Palo Alto Networks
下一代教育行業資安方案

Brook Lin(林揚城)

Security Consultant

blin@paloaltonetworks.com

主題

- 今天的教育行業現狀
- 面臨的安全挑戰
- 下一代網路安全Next-Generation Cybersecurity
  - 預防(Prevention)勝於治療(Defense&Remediate)的方式
  - 全局可視性以及自動化機制
- 總結

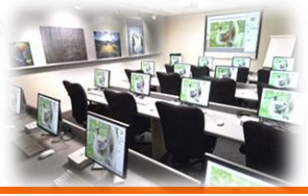
The Cybersecurity Risk

日程

- 今天的教育行業現狀
- 面臨的安全挑戰
- 下一代網路安全Next-Generation Cybersecurity
  - 預防(Prevention)勝於治療(Defense&Remediate)的方式
  - 全局可視性以及自動化機制
- 總結

“數位化校園”

智能教學



互聯網

ISP1 ISP2 TANET

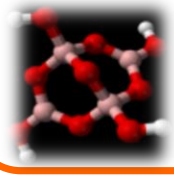
校園無線網路

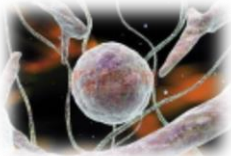
數據中心

宿舍

圖書館

研究機構
Data Centers





“數位化校園”的多種應用

基礎架構	資訊系統, e-Card, Forum/BBS, IPTV, FTP… 視訊會議, DNS, VPN…
教育系統	課程系統, 文件系統, 財務, 人員管理, 學生資料管理…
線上教學	線上課程, 考試中心, 智能化教學…
圖書館和實驗室	圖書館線上服務… 各個學院科系的實驗室系統….

主題

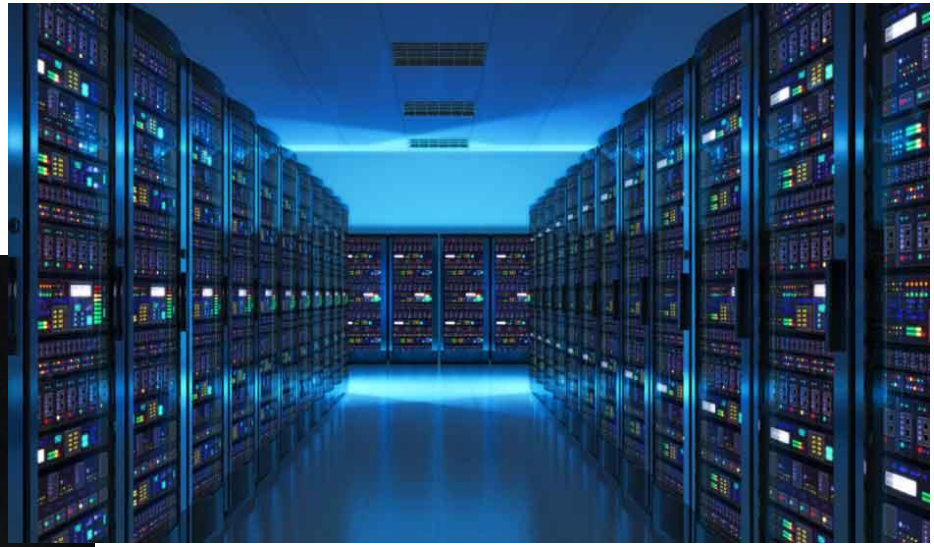
- 今天的教育行業現狀
- **面臨的安全挑戰**
- 下一代網路安全Next-Generation Cybersecurity
  - 預防(Prevention)勝於治療(Defense&Remediate)的方式
  - 全局可視性以及自動化機制
- 總結

The Cybersecurity Risk

The Cyber Breach of Sony

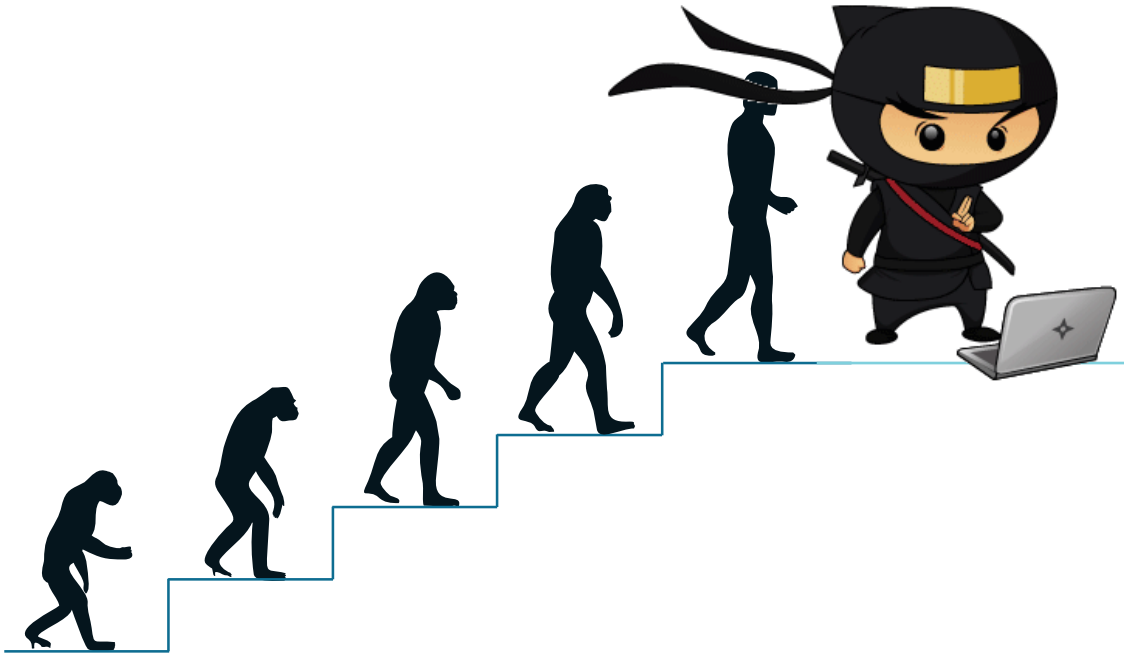
Compute Power and Machine Learning

The downside of the ever-decreasing cost of computing power:



Cybercriminals can launch automated and sophisticated attacks at lower costs

The Evolution of the Attacker



CYBERCRIME

$1+ trillion industry*

CYBER WARFARE

100+ nations

*http://cybersecurityventures.com/cybersecurity-market-report/

Multi-dimensional Attacks And Evasion Tactics

Average Breach Cost

$7.2 Million*

THE EVOLUTION OF THE **ATTACK**

*2017 Cost of Data Breach Study (Benchmark research independently conducted by Ponemon Institute LLC

