Advanced Threat Kill Chain

思科新世代防禦方案

Jaguar Lee
李俊瑩
思科資安業務經理

目前資安面臨的挑戰

© 2018 Cisco and/or its affiliates.

這是一門生意：網路犯罪

黑客攻擊僱傭價碼大公開

2016-04-08 由 安全牛 發表于科技

遠程木馬5到10美元；

黑客教學20至40美元；

入侵谷歌、微軟或雅虎郵箱129美元；

入侵俄羅斯社交媒體賬戶194美元；

入侵網站盜取數據350美元；

DDoS攻擊5$/小時、200$/星期、1000$/月；

有效的銀行賬戶登錄憑證最高可達數萬美元……

戴爾安全工作室最近發佈的一份俄羅斯地下黑客市場的報告，披露了諸多黑客攻擊手法的僱傭價格。從軟件售賣到黑客教學，再到銀行卡盜竊、DDoS攻擊等各種網絡攻擊服務，應有盡有。

身份证户籍信息	10-40 元/条	• 冒名办理信用卡等进行恶意透支； • 冒名在网贷平台进行恶意贷款； • 冒名开办银行卡及第三方支付账号，接收和转移非法资金及洗黑钱； • 冒名挂失他人手机号码，为实施诈骗等犯罪作准备；
车辆信息	10-40 元/条	• 仿冒交通违章类电话短信实施诈骗； • 发送车险等恶意推销广告；
高学历人口信息	20-60 元/条	• 制作假文凭、证书； • 进行 MBA 培训班等精准营销；
开房记录	150-500 元/次	• 私家侦探业务：捉奸、查婚外情； • 非法讨债
手机基站位置	200-500 元/次	• 私家侦探业务； • 非法讨债
手机话单	2000-3000/次	• 私家侦探业务； • 非法讨债； • 商业间谍
银行开户资料	1-10 元/条	• 精准发送钓鱼或木马链接，实施银行卡盗刷等诈骗； • 冒充银行职员或公检法人员进行电信诈骗； • 非法查询他人财产状况，为其他犯罪作准备；
银行流水单	1000-3000 元/份	• 私家侦探业务； • 非法讨债；
火车购票信息	100-200 元/次	• 私家侦探业务； • 行踪调查；
PS 手持身份证	150-200 元/张	• 冒用他人身份注册网店，或进行第三方支付平台账户实名认证； • 申请 POS 机，用于转移非法资金及洗黑钱；

勒索軟體針對企業而來

全球99國日前受到大規模電腦駭客攻擊，並且散播名為「WCry」（亦稱WannaCry）惡意勒索軟體，鎖住受害者的所有電腦檔案，要求約1.8萬元台幣贖金，否則永遠無法取回檔案。

對於日前全球範圍內出現了大規模的勒索軟體感染事件，思科表示，此次勒索軟體的影響範圍非常大，本次勒索軟體爆發的一個明顯特徵是，針對企業使用者進行勒索軟體的傳播，國外發現受到影響的用戶包括醫療行業、快遞行業等。

在中國也發現了金融、教育等大量企業用戶收到了影響。

思科Talos安全團隊已經在第1時間，發針對這次爆發的勒索軟體進行了深入的分析和研究，思科Talos研究報告指出，此次大範圍傳播的勒索軟體名為WannaCry，通過掃描TCP 445埠，採用蠕蟲病毒的傳播方式，感染主機並且加密檔，這是此次大規模爆發的一個原因。

思科表示，勒索軟體WannaCry利用了在Windows系統上被稱為DOUBLEPULSAR的後門，在入侵的系統上安裝和啟動惡意程式碼。

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

至於使用者是在何處「染毒」？思科指出，此次加密勒索軟體的傳播途徑有四：一是透過帶有惡意檔案附件或者釣魚網站連結的郵件的來傳播，二、網站的惡意程式碼下載，三、綁定在某些惡意軟體上傳播，四、藉助卸除式存放裝置作為媒介來傳播。

思科指出，如果不幸被鎖定，含有加密勒索軟體代碼在使用者電腦上運行時，主動連接上僵屍網路C&C主機，下載加密程式或者獲取加密金鑰，隨後入侵個人的檔案系統，並對特定檔案進行加密，跟進攻擊者就會發出勒索資訊，通知使用者支付贖金，才會提供解密的方法。

