

# Palo Alto Networks

## 下一代教育行業資安方案

Brook Lin(林揚城)

Security Consultant

[blin@paloaltonetworks.com](mailto: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

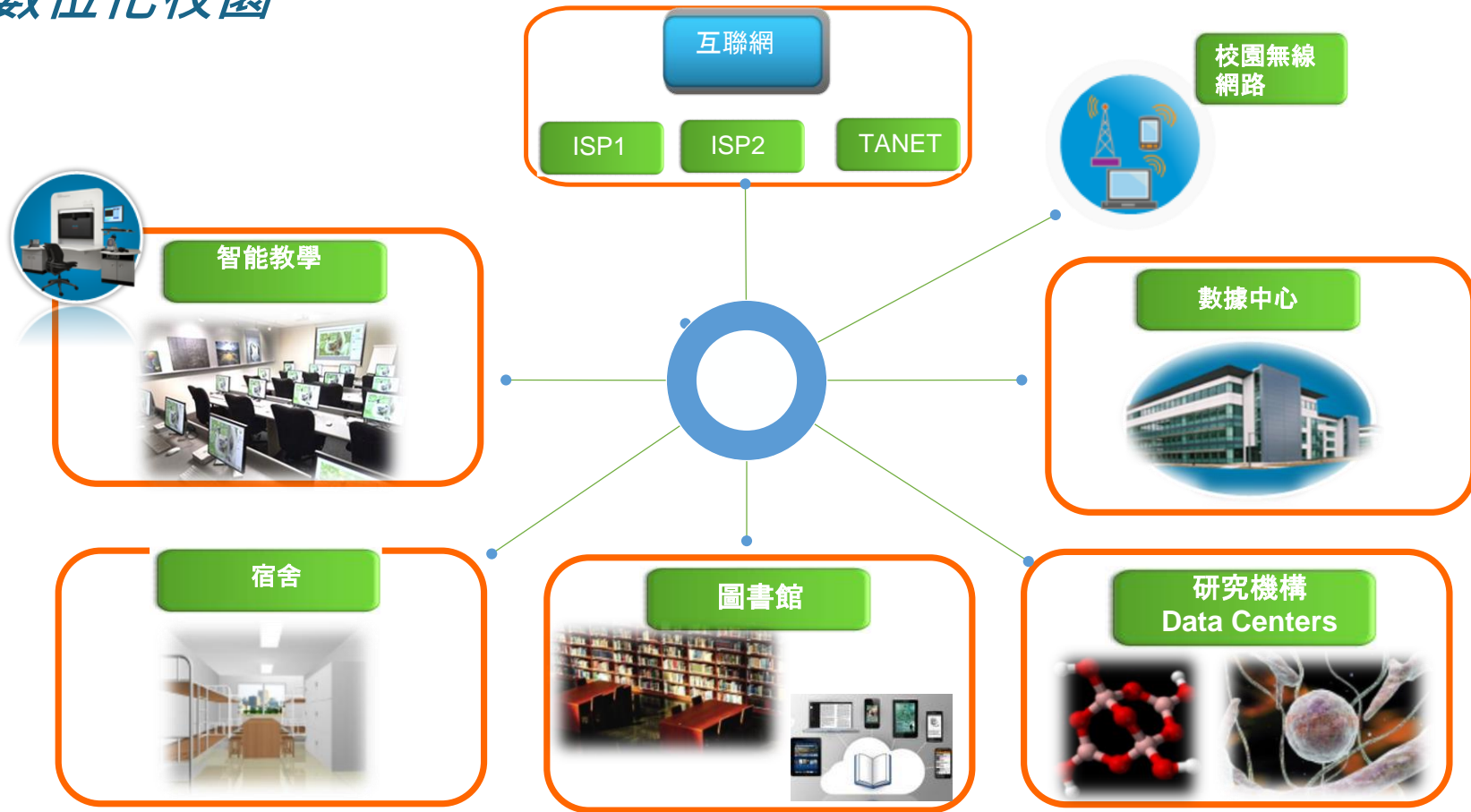
# The Cybersecurity Risk



## 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”



# “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



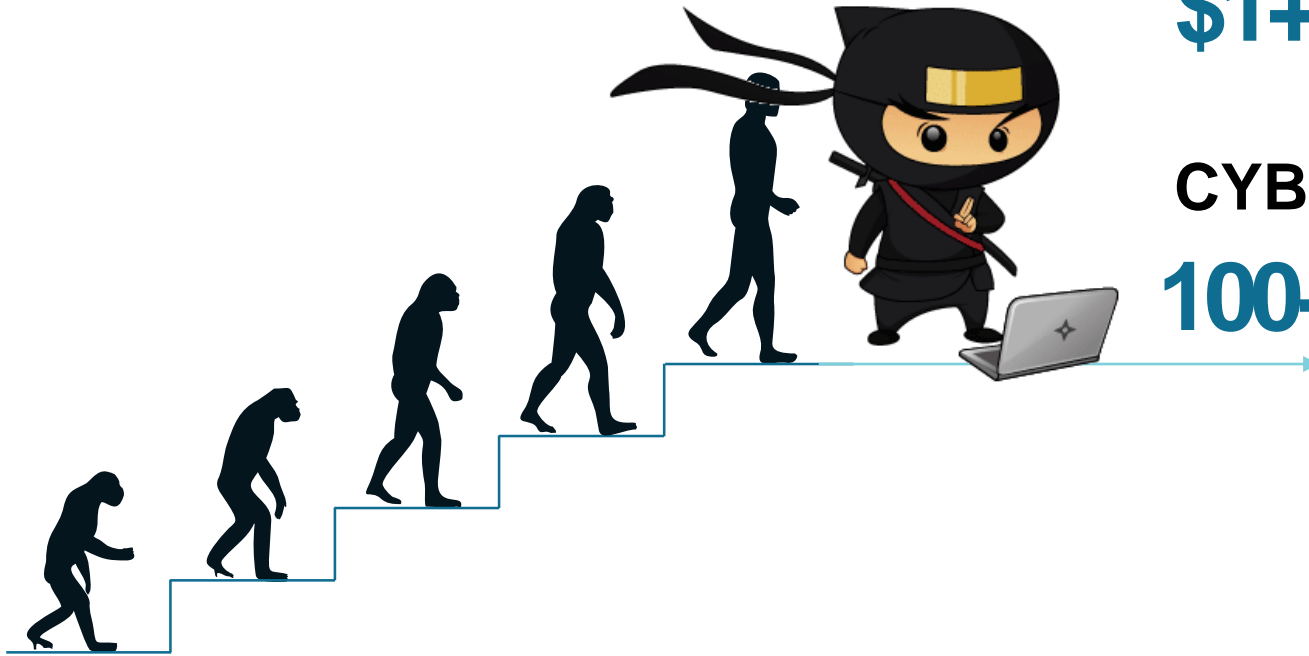
# Compute Power and Machine Learning

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



## THE EVOLUTION OF THE ATTACK

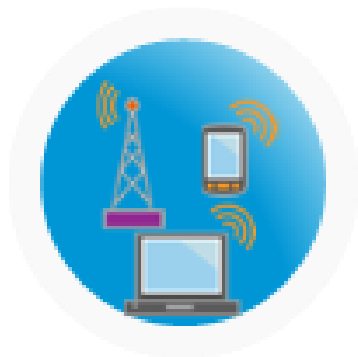


\*2017 Cost of Data Breach Study (Benchmark research independently conducted by Ponemon Institute LLC)