Today's Threat Landscape

1、教師和學生在任何地方訪問系統

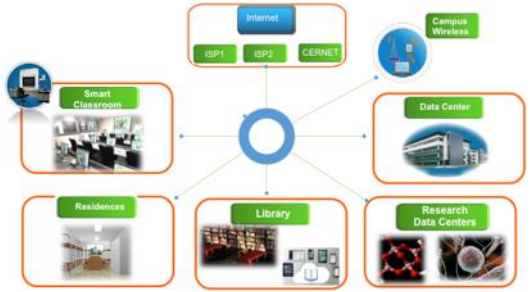
地點多樣化
教室, 宿舍, 咖啡店, 實驗室, 圖書館…
有線的/無線的…

設備多樣化
Public Computer, Laptop, Smart Phone, Pad…

- 需要在任何地點都能夠訪問資料
- 要求能夠利用個人設備來工作和學習
- 基於IP的控制遠遠不滿足需求!

2、重要系統的訪問與防護不能做到視覺化

- 不瞭解核心系統的使用情況和網路應用組成情況
  - 那些應用是正常並且常見的?
  - 那些應用佔用了更多的資源?
  - 網路是否需要改造和升級?
- 需要更靈活和安全的啟用應用，而不僅僅是控制埠
  - 允許, 阻斷, 限制, 掃描, 規範化
- 管理未知流量

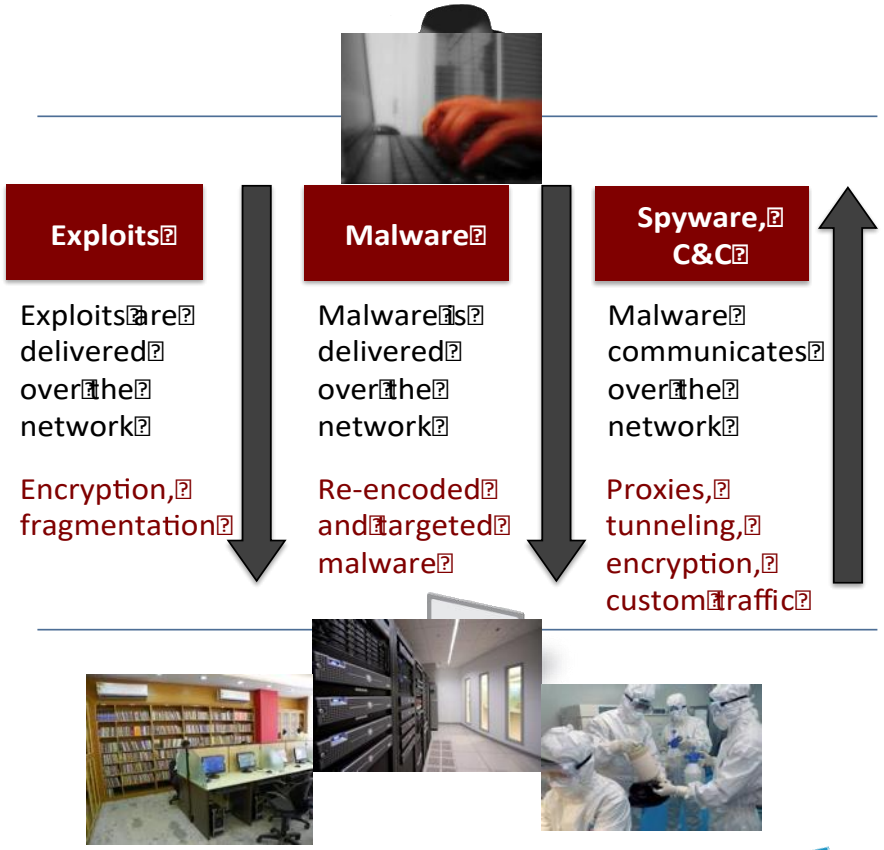


Inspect All Traffic

paloalto NETWORKS

3、學生數量巨大，駭客活動疲於對付

- 漏洞掃描, 組合攻擊, 構造的新型病毒/惡意程式碼
  - 為了好玩和出名而攻擊!
- 伺服器沒辦法及時應用更新
- 對所有區域、埠的流量一視同仁 (沒有標準!)
  - 沒有能夠信任的區域!
- 缺乏綜合的安全防禦手段
  - 攻擊, 新型病毒, 垃圾流量
  - 維護統一的安全性原則和標準
  - 確保良好的性能



4、無法審計使用者的網路行為

- 審計互聯網行為
  - *Yes! We have… “helper”!*
  - with user info?.....*No, only “IP”.*
- 基於不同的應用、實驗室、資料中心?
  - *No…*

5、桌上型電腦與伺服器的安全性漏洞

- 太多的安全性漏洞
  - 薄弱的密碼
  - 共用帳號
  - 作業系統
    - Windows XP to Windows 10
    - MacOS
    - Linux
  - Anti-Virus/Anti-Spyware
    - 免費版本, 被更改的版本
    - 沒有統一的安全性原則

- 一台複雜的電腦對每個人都是充滿風險的
  - *研究資料面臨資訊洩漏的風險*
  - *丟失學校有價值的資訊!*
  - *個人資訊和諮詢的丟失風險*

主題

- 今天的教育行業現狀
- 面臨的安全挑戰
- 下一代網路安全Next-Generation Cybersecurity
  - **預防(Prevention)勝於治療(Defense&Remediate)的方式**
  - 全局可視性以及自動化機制
- 總結

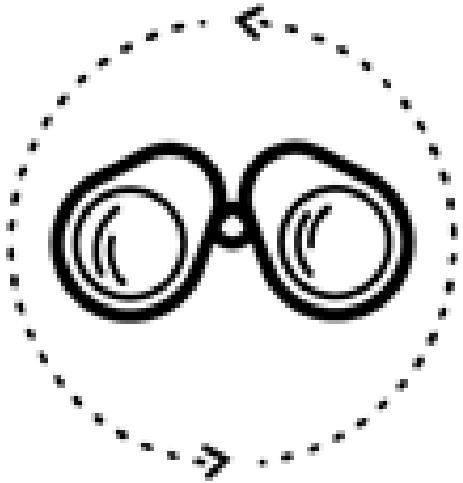
Security Must Transform

ANALYTICS

AUTOMATION

CLOUD-DELIVERED

Visibility and Enforcement



Consumption

operations
data
$$$
decisions
reports
choices
risk
$$$
cost
shadow IT
reports
exposure
decisions
cost
too much data
choices
decisions
applications
consumption
$$$
security
threats
resources
buy
choices
$$$
analysts
$$$
decisions
consume
stolen credentials
decisions
reports
security tools
choices
network security
resources

