



The bridge to possible

# Detecting Critical Threats

## Behavior based detection & response

### 透過基於行為分析的事件反應調查來偵測關鍵威脅

with Secure Network Analytics/XDR

Derek Chia  
XDR Sales Lead, Greater China/ASEAN



# Agenda

## 議程

- Introduction
- Cisco NDR & XDR
- Cisco NDR Solution Overview
- Use Cases
- Demo



# Detecting Critical Threats with your Existing Network Elements

使用現有網路機制檢測關鍵威脅

# 網路和安全維運的挑戰

## 網路威脅變得更加聰明



### Motivated and targeted adversaries

- State sponsored
- Financial/espionage motives
- \$1T cybercrime market



### Insider Threats

- Compromised credentials
- Disgruntled employees
- Admin/privileged accounts

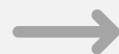


### Increased attack sophistication

- Advanced persistent threats
- Encrypted malware
- Zero-day exploits

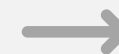
**207**  
DAYS

Industry average detection time for a breach



**73**  
DAYS

Industry average time to contain a breach



**\$3.86M**

Average cost of a data breach

# How Can We Detect and Respond to All of This

## 我們如何檢測和應對所有的攻擊分析指標 (MITRE ATT&CK Matrix for Enterprise)?

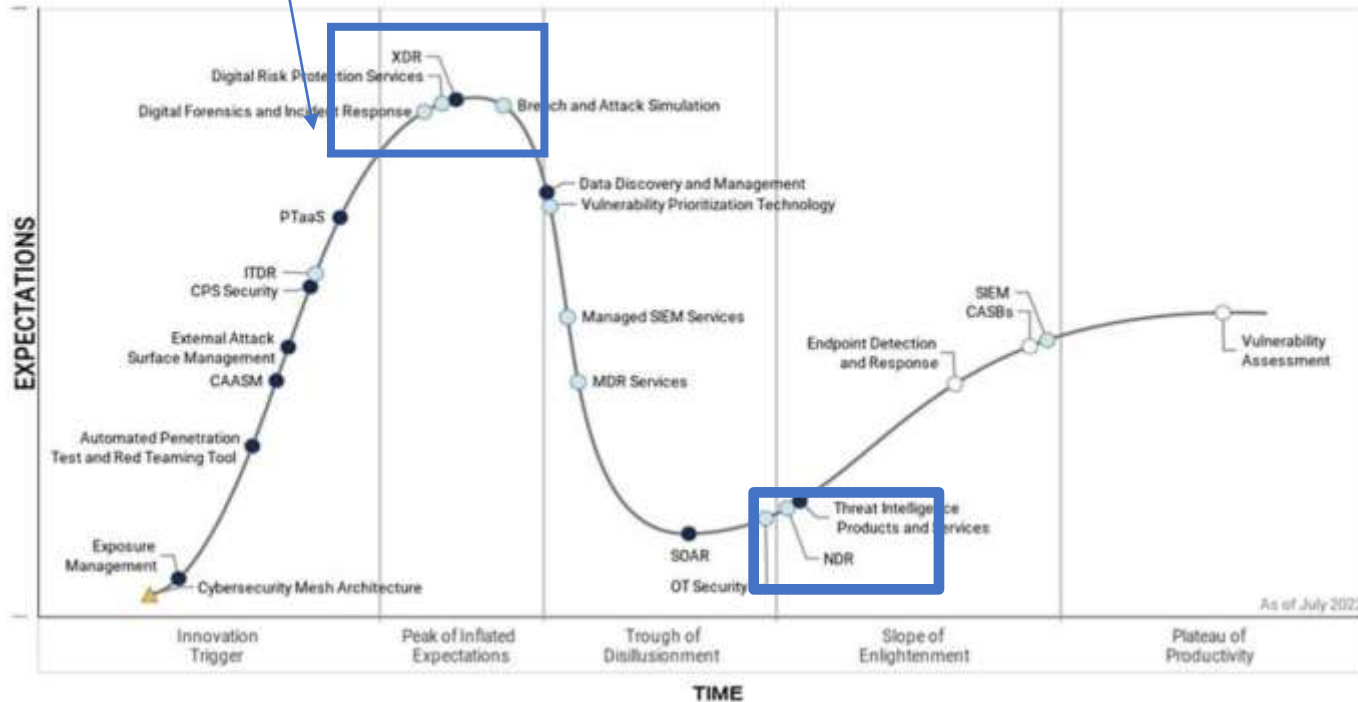
TA0001: Initial Access		TA0002: Execution		TA0008: Lateral Movement		TA0009: Collection	
T1189: Drive-by Compromise		T1059: Command and Scripting Interpreter	T1098: Remote Services	T1210: Exploitation of Remote Services	T1557: Adversary-in-the-Middle	T1560.003: Archive via Custom Method	
T1190: Remote Services			T1099: Remote Services	T1534: Internal Spearphishing	T1560: Archive Collected Data	T1560.002: Archive via Library	
T1133: Abuse Elevation Control Mechanism	TA0004: Privilege Escalation	T1548: Abuse Elevation Control Mechanism	TA0005: Defense Evasion	T1570: Lateral Tool Transfer	T1563.002: RDP Hijacking	T1560.001: Archive via Utility	
T1200: Access Token Manipulation		T1548.002: Bypass User Account Control		T1563.001: SSH Hijacking	T1123: Audio Capture		
T1547: Boot or Logon Autostart Execution		T1548.001: Setuid and Setgid		T1021: Remote Services	T1119: Automated Collection		
T1566: Boot or Logon Initialization Scripts	T1037.001: Logon Script (Windows)	T1548.003: Sudo and Sudo Caching		T1021.003: Distributed Component Object Model	T1021.001: Remote Desktop Protocol	T1185: Browser Session Hijacking	
T1037: Boot or Logon Initialization Scripts		T1134: Access Token Manipulation	T1134.002: Create Process with Token	TA0011: Command and Control			
T1543: Create Account	TA0006: Credential Access	T1087: Account Discovery	T1087.001: Local Account Discovery	T1071: Application Layer Protocol	T1071.004: DNS	TA0010: Exfiltration	T1026: Automated Exfiltration
T1091: Domain Accounts	T1110: Brute Force	T1087.002: Local Service Discovery	T1087.003: Local Group Discovery	T1071.002: File Transfer Protocols	T1071.003: Mail Protocols	T1030: Data Transfer Size Limits	T1048: Exfiltration Over Alternative Protocol
T1195: Domain Credentials	T1110.004: Credential Stuffing	T1087.004: Local Device Discovery	T1087.005: Local File Discovery	T1071.001: Web Protocols	T1071.002: Web Protocols	T1041: Exfiltration Over C2 Channel	T1041: Exfiltration Over C2 Channel
T1611: Escalate Local Privileges	T1110.002: Password Cracking	T1010: Application Window Discovery	T1010.001: Application Window Discovery	T1092: Communication Through Removable Media	T1132.002: Non-Standard Encoding	T1011: Exfiltration Over Other Network	T1052: Exfiltration Over Physical Medium
T1199: Escalate Remote Privileges	T1110.001: Password Guessing	T1217: Browser Bookmark Discovery	T1217.001: Browser Bookmark Discovery	T1132: Data Encoding	T1132.001: Standard Encoding	T1052: Exfiltration Over Physical Medium	T1567: Exfiltration Over Web Service
T1546: Evict Other Users	T1110.003: Password Spraying	T1622: Debugger Evasion	T1622.001: Debugger Evasion	T1001: Data Obfuscation	T1001.001: Junk Data	T1029: Scheduled Transfer	
T1078: Impersonate Service	T1555: Credentials from Password Store	T1492: Domain Trust Discovery	T1492.001: Domain Trust Discovery	T1001.002: Steganography	T1001.003: Protocol Impersonation		
	T1112: Modify Registry	T1027: Directory Discovery	T1027.001: Binary Padding	T1568: Dynamic Resolution	T1573.002: Asymmetric Cryptography		
	T1027: Obfuscated Files or Information	T1027.004: Compile After Delivery	T1027.004: Compile After Delivery	T1573: Encrypted Channel	T1573.001: Symmetric Cryptography		
		T1027.006: HTML Smuggling	T1027.006: HTML Smuggling	T1008: Fallback Channels			
		T1027.005: Indicator Removal from Tools	T1027.005: Indicator Removal from Tools	T1105: Ingress Tool Transfer			
		T1027.002: Software Packing	T1027.002: Software Packing	T1104: Multi-Stage Channels			
		T1027.003: Steganography	T1027.003: Steganography	T1096: Non-Application-Layer Protocol			
	T1542: Pre-OS Boot	T1069.002: Local Service Discovery	T1069.002: Local Service Discovery	T1571: Non-Standard Port			
	T1055: Process Injection	T1069.001: Local Group Discovery	T1069.001: Local Group Discovery	T1572: Protocol Tunneling			
		T1055.004: Asynchronous Procedure Call	T1055.004: Asynchronous Procedure Call	T1090: Proxy			
		T1055.001: Dynamic-Link Library Injection	T1055.001: Dynamic-Link Library Injection	T1090.004: Domain Fronting			
		T1055.011: Extra Window Memory Injection	T1055.011: Extra Window Memory Injection	T1090.002: External Proxy			
		T1055.015: List Planting	T1055.015: List Planting	T1090.001: Internal Proxy			
		T1055.002: Portable Executable Injection	T1055.002: Portable Executable Injection	T1090.003: Multi-hop Proxy			
		T1055.009: Proc Memory	T1055.009: Proc Memory	T1205.001: Port Knocking			
		T1055.013: Process Doppelgänger	T1055.013: Process Doppelgänger	T1102.002: Bidirectional Communication			
		T1055.012: Process Hollowing	T1055.012: Process Hollowing	T1102.001: Dead Drop Resolver			
		T1055.008: Trace System Calls	T1055.008: Trace System Calls	T1102.003: One-Way Communication			
		T1055.003: Thread Execution Hijacking	T1055.003: Thread Execution Hijacking				
		T1055.005: Thread Local Storage	T1055.005: Thread Local Storage				
		T1055.014: VDSO Hijacking	T1055.014: VDSO Hijacking				
	T1620: Reflective Code Loading	T1553.002: Code Signing	T1553.002: Code Signing				
	T1207: Rogue Domain Controller	T1553.006: Code Signing Policy Modification	T1553.006: Code Signing Policy Modification				
	T1014: Rootkit	T1553.004: Install Root Certificate	T1553.004: Install Root Certificate				
	T1553: Subvert Trust Controls	T1553.005: Mark-of-the-Web Bypass	T1553.005: Mark-of-the-Web Bypass				
		T1553.003: SIP and Trust Provider Hijacking	T1553.003: SIP and Trust Provider Hijacking				

