CATO NETWORKS

AI in Action
AI 浪潮下 SASE 雲平台的應用

Power of the Cato SASE Cloud Platform

Patrick Sung
patrick.sung@catonetworks.com

CATO
NETWORKS

我們正處於 AI 浪潮下的數位化變革

CATO NETWORKS

IT 科技帶來了巨大的變革

智慧 IT, 數位轉型

- 人工智慧 (AI)
- 物聯網 (IoT)
- 機器人流程自動化 (RPA)

科技變革, 轉型挑戰

- 全球連接與傳輸效能
- 網路安全
- IT 資源限制
- 不斷高昇的營運成本

CATO NETWORKS

資安威脅無所不在

內部威脅 → 人為因素構成資安挑戰

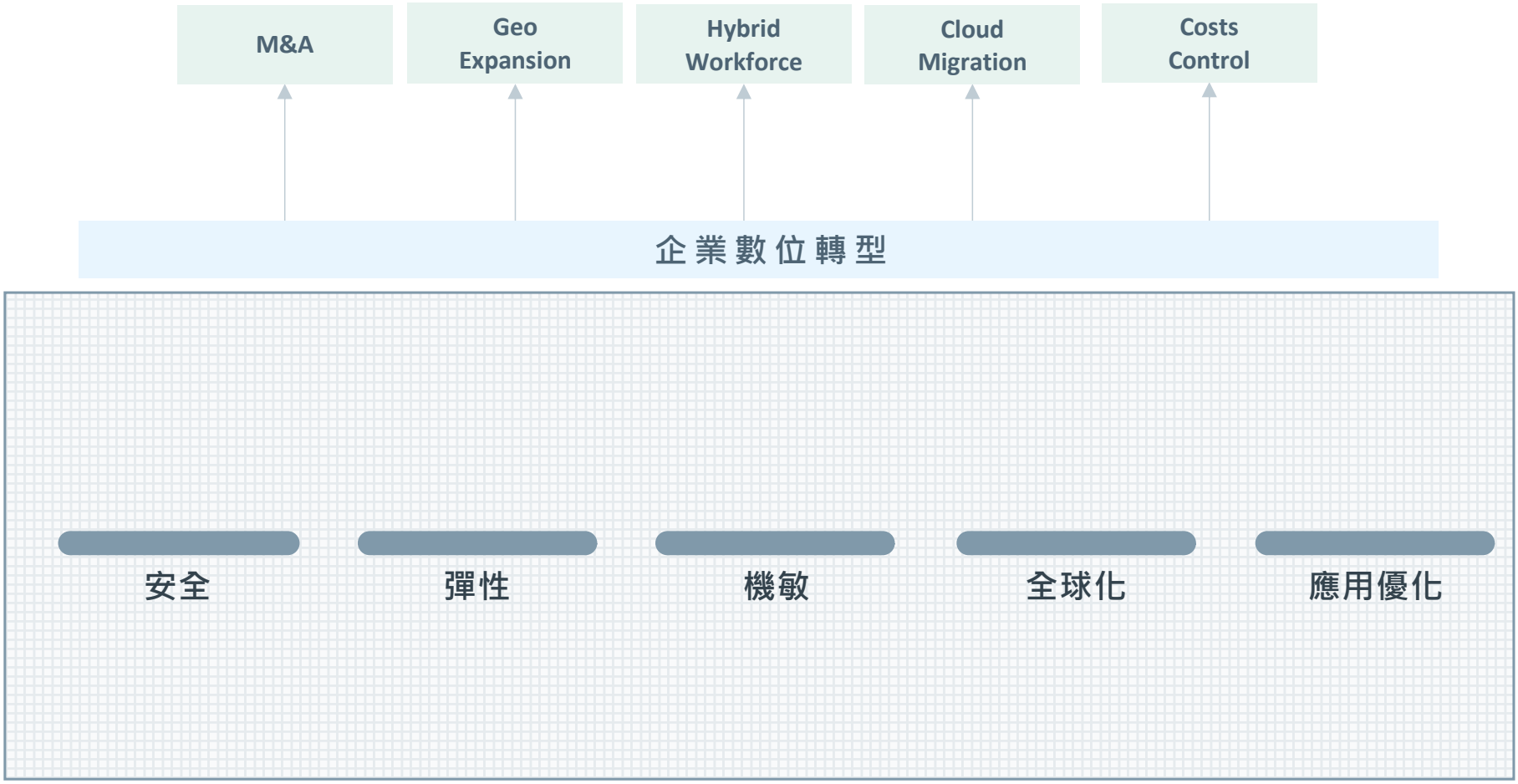
隨時隨地存取 → 擴大的攻擊表面

組織化的網路犯罪 → 更廣、更迅速、更智慧

風險無所不在

CATO NETWORKS

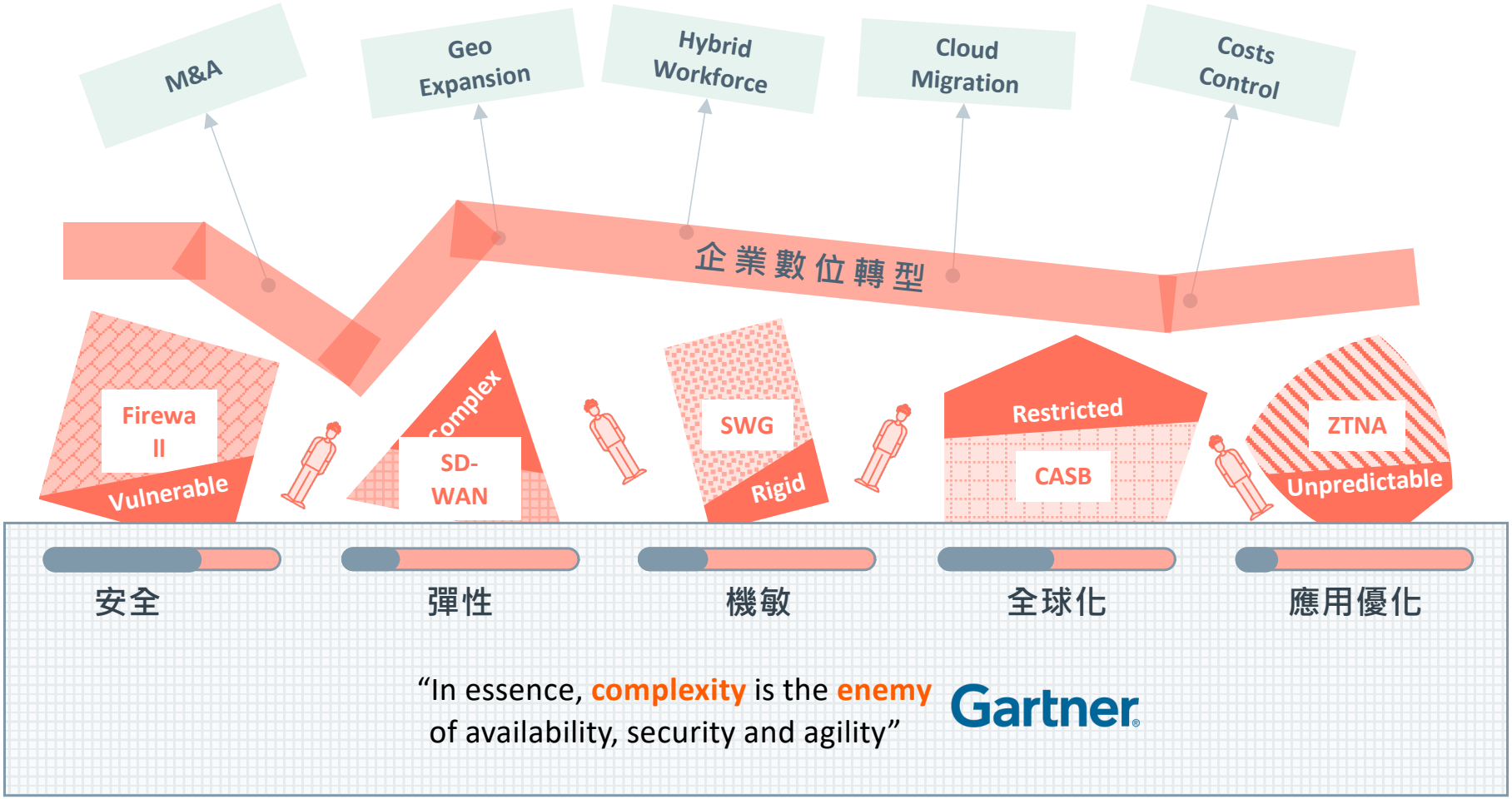
IT 需要協助轉型至數位化企業



CATO NETWORKS

Enterprise Networking and Security Platform

複雜的網路與資安設備導致數位化企業效率低落



CATO NETWORKS

Enterprise Networking and Security Platform

