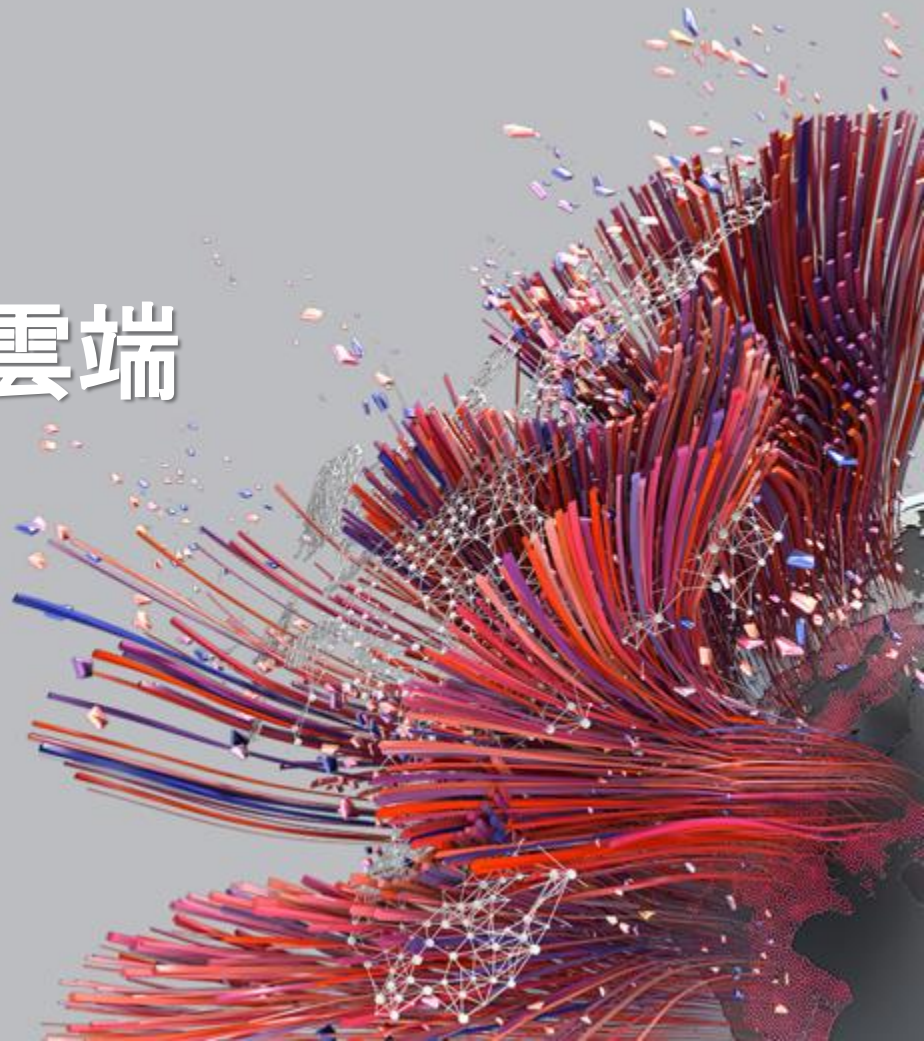
實體、虛擬、容器到雲端

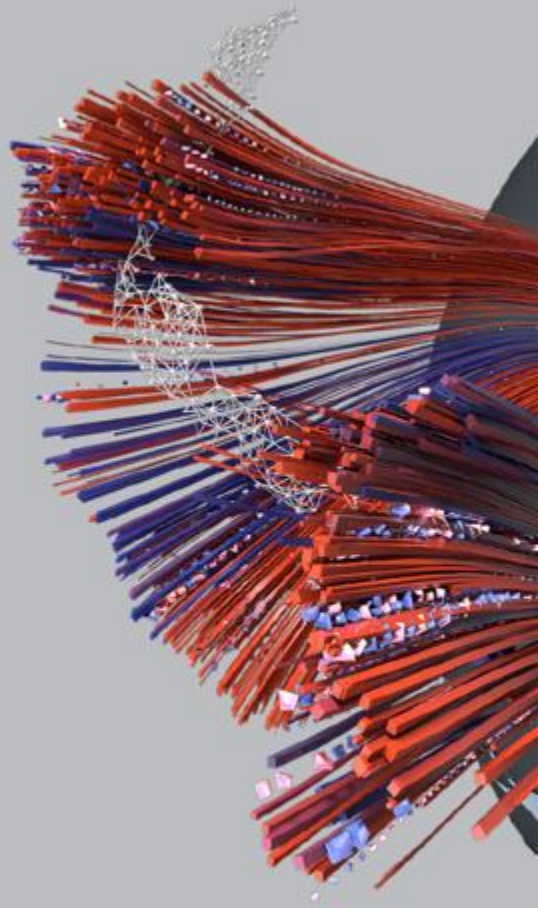
全方位主機保護



趨勢科技 楊肇謙

近期網路威脅之

攻擊手法



© 2021 Trend Micro Inc.

勒贖加密及駭客持續威脅校園

WannaCry Ransomware Clones Still a Threat to US Schools

By Rencio in Computer Security

Translate To: English

of state-operated organizations like s
notably old versions of Windows tha

WannaCry stays alive

Following the recent early 2019 rans
the US, including the RobinHood atta
against the Boston Public Defenders