# 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...



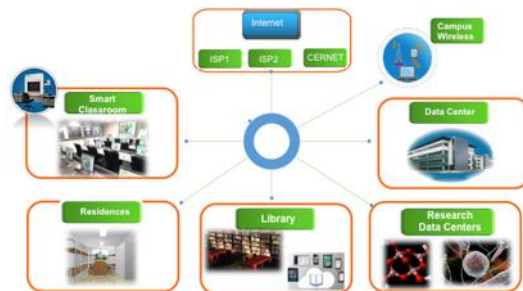
## 設備多樣化

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

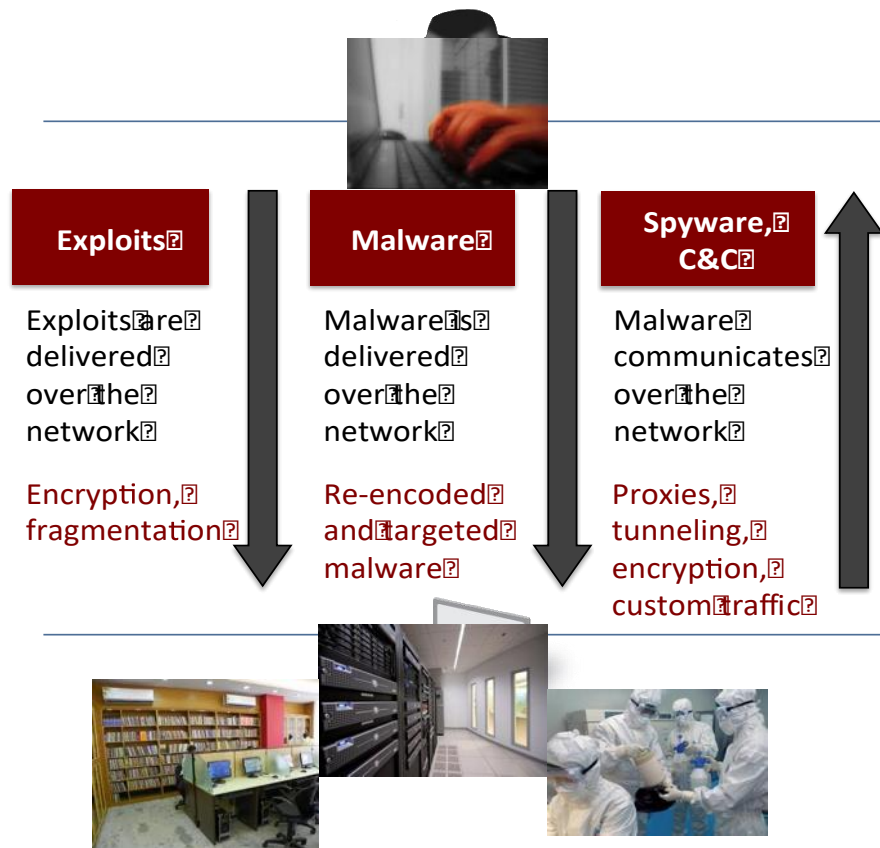
- 不瞭解核心系統的使用情況和網路應用組成情況
  - 那些應用是正常並且常見的？
  - 那些應用佔用了更多的資源？
  - 網路是否需要改造和升級？
- 需要更靈活和安全的啟用應用，而不僅僅是控制埠
  - 允許, 阻斷, 限制, 掃描, 規範化
- 管理未知流量



Inspect All Traffic

### 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...*

10.0.0.207  
10.0.0.211  
10.0.0.232  
10.0.0.230 10.0.0.239  
10.0.0.242  
10.0.0.225 10.0.0.209  
10.0.0.217  
10.0.0.232  
10.0.0.221



