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”

攻破網路入口
通過釣魚郵件或滲透外部網站

下載惡意軟體
植入惡意軟體

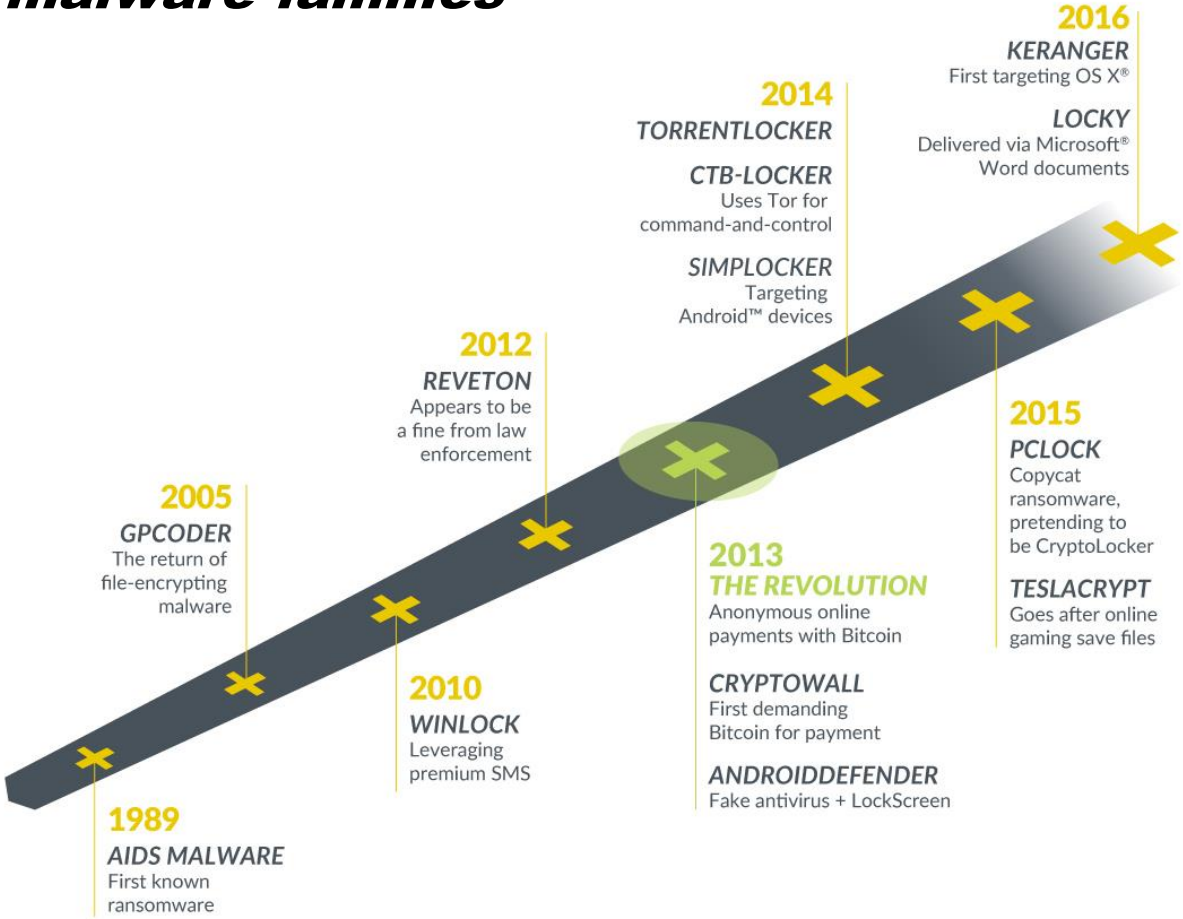
與C2伺服器通訊
與攻擊者進行連接和通訊

實施勒索
對檔案進行加密

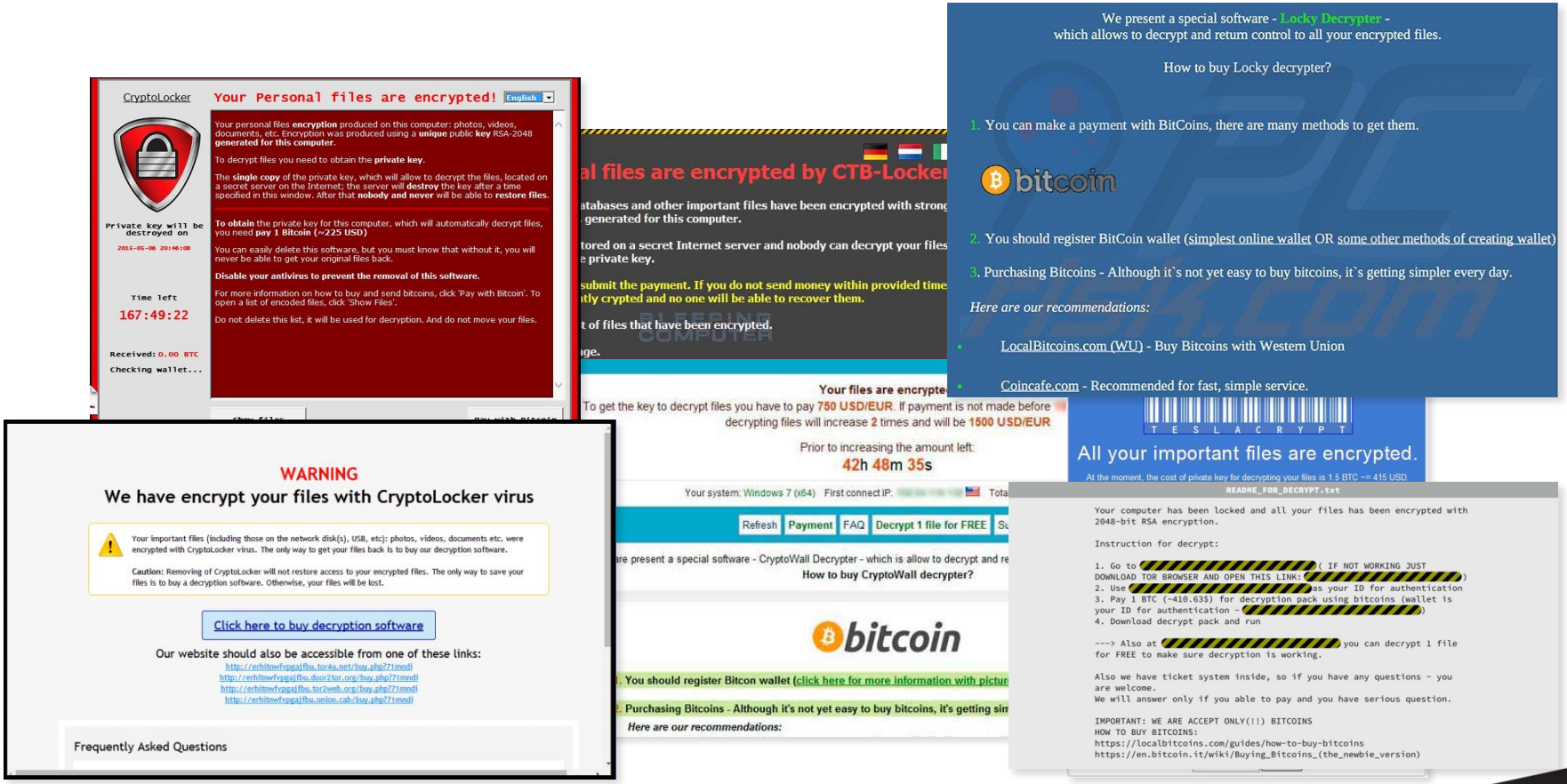
任何一個環節的阻擋都可以破解攻擊鏈

paloalto NETWORKS

30 active malware families



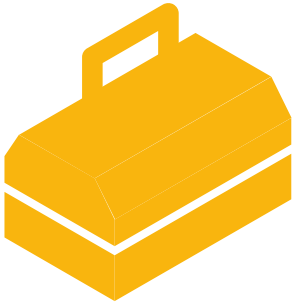
Ransomware today



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

1

REDUCE THE ATTACK SURFACE

2

PREVENT KNOWN THREATS

3

IDENTIFY & PREVENT UNKNOWN THREATS

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)