iThome 新聞 產品&技術 專題 AI Cloud DevOps 資安 研討會 社群 零信任資安講堂

公布2021年全球的威脅趨勢回顧報告，在3月10日，該公司臺灣總經理劉基章進一步揭露了近期的臺灣資安現況。

教育與研究、軟體供應商遭攻擊情況，較往年大增

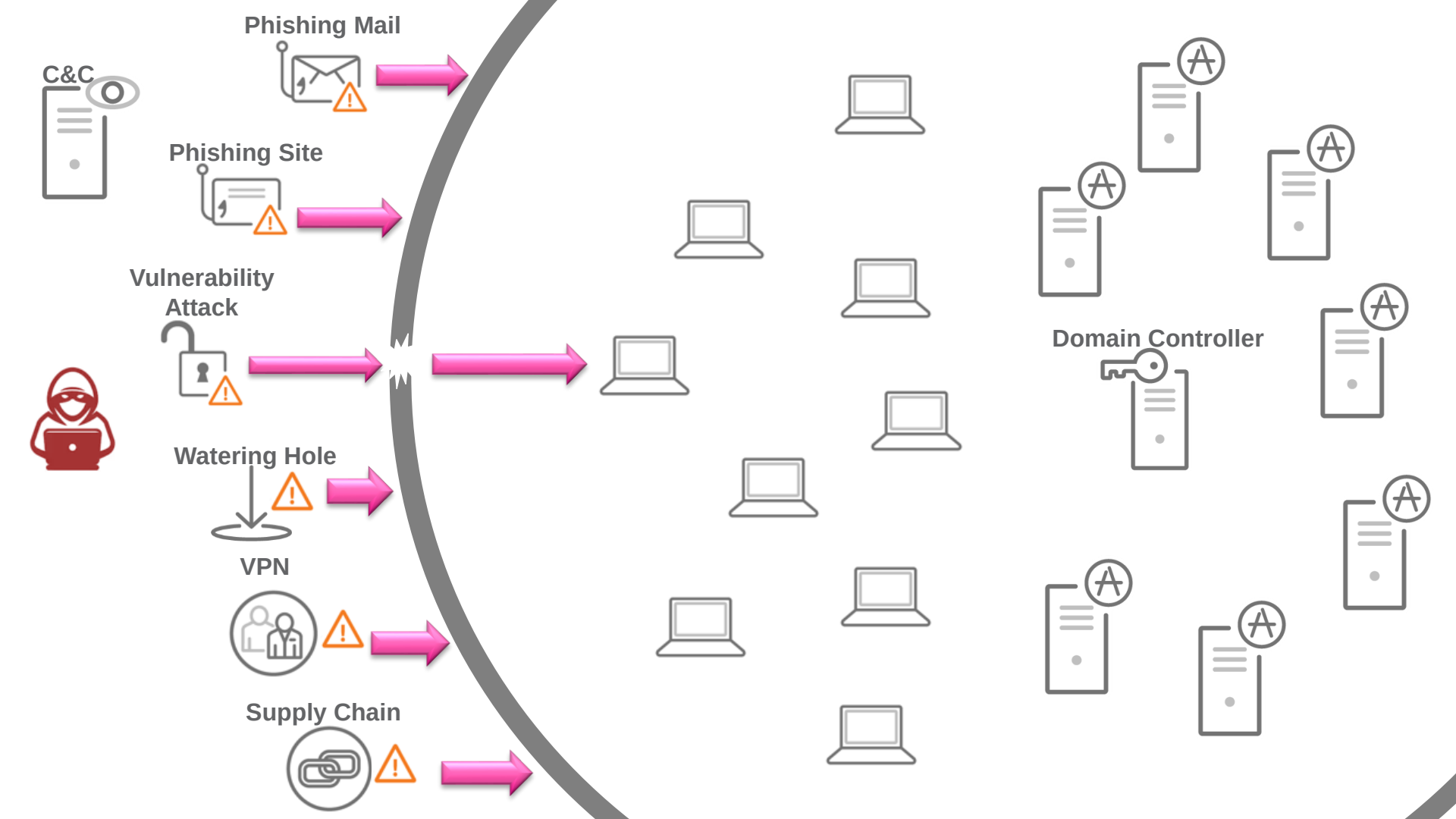
縱觀全球威脅趨勢，APT攻擊與勒索軟體仍最受矚目，從過去一年度來看，許多重大資安事件大多與之有關，劉基章指出，但要注意的是，去年出現更多針對供應鏈與韌體弱點的攻擊事件。

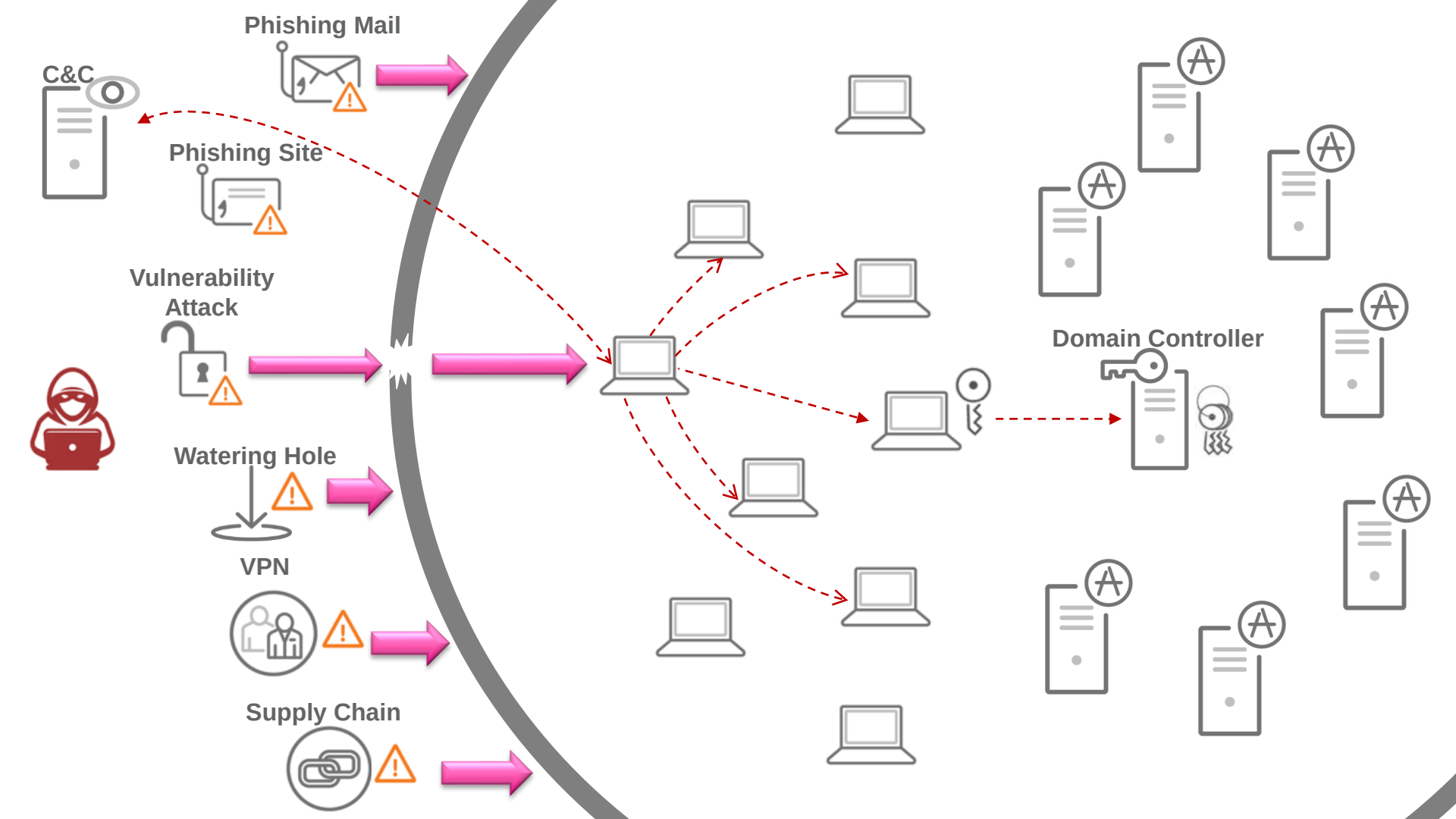
就攻擊頻率而言，企業每週遭受網路攻擊次數持續大增，以2021年而言，較2020年增長5成，而且，在Check Point統計的1千萬次攻擊事件中，有多達40萬次是零時差濫用活動。