Evolving Network Usage

Desire

- Open network and unlimited access

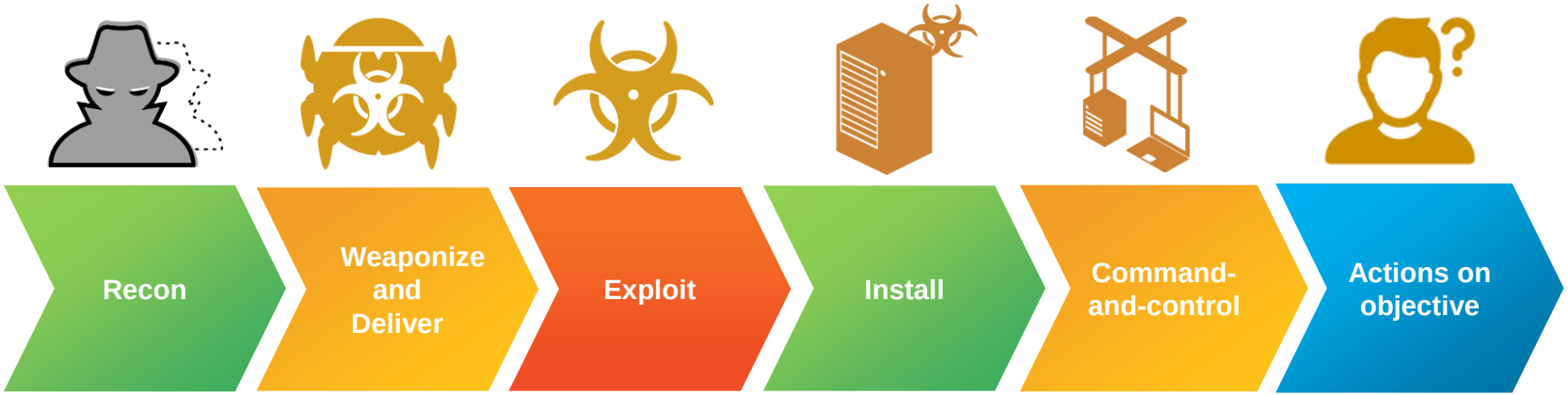
Tension

- Security
- Control
- Visibility
- Performance

Balance

- Granularity

Threat Prevention at All Stages of the Attack Lifecycle



Restrict access based on apps, users, content

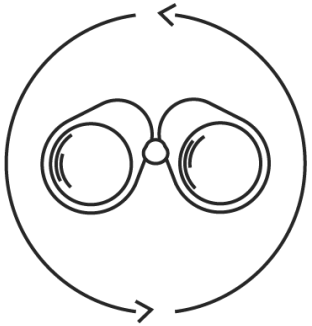
Protect systems and apps from vulnerabilities with threat prevention

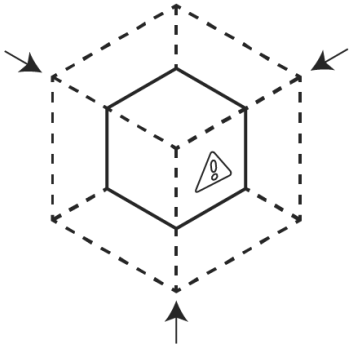
Block Command and Control traffic

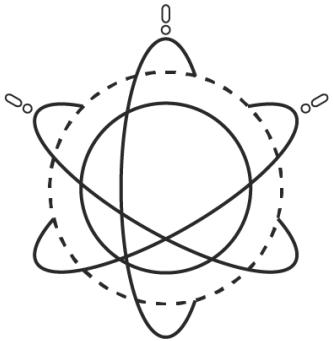
Control sensitive data exfiltration with principle of least privilege

paloalto NETWORKS

Threat Prevention Requirements







COMPLETE VISIBILITY

REDUCE ATTACK SURFACE

PREVENT KNOWN THREATS

PREVENT UNKNOWN THREATS

主題

- 今天的教育行業現狀
- 面臨的安全挑戰
- 下一代網路安全Next-Generation Cybersecurity
  - 預防(Prevention)勝於治療(Defense&Remediate)的方式
  - **全局可視性以及自動化機制**
- 總結

Places Where Visibility and Enforcement are Required

Detect *and* prevent threats at every point across the organization.