思科通過對多種案例和勒索軟體的傳播路徑的分析，如果能夠切斷傳播路徑，應該就可以大幅減少遭勒索軟體感染和入侵的機會，消費者可以先從不要隨意打開陌生郵件、或是瀏覽不熟悉的網站做起，若再不安心，可採用主動的威脅防禦模式，借助於安全解決方案，從阻斷加密勒索軟體的傳播路徑入手，應該就可以防患於未然。

(工商時報)

擁有1.3億用戶的著名電腦系統清理軟體「CCleaner」，傳出遭到駭客植入惡意軟體，可能透過2階段的後門程式 進一步感染目標裝置，官方也呼籲用戶盡快升級到最新版本，尷尬的是研發CCleaner的軟體公司Piriform，今年七月才被的防毒軟體巨頭Avast收購。

遭植入惡意程式，用戶重要資訊可能被竊取

思科（Cisco）資安團隊Talos，發現有「垃圾清潔劑」之稱的電腦系統清理軟體「CCleaner」遭到植入惡意後門程式，受影響的版本包括CCleaner v5.33.6162的32位元版本及CCleaner Cloud v1.07.3191，這兩款軟體分別在8月15日與8月24日釋出，目前約有3%的CCleaner用戶經安裝，估計受影響用戶約有230萬。

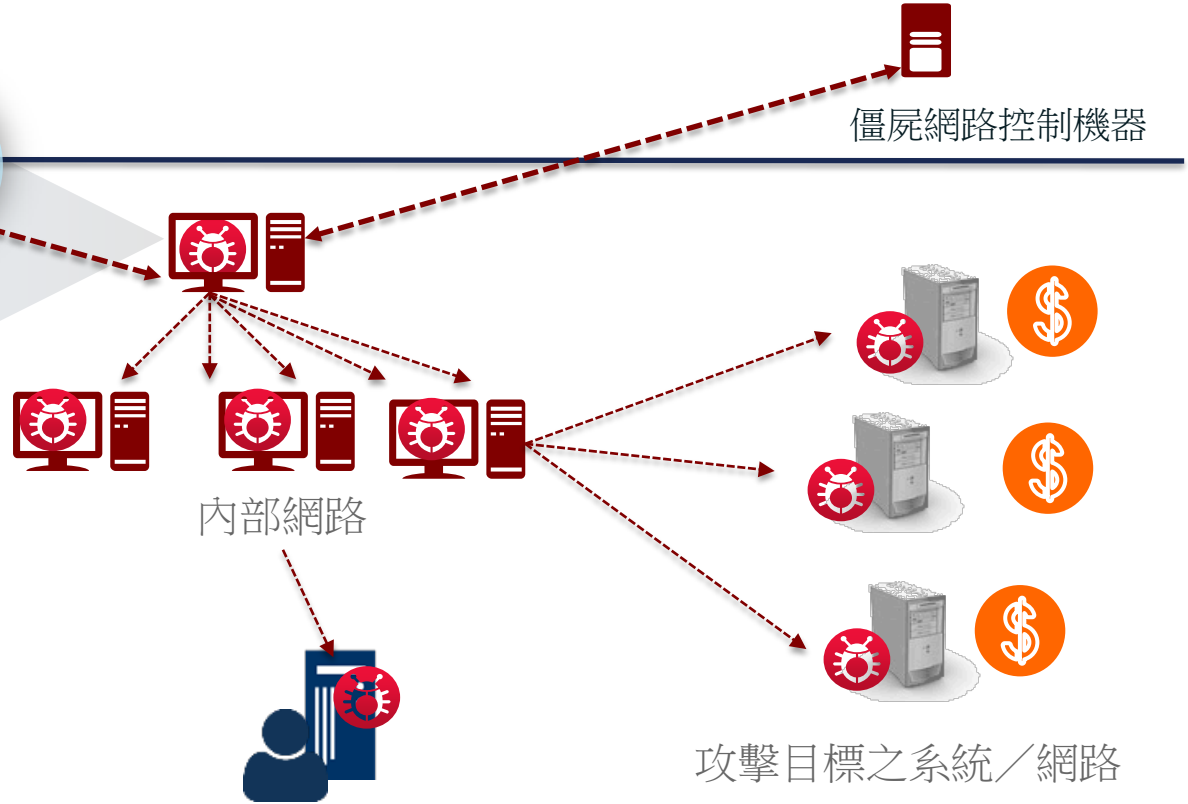
CCleaner可以清理裝置上的暫存檔案、垃圾程式、廣告、Cookies來維護電腦效能，在個人電腦及Android手機都可以使用，在全球累積超過20億次下載量，且以每個月500萬用戶的速度增加，這款軟體隸屬Avast旗下的英國軟體公司Piriform。

