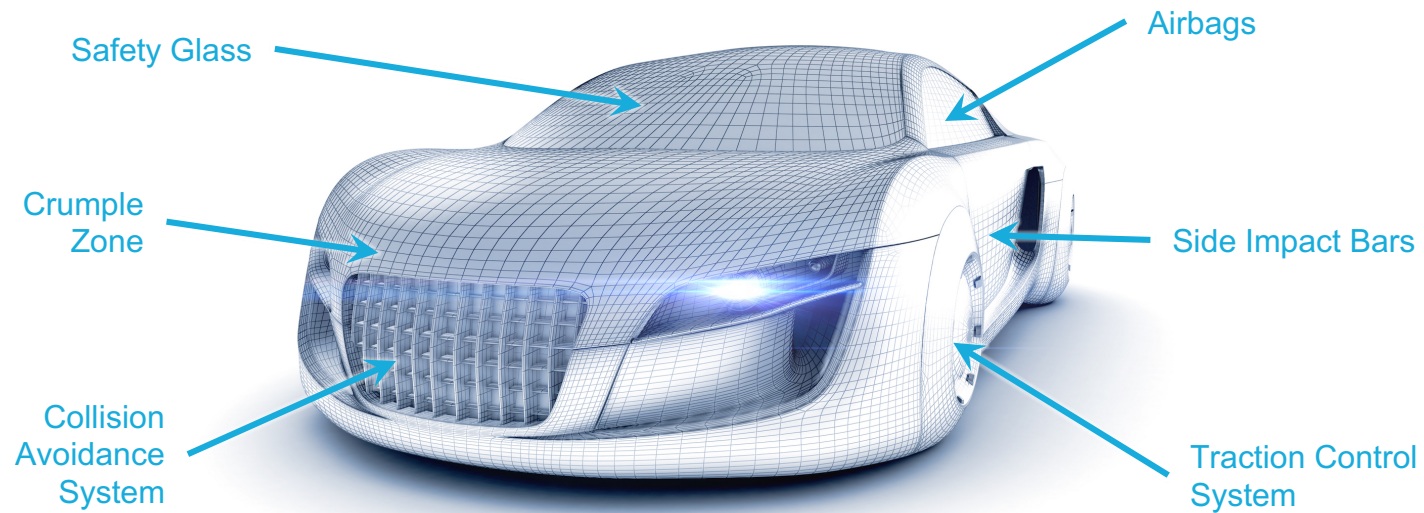
- Malicious code
- Does not rely on application vulnerabilities
- Contains executable code



