

HOW TO (EFFECTIVELY) PREVENT RANSOMWARE INFECTIONS

RE-THINKING SECURITY ARCHITECTURE

Speaker: Brook Lin (林揚城)

GC Channel Consultant



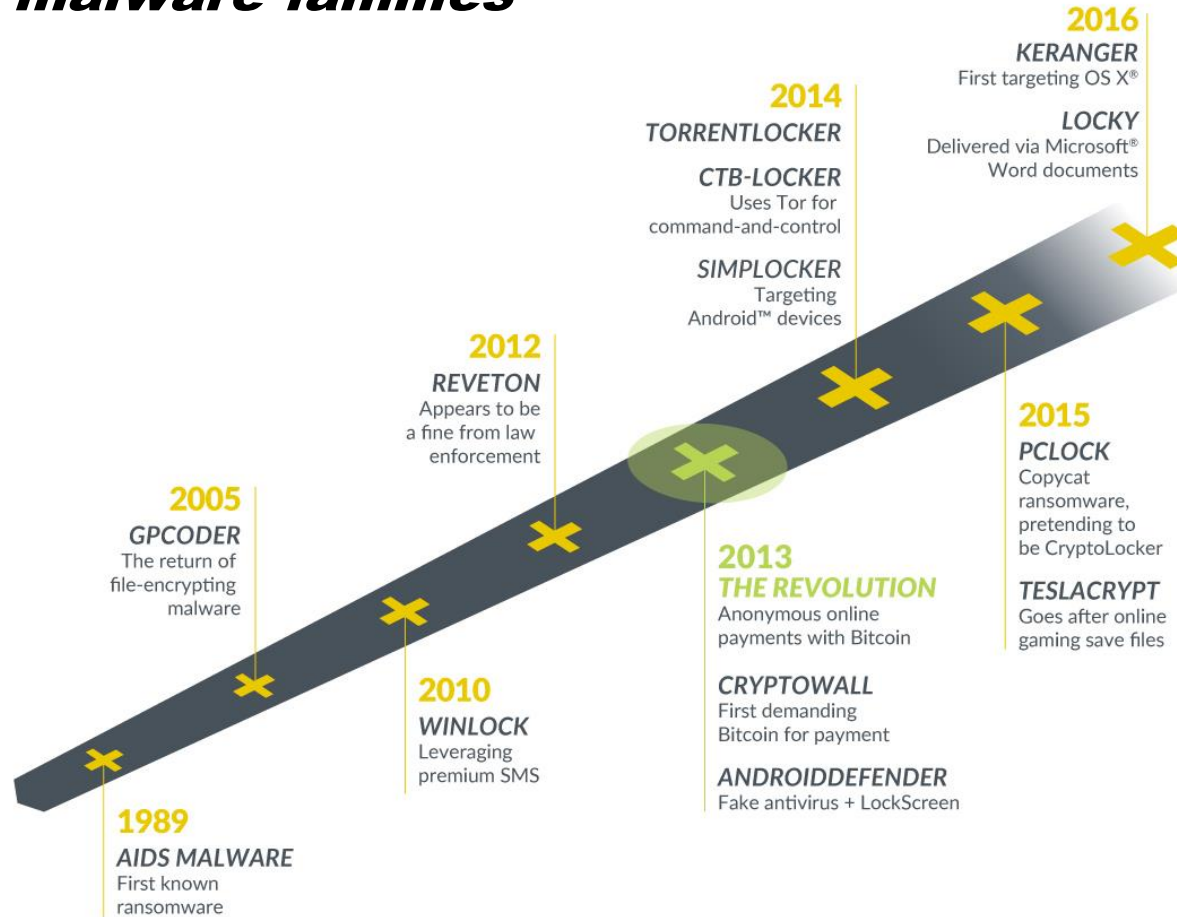
“攻擊鏈” — 勒索軟體**Attack Kill-chain** 解析 (多型態惡意軟體&Botnet)

“攻擊鏈”



任何一個環節的阻擋都可以破解攻擊鏈

30 active malware families



Ransomware today

CryptoLocker Your Personal files are encrypted! English



Your personal files **encryption** produced on this computer: photos, videos, documents, etc. Encryption was produced using a **unique public key RSA-2048 generated for this computer**.