## 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**

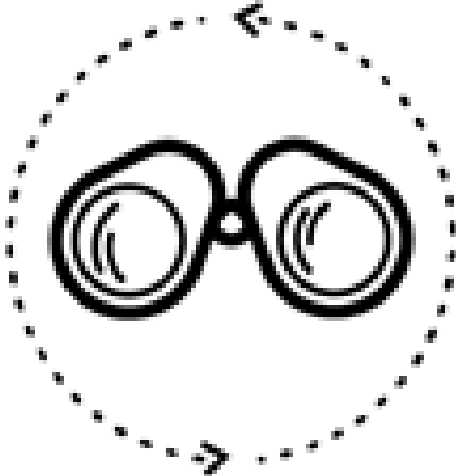


**AUTOMATION**



**CLOUD-DELIVERED**

# Visibility and Enforcement



# Consumption



# Evolving Network Usage

## Desire

- Open network and unlimited access

## Tension

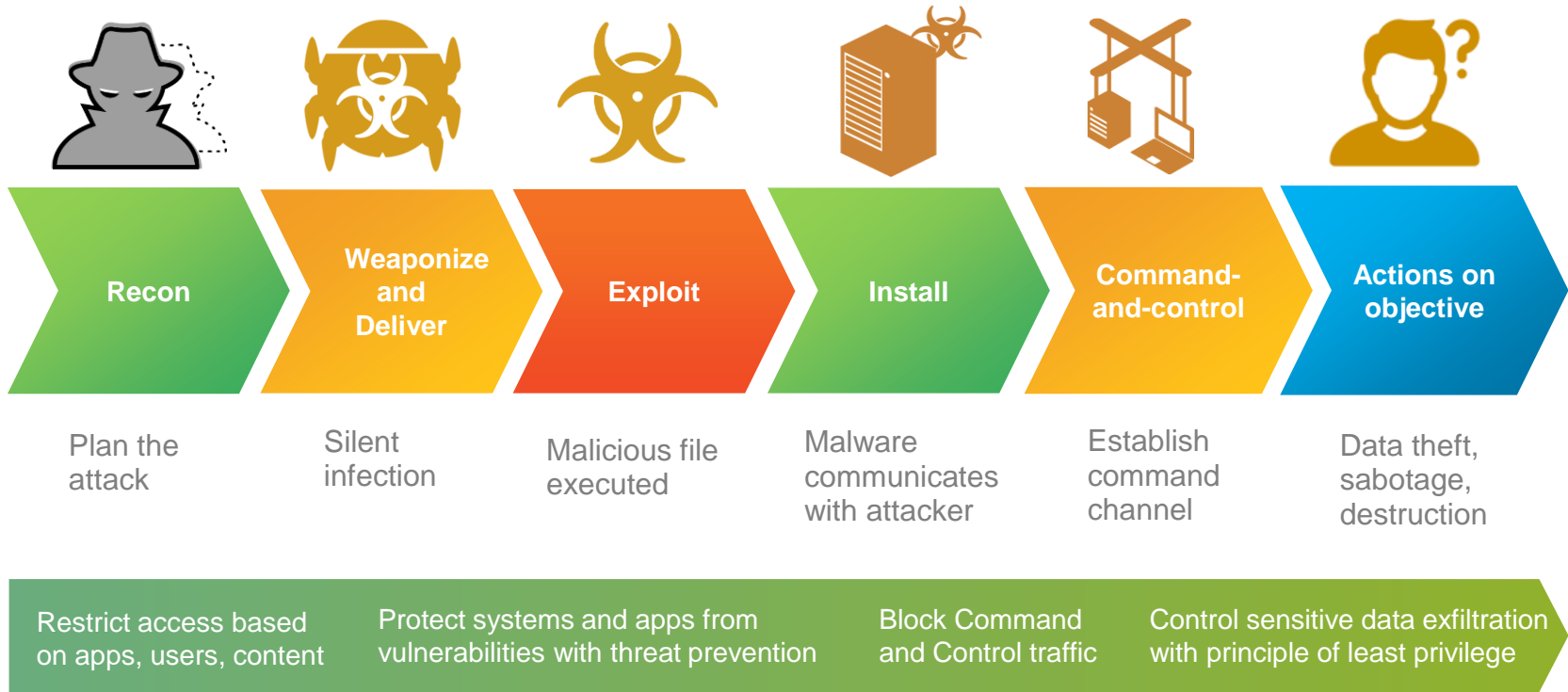
- Security
- Control
- Visibility
- Performance

## Balance

- Granularity

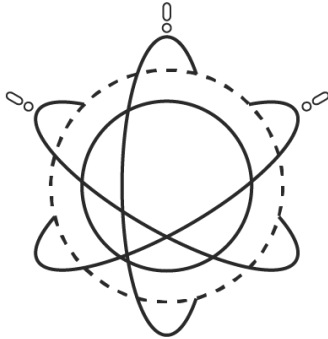
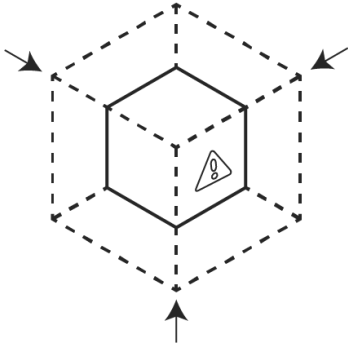
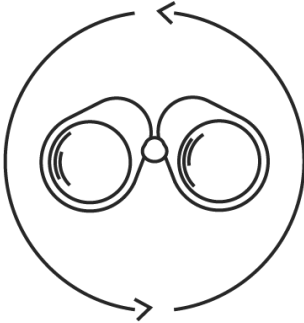


# Threat Prevention at All Stages of the Attack Lifecycle





# 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



Category	Subcategory	Technology	Risk	Characteristic
116 business-systems	0 auth-service	41 browser-based	179 0.4	107 Vulnerabilities
129 collaboration	13 database	129 client-server	63 2.7	53 Prone to Misuse
73 general-internet	11 encrypted-tunnel	160 network-protocol	49 3.3	151 Widely used
49 media	7 erp-crm	4 peer-to-peer	17 4.4	20 Excessive Bandwidth
218 networking	10 general-business		26 5.8	103 Transfers Files
2 unknown	23 infrastructure			53 Evasive
	10 ip-protocol			44 Used by Malware
	27 management			61 Tunnels Other Apps

Name	Shared	Category	Subcategory	Risk	Technology
3pc	✓	networking	ip-protocol	1.8	network-protocol
active-directory	✓	business-systems	auth-service	2.8	client-server
activenet	✓	networking	ip-protocol	1.8	network-protocol
afp	✓	business-systems	storage-backup	3.1	client-server
ahrs	✓	business-systems	management	1.1	client-server
app-powerchute	✓	business-systems	general-business	2.8	client-server
apple-airport	✓	networking	infrastructure	2.8	network-protocol
apple-update	✓	business-systems	software-update	3.1	client-server
argus	✓	networking	ip-protocol	1.1	network-protocol
aris	✓	networking	ip-protocol	1.1	network-protocol
asproxy	✓	networking	proxy	3.8	browser-based
axshare	✓	business-systems	storage-backup	2.8	client-server
axshare-phone-ping	✓	business-systems	management	3.8	client-server
axshare	✓	networking	remote-access	3.1	client-server
avoid	✓	networking	proxy	1.8	browser-based
backip-exec	✓	business-systems	storage-backup	3.1	client-server
backweb	✓	business-systems	erp-crm	1.8	browser-based
bbn-icc-mon	✓	networking	ip-protocol	1.1	network-protocol
beinsync	✓	networking	remote-access	2.8	client-server