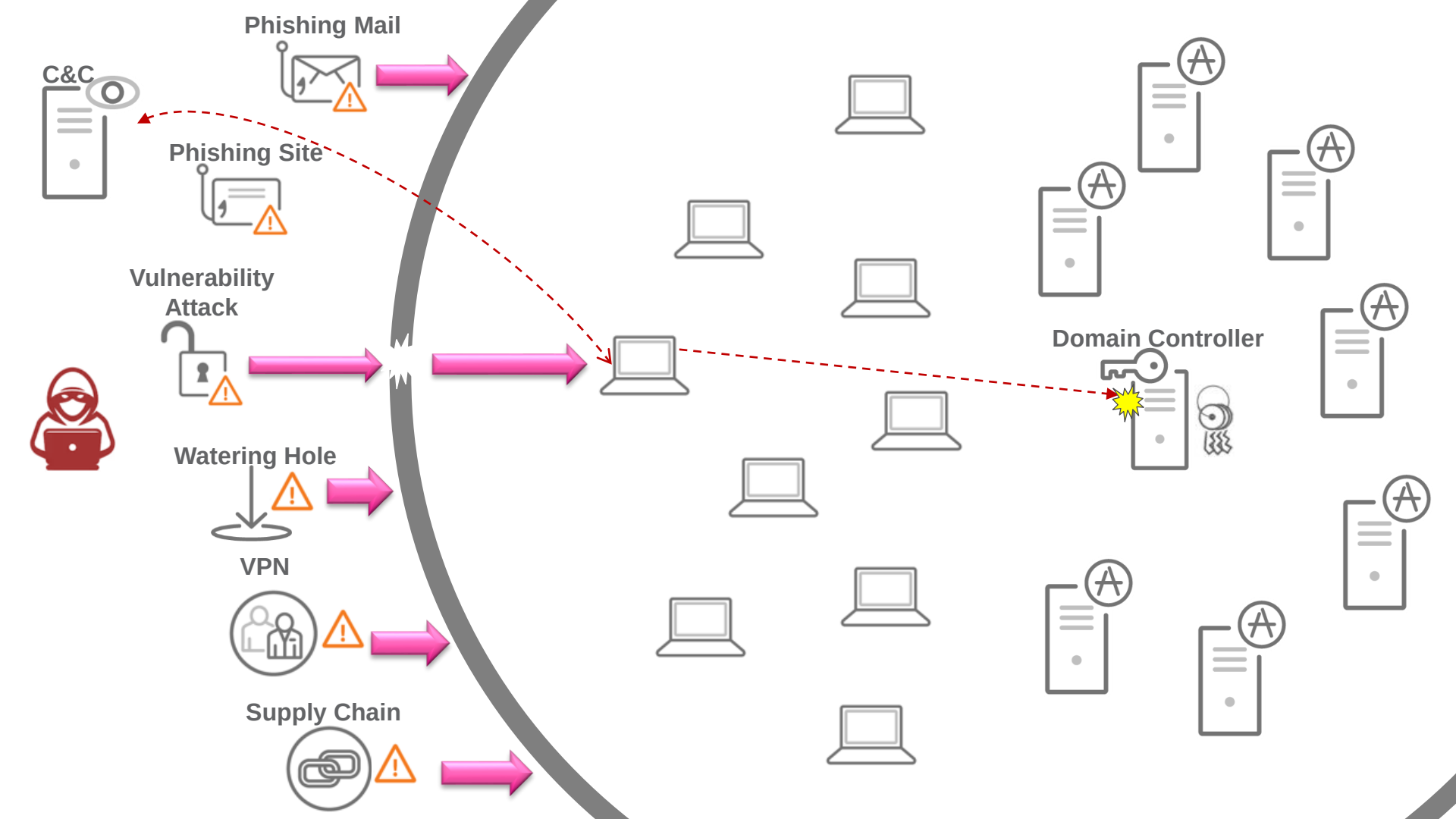
若從產業面來看，全球資安威脅態勢有兩大重要現象。首先，教育與研究機構在2021年成為最大目標，劉基章表示這是過去不曾看到的現象，每週遭受攻擊

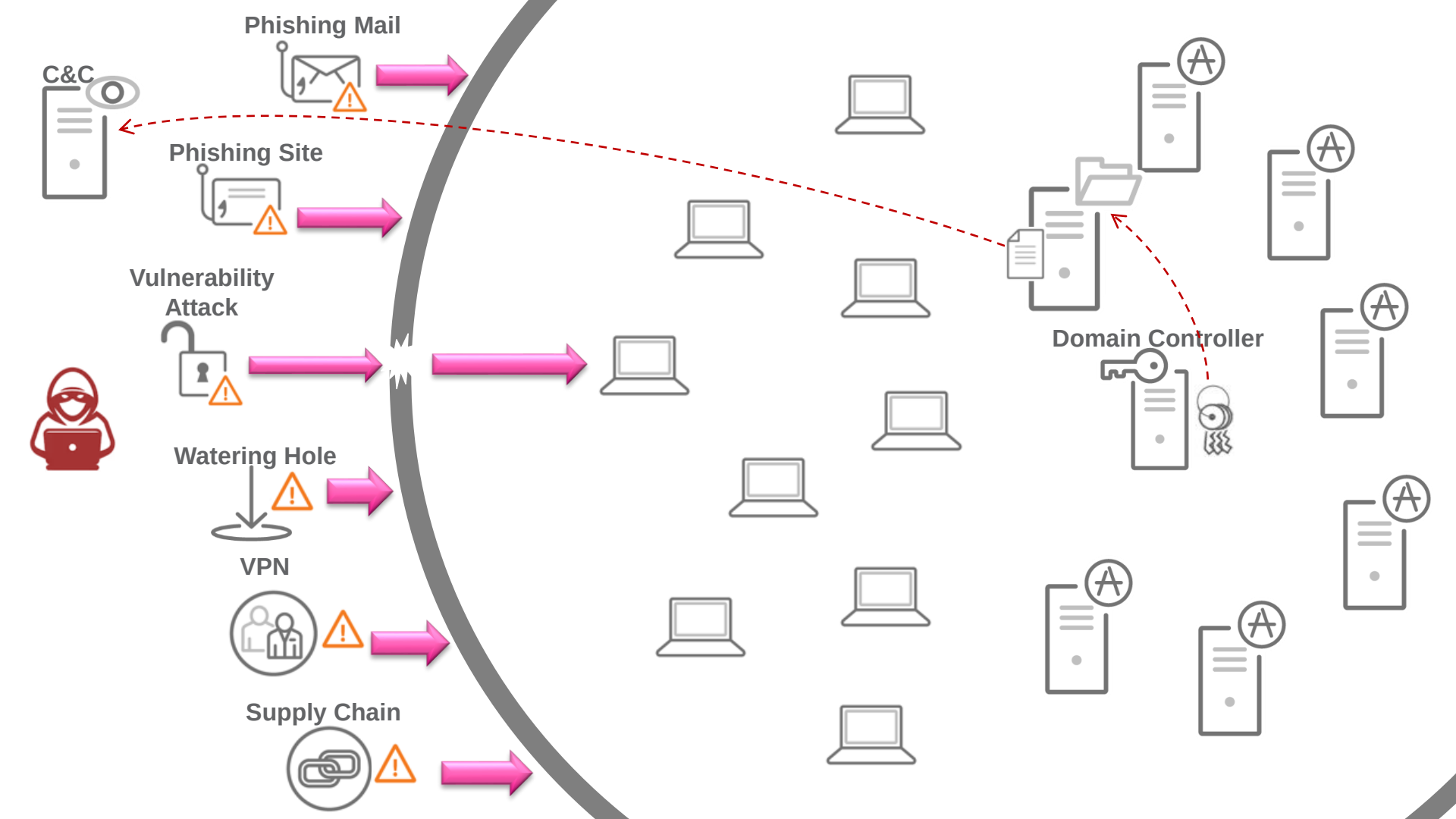
© 2021 Trend Micro Inc.