At the mobile device

At the internet edge

Between employees and devices within the LAN

At the data center edge, and between VMs

Within private, public, and hybrid clouds

Foundation for Visibility and Enforcement

Next-Generation Firewall

Leader In Network Security

Growing 3x the market

Advanced Endpoint Protection

Total Endpoint Protection

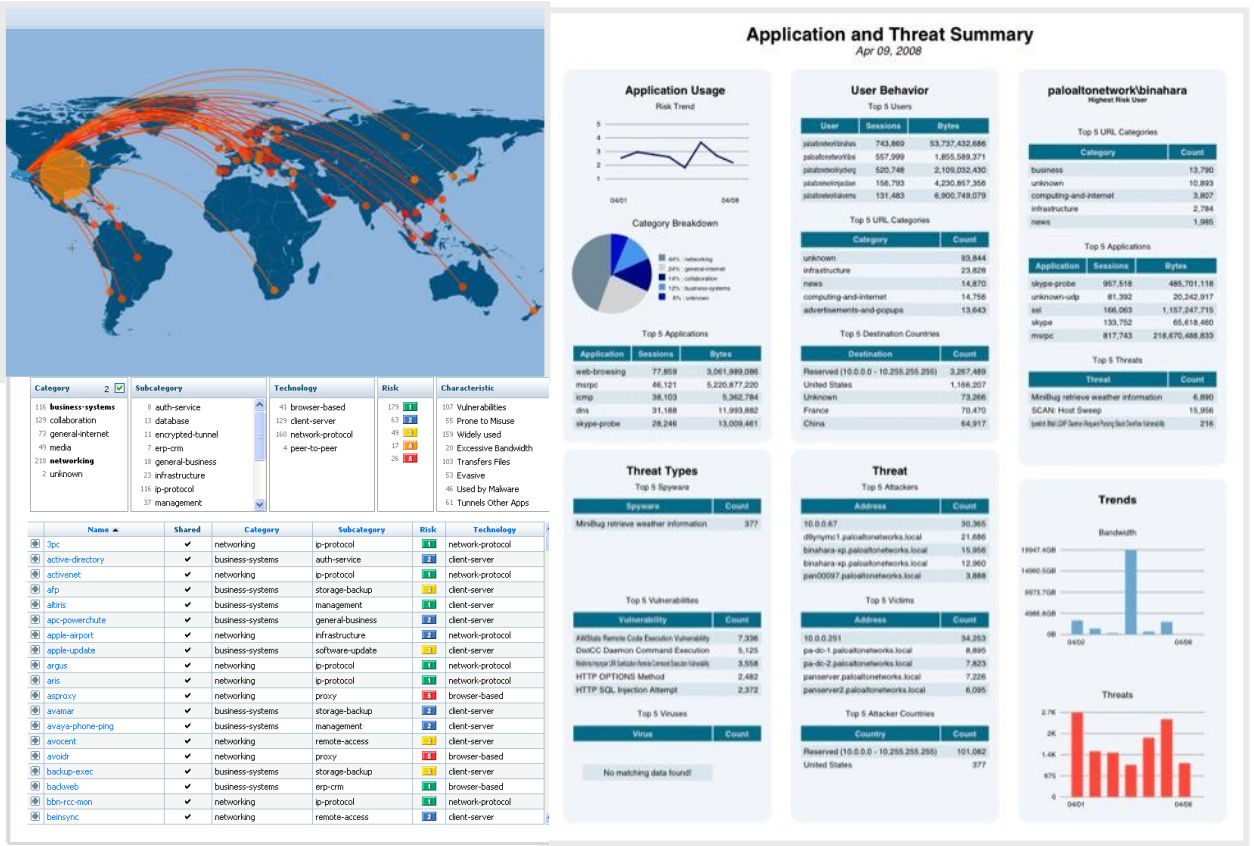
Ransomware & malware
File-less attacks
Exploits

Continuous Cloud Security

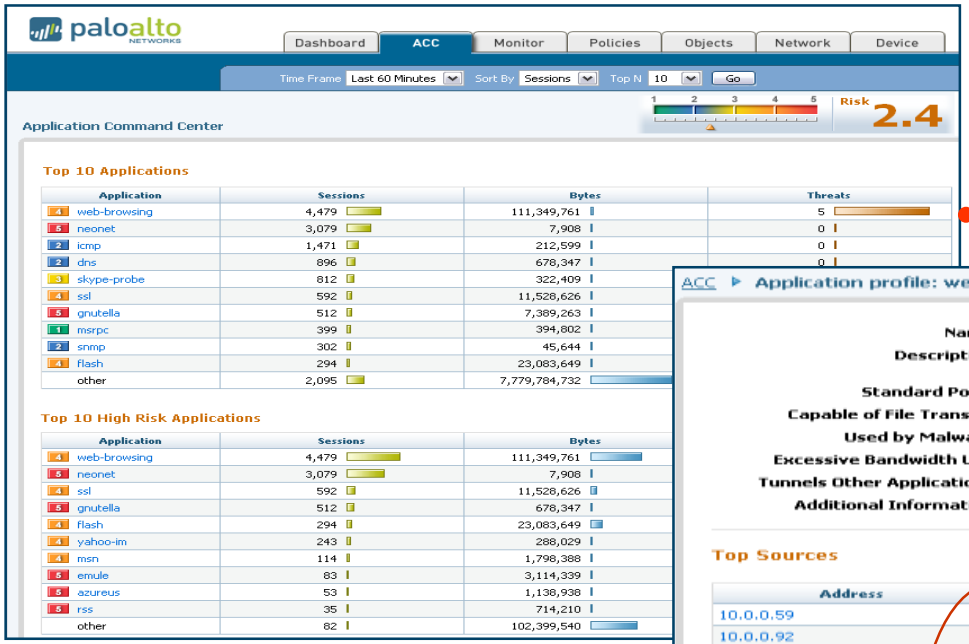
Most Complete Cloud Offering

Inline
API
Host

強大的可視性功能：應用, 用戶, 內容

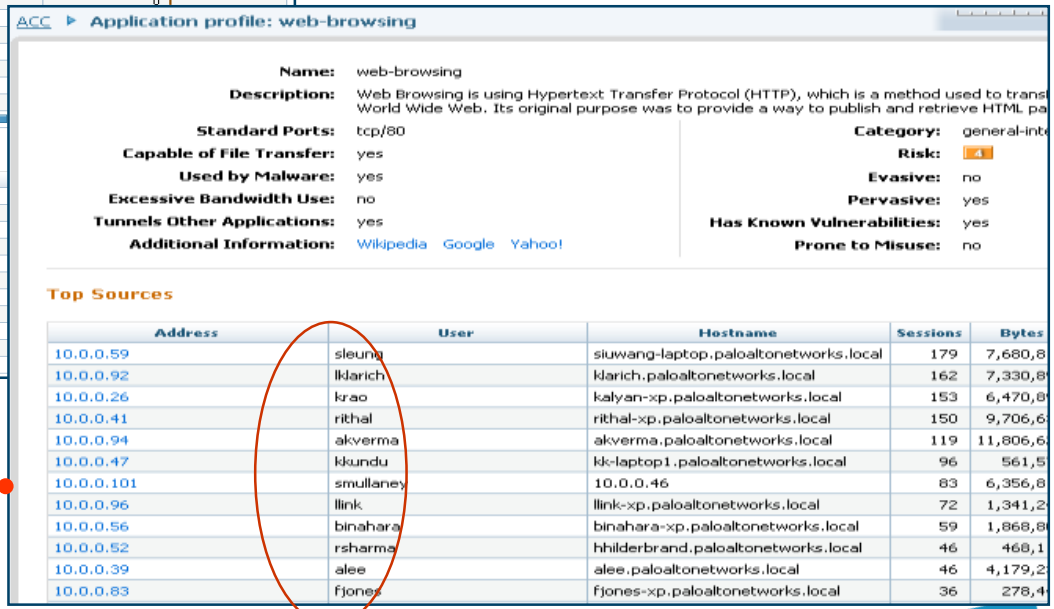


基於使用者網路的可視性



Application Command Center (ACC)