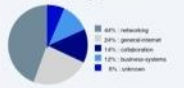
## Application and Threat Summary

Apr 09, 2008

### Application Usage



### Category Breakdown



### Top 5 Applications

Application	Sessions	Bytes
web-browsing	77,859	3,041,989,086
msrpc	46,121	5,220,877,220
icmp	36,103	5,362,784
dns	31,188	11,993,882
skype-probe	28,248	13,009,481

### Threat Types

Spynware	Count
Mirlib retrieve weather information	377

### Top 5 Vulnerabilities

Vulnerability	Count
AKISite Remote Code Execution Vulnerability	7,336
DirCC Daemon Command Execution	6,125
WinExec @lan-hack/remote-access	5,556
HTTP OPTIONS Method	2,482
HTTP SQL Injection Attempt	2,372

### Top 5 Viruses

Virus	Count
No matching data found!	

### User Behavior

#### Top 5 Users

User	Sessions	Bytes
palto@netbinars	743,869	53,737,432,686
palto@network	557,999	1,855,589,371
palto@network	520,748	2,109,032,450
palto@network	156,793	4,230,867,356
palto@network	131,483	6,900,749,079

#### Top 5 URL Categories

Category	Count
unknown	93,844
infrastructure	23,828
news	14,670
computing-and-internet	14,758
advertisements-and-popups	13,643

#### Top 5 Destination Countries

Destination	Count
Reserved (10.0.0.0 - 10.255.255.255)	3,267,489
United States	1,186,207
Unknown	73,286
France	70,470
China	64,917

### palto@network/binahara

#### Highest Risk User

#### Top 5 URL Categories

Category	Count
business	13,790
unknown	10,893
computing-and-internet	3,807
infrastructure	2,784
news	1,985

#### Top 5 Applications

Application	Sessions	Bytes
skype-probe	967,518	485,701,118
unknown-rdp	81,392	20,242,917
ssl	166,063	1,137,247,715
skype	133,752	65,618,460
msrpc	817,743	218,670,488,833

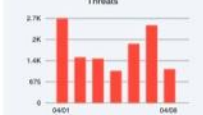
#### Top 5 Threats

Threat	Count
Mirlib retrieve weather information	6,890
SCAN: Host Sweep	15,956
Just for Fun host/reqs/reqs/reqs/reqs	216