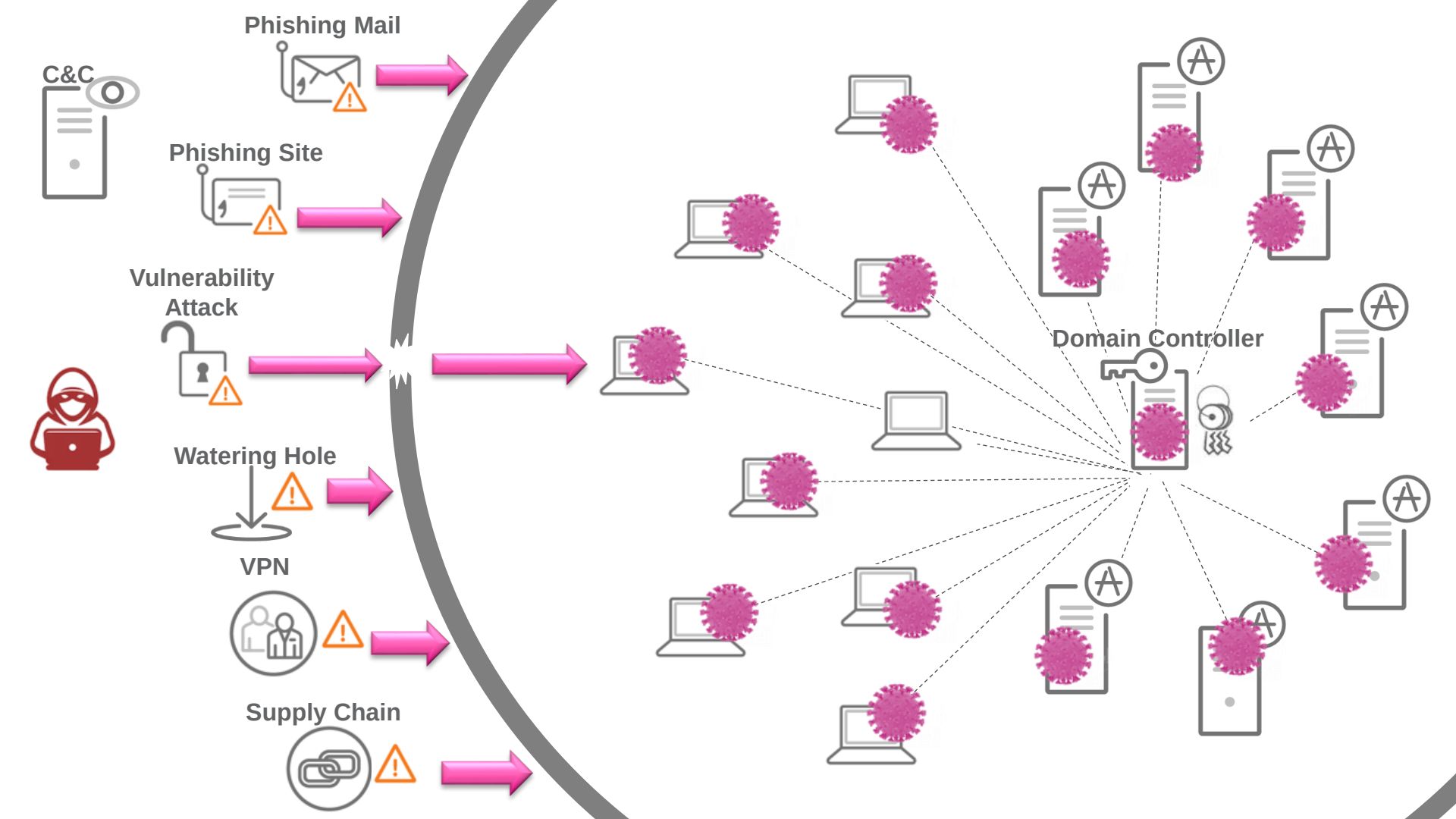

C&C
Domain Controller


Phishing Mail
C&C
Phishing Site
Vulnerability
Attack
Watering Hole
VPN
Supply Chain
Domain Controller

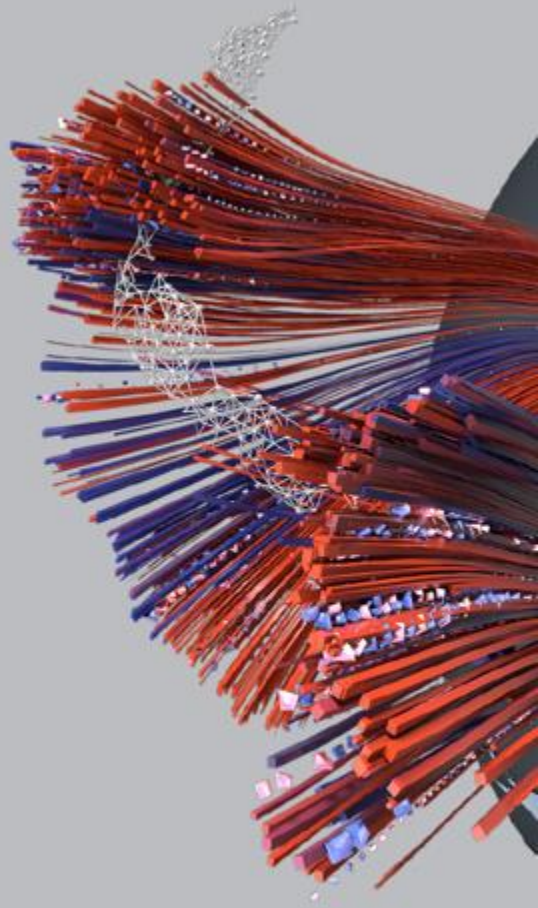

Phishing Mail
C&C
Phishing Site
Vulnerability Attack
Watering Hole
VPN
Supply Chain
Domain Controller


Phishing Mail
C&C
Phishing Site
Vulnerability
Attack
Watering Hole
VPN
Supply Chain
Domain Controller


Phishing Mail
C&C
Phishing Site
Vulnerability
Attack
Watering Hole
VPN
Supply Chain
Domain Controller


Phishing Mail
C&C
Phishing Site
Vulnerability
Attack
Watering Hole
VPN
Supply Chain
Domain Controller

常見問題與建議措施



© 2021 Trend Micro Inc.