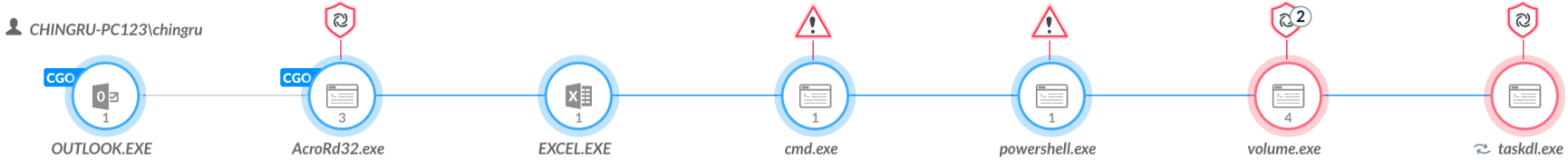
- 準確而詳細的顯示網路中的應用情況
- 顯示top applications, high risk以及應用類別



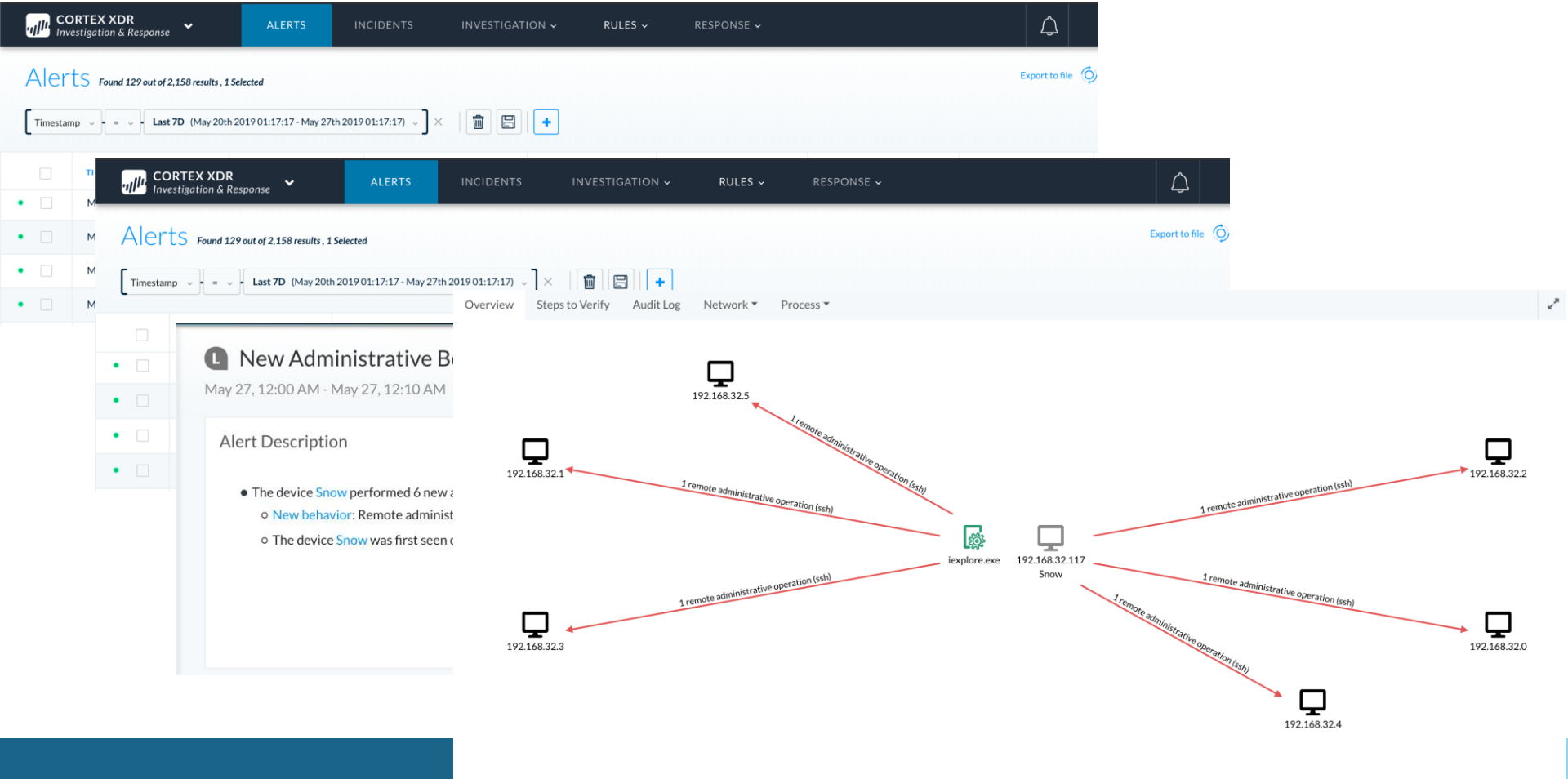
挖掘到具體用戶的行為

- 特定應用的用戶使用量
- 特定用戶訪問的所有應用
- 使用者行為檢測到的病毒、惡意程式或者攻擊行為

基於使用者主機的可視性



基於使用者行為的可視性



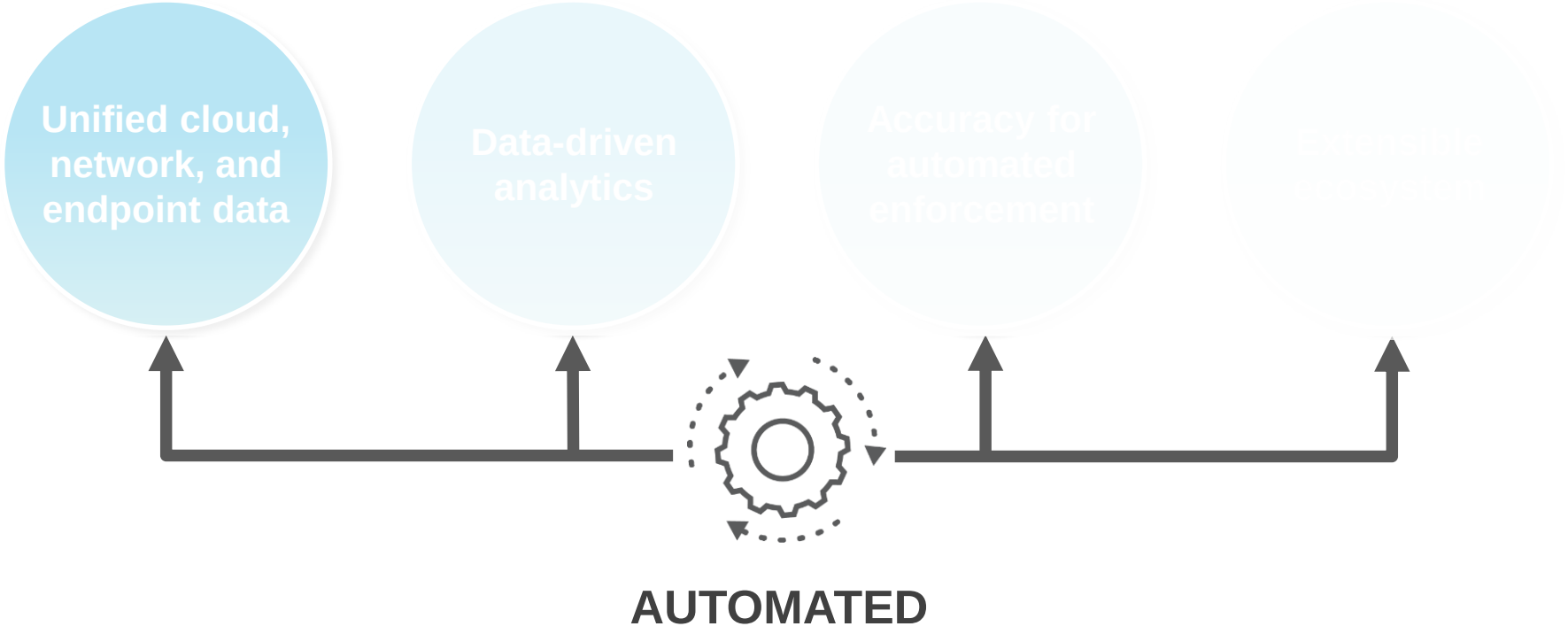
Multiple Approaches to Automation

Immediate detection and prevention of threats

Security policy that dynamically adapts to the environment