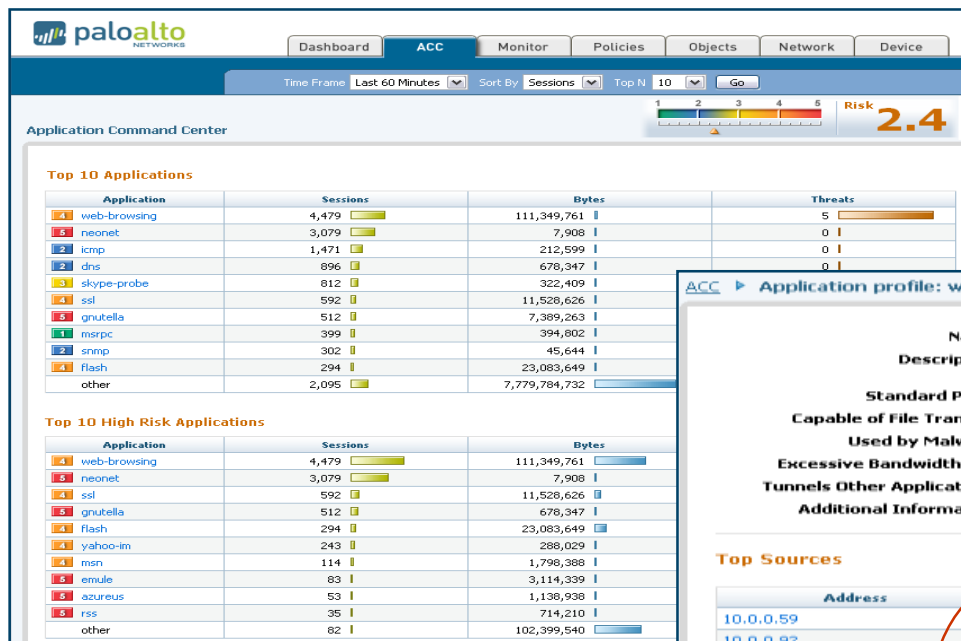
### Trends



### Threats

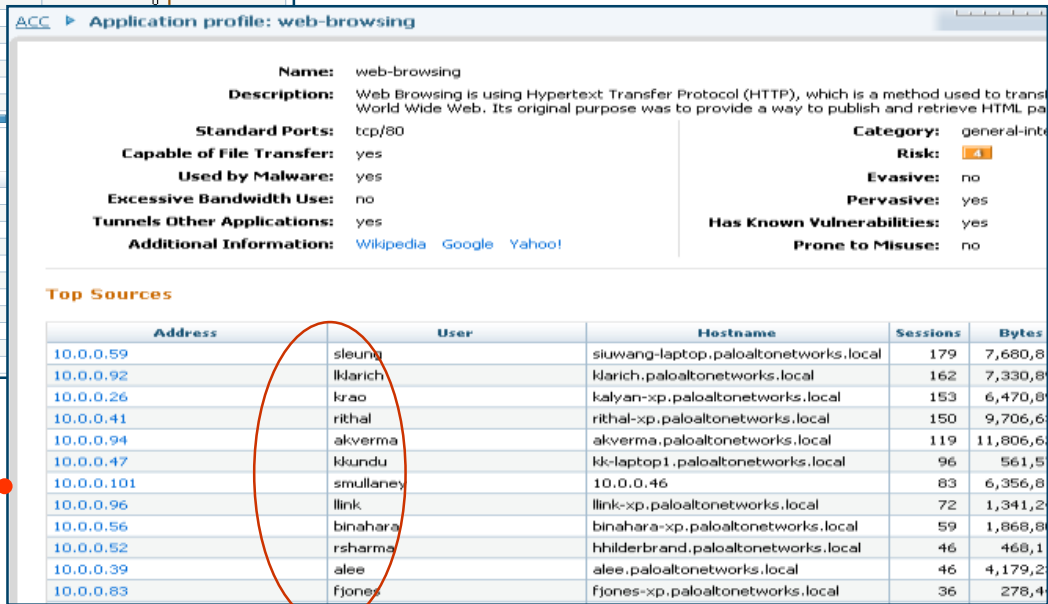


# 基於使用者網路的可視性



## Application Command Center (ACC)

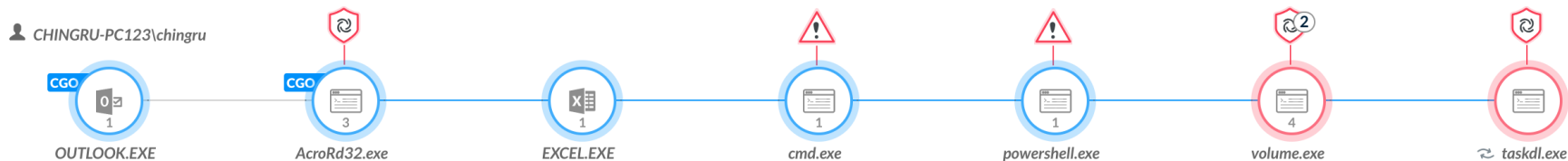
- 準確而詳細的顯示網路中的應用情況
- 顯示top applications, high risk以及應用類別



## 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

CORTEX XDR Investigation & Response

ALERTS INCIDENTS INVESTIGATION RULES RESPONSE

Alerts Found 129 out of 2,158 results, 1 Selected

Export to file

Timestamp Last 7D (May 20th 2019 01:17:17 - May 27th 2019 01:17:17)

CORTEX XDR Investigation & Response

ALERTS INCIDENTS INVESTIGATION RULES RESPONSE

Alerts Found 129 out of 2,158 results, 1 Selected

Export to file

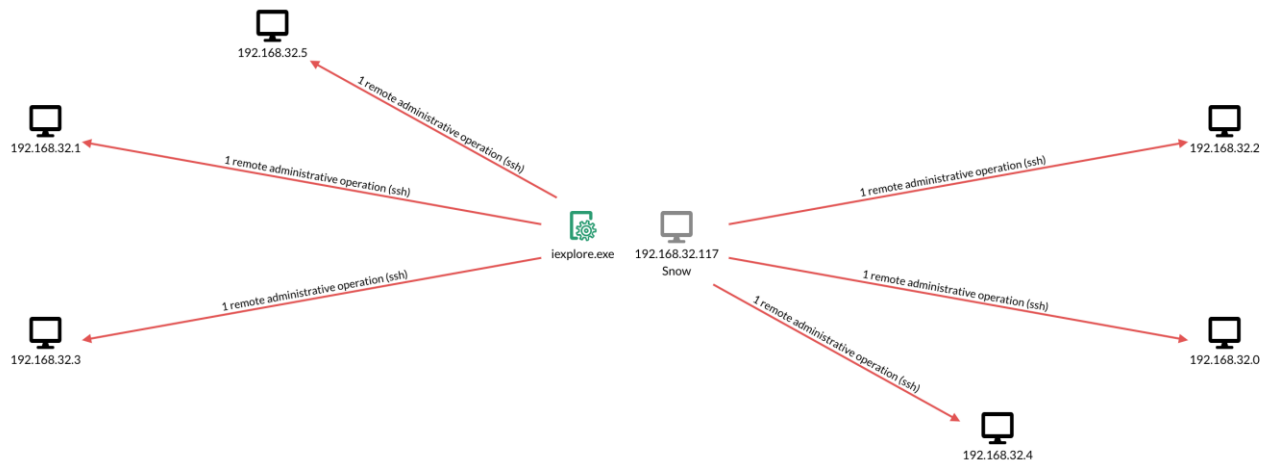
Timestamp Last 7D (May 20th 2019 01:17:17 - May 27th 2019 01:17:17)

Overview Steps to Verify Audit Log Network Process

**New Administrative Behavior**  
May 27, 12:00 AM - May 27, 12:10 AM

Alert Description

- The device **Snow** performed 6 new administrative operations:
  - New behavior:** Remote administrative operation (ssh) to 192.168.32.1
  - The device **Snow** was first seen on May 27, 12:00 AM