常見問題

- 系統漏洞未修補或屏蔽
- 輕易地由遠端存取公司內部系統 (RDP, VPN…)
- 高權限帳號浮濫使用，而易遭竊取
- 單點突破，全區淪陷
- 公司內部網路的可疑行為，沒有能見度
- 重要系統未備份，或備份也被加密

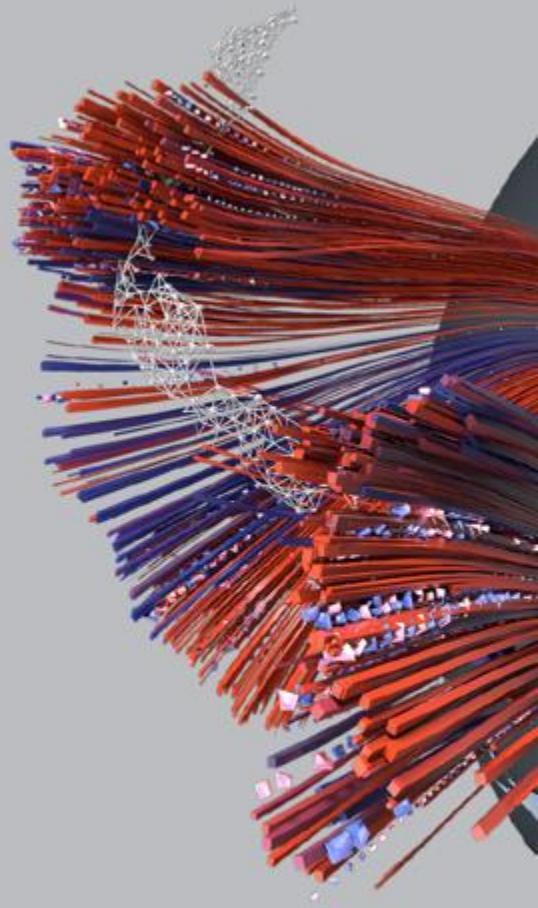
© 2021 Trend Micro Inc.

建議措施

- 定期修補漏洞，或利用IPS及Virtual Patch進行防護
- 導入及應用雙因子認證機制，加強身分辨識
- 強化帳號密碼與權限的控管，避免高權限帳號落入駭客手中
- 強化網路架構的設計，避免大內網讓駭客暢行無阻
- 部署網路及用戶端的偵測回應機制(NDR、EDR)，並配置代管服務(MxDR)
- 加強備份機制的安全性及有效性

© 2021 Trend Micro Inc.

資安如何加強



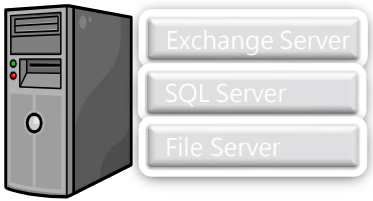
© 2021 Trend Micro Inc.

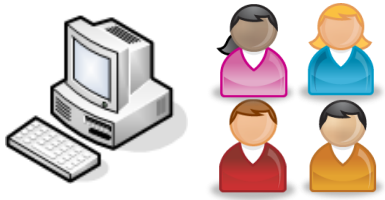
資安問題一大堆，到底該如何下手?

先從保護重要伺服器開始

© 2021 Trend Micro Inc.

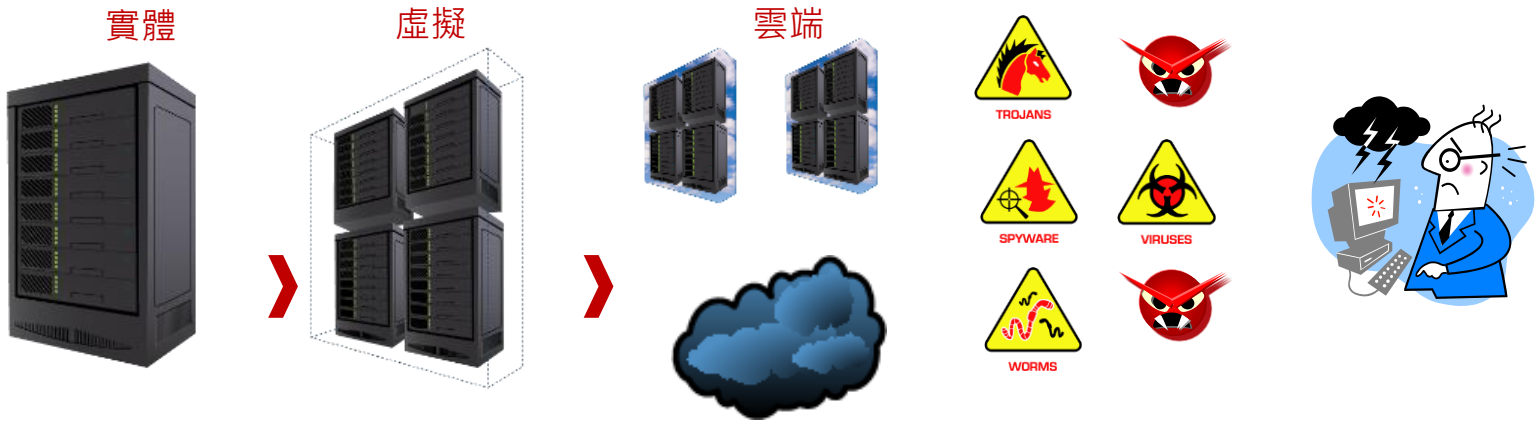
伺服器 vs. 一般電腦的不同





	伺服器	一般PC
用途	於網路上提供服務給其他電腦	提供使用者本機操作
軟體安裝	建置完成後就固定了,頂多是版本更新	使用者常會自行安裝各式軟體
使用自行開發軟體	較常見於中大型企業	大多數為套裝軟體
作業系統	Windows約70%, Unix約30%	MS Windows > 95%
Patch修補	通常不會套用自動更新	大多會套用自動更新
風險來源	系統漏洞、駭客攻擊、權限設定不當	使用者執行或下載惡意程式
危機發生的應變	需要審慎評估，有時候斷線或關機，會造成比危機更大的損失更大	通常會可以直接斷線或關機

伺服器環境的變遷



歷史共業

- XXX已經公布新的Patch，但不能馬上安裝？
- CVE 發布一個新的弱點，但是還沒有Patch?
- 使用中的系統已經EOS，但是AP只能在上面跑?
- 資安防護不能只有防毒?
- 如何符合資安法規要求？

新興問題

- Workload的可視性？
- 容器的安全怎模作？
- 如何同時管理多個雲端平台的資安？
- 需要更自動化的進行佈署與管理

Copyright 2021 Trend Micro Inc.