Triggered by analytics and machine learning

Built for Automation



Automation Example: Immediate Prevention

1

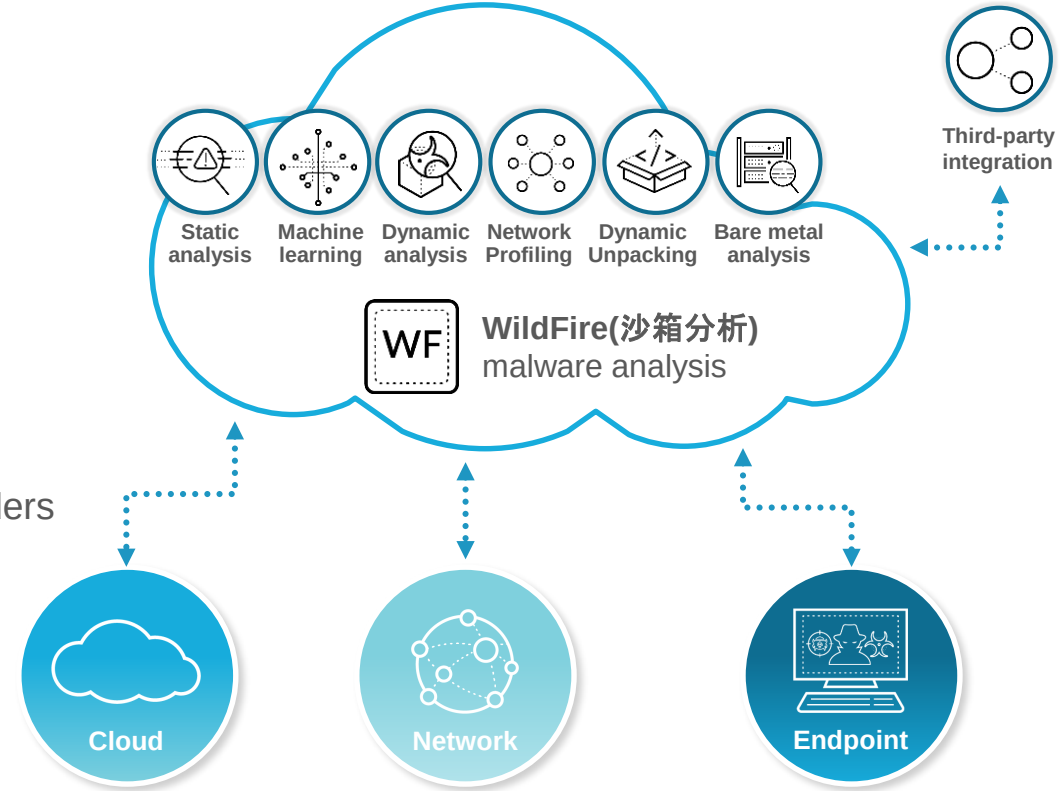
NGFWs, Prisma SaaS, and Traps send unknown or suspicious files and links to WildFire

2

WildFire analyzes the unknown sample, renders a verdict, and shares threat intelligence

3

Platform automatically reprograms network, endpoint, and cloud to protect against new threats