To decrypt files you need to obtain the **private key**.

The **single copy** of the private key, which will allow to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that **nobody and never** will be able to restore files.

To obtain the private key for this computer, which will automatically decrypt files, you need **pay 1 Bitcoin (~225 USD)**.

You can easily delete this software, but you must know that without it, you will never be able to get your original files back.

Disable your antivirus to prevent the removal of this software.

For more information on how to buy and send bitcoins, click 'Pay with Bitcoin'. To open a list of encoded files, click 'Show Files'.

Do not delete this list, it will be used for decryption. And do not move your files.

Private key will be destroyed on 2015-05-06 20:46:06

Time left **167:49:22**

Received: 0.00 BTC
Checking wallet...

al files are encrypted by CTB-Locker

databases and other important files have been encrypted with strong encryption generated for this computer.

tored on a secret Internet server and nobody can decrypt your files without a private key.

submit the payment. If you do not send money within provided time, your files will be crypted and no one will be able to recover them.

t of files that have been encrypted.

ge.


Your files are encrypted

To get the key to decrypt files you have to pay **750 USD/EUR**. If payment is not made before decrypting files will increase 2 times and will be **1500 USD/EUR**.

Prior to increasing the amount left:
42h 48m 35s

WARNING

We have encrypt 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://crlh1mefvgal1fw.torcs.net/buy.php?21mmjd>
- <http://crlh1mefvgal1fw.dns2tor.org/buy.php?21mmjd>
- <http://crlh1mefvgal1fw.tor2web.org/buy.php?21mmjd>
- <http://crlh1mefvgal1fw.onion.cab/buy.php?21mmjd>

Frequently Asked Questions

Your system: Windows 7 (x64) First connect IP: 192.168.1.1 Total

[Refresh](#) [Payment](#) [FAQ](#) [Decrypt 1 file for FREE](#) [Support](#)

are present a special software - CryptoWall Decrypter - which is allow to decrypt and remove the private key.

How to buy CryptoWall decrypter?

 **bitcoin**

You should register Bitcon wallet ([click here for more information with picture](#))

Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.

Here are our recommendations:

We present a special software - **Lucky Decrypter** - which allows to decrypt and return control to all your encrypted files.

How to buy Lucky decrypter?

1. You can make a payment with BitCoins, there are many methods to get them.
2. You should register BitCoin wallet (simplest online wallet OR some other methods of creating wallet)
3. Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.

Here are our recommendations:

- [LocalBitcoins.com \(WU\)](#) - Buy Bitcoins with Western Union
- [Coincave.com](#) - Recommended for fast, simple service.


T E S L A C R Y P T

All your important files are encrypted.

At the moment, the cost of private key for decrypting your files is 1.5 BTC → 415 USD.

README_FOR_DECRYPT.txt

Your computer has been locked and all your files has been encrypted with 2048-bit RSA encryption.

Instruction for decrypt:

1. Go to  IF NOT WORKING JUST DOWNLOAD TOR BROWSER AND OPEN THIS LINK:  has your ID for authentication
2. Use  for decryption pack using bitcoins (wallet is your ID for authentication - )
3. Pay 1 BTC (~410.63\$) for decryption pack using bitcoins (wallet is your ID for authentication - )
4. Download decrypt pack and run

---> Also at  you can decrypt 1 file for FREE to make sure decryption is working.

Also we have ticket system inside, so if you have any questions - you are welcome.
We will answer only if you able to pay and you have serious question.