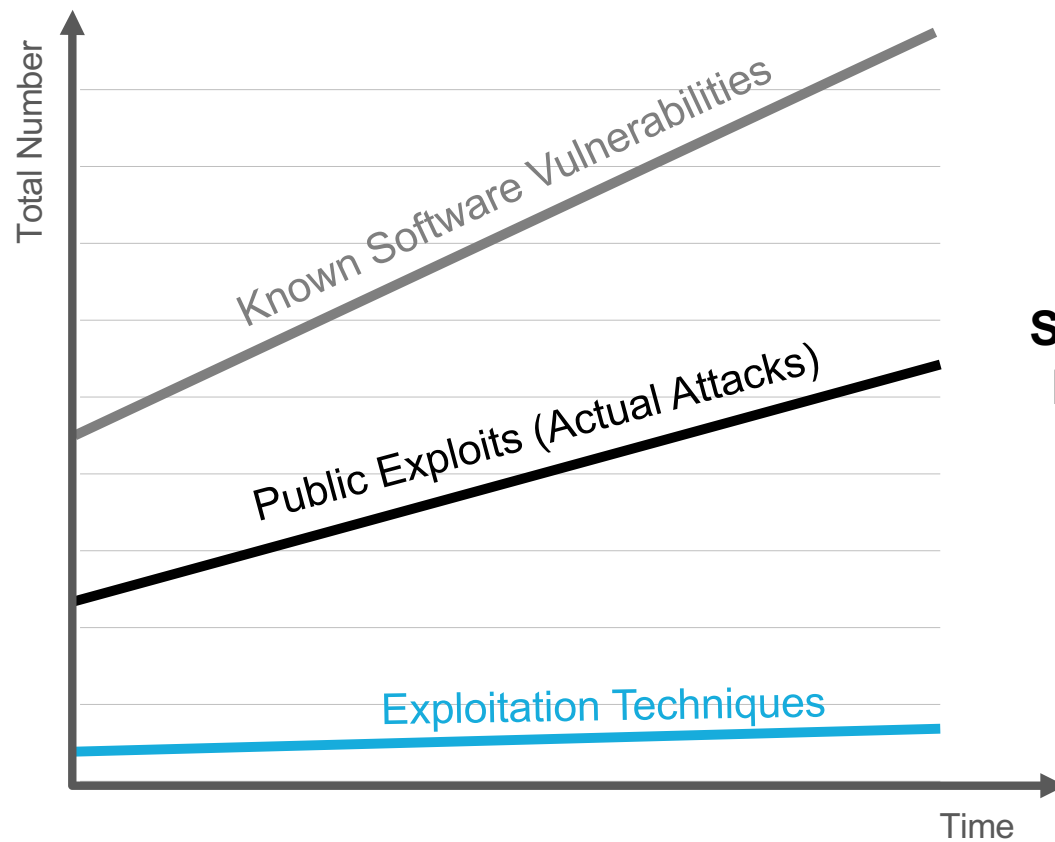
**“Next Gen” Anti-Malware Solutions
Signature-based AV**

Palo Alto Networks Traps

Prevention Requires a Combination of Multiple Purpose-built Methods



Blocking the usage of core exploitation techniques



Patching

Requires Prior Knowledge,
Proactive Application

**Signature /
Behavior**

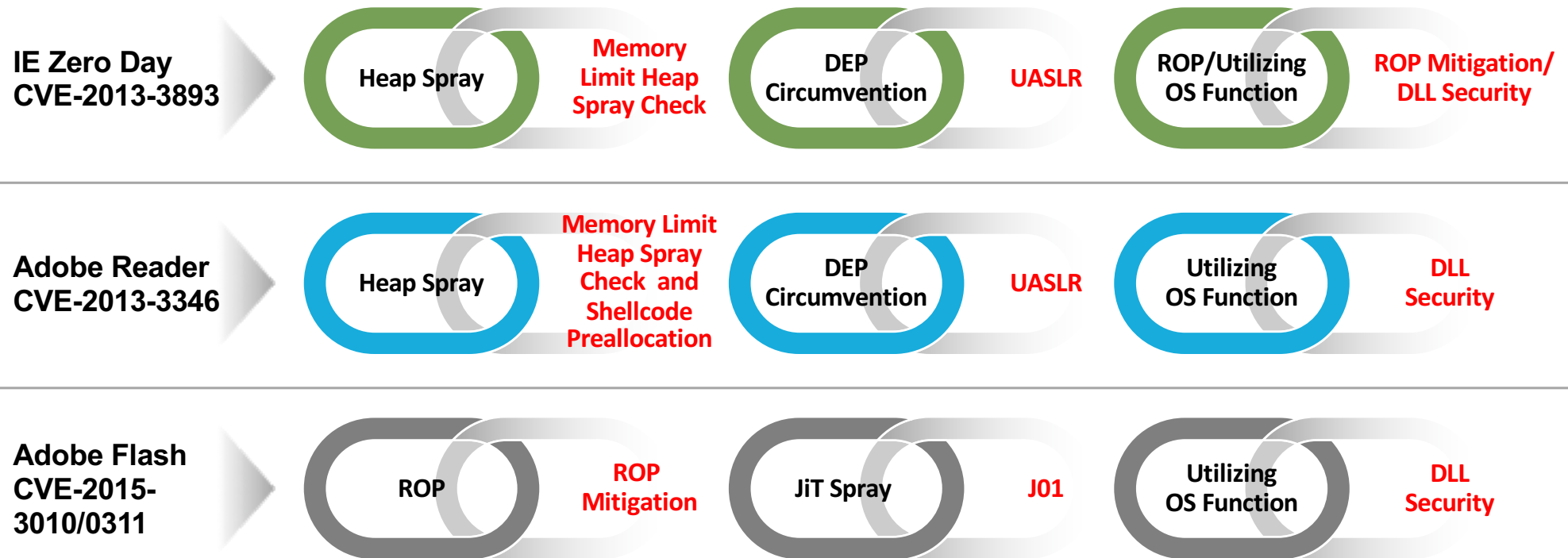
Requires Prior Knowledge
of Weaponized Exploits