Automation Example: Dynamic Enforcement

User Policy

User Group

User Abstraction

User

Location

In office

Remote

Device

Application Policy

Application

Application Abstraction

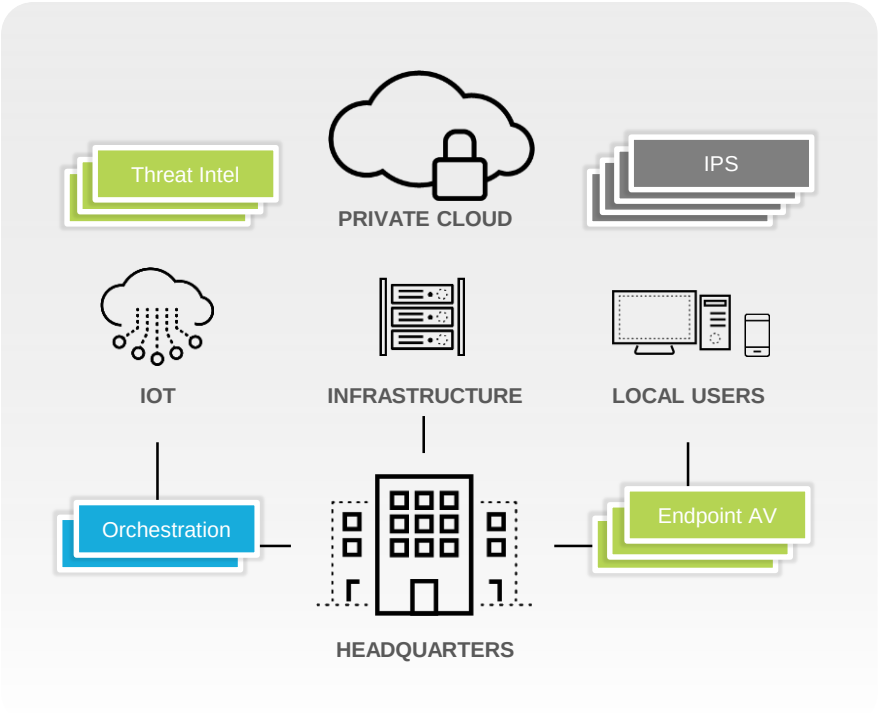
Application

Deployment

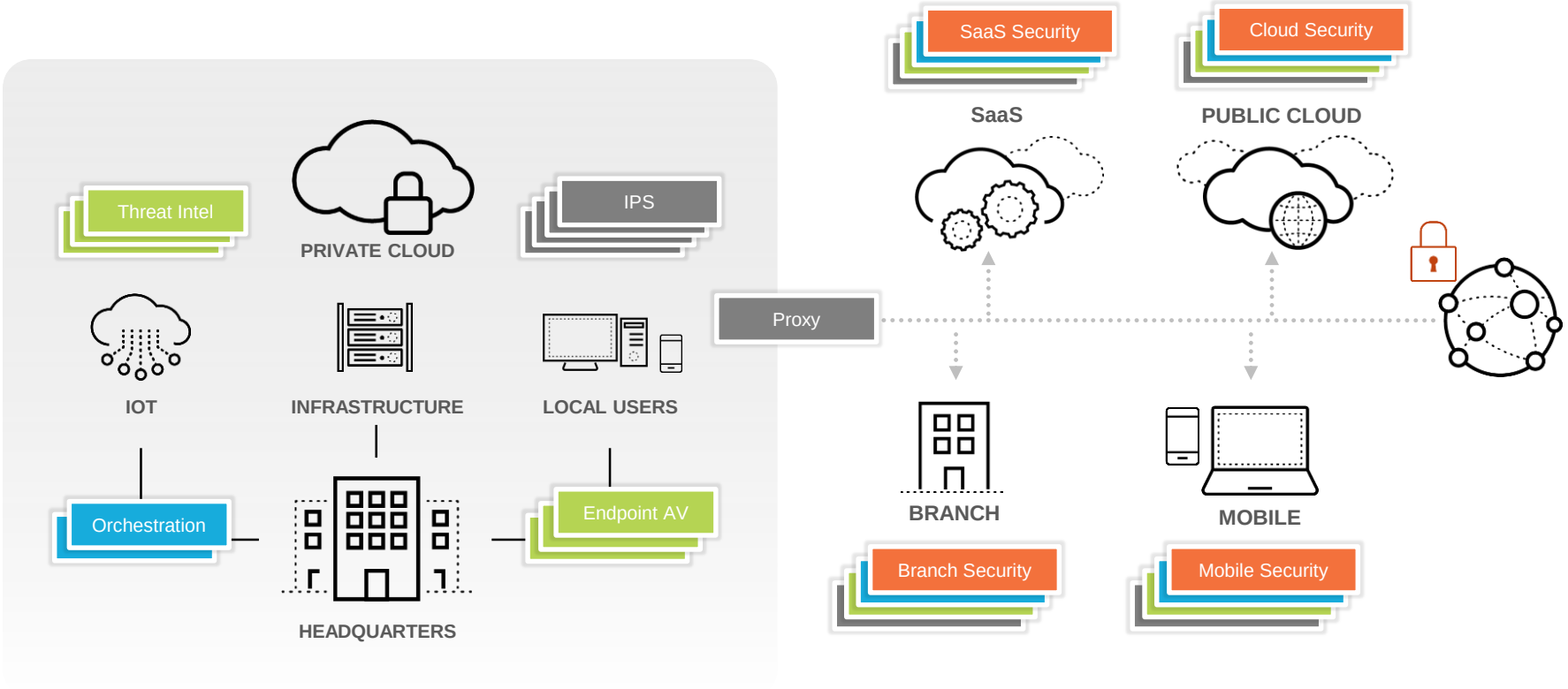
Context

Dev, Test, Prod

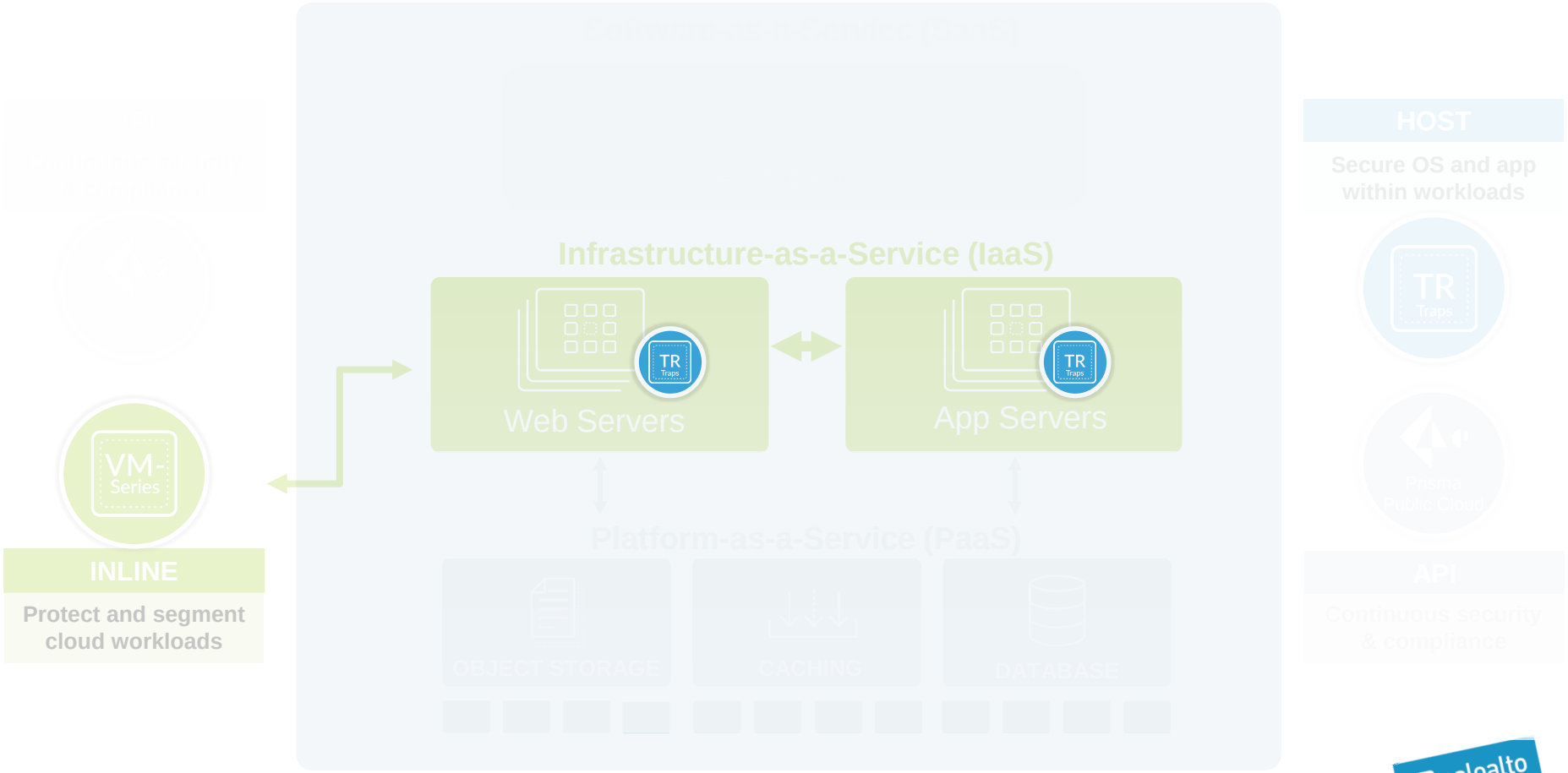
Point Solutions are Not Effective in the Campus