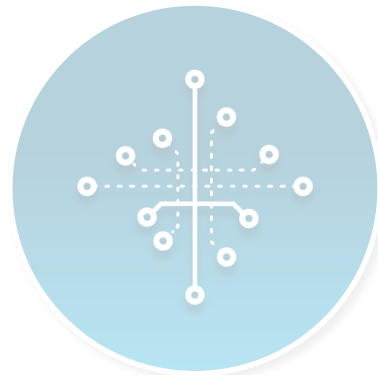
# Multiple Approaches to Automation



Immediate detection  
and prevention of  
threats

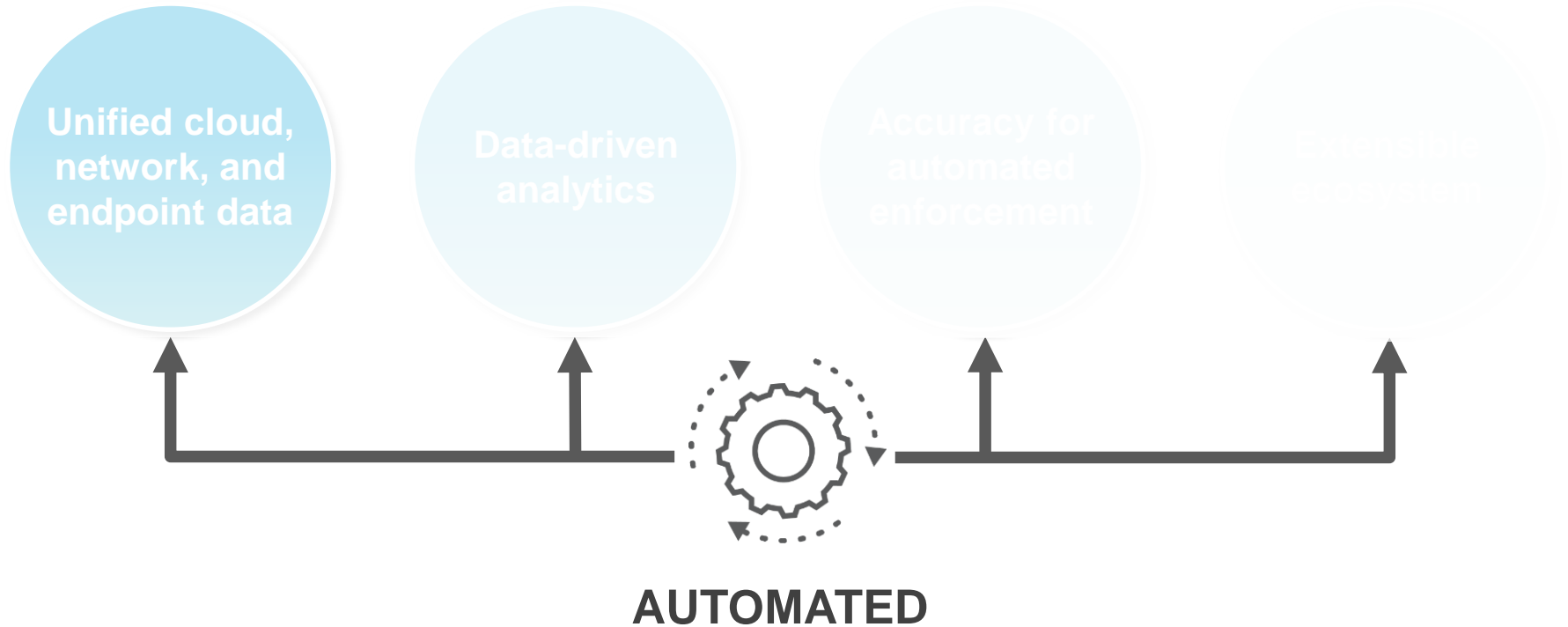


Security policy that  
dynamically adapts to the  
environment



Triggered by  
analytics and  
machine learning

# Built for Automation



# Automation Example: Immediate Prevention

1

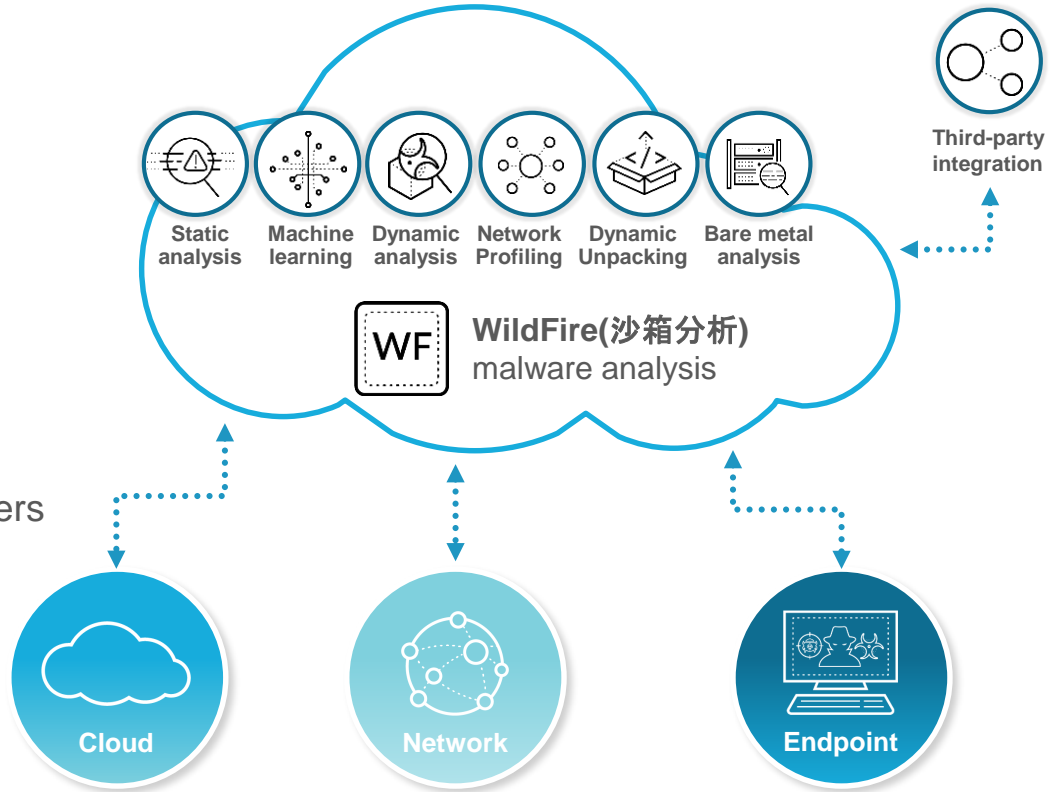
NGFWs, Prisma SaaS, and Traps send unknown or suspicious files and links to WildFire