We Are Here

# Hype Cycle for Security Operations, 2022

Published 5 July 2022 - ID G00770249

Gartner



## XDR

Extended detection and response (XDR) is a vendor-specific threat detection and incident response tool that unifies multiple security products into a security operations system. Primary functions include security analytics, alert correlation, incident response and incident response playbook automation.

### Why This Is Important

Extended detection and response (XDR) is similar in function to security information and event management (SIEM) and security orchestration, automation and response (SOAR). However, XDR is differentiated by its level of integration and automation, ease of use, and focus on threat detection and incident response. XDR solution providers must also provide multiple security controls such as EDR, CASB, Firewall, IAM, IDS, directly.

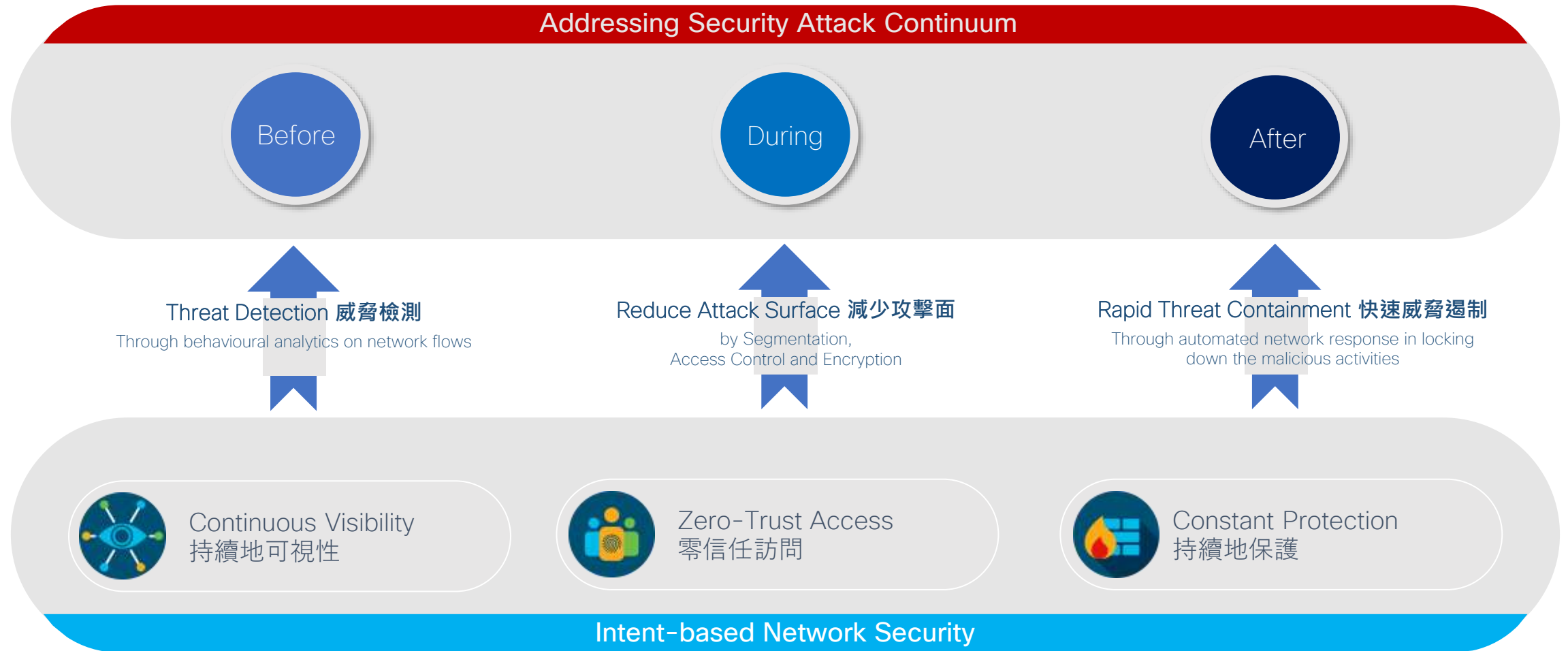
### Business Impact

XDR products can reduce the total cost of managing security incidents, improve the productivity of the incident response team and reduce the overall cybersecurity risk posture of the organization.