IMPORTANT: WE ARE ACCEPT ONLY(!!) BITCOINS

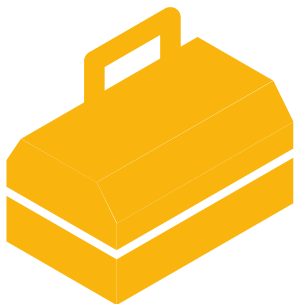
HOW TO BUY BITCOINS:
<https://localbitcoins.com/guides/how-to-buy-bitcoins>
[https://en.bitcoin.it/wiki/Buying_Bitcoins_\(the_newbie_version\)](https://en.bitcoin.it/wiki/Buying_Bitcoins_(the_newbie_version))



Ransomware today

- Multiple cryptovariants exist today, riding off the success of CryptoLocker
- Use of different attack vectors, such as malicious macros and exploit kits
- More sophisticated tactics, such as using anonymous networks like TOR or I2P for command and control, CAPTCHAs for limited access to payment systems, and language localization efforts
- Attacks are largely victim agnostic
- Multiple platforms targeted, including Android and OS X
- **Ransomware as a Service** now exists

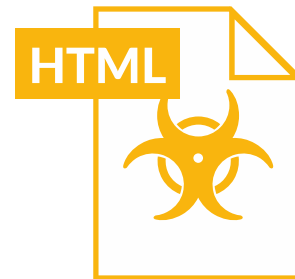
How does ransomware get in?



EXPLOIT KITS



**MALICIOUS EMAIL
ATTACHMENTS**



**MALICIOUS LINKS
IN EMAILS or YOUR Social
Networking!**

Infected website or malicious ad via exploit kit



STEP 1

User visits compromised website, which is often a trusted location.



STEP 2

Malicious code redirects to exploit kit landing page.

OR

Malicious advertisement silently redirects to malicious web page.



STEP 3

Exploit kit web page loads and determines best route to infect user.



STEP 4

Exploit kit takes advantage of **vulnerable software**.



STEP 5

Exploit kit delivers ransomware payload.



STEP 6

Victim's sensitive files are encrypted and held for ransom.

Compromised Microsoft Word document



STEP 1

Targeted email with infected Microsoft® Office Word document delivered to user.



STEP 2

User opens Word document, thinking it is a legitimate file.



STEP 3

Office macros run, downloading ransomware from URLs within the document.



STEP 4

Victim's sensitive files are encrypted and held for ransom.

Ransomware attack vectors



OVER THE NETWORK

Infection vectors like web and email



SAAS-BASED APPLICATIONS

File-sharing applications



DIRECTLY TO THE ENDPOINT

Off-premise or targeted attack

IT relevant, coordinated security, prevention oriented platform



Automatically turn unknown threats to known

Reprogram the network with new protections

Seek first to gain visibility and reduce the attack surface

1

Gain full visibility and
block unknown traffic

2


Enforce application and
user-based controls

3

Stop dangerous file-types

4

Implement endpoint policy
aligned to your risk



**REDUCE
THE ATTACK
SURFACE**

Prevent known threats

1 Stop known exploits, malware & command-and-control traffic

2 Block access to malicious and phishing URLs

3 Scan for known malware on SaaS-based applications

4 Block known malware & exploits on the endpoint



**PREVENT
KNOWN
THREATS**

Prevent unknown threats: Understand the power of context

1

Detect and analyze unknown threats in files and URL

2

Update the protections across the organization and prevent previously unknown threats

3

Add context to threats and create proactive protections and mitigation

4

Block unknown malware & exploits on the endpoint

**IDENTIFY
& BLOCK
UNKNOWN
THREATS**

Requirements for an integrated prevention platform (One Platform)

- 1 Be in the right position
- 2 Both virtual and physical
- 3 Best-of-breed security technologies
- 4 Multiple detection techniques
- 5 Global Analysis and threat knowledge
- 6 Control all, with the ability to reprogram in seconds