Avast及Piriform都已經證實軟體遭駭，研究人員發現攻擊者透過竄改CCleaner.exe binary，植入一個兩階段的後門程式，接著從遠端IP位址傳送惡意程式碼，一旦用戶安裝受到感染的軟體，攻擊者就能竊取用戶重要系統資訊、檔案，再回傳給外部的C&C伺服器。

© 2018 Cisco and/or its affiliates. All

駭客攻擊手法

1. 後門建立，取得控制權
2. 偵察和網路感染
   事先偵測，再進行滲透
   （橫向傳播）
3. 發展和
   特權提升
4. 分次和
   持續性（重複2,3,4）
5. 系統被攻佔



事前 Before the Attack – Control, Enforce, Harden

- 需要全盤了解內網之中的所有內容資訊, 包含: devices, OS, services, applications, and user information
- 有此內容資訊, 方可建立細緻而完整的存取權限控管, 包含網路分割(network segmentation)
- 發現所有的安全漏洞並立即修補
- 進行對即有的存取權限評估並盡可能降低特權帳號的數量與人員的權限
- 加強維運與危機處理小組之相關知識與技能

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

事中 During the Attack – Detect, Block, Defend

- 偵測與阻擋惡意軟體的橫向傳播
  - 行為分析機制, 包含資安沙箱模擬
- 偵測與阻擋惡意軟體的終端設備常駐與執行
  - 結合 signature-based 技術加快偵測已知惡意軟體時間, 並使用行為分析模式來發現尚未知/尚未公布的資安威脅
- 偵測與阻擋惡意網站
  - 結合全球安全情資去加快惡意網站的名單
- 偵測與阻擋應該懷疑的網路行為, 包含橫向封包移動
  - 完整的網路行為可視度與有能力去辨別異常的網路流量

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

事後 After the Attack – Scope, Contain, Remediate

- 記錄資安意外事件, 並開始資安意外處理程序

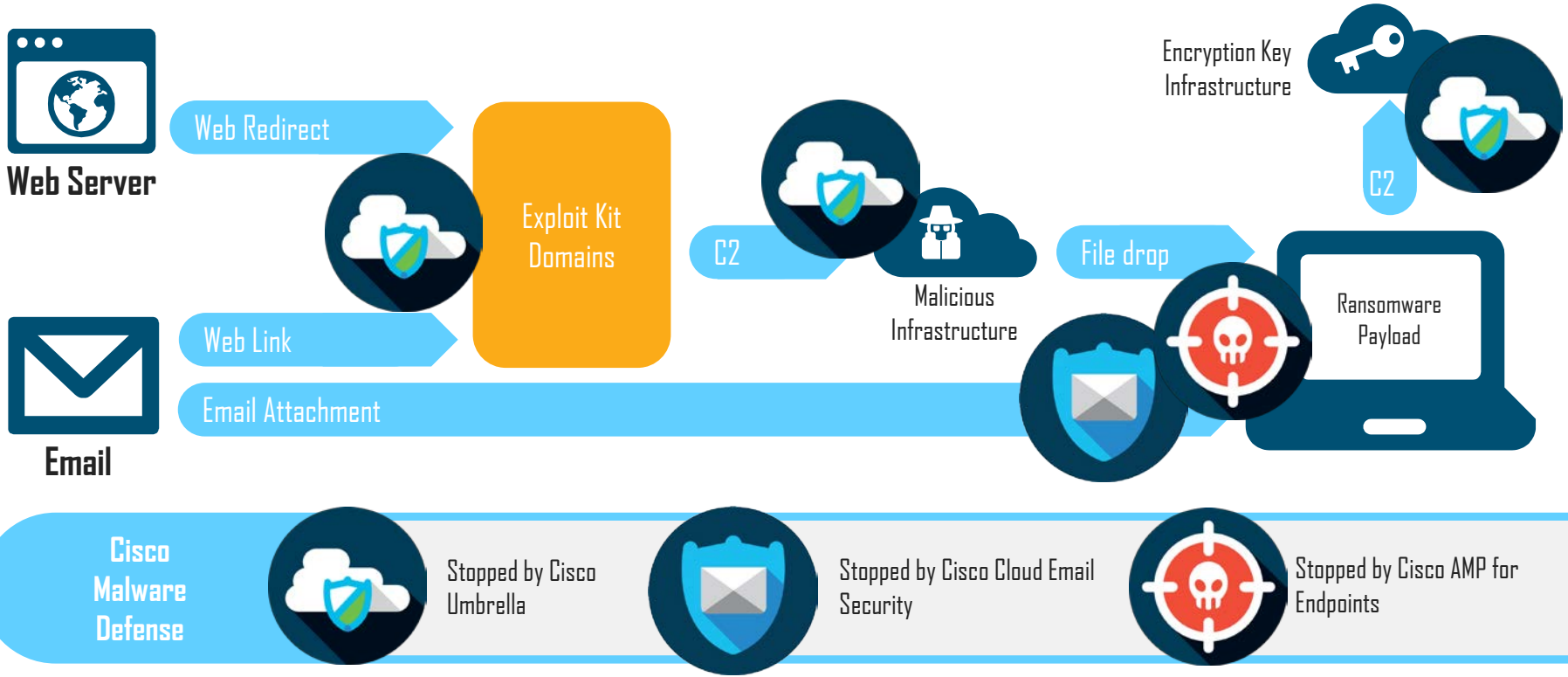
- 確認資安意外影響範圍
  - 分析網路行為記錄, 啟動資安鑑識, 包含進行惡意軟體逆向分析
  - 比較被感染設備的網路流量行為, 並擴大至整個網路環境已找出是否有其他惡意軟體目前尚在潛伏期