# Intent-Based Network Security 基於意圖的網路安全

Building a Trusted Workplace that aligns and optimise network to security needs



# Cisco XDR



**Email Security**  
Cisco Secure Email



**EDR** (Endpoint Detection & Response)  
Cisco Secure Client



**NDR** (Network Detection & Response)  
Cisco Secure Cloud Analytics  
Cisco Secure Network Analytics



**ITRM** (IT Risk Management)  
Cisco Secure Cloud Insights

**RBVM** (Risk based vulnerability Management)  
Cisco Kenna Security

**Security platform**  
Cisco SecureX



SecureX



Unified  
Visibility



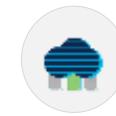
Incident  
Investigation



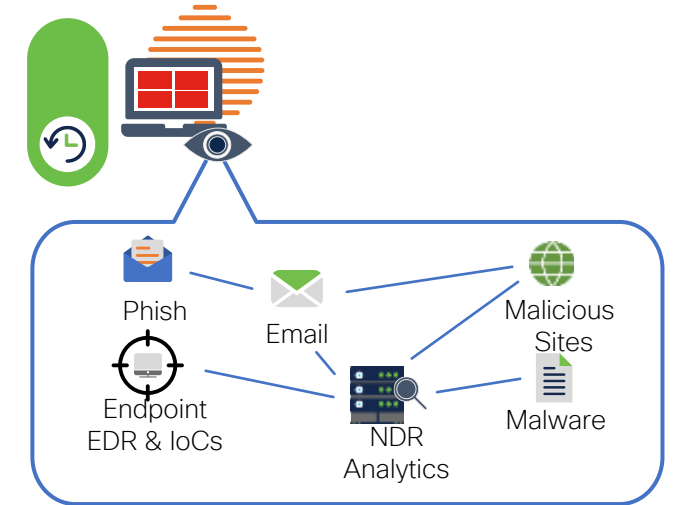
Orchestration



Threat Response  
Automation



Open  
Integration







# What is NDR and Why Do Customers Need It?

[NDR tools] detect suspicious traffic  
*that other security tools are missing*

## Benefits:

- Gain comprehensive visibility into network traffic
- Quickly detect advanced attacks and abnormal behavior
- Rapidly respond to and remediate threats found across the network



Use the existing **network as a security sensor** to find hidden threats, on-prem or in the cloud

使用既有網路設備作為安全偵測工具來發現隱藏在本地或雲端的威脅



**未知威脅 Unknown threat** Identify suspicious behavior and communications to malicious domains

---



**內部威脅 Insider threat** Get alarmed on data hoarding or exfiltration, suspicious lateral movement

---



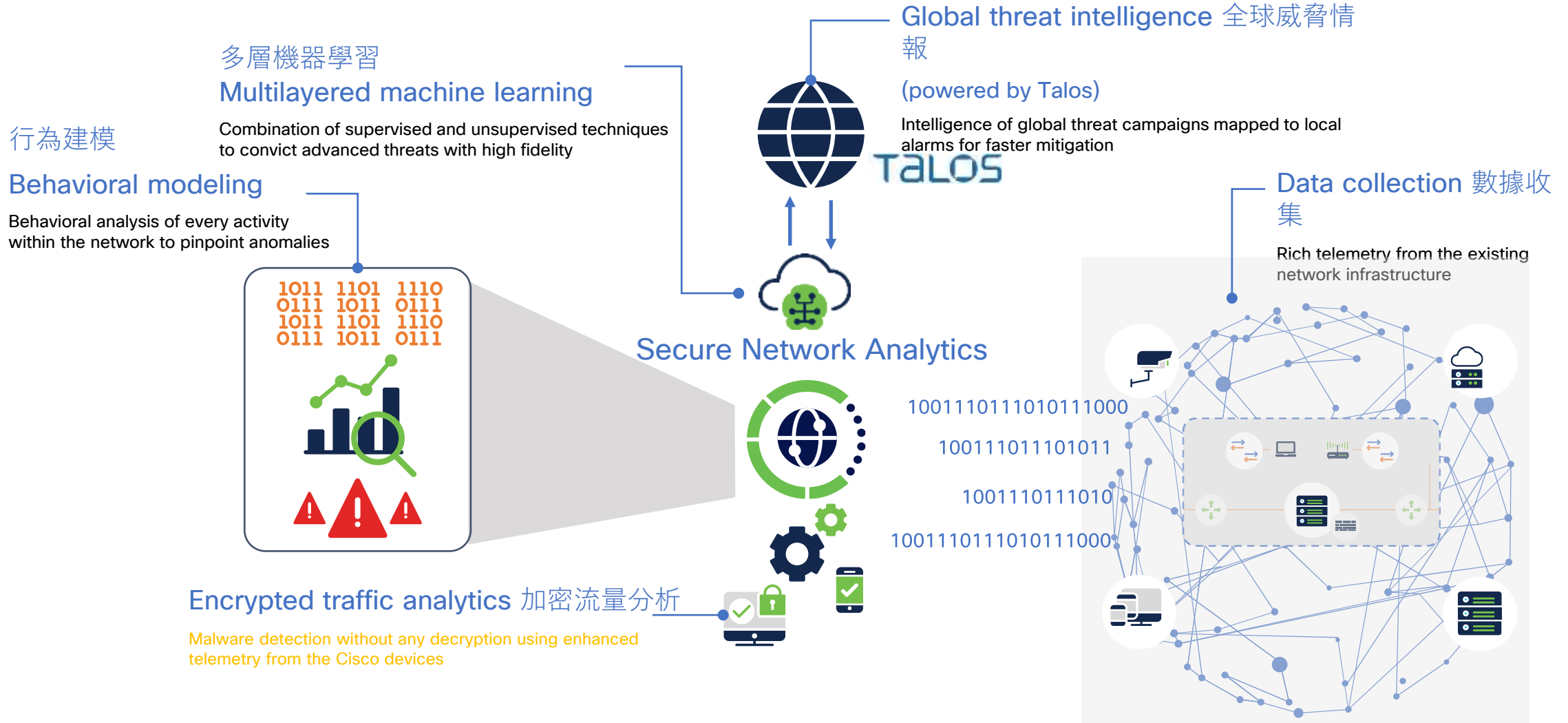
**加密的惡意軟件 Encrypted malware** Use multilayered machine learning to analyze traffic without decryption

---



**違反政策 Policy violation** Ensure security and compliance policies set in other tools are enforced

# Secure Network Analytics

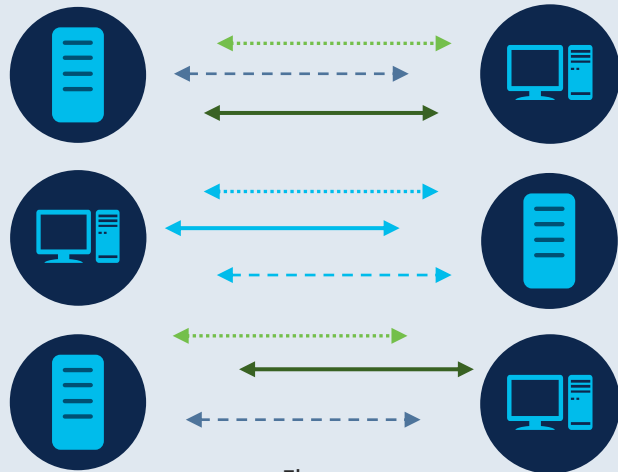


# Anomaly Detection Using Behavioral Models

## 利用行為模型進行異常檢測

Collect & Analyze Data  
收集和分析資料

進行數據關聯最佳化並消除重複資料



Flows

Establish a baseline for normal network behavior  
為正常網路行為建立基線

檢測異常流量和行為

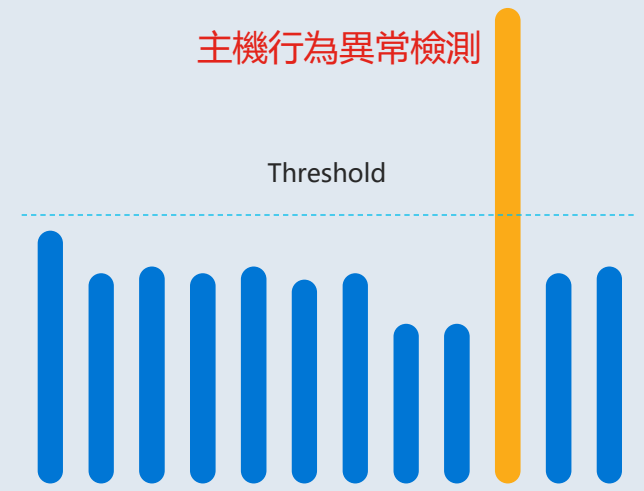
異常流量和安全事件

Number of concurrent flows	New flows created	Number of SYNs received
Packet per second	Number of SYNs sent	Rate of connection resets
Bits per second	Time of day	Duration of the flow

Detect abnormal traffic and alert  
發現異常網路流量並告警

高風險的告警分類  
低誤報告警並提高反應能力

主機行為異常檢測



Exchange Servers

# 整合全網資訊，實現多雲環境可視化



SRC/DST IP Address  
SRC/DST Port  
Bytes/Pkts Sent  
Bytes/Pkts Received  
...  
(Netflow, IPFIX)

L7 Application  
HTTP Requests  
HTTP Responses  
SRT/RTT  
TCP Flags  
Payload

Flow Action  
Translated Port/IP  
SYSLOG  
Malware events  
File events

TLS Version  
Key Exchange  
Authentication  
Alg.  
MAC

VPC/NSG  
flow log  
trans-  
formation  
via CTB

Process name  
Process hash  
Process account  
Parent process name  
Parent process hash  
OS Version  
Connected interface  
...