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



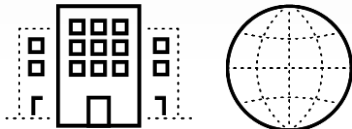
User Group

User Abstraction

User



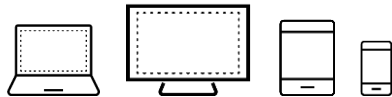
Location



In office

Remote

Device



## Application Policy



Application

Application Abstraction

Application



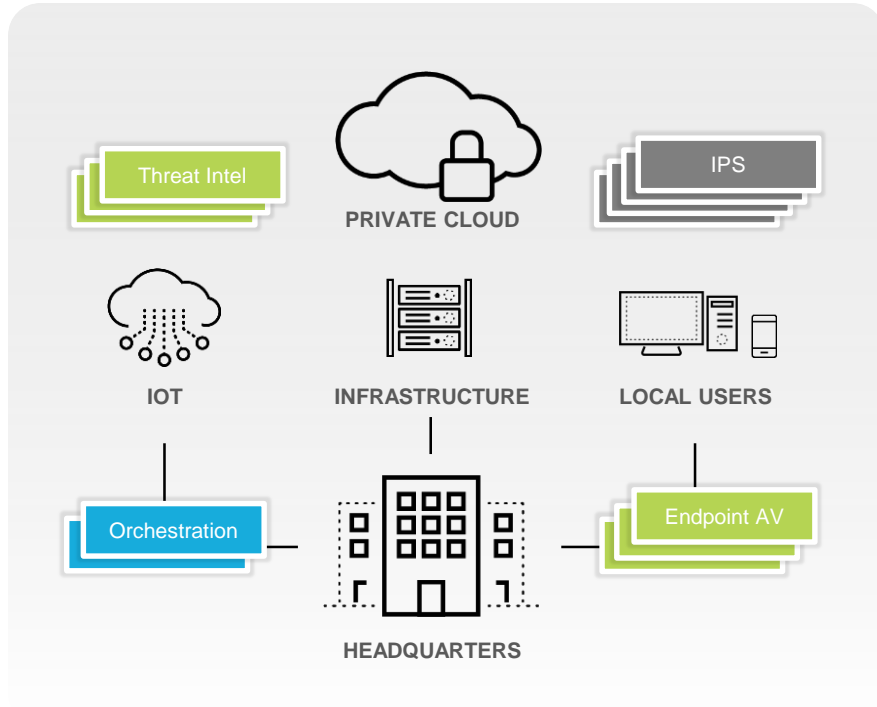
Deployment