趨勢科技Workload Security

保護環境

Containers

Cloud

Virtual Server

Data Center

docker

kubernetes

aws

Google Cloud

vmware

OPENSHIFT

Azure

Microsoft Hyper-V

作業系統支援

ORACLE SOLARIS

IBM AIX

自動化整合與API

ANSIBLE

servicenow

Microsoft System Center

splunk>

CHEF

puppet

Jenkins

提供Cloud workload、Container和伺服器運行的資安防護

多重防護，一氣呵成

網路安全

Intrusion Prevention

Firewall

Vulnerability Scanning

系統安全

Application Control

Integrity Monitoring

Log Inspection

惡意程式防護

Anti-Malware

Behavioral Analysis Machine Learning

Sandbox Analysis

偵測與回應

Detect

Respond

Investigate

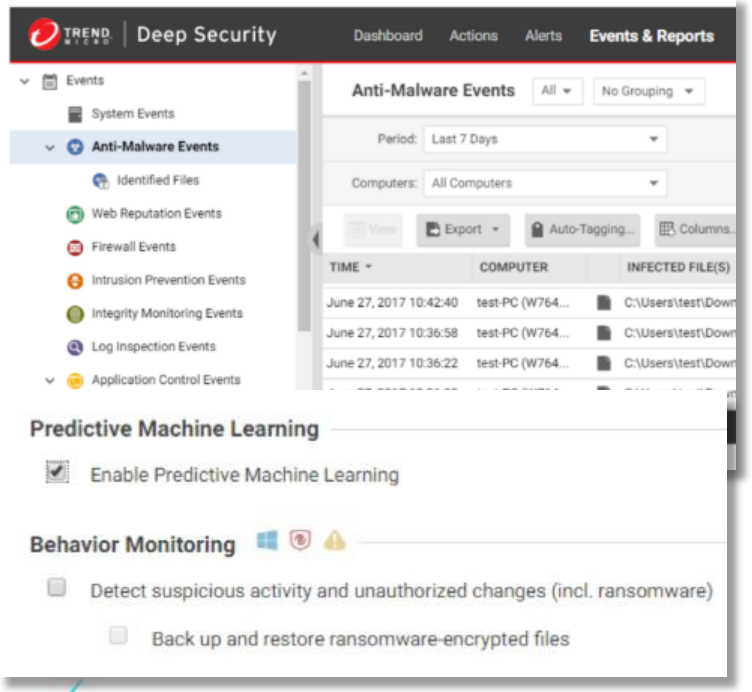
© 2021 Trend Micro Inc.

TREND MICRO

惡意程式防護

提供對惡意程式, 勒索軟體 & 未知威脅的防護 - Anti-Malware

- 雲端病毒碼及檔案信譽評等，隨時取得最新防護
- 深入的檔案分析，找出可疑行為或攻擊指標 (IOA)
- 檔案及記憶體內掃描，提供端點全面防護
- 內建機器學習及行為監控技術
- 阻止未知程序對於混淆文件或加密檔案的嘗試
- 刪除惡意程序並嘗試恢復文件與檔案



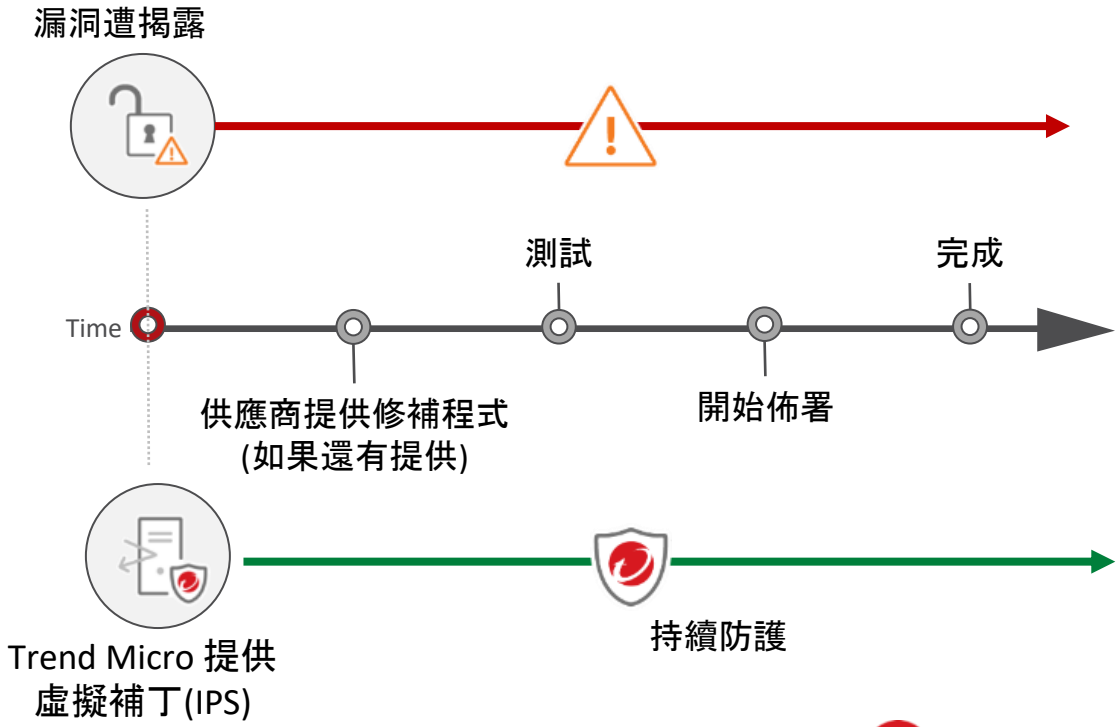
© 2021 Trend Micro Inc.

減少運營衝擊

虛擬補丁 (IPS) - 防護對於作業系統以及應用程序的漏洞攻擊

在OS/AP原廠釋出Patch/Hotfix前，持續提供防護

提供EOS系統防護

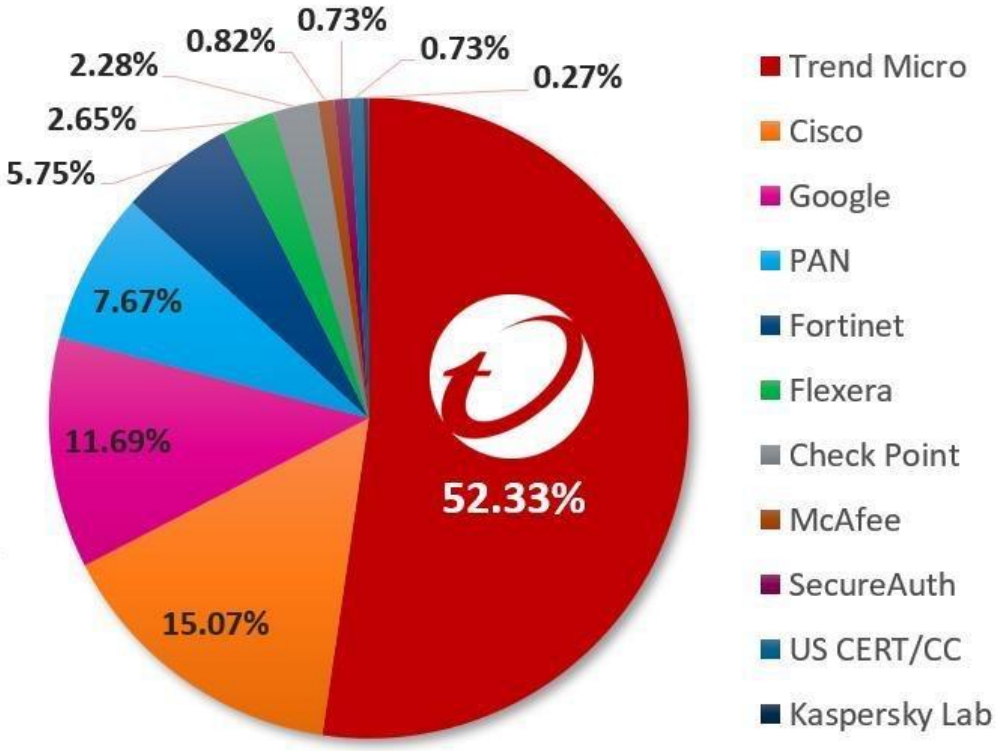


© 2021 Trend Micro Inc.