- 抑制感染行為去預防其他的設備資安意外
  - 將已感染設備從網路獨立出來

- 將惡意軟體移除並恢復正常程序

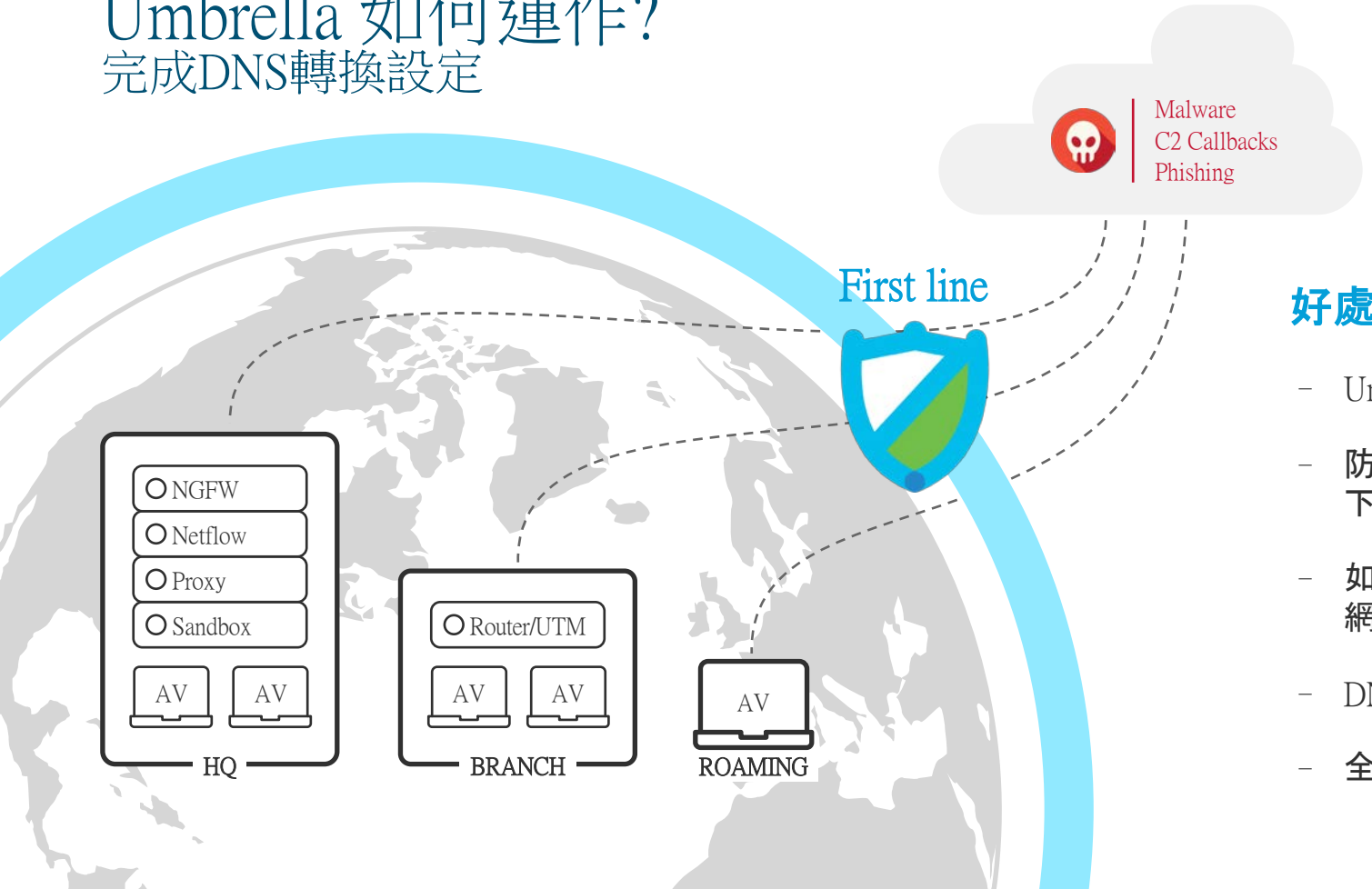
© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Break the Malware Chain



© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Umbrella 如何運作?
完成DNS轉換設定



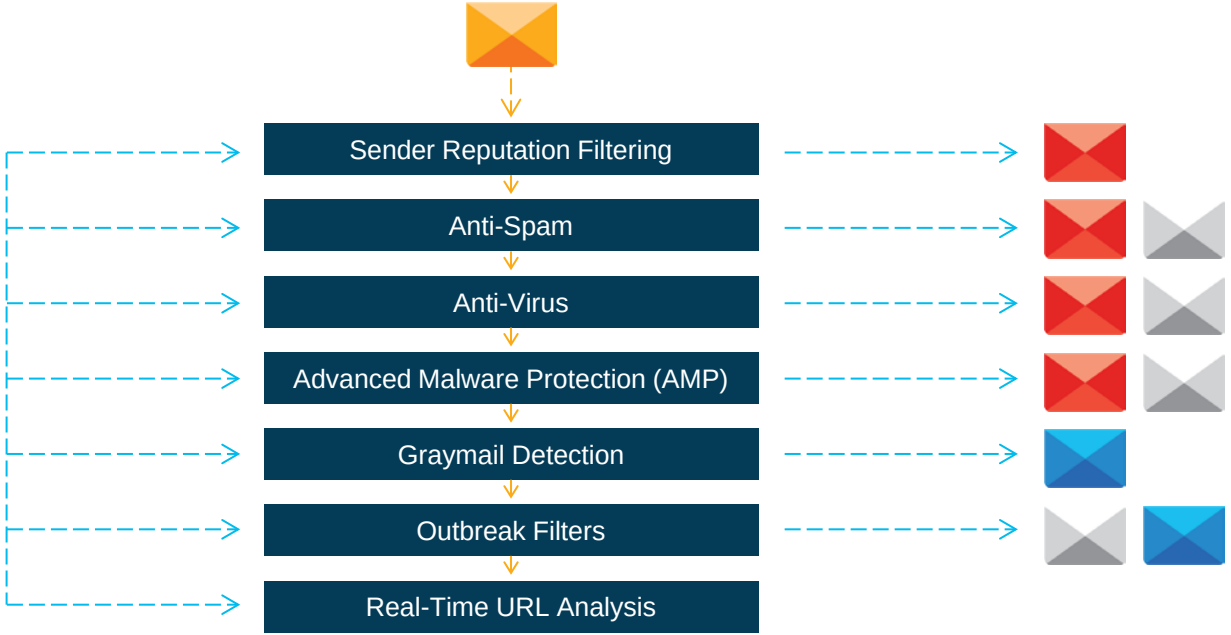
好處

- Umbrella提供即時黑名單
- 防釣魚網站與惡意軟體下載
- 如果惡意軟體已經在內網, 可以隔絕對外連線
- DNS 解析加快
- 全區部署簡單

思科郵件防護
Talos on Cisco Email Security

TALOS

Constant and integrated security feeds



Incoming email Drop Rewrite Quarantine

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Advanced Malware Protection for Endpoints (AMP4E)
事先預防與事後偵測