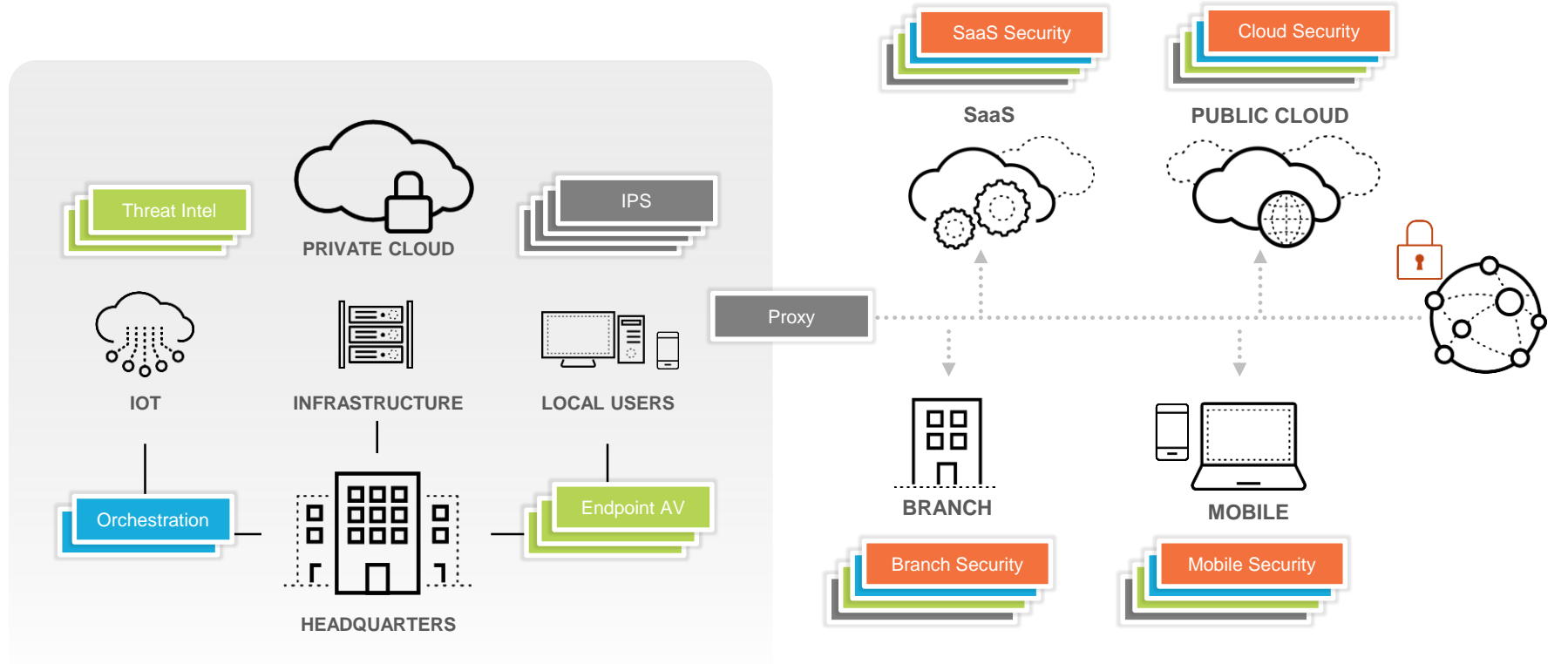
Context

Dev, Test, Prod

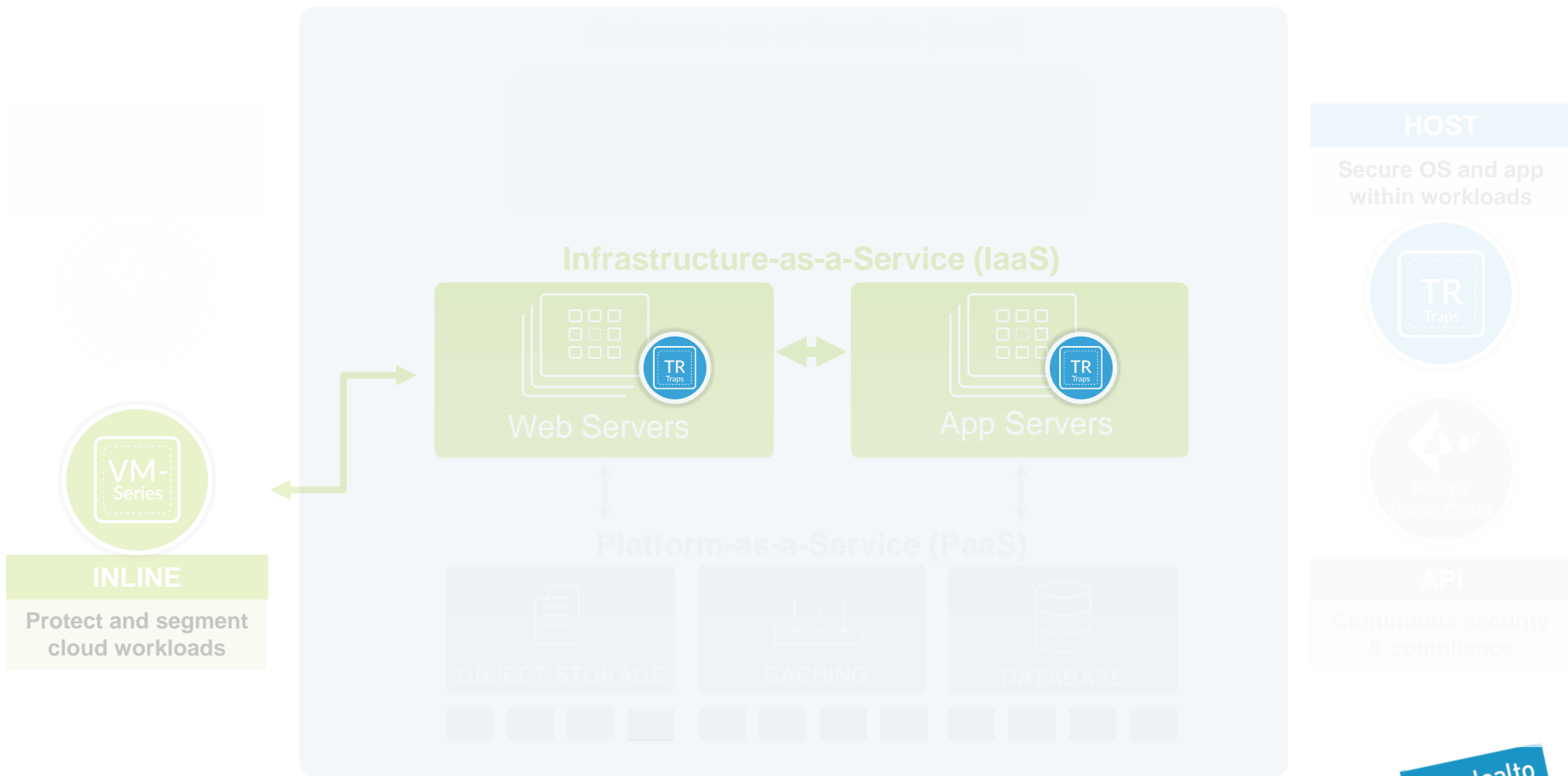
# Point Solutions are Not Effective in the Campus



# Totally Ineffective for Cloud and for Mobile Workforce



# The Most Complete Offering For The Public Cloud

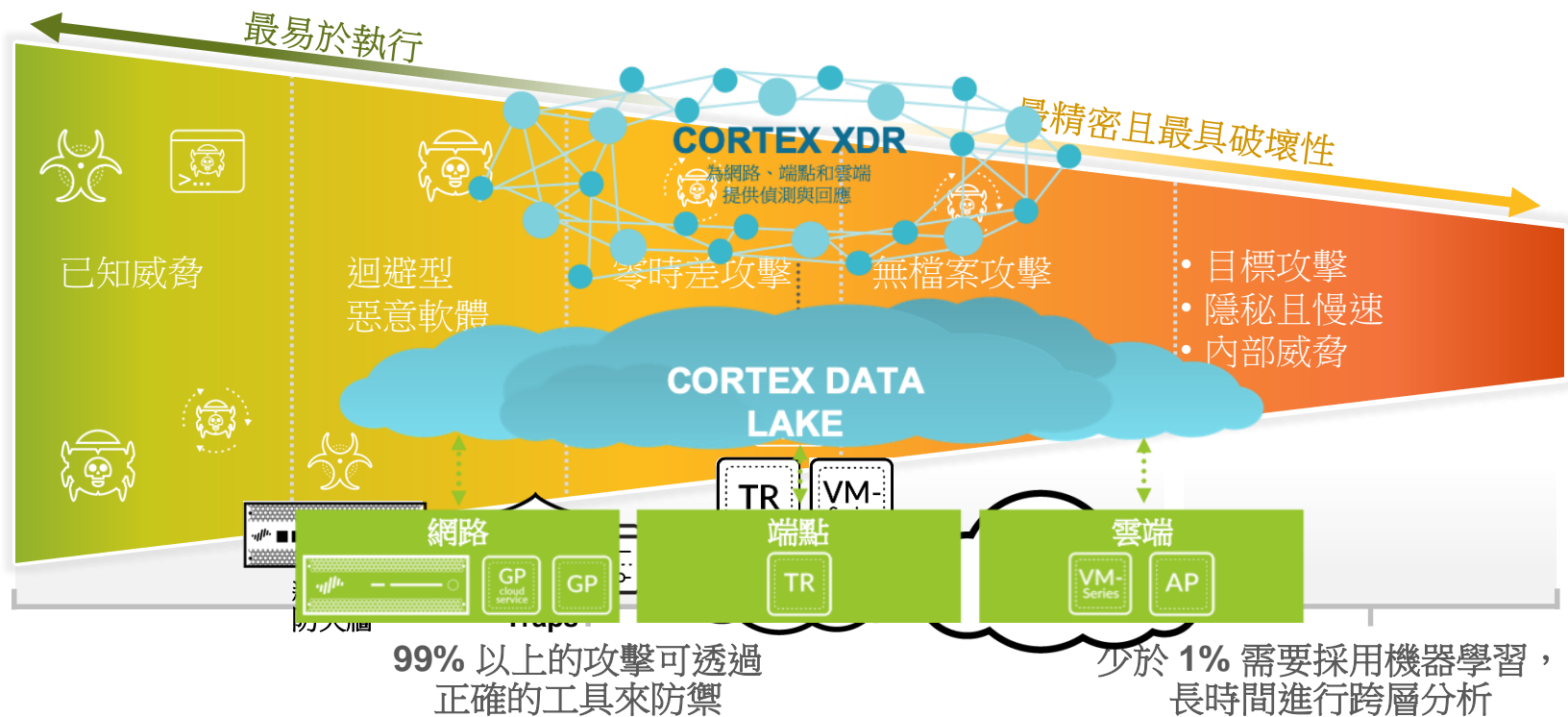


# 主題

- 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