Traps

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

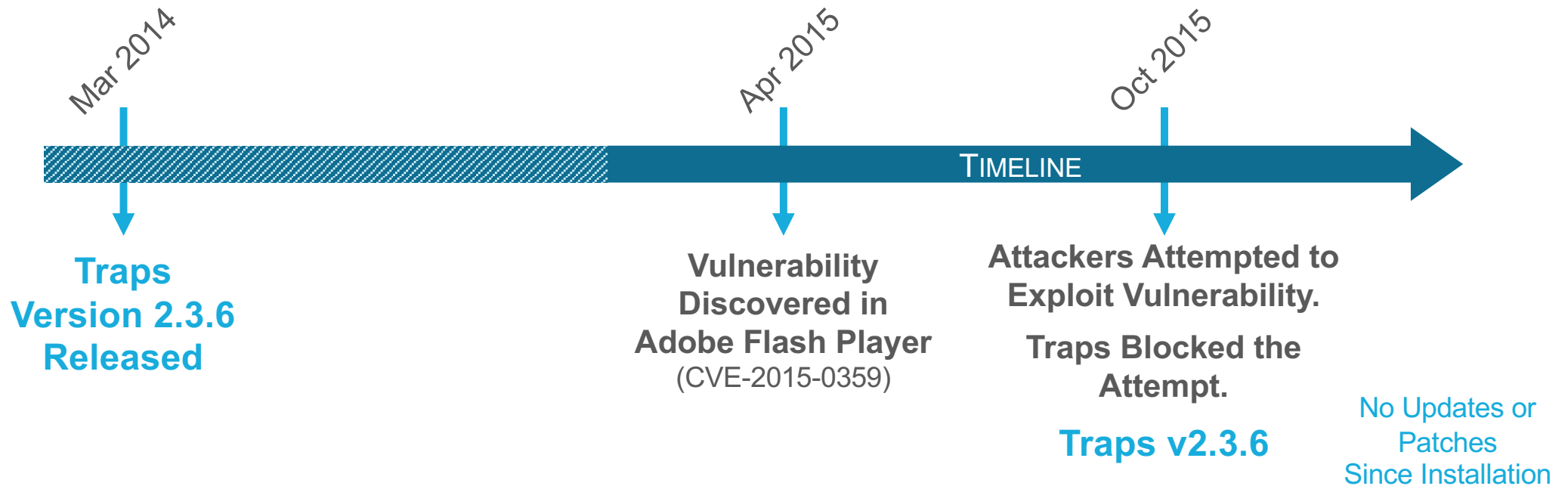
Exploit Prevention Case Study

Unknown Exploits Utilize Known Techniques



Prevention of One Technique in the Chain will Block the Entire Attack

Example: Traps blocking “unknown” vulnerability



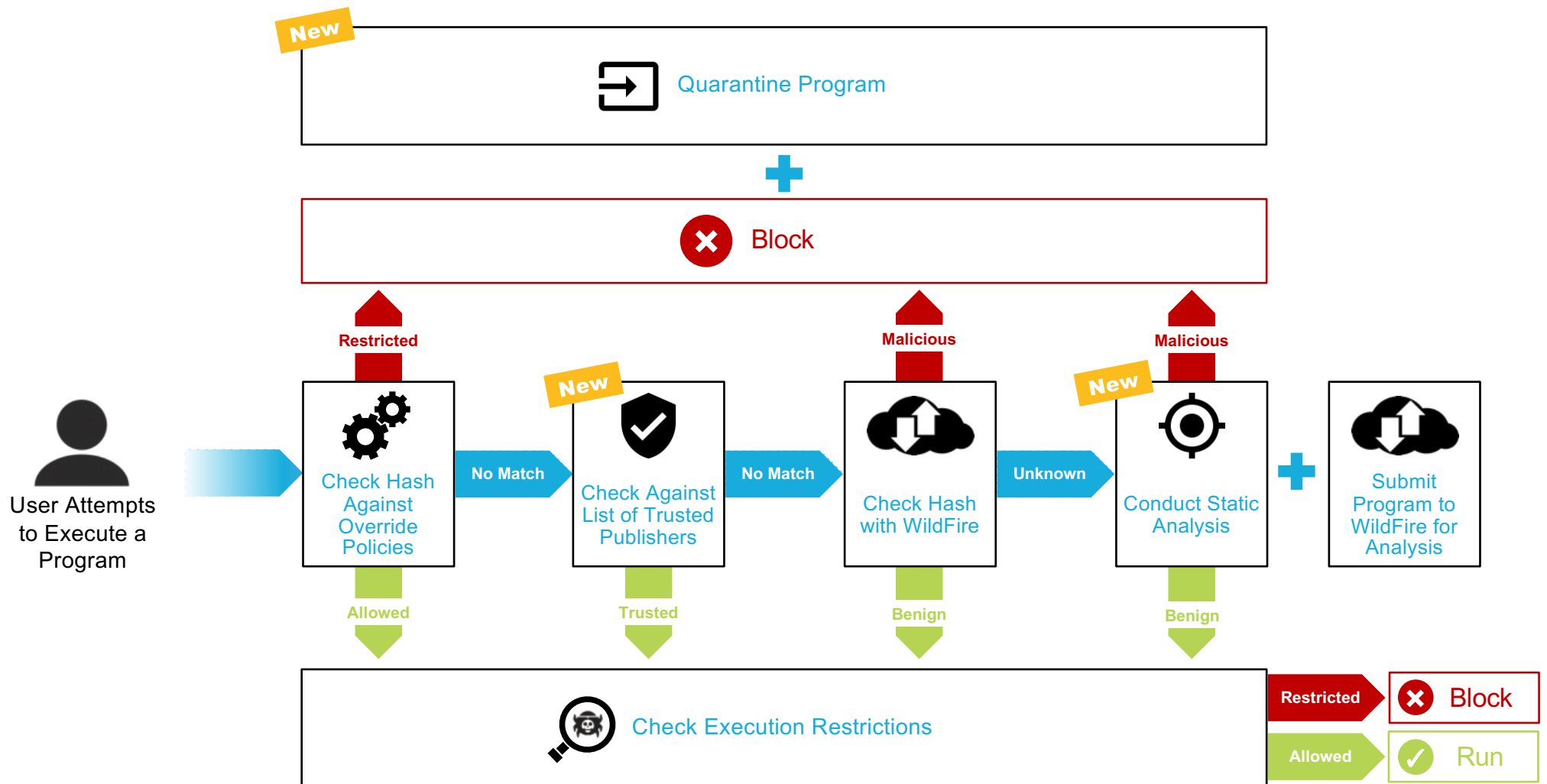
Traps Prevents Zero-day and Unknown Exploits That Have Yet to be Discovered

Traps vs. Top 10 Zero-Day Exploits of 2015

Discovery Date	Application	Exploit Identifier	Did Traps Block <u>Zero-Day</u> 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	✓

Source: Palo Alto Networks. Go.PaloAltoNetworks.com/2015ZeroDays





Protected with Traps

Traps Prevention Alert

Traps has detected a suspicious activity!