Username  
MAC Address  
TrustSec Groups  
OS Type

HTTP(S) Requests  
HTTP(S) Responses  
HTTP(S) URL  
Custom HTTP(S)  
Headers  
Username

Host  
Groups



\* Delivered through Advanced Services

# Cisco Secure Network Analytics Use Cases

## 主要使用場景

- Full library of support documentation for gaining visibility, detecting threats, enhancing integration, and increasing your Secure Network Analytics use.
- Use cases are organized by category and across the product lifecycle.
- Find the support you need to customize Secure Network Analytics and integrate it into your security and networking ecosystems.

Compliance  
合規



Forensic  
Investigation  
調查取證



Incident  
Response  
事件反應



Network  
Visibility  
網路可視性



Threat  
Detection  
威脅檢測





# Cisco Secure Network Analytics 優勢

1. **NetFlow deployment** for full network visibility, better than only SPAN traffic
2. Combining **machine learning, threshold fine tuning and policy customization** produces high fidelity results and low false positive
3. **Encrypted Traffic Analytics** provides malware detection without traffic decryption
4. Working with **Cisco Catalyst network switches, Cisco ISE and SecureX** provides additional values of enhanced NetFlow for visibility, threat mitigation and response
5. **Long term data retention** for compliance and forensic (1 year+)

# Detection and investigation based on contextual information

## 基於上下文資訊進行檢測與調查

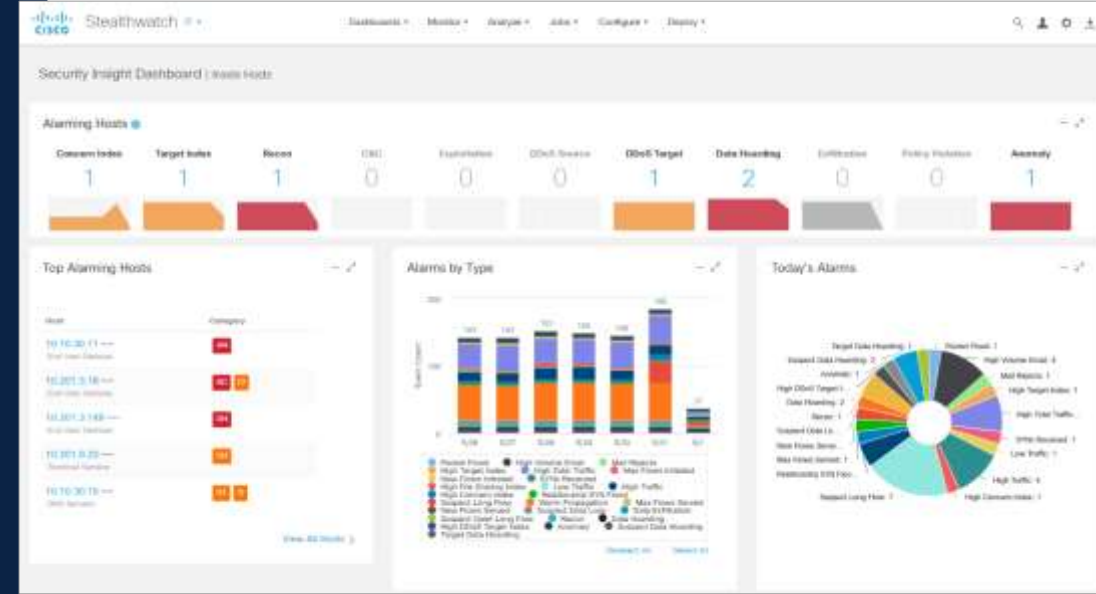
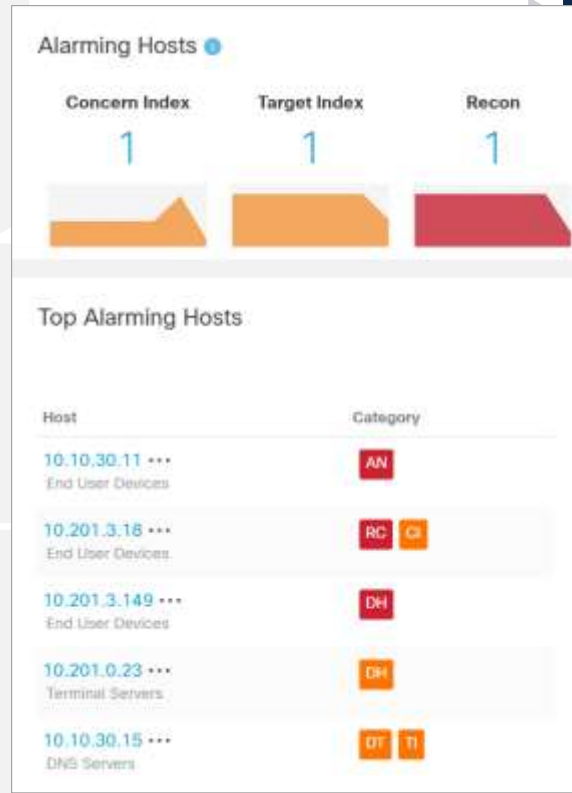
Spot Malicious traffic  
快速發現惡意活動報告