漏洞威脅研究的市場領導者

ZDI (Zero Day Initiative)

- 3500+ 獨立漏洞研究人員
- 在2021發現了超過一半以上的漏洞



Source: Omdia Research, 2019

© 2021 Trend Micro Inc.

偵測可疑的系統變更

異動監控(Integrity monitoring)與日誌分析(log inspection)

- 偵測和回報重要的安全事件
- 監控檔案、機碼、函式庫和服務的變化
- 建立檢測基準線(baseline)，作為持續監控的依據
- 無需對日誌進行排序，即可在儀表板中突顯可疑事件

File Integrity

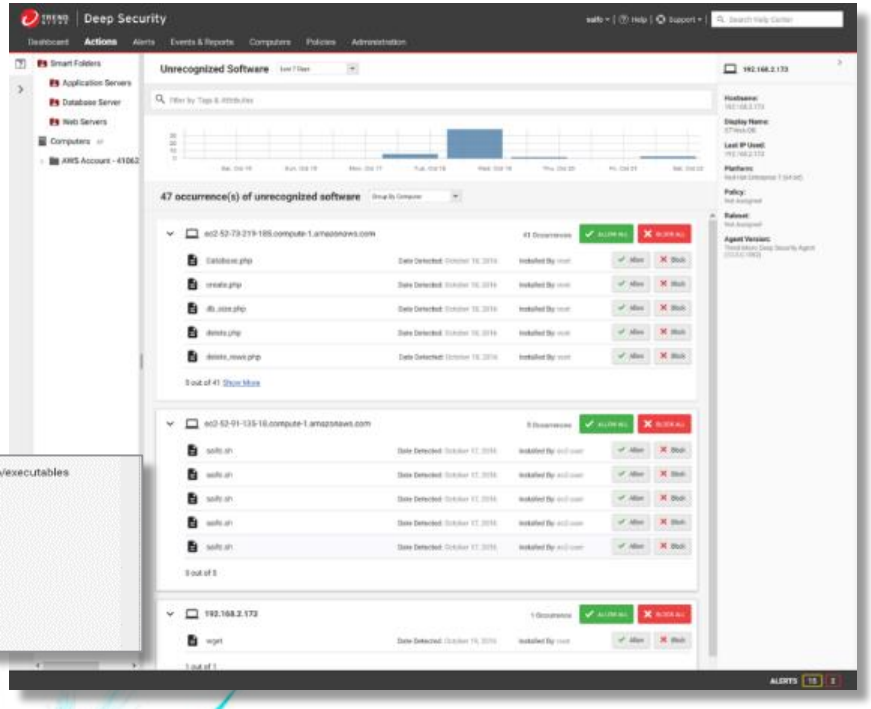
Log Inspection

© 2021 Trend Micro Inc.

阻止未經授權的執行

應用程式控管 - Application Control

- 提供主機可執行檔案的完整可視性
- 鎖定主機上的各種應用程式
- 搭配Trusted updater自動更新白名單，
- 具備自動化機制，持續檢查更新及變更
- 通過Hash檢測，快速回應新發現的威脅（例如 IOC）

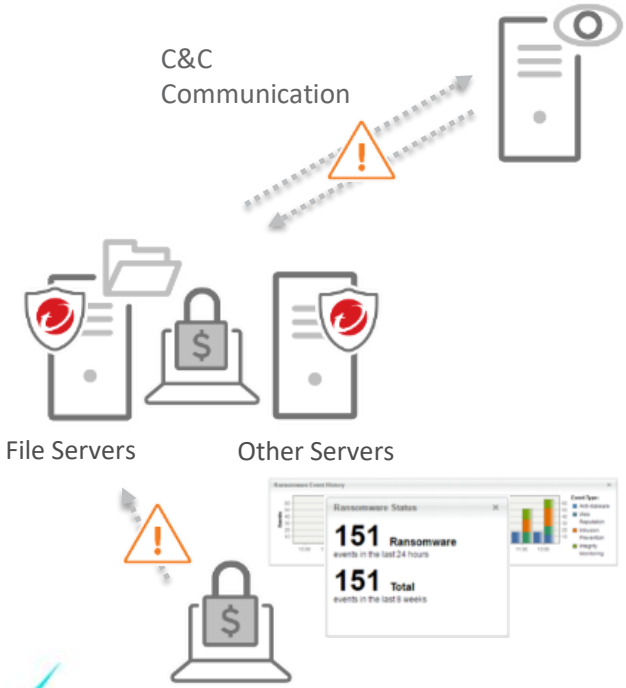


© 2021 Trend Micro Inc.

阻擋勒索軟體攻擊

具備多重防護機制：

- 採取包括行為監控和機器學習在內的進階惡意軟體預防措施，阻止勒索軟體執行
- 應用程序控制，禁止執行任何未許可的程式
- 使用 IPS 抵禦網路攻擊
- 中斷橫向擴散移動(lateral movement）以及中繼站(C&C)連線行為



© 2021 Trend Micro Inc.