Application name: Spheres Knowing Foundation Uplo...

Application publisher: **Outerspace Software (unverified)**

Prevention description: Attempted execution of unsigned r...

Hide details OK

6.1.7601.2.1.0.256.1
Unsigned executables
80400039
Attempted execution of unsigned restricted executable

For additional information contact your system administrator

Traps Prevention Alert

Traps has detected a suspicious activity!

Application name: Spheres Knowing Foundation Uplo...

Application publisher: **Outerspace Software (unverified)**

Prevention description: Attempted execution from a restri...

Hide details OK

11:24:00 AM
6.1.7601.2.1.0.256.1
Execution protection
8040002e
Attempted execution from a restricted folder

For additional information contact your system administrator

20

21 **Microsoft Office 2007**

22 1. To display the contents of the document click on Options button.

23 2. Then select Enable this content and click on OK button.

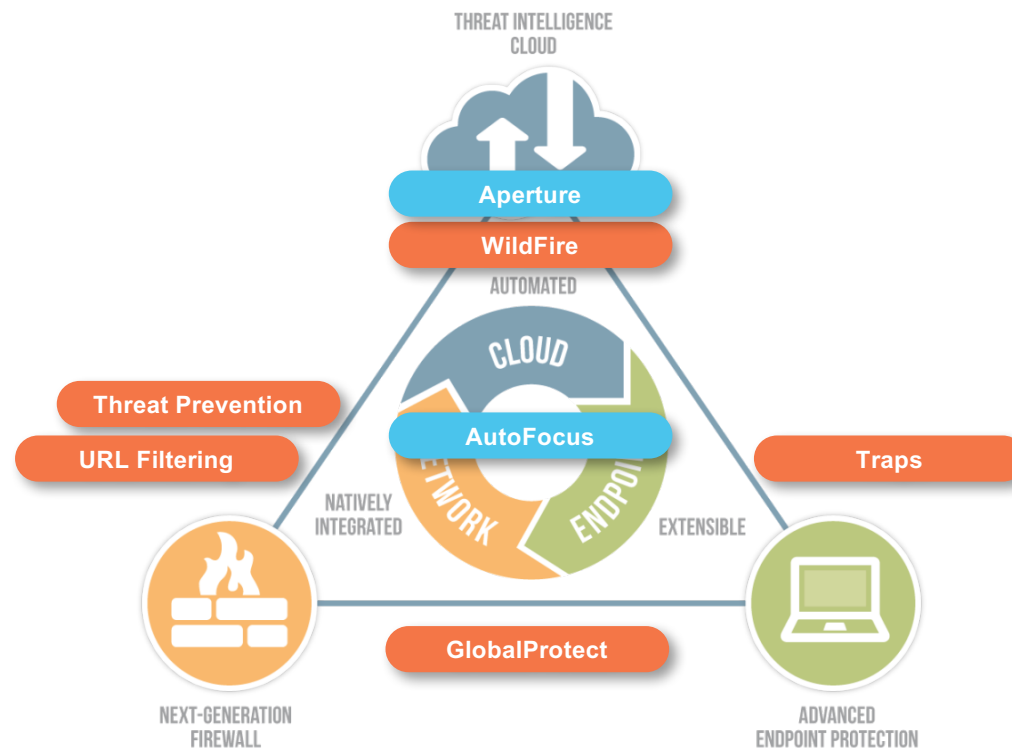
24

25 **Microsoft Office 2003**

26 1. Go to Tools > Macro submenu and select Security.

27 2. Select Low option and click on OK button.

Approach that works : Security Platform



(even the partial platform works for its purpose = You can buy Traps or FWs as separate solutions)

***Preventing ransomware is
not just possible, with Palo
Alto Networks it is likely.***

Thank You

jhemminki@paloaltonetworks.com