Talos 資安情報 45% of detections did not exist in VirusTotal at time of detection

內建防毒軟體機制

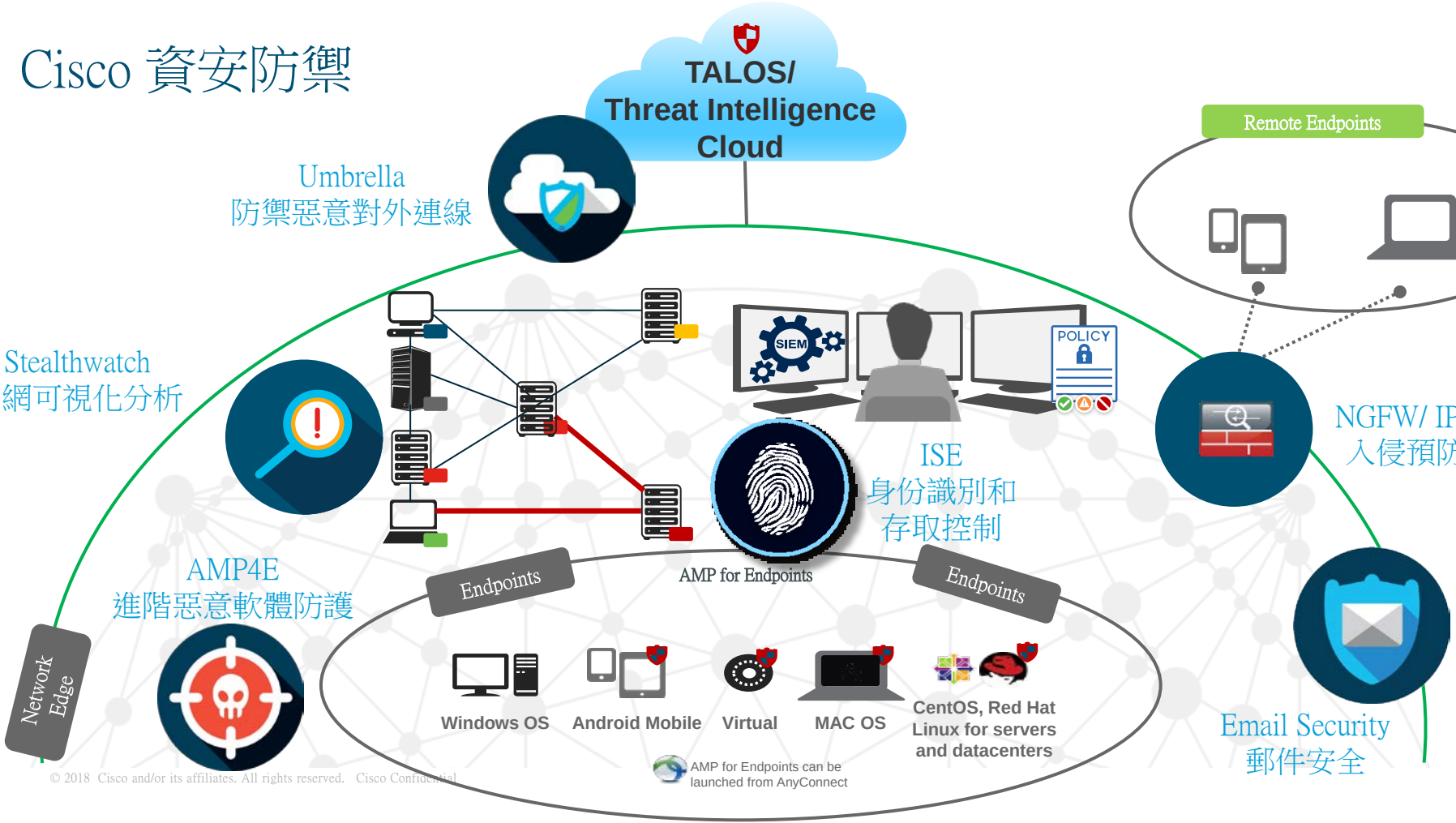
整合沙箱機制
19% of detections did not exist in VirusTotal at time

自動分析”低普及率軟體“
- 10% turn out to be new malware

提醒安裝軟體之漏洞

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cisco 資安防禦



© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Q and A