information associated  
with hosts and  
applications

關聯到主機、應用等上下文信心

Prioritize according to risk

根據風險劃分優先級進行處理



# Encrypted Traffic Analytics Increases Visibility

## 加密流量分析提高可視性

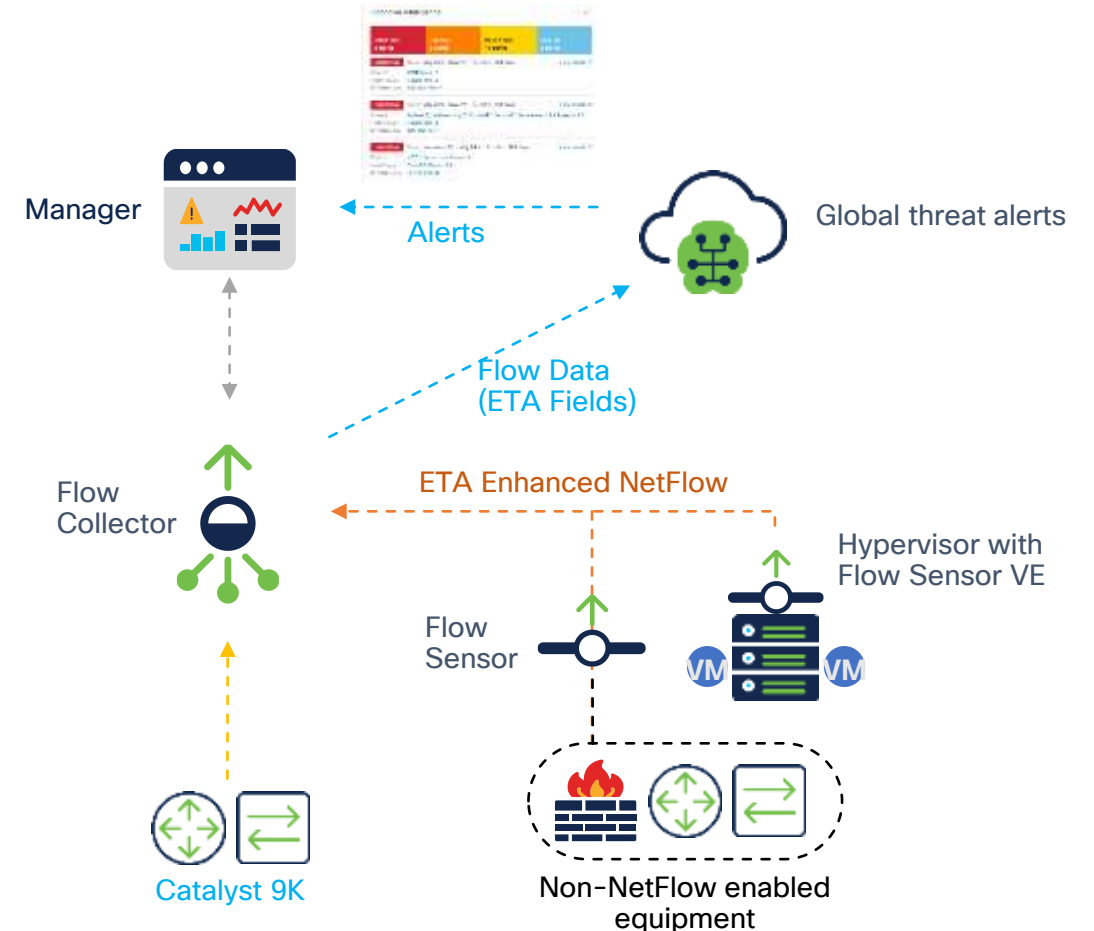


### Cryptographic Audit



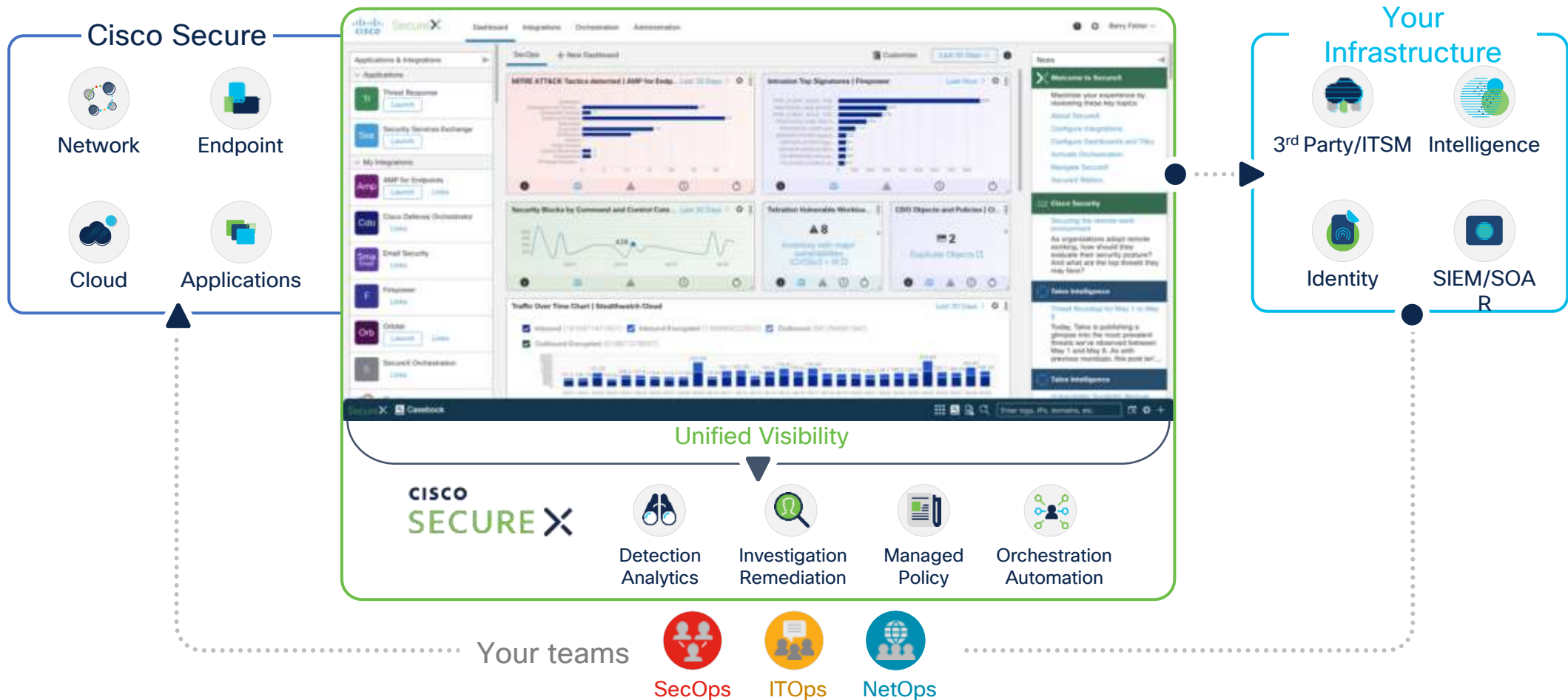
### Malware Detection within Encrypted Traffic

- Cisco Catalyst network switches feed enhanced NetFlow to Flow Collector
- Meta data sent to the cloud through a secure channel
- Malware detection analysis is done in the cloud, cryptographic audit is done on-premises

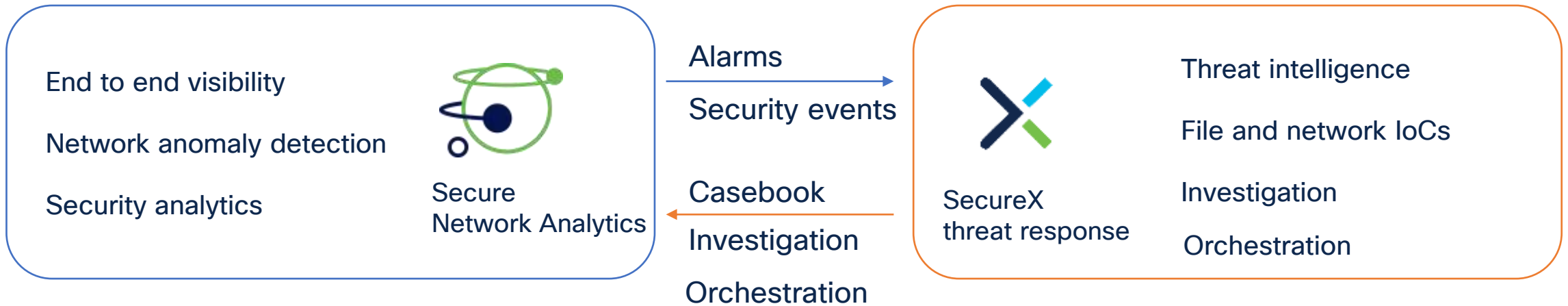


# SecureX - XDR

A cloud-native, built-in platform experience within Simplicity, Visibility and Efficiency



# Secure Network Analytics & SecureX threat response



## Agentless detection

Secure Network Analytics network-based visibility and security analytics will enrich SecureX threat detection and response with agentless behavioral and anomaly detection capabilities

## Correlate, enrich, and resolve

SecureX threat response integrations with other sources of global threat intelligence and internal visibility, will affirm and enrich Secure Network Analytics findings with confirmed threat intel and local sightings. Integrations with Cisco control devices provide two-click mitigation and resolution