加速事件調查與回應

雲端工作負載及伺服器的EDR

受到了什麼影響？

DETECT

檢測逃避標準防禦的進階惡意軟體和可疑行為

被注入了什麼？

RESPOND

採用多種矯正機制及結合工作流，對偵測結果進行回應

傳播到哪裡去了？

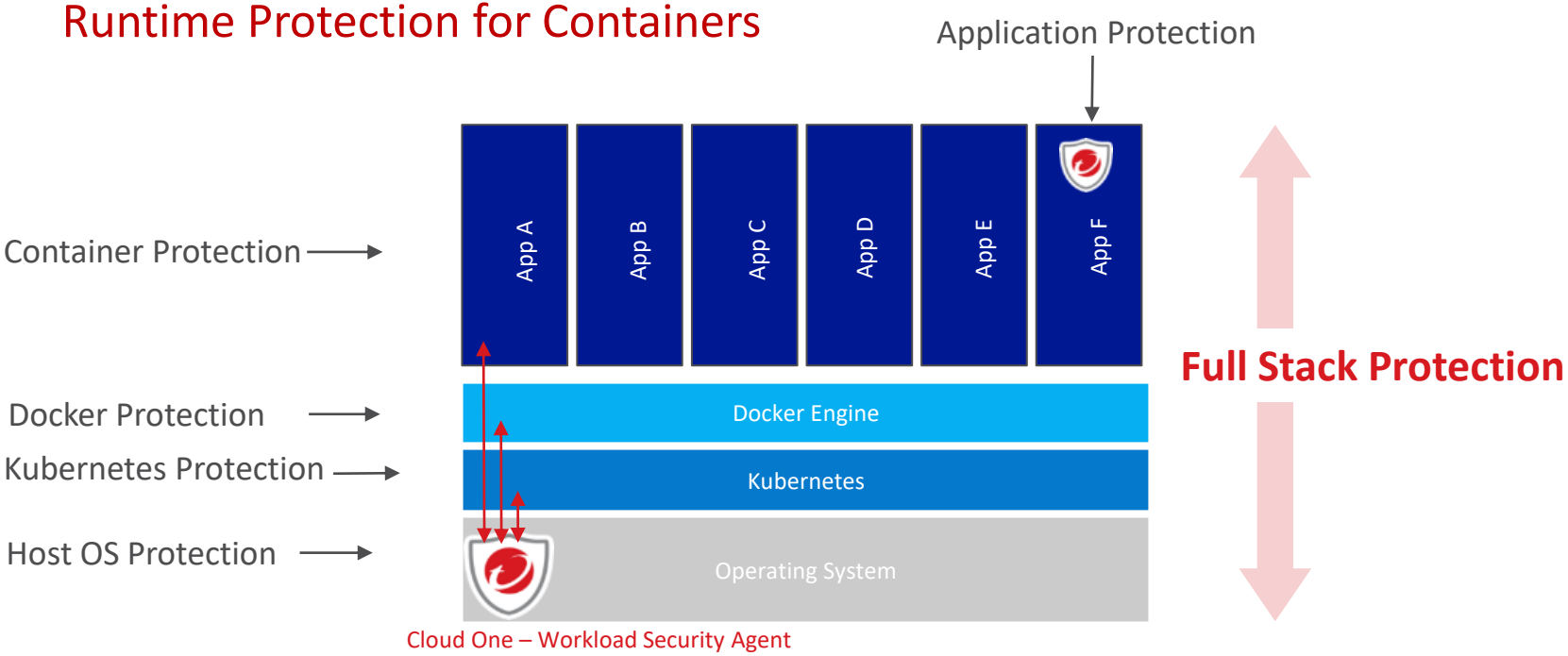
INVESTIGATE

獲得威脅對於運營風險的可視性，並調查威脅嚴重性和影響範圍

© 2021 Trend Micro Inc.

提供容器運行時的防護

Runtime Protection for Containers



提供實體，虛擬以及雲端的Container Node防護

© 2021 Trend Micro Inc.

業界評比

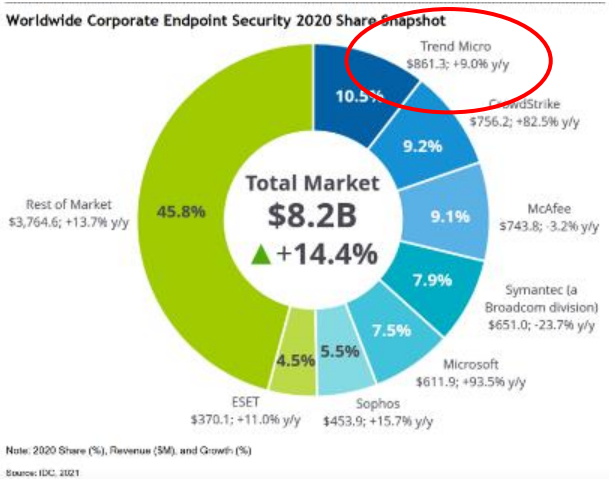
Gartner

7 of 7

Recommendations *

(April 2020)

IDC ANALYZE THE FUTURE



Ranked #1 for

Corporate Endpoint Security market share

(June 2021)

FORRESTER®

Highest Score

for Cloud Workload Security

(Dec 2019)

競爭優勢 Workload Security

跨平台的可視性

aws Azure Google Cloud vmware

支援最多的作業系統

ORACLE SOLARIS IBM AIX

Marketplace出帳用多少算多少

aws marketplace

API自動化

工作負載安全領導者

Gartner IDC FORRESTER

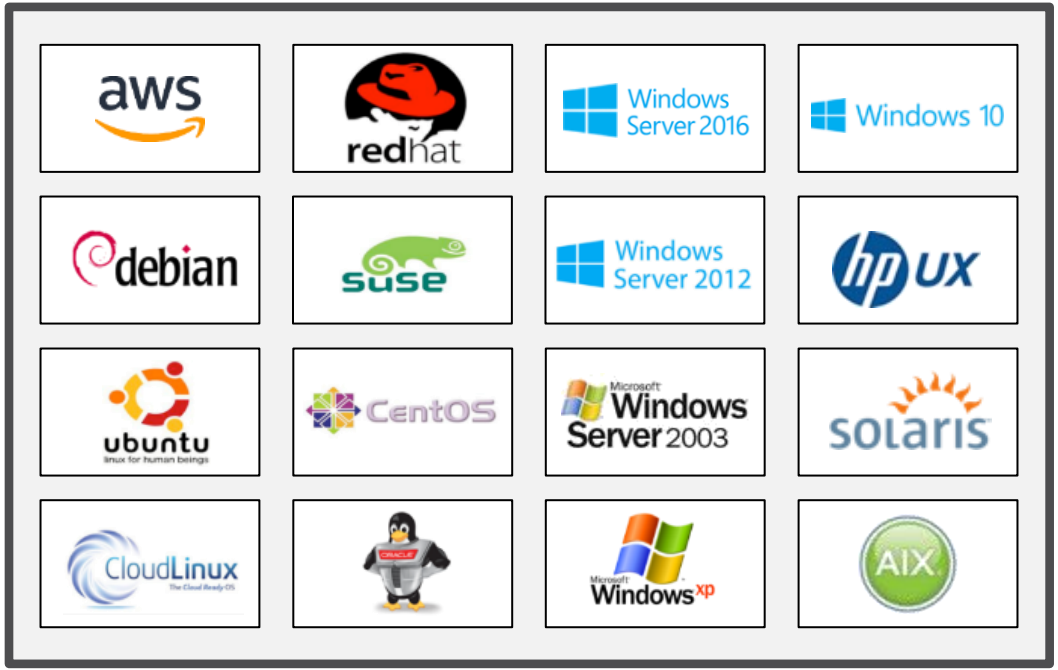
單一代理程式多重防護機制

© 2021 Trend Micro Inc.

TREND MICRO

支援多種平台

支援數以千計的Kernel,
持續快速更新



© 2021 Trend Micro Inc.

TREND MICRO

TREND MICRO

THE ART OF CYBERSECURITY

The global shift of Trend Micro customers from on-premises to SaaS-based security. **Created with real data by artist Brendan Dawes.**