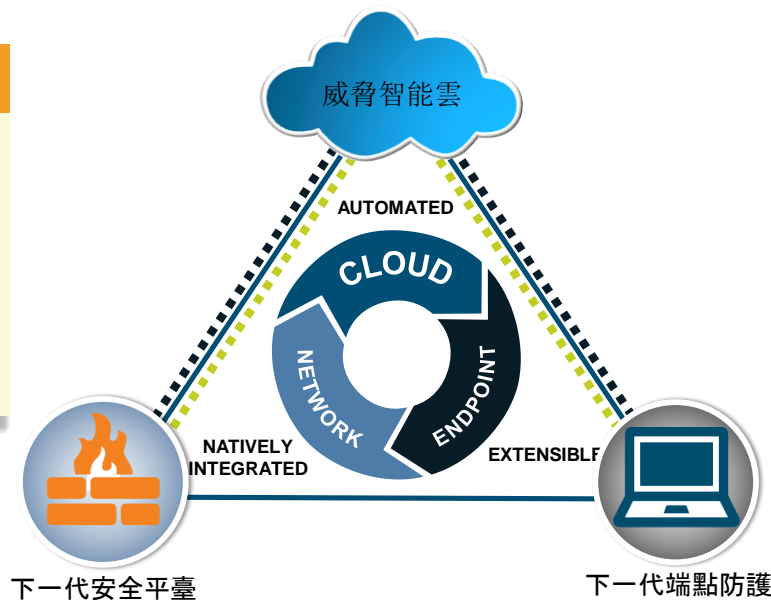


**DISRUPT
ADVANCED
ATTACKS
LIFECYCLE**

Palo Alto Networks的下一代安全解決方案

下一代安全平臺NGFW

- 檢測所有應用流量
- 應用安全保護
- 阻止已知威脅
- 傳送未知威脅到雲
- 移動和虛擬安全網路擴展



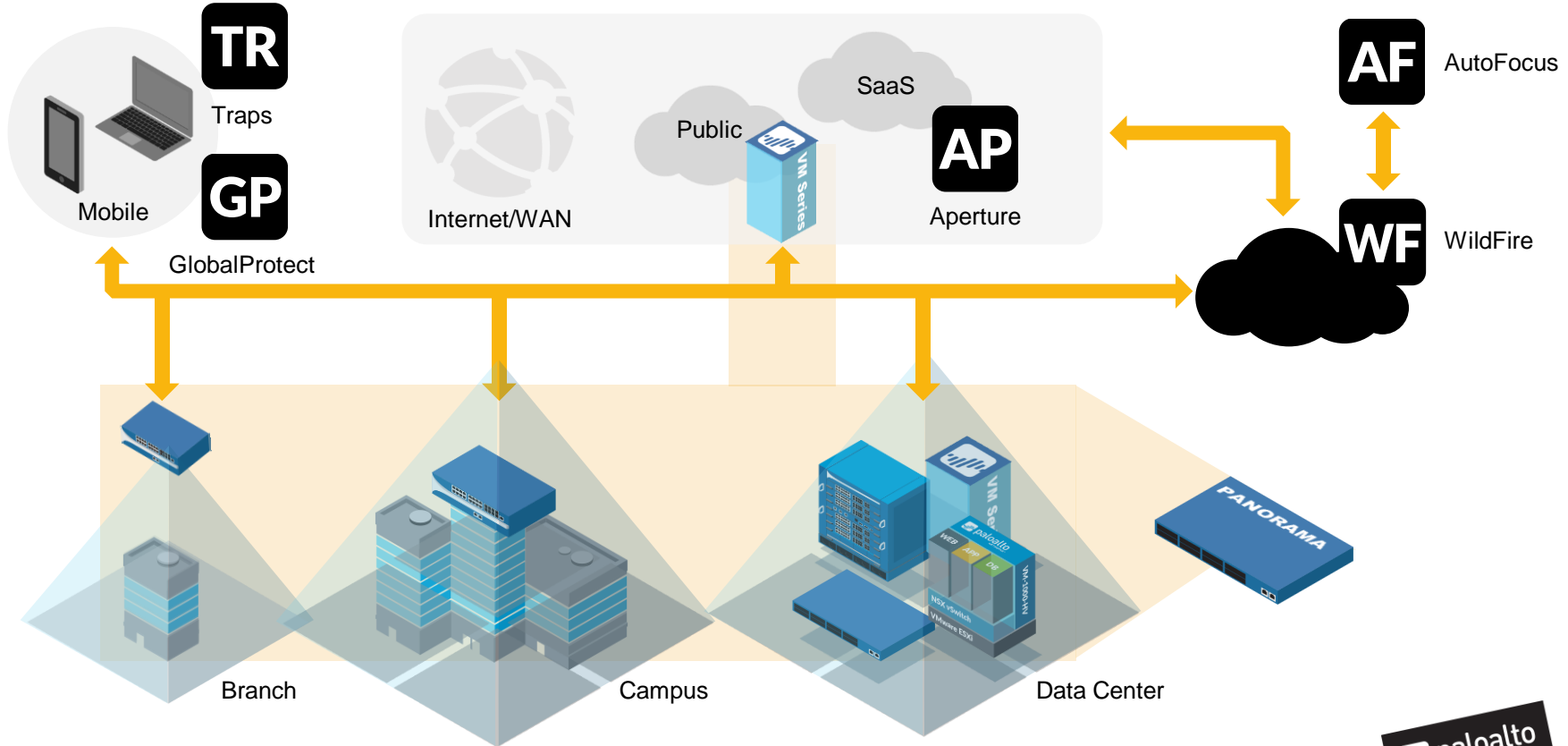
下一代端點安全防護

- 檢測所有執行的進程和檔
- 阻止已知/未知的可利用漏洞
- 雲協同，防護已知和未知惡意軟體

威脅智能雲

- 從網路和端點收集潛在威脅
- 智慧分析和處理未知威脅
- 回傳威脅信息到網路和端點

Everywhere you have to be, both physical and virtual with best-of-breed technologies



Multiple detection and prevention techniques; Traps

1



Exploit Software Vulnerabilities