# Demo - booth





The bridge to possible

# Thank you

CISCO *Engage* Taipei

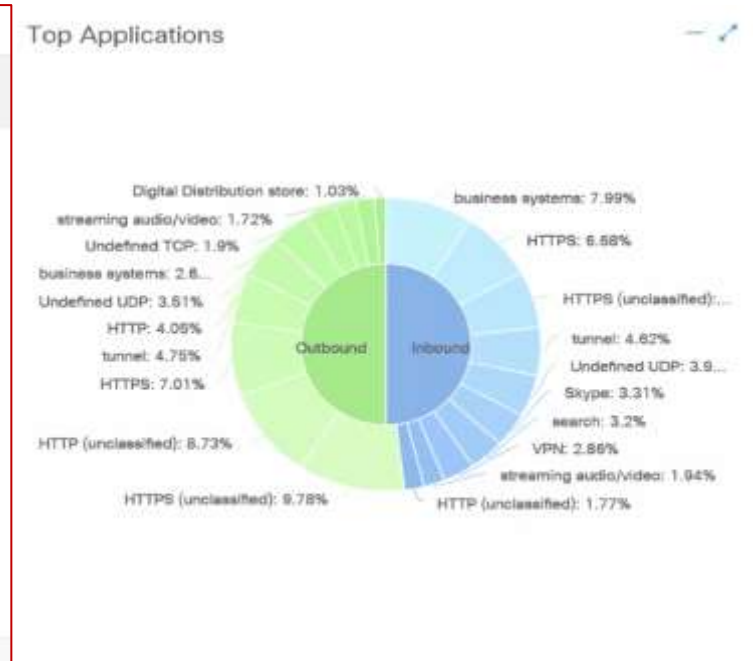
ALL IN

# Use Cases Screenshot 主要功能使用場景

# 一、Monitor and manage traffic by application group

## 按照應用分組監控和管理流量

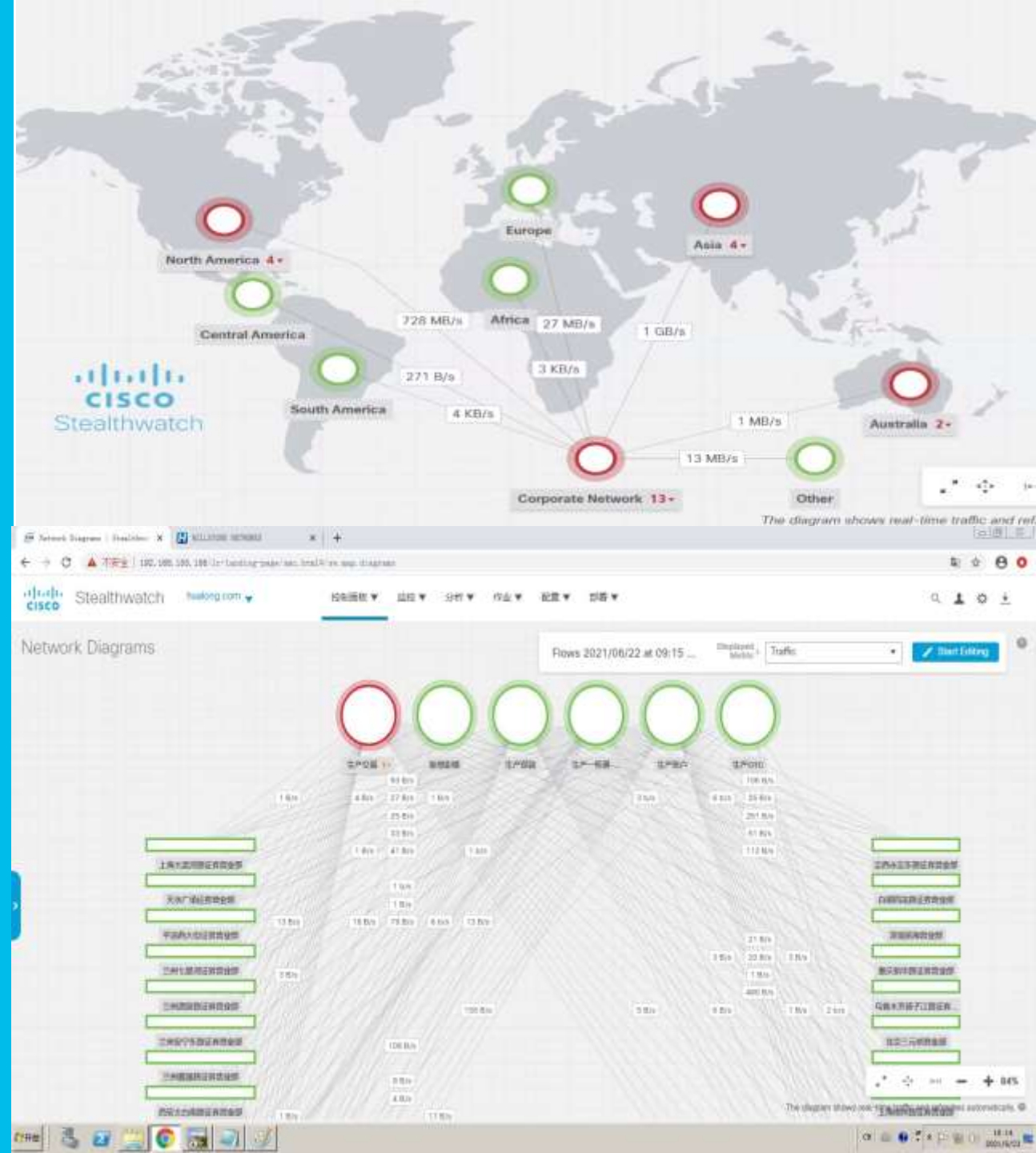
- 根據IP位址範圍定義主機分組，把網路流量關聯到業務和應用
- 按照應用分組可視化呈現
  - 流量分布情況
  - 硬用訪問趨勢
  - 異常流量告警



## 二、 Application access real-time traffic monitoring view

### 應用訪問即時流量監控可視圖

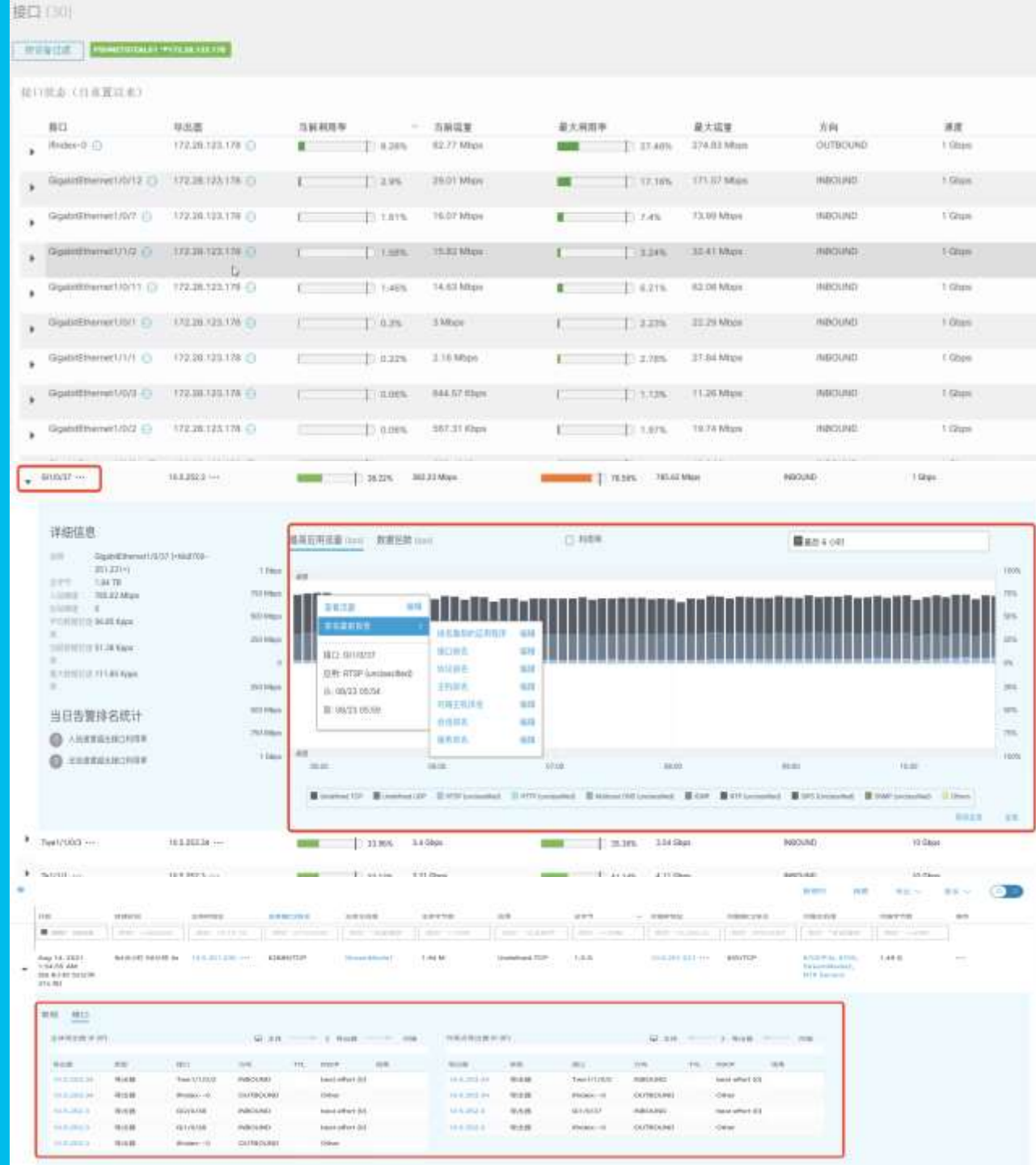
- 根據流量查詢結果，按照需要自動生成應用訪問流量監控可視圖
- 監控可視圖實現
  - 應用分組的訪問關係
  - 即時的流量分布情況
  - 分組之間異常流量發現 ( 機器學習 )
  - 快速調查