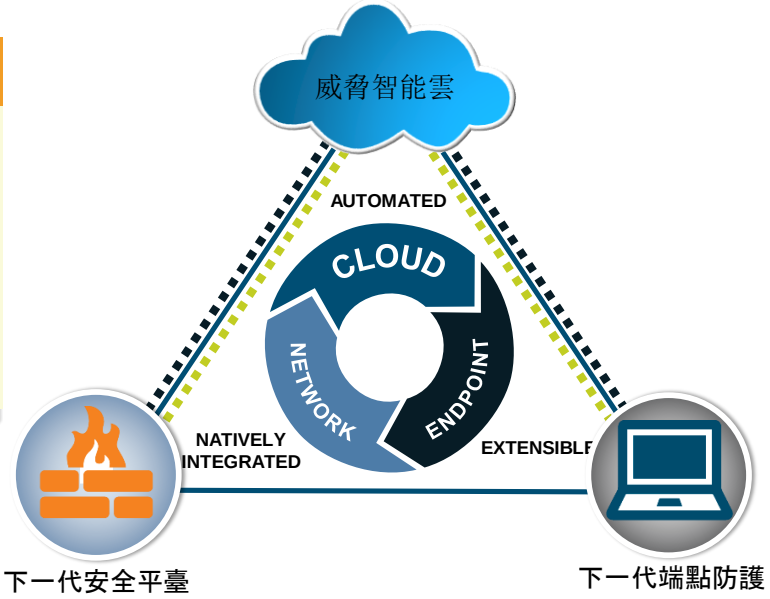
1. Be in the right position
2. Both virtual and physical
3. Best-of-breed security technologies
4. Multiple detection techniques
5. Global Analysis and threat knowledge
6. Control all, with the ability to reprogram in seconds