Totally Ineffective for Cloud and for Mobile Workforce



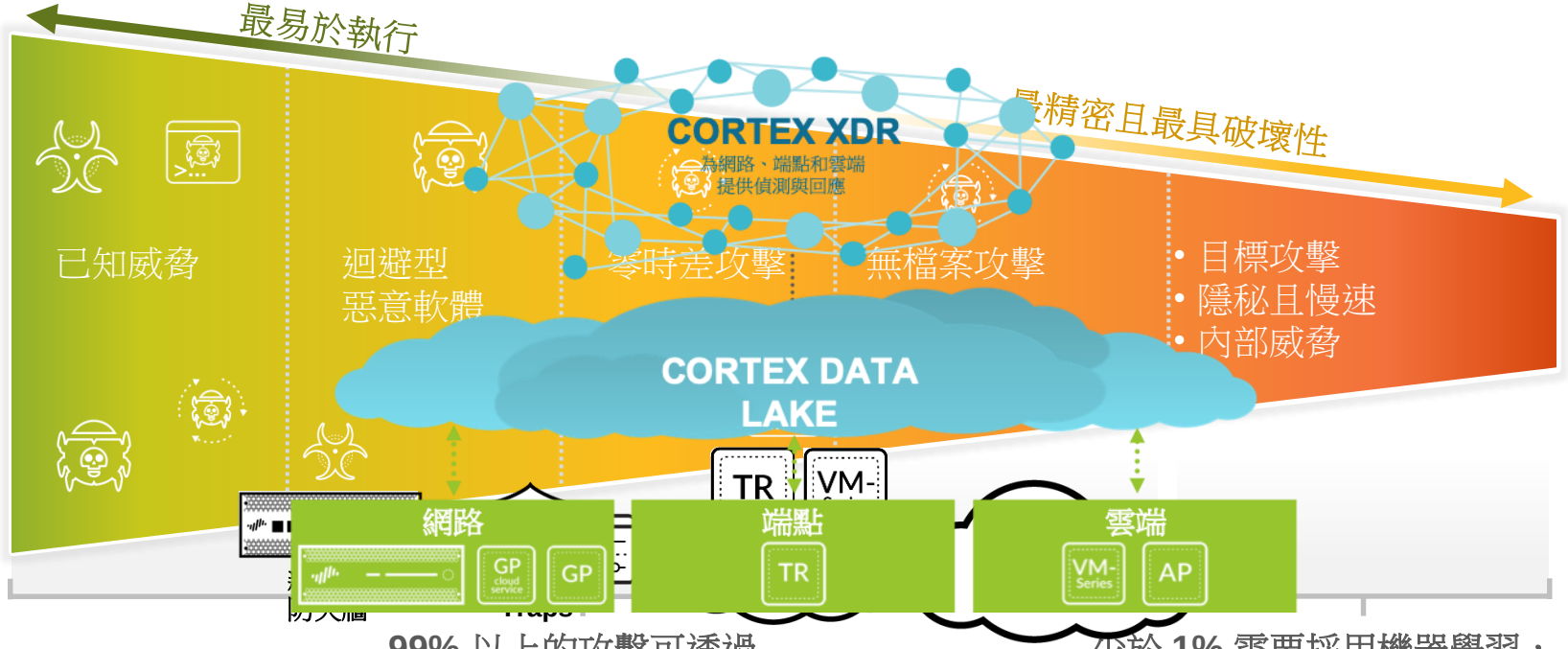
The Most Complete Offering For The Public Cloud



主題

- 今天的教育行業現狀
- 面臨的安全挑戰
- 下一代網路安全Next-Generation Cybersecurity
  - 預防(Prevention)勝於治療(Defense&Remediate)的方式
  - 全局可視性以及自動化機制
- 總結

下一代以AI為主的資安平台



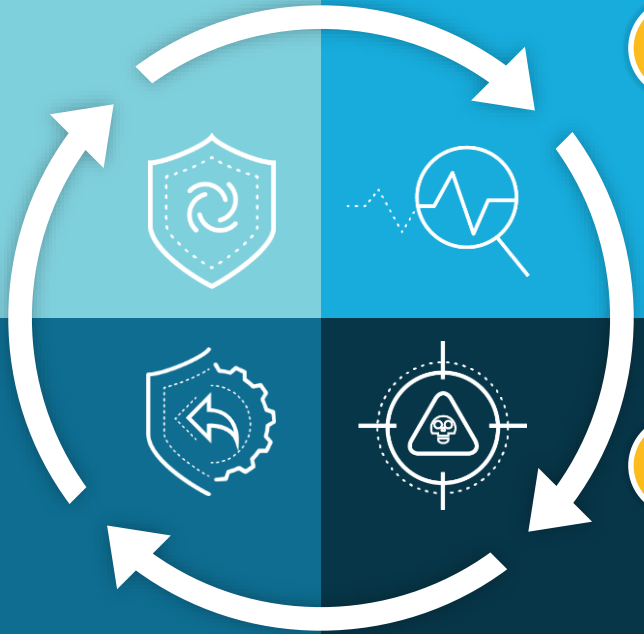
你需要下一代以AI為主的資安平台

1 **預防以及防禦**

針對已知與未知威脅採取持續性防禦措施以保護數據安全

2 **自動偵測**

以機器學習偵測您的環境中的獨特攻擊



3 **快速調查**

在整個安全團隊中加速調查

4 **回應與調整**

運用既得知識增加未來的防禦措施