# 三、 Network device interface traffic analysis

## 網路設備接口流量分析和調查

- 設備接口利用率分析  
( 歷史、平均、當前 )
- 每個接口流量按照應用類型分布和統計
- 接口流量異常時，快速調查流量 Top 排名的 IP 和 Session

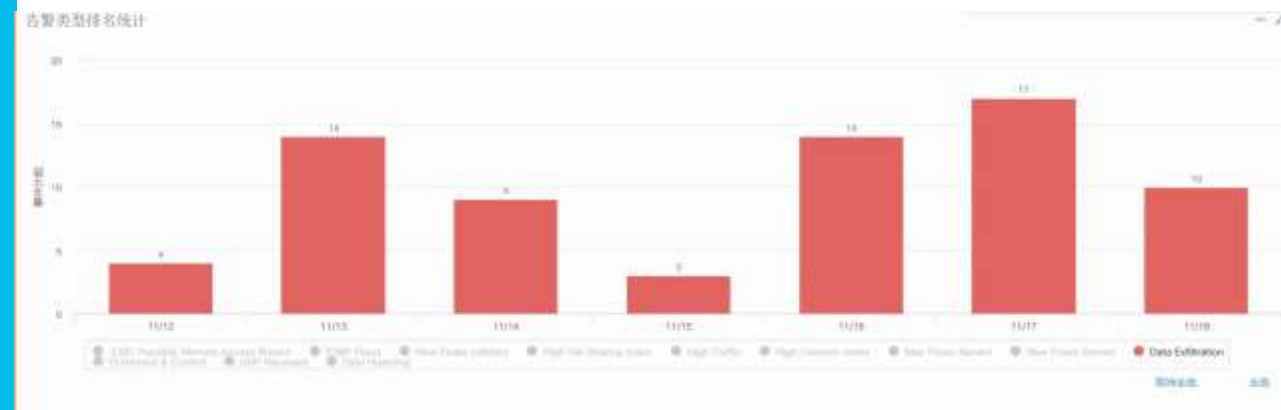




# 四、 Early warning and investigation of abnormal network traffic

## 網路流量異常告警和調查

- 主要異常網路流量發現：
  - 大流量告警
  - 資料收集告警
  - 資料外傳告警
- 快速調查分析
  - TOP的IP排名
  - TOP的Session排名
  - TOP的服務、端口排名
  - 關聯到應用分組和網路設備接口



### 主機報告 | 10.128.220.228

告警類別

源IP異常(CD)	目標IP異常(CD)	異常行為(HC)	命令和特權(CC)	異常利用(EI)	DDoS源(DS)	DDoS源(DT)	數據收集(DK)	信息洩漏(EX)	惡意重定向(PV)	異常認證(AU)
1	0	0	0	0	0	0	0	1	0	0

主機摘要

主機IP: 10.128.220.228

主機類型: Desktop

主機名: PSH-DA-User

IP地址: 10.128.220.228

首次發現: 11/18/20 7:35 PM

最近發現: 11/18/20 2:38 PM

狀態: Inactive

MAC地址: --

按主機IP查詢的流量統計 (最近 12 小時)

按類型分布的告警統計 (最近 7 天)

Alert Type	Count
High Concern Index	1
Data Estimation	1

% OF BYTES	HOST IP ADDRESS	HOST NAME	HOST ROLE	PEER IP ADDRESS	PEER NAME	PORT	BYTES	PACKETS	FLWS	HOST BYTES RATIO	ACTIONS
6.3%	10.106.20.246	--	Client	113.86.65.158	--	443 / TOP (https)	4.02 G	4.57 M	1	6.3%	
6.2%	10.106.20.246	--	Client	103.81.69.198	--	80 / TOP (http)	402.87 M	434.94 K	1	6.2%	
4.8%	10.106.20.246	--	Client	129.44.162.152	msd.ny.ahk	443 / TOP (https)	304.88 M	278.03 K	1	4.8%	
4.3%	10.106.20.246	--	Client	23.211.138.89	--	80 / TOP (http)	278.81 M	286.28 K	1	4.3%	
4.2%	10.106.20.246	--	Client	19.86.12.131	mail.lnovo.com	443 / TOP (https)	268.82 M	244.89 K	1	4.2%	
1.9%	10.106.20.246	--	Client	88.216.209.209	--	443 / TOP (https)	84.89 M	83.74 K	1	1.9%	
1.8%	10.106.20.246	--	Client	129.44.162.158	--	443 / TOP (https)	50.34 M	44.75 K	1	1.8%	

# 五、 Early warning and investigation of intranet security threats

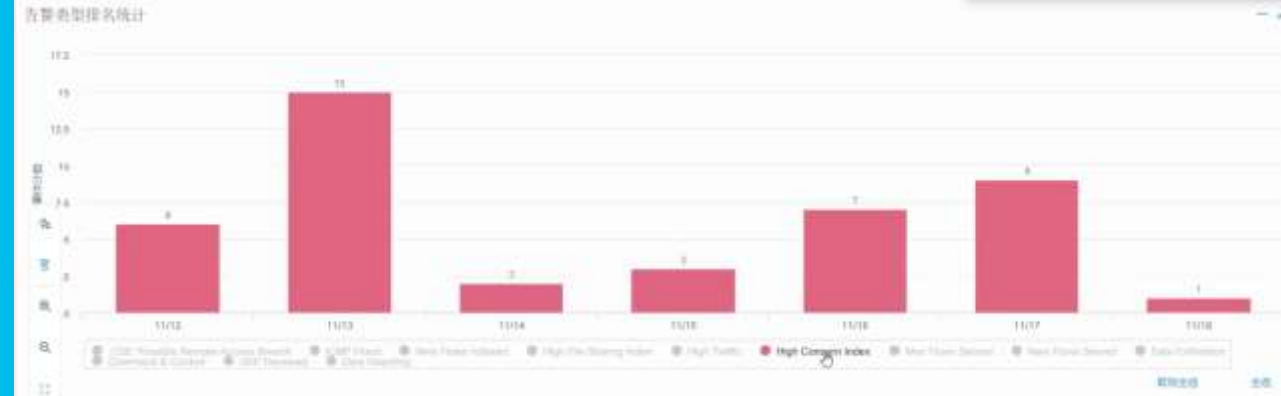
## 內網安全威脅告警和調查

- 主要安全威脅發現

- 掃描探測
- 駭客控制
- 勒索軟體
- 資料外洩
- 違規存取

- 快速調查分析

- 自動告警
- 快速定位和追蹤IP位址
- 縮短反應時間



安全事件 | 10.20.5.49 (20)