DISRUPT ADVANCED ATTACKS LIFECYCLE

PaloAlto 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



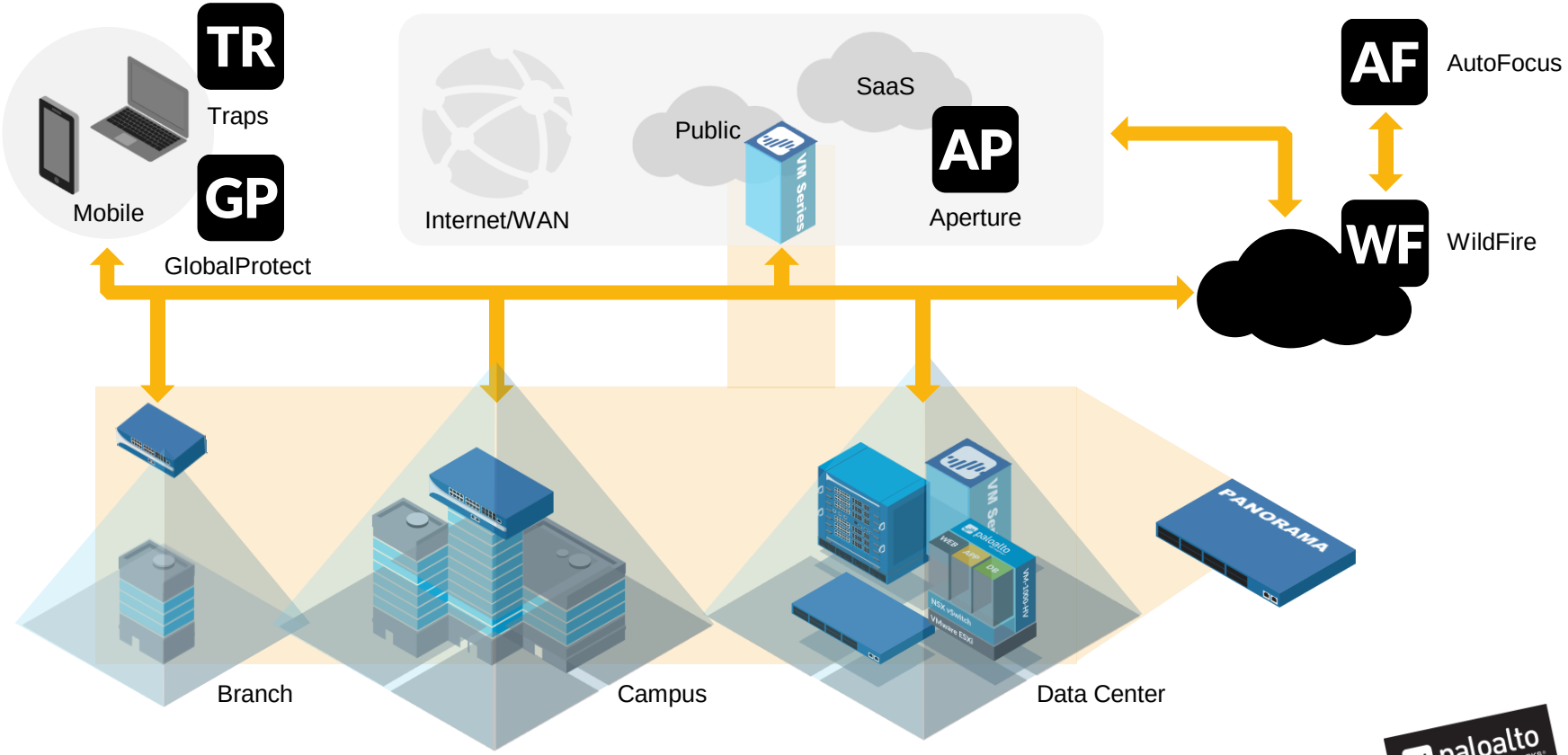
威脅智能雲

- 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

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

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

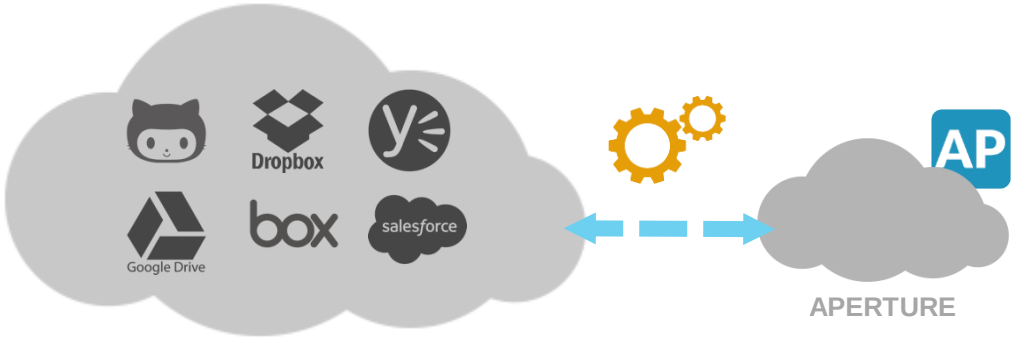
2

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



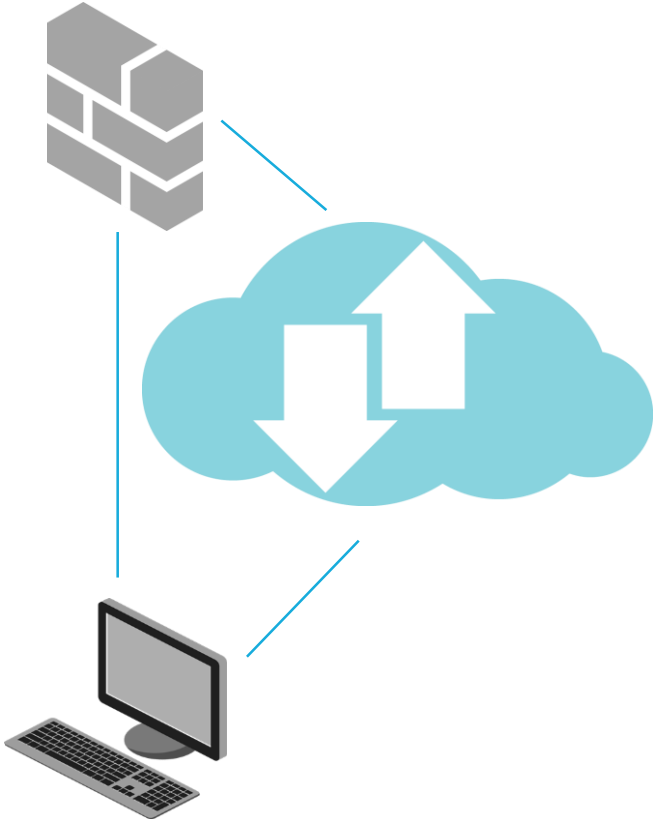
DETAILED CONTENT INSPECTION & ANALYTICS

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

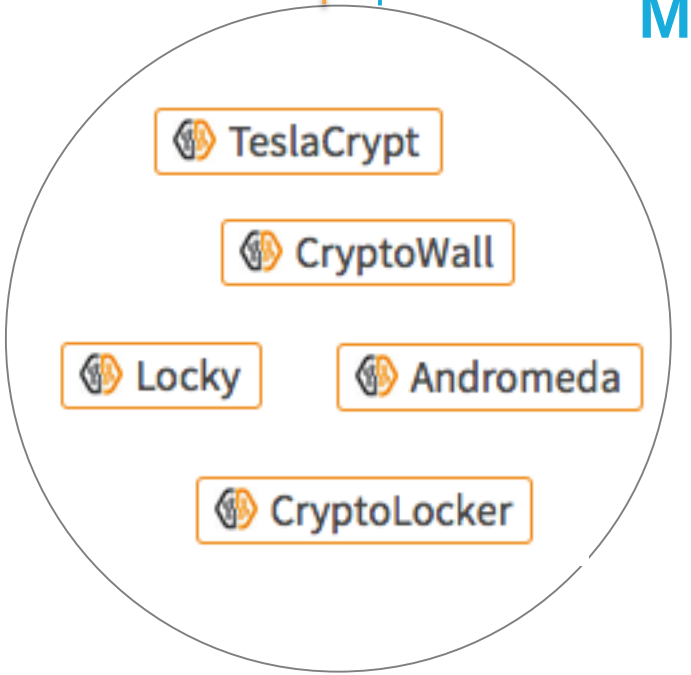
PROTECT

Prevent ransomware proactively

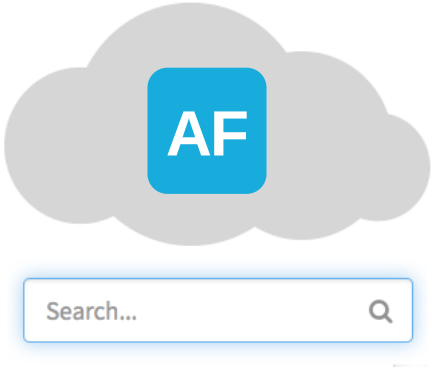
AutoFocus: quickly analyze threat intelligence