(leveraged by exploit kits)

Prevents known and unknown exploits

Blocks core exploitation techniques

No scanning
No signatures

No prior knowledge necessary

2



Execute Malicious Programs

(including email attachments)

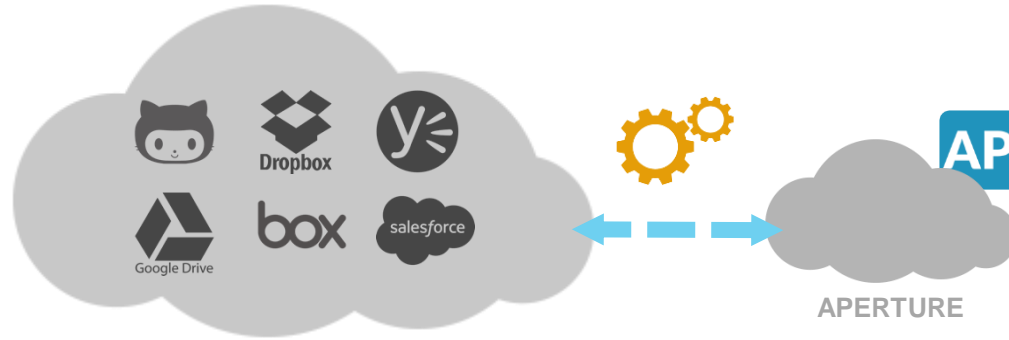
Prevents known and unknown ransomware

Local policy restrictions to reduce attack surface

Fully integrated with WildFire

Shares unknown ransomware with WildFire

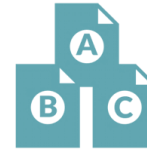
Multiple detection and prevention techniques; Aperture