10.20.5.49 的所有安全事件

安全事件	计数	源IP的威胁ID	第一个威胁	源主机	源主机IP	目标主机	目标主机IP	操作
Alert_Scanstop - 445	5,269	3,072,000	11/17 10:34:10	10.20.5.49	IP Status	172.26.128.0/24	WSH ServerFarm	
Alert_Scanstop - 445	4,693	3,120,000	11/17 11:02:27	10.20.5.49	IP Status	172.26.128.0/24	WSH ServerFarm	
Alert_Scanstop - 445	2,212	2,208,000	11/17 10:27:16	10.20.5.49	IP Status	172.26.144.0/24	WSH ServerFarm	
Alert_Scanstop - 445	1,806	1,320,000	11/17 10:39:40	10.20.5.49	IP Status	172.26.144.0/24	WSH ServerFarm	
Alert_Scanstop - 445	1,404	896,000	11/17 10:42:15	10.20.5.49	IP Status	172.26.128.0/24	WSH ServerFarm	
Alert_Scanstop - 445	826	362,000	11/17 12:02:24	10.20.5.49	IP Status	172.26.144.0/24	WSH ServerFarm	
Alert_Scanstop - 445	480	348,000	11/17 10:11:11	10.20.5.49	IP Status	172.26.144.0/24	WSH ServerFarm	
Alert_Scanstop - 445	442	368,000	11/17 10:51:20	10.20.5.49	IP Status	172.26.144.0/24	WSH ServerFarm	
Alert_Scanstop - 445	80	60,000	11/17 10:18:33	10.20.5.49	IP Status	172.26.132.0/24	Cloud-All	
Alert_Scanstop - 445	76	52,000	11/17 10:49:04	10.20.5.49	IP Status	172.26.128.0/24	WSH ServerFarm	

开始时间	主机	主机端口/协议	源IP地址	源端口/协议	目标IP地址	目标端口/协议	操作
开始: 2020年11月17日 10:34:10 结束: 2020年11月17日 10:34:30 持续时间: 20s	10.20.5.49	45327/TCP	10.20.5.49	444/TCP	172.26.128.0/24	444/TCP	RAW (unclassified)
开始: 2020年11月17日 10:39:40 结束: 2020年11月17日 10:39:50 持续时间: 10s	10.20.5.49	45894/TCP	10.20.5.49	444/TCP	172.26.144.0/24	444/TCP	RAW (unclassified)
开始: 2020年11月17日 10:27:16 结束: 2020年11月17日 10:27:30 持续时间: 14s	10.20.5.49	42460/TCP	10.20.5.49	444/TCP	172.26.144.0/24	444/TCP	RAW (unclassified)
开始: 2020年11月17日 10:39:40 结束: 2020年11月17日 10:39:41 持续时间: 1s	10.20.5.49	45833/TCP	10.20.5.49	444/TCP	172.26.128.0/24	444/TCP	RAW (unclassified)
开始: 2020年11月17日 10:39:40 结束: 2020年11月17日 10:39:39 持续时间: 1s	10.20.5.49	45834/TCP	10.20.5.49	444/TCP	172.26.128.0/24	444/TCP	RAW (unclassified)
开始: 2020年11月17日 10:39:40 结束: 2020年11月17日 10:39:39 持续时间: 1s	10.20.5.49	45835/TCP	10.20.5.49	444/TCP	172.26.128.0/24	444/TCP	RAW (unclassified)

# 六、Forensics 歷史資料保存、回溯和稽核

- Netflow保存時間長
- 歷史問題回溯和調查
- 合規稽核的要求

Policy Management | Custom Security Event

NAME *	DESCRIPTION
Audit policy1	audit management from internet

When any host within *Outside Hosts*; using any disallowed *application* communicates with any *peer host*; between 12:00 AM - 11:59 PM, a

FIND ⓘ

SUBJECT HOST GROUPS ⓘ	Outside Hosts X	⊙ AND
SUBJECT APPLICATIONS	remote desktop X IPC X SSH X Telnet X	⊙ AND
TIME OF DAY	12:00 AM - 11:59 PM X	⊙

Database Storage Statistics

Capacity

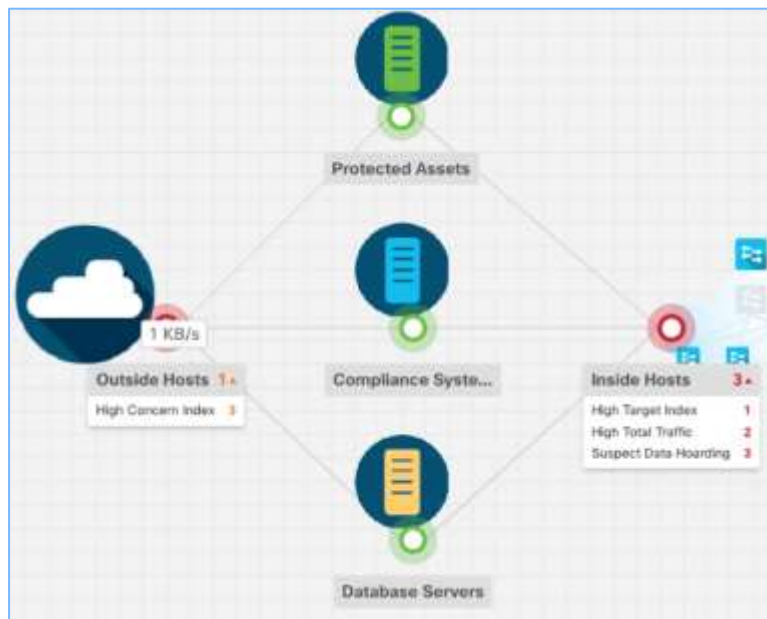
	Average	Worst Case
Capacity in Days	482	60
Remaining Days	145	17
Bytes Per Day	4.61G	12.31G

Flow Data Summary

Data	Rows					Bytes		
	Days	Containers	Total	Average Per Day	Largest Day	Total	Average Per Day	Largest Day
Flow Details	337	377	16.78G	49.8M	137.19M	500.58G	1.49G	4.35G
Flow Interface Details	8	36	812.53M	101.57M	251.3M	24.67G	3.08G	7.69G
Total	337	413	17.59G	151.36M	388.49M	525.24G	4.57G	12.04G

# Logical diagrams for monitoring metrics 為重要的監控指標創建邏輯可視監控圖

## 觸發告警



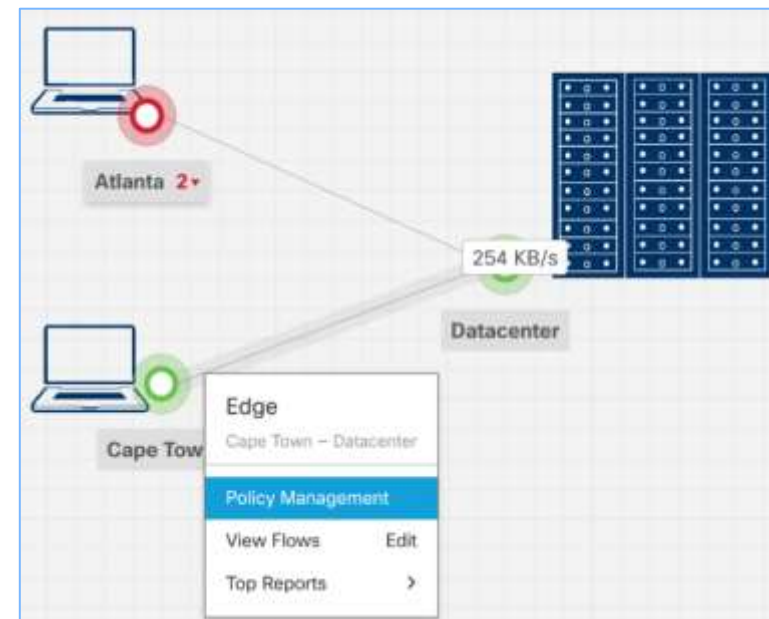
基於主機分組監控異常流量、安全威脅告警，方便調查

## 網路訪問指標



應用分組流量、頻寬、效能監控

## 訪問關係策略



圖像化的分組訪問關係策略