HOURS

- Open-source tools
- Public data
- Scripts
- Multiple intel sources



MINUTES



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	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
SaaS Applications			
Endpoint			

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	Prevent all exploits, including zero-days	Block execution of malicious attachments	Prevent drive-by downloads of malware
SaaS Applications	Block execution of malware	Prevent exploitation of email software itself	Block exploitation of browser vulnerabilities
Endpoint			

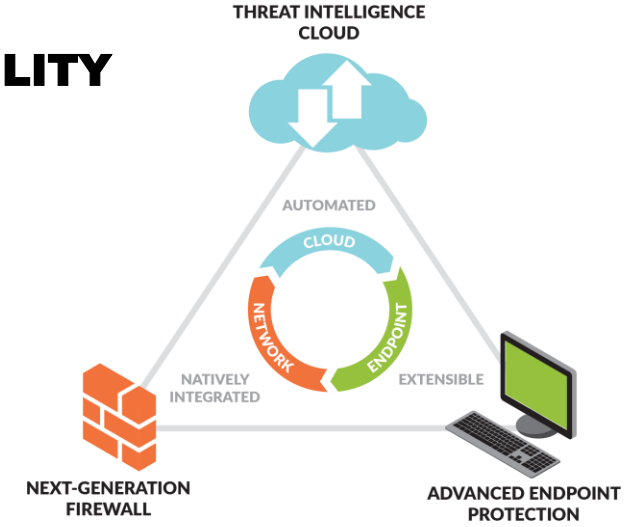
Key takeaways

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




paloalto
NETWORKS®