**DETAILED CONTENT
INSPECTION
& ANALYTICS**



**CONTEXTUAL
CONTROL OF
DATA EXPOSURE**

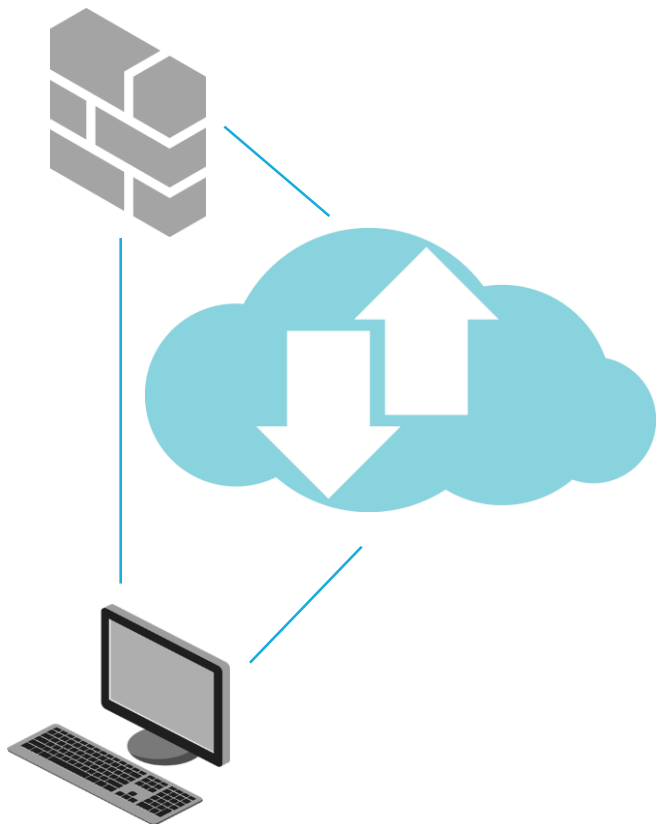


**PROGRAMABLE
DOCUMENT
CLASSIFICATION**



**MALWARE
DETECTION
& REMOVAL**

Global analysis & threat knowledge; Threat intelligence cloud



WILDFIRE

Discover new threats on popular platforms and deliver protections to the network and endpoint as quickly as possible

PAN-DB

Safely enable access to the web, and discover and block access exploit kits and phishing pages

AUTOFOCUS

Provide context for attacks on the network, and put actionable threat intelligence to work across the enterprise

AutoFocus: speed threat analysis workflows

PRIORITY NOTIFICATION



Alerts when
ransomware is
targeting you



ADD CONTEXT



Details around
ransomware
families



ANALYZE



Correlate local &
global threat
intelligence

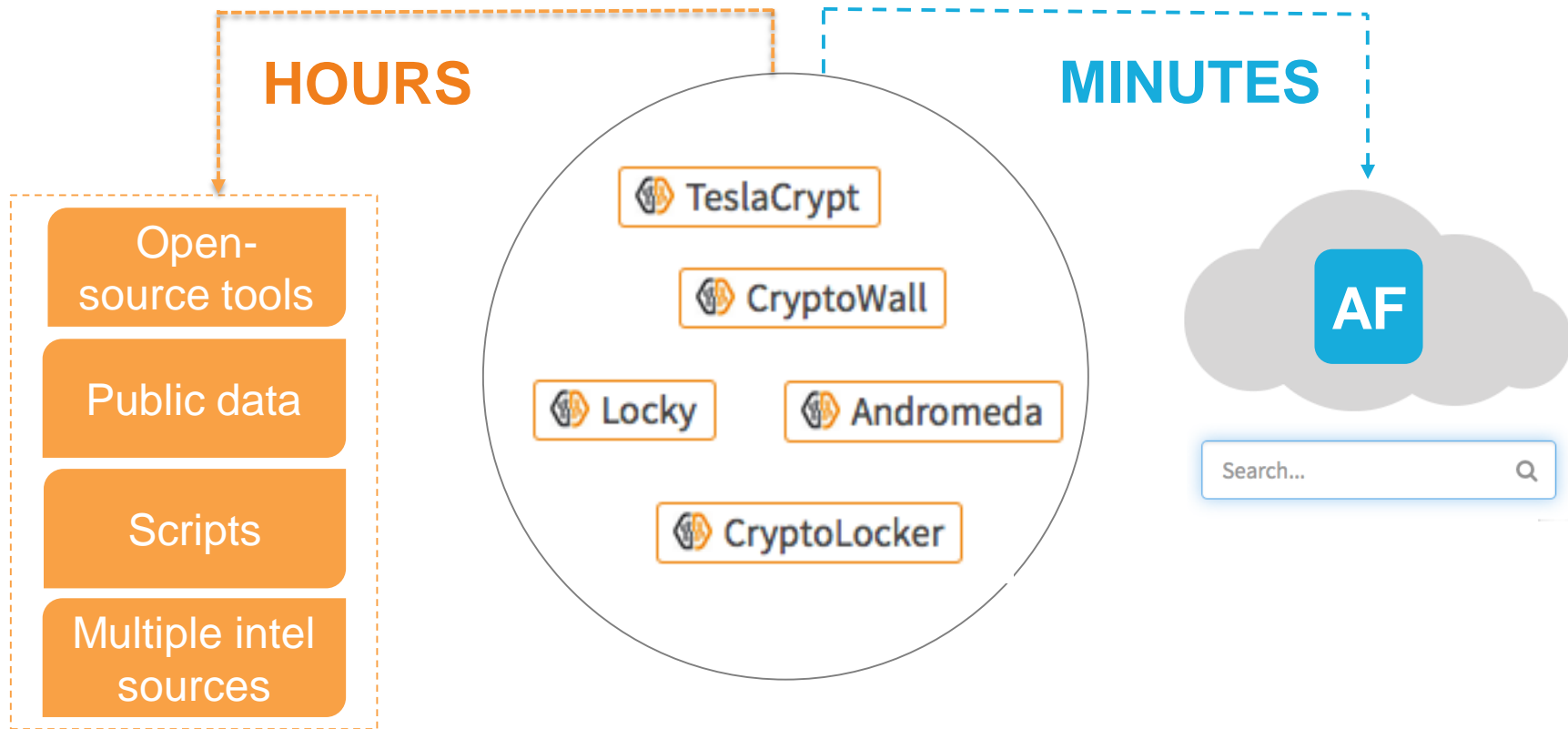


PROTECT



Prevent
ransomware
proactively

AutoFocus: quickly analyze threat intelligence



Why does this matter?

Global threat intelligence sharing



Exploit kits



Email attachments



Links in emails



Network & Cloud



SaaS Applications



Endpoint

**Ransomware Prevention
Across Multiple Attack Vectors
and Attack Surfaces
Is Only Possible With an
Integrated Security Platform**

Coordinated prevention of ransomware, network

Global threat intelligence sharing



Exploit kits



Email attachments



Links in emails



Network & Cloud



SaaS Applications



Endpoint

Block unknown traffic

Evaluate encrypted traffic

Disallow dangerous attachments

Examine email attachments for malware or exploits

Block malicious URLs

Examine unknown URLs for malicious activity

Coordinated prevention of ransomware, SaaS

Global threat intelligence sharing



Exploit kits



Email attachments



Links in emails



Network & Cloud



SaaS Applications



Endpoint

Block storage or
transmission of
files containing
exploits

Scan cloud
storage for
malicious files

Scan cloud
storage for
malicious files

Coordinated prevention of ransomware, endpoint

Global threat intelligence sharing



Exploit kits



Email attachments



Links in emails



Network & Cloud



SaaS Applications



Endpoint

Prevent all exploits, including zero-days

Block execution of malware

Block execution of malicious attachments

Prevent exploitation of email software itself

Prevent drive-by downloads of malware

Block exploitation of browser vulnerabilities

Key takeaways

PREVENTION IS POSSIBLE...

...with the right architecture.

- **PRECISION CONTROL AND IT-LEVEL VISIBILITY**

Reduce attack surface, stop threats

- **PLATFORM BREADTH AND INTEGRATION**

Disrupt the advanced attack lifecycle (feedback + automation)
integrate with people, processes, and IT architectures