*Avoid These 'Bottom 10' Networking Worst Practices”, Gartner 2019

CATO SASE –
幫助企業 IT 克服挑戰

CATO
NETWORKS

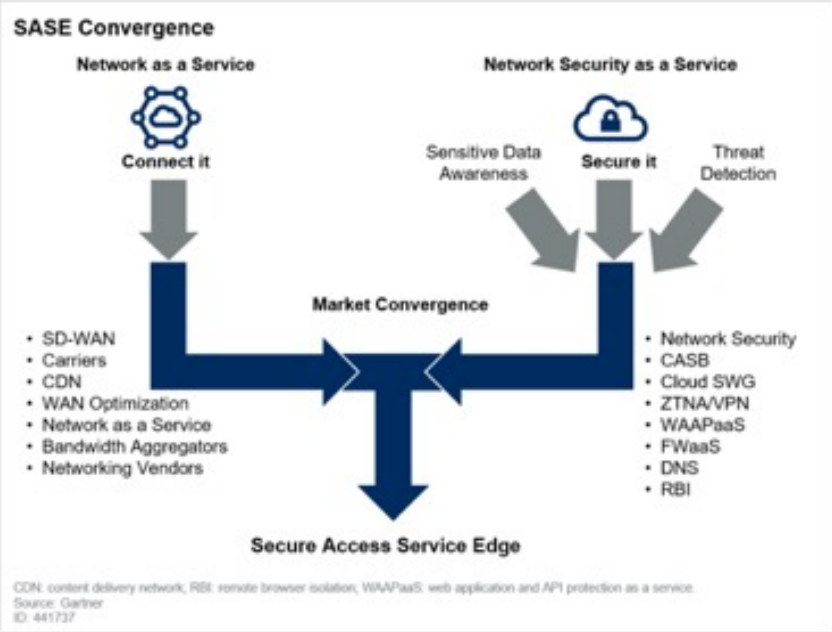
The Convergence – 整合網路與資安的單一雲平台解決方案

With the Secure Access Service Edge (SASE)

“ Customer demands for simplicity, scalability, flexibility, low latency and pervasive security force ***convergence*** *of the* ***WAN edge*** *and* ***network security*** *markets”.*

Gartner

Market Trends: How to Win as WAN Edge and Security Converge Into the Secure Access Service Edge, 2019



CATO NETWORKS

SASE 雲平台解決方案領導者

“First Mover” Advantage in the Single-Vendor SASE Market

Gartner

Leader in the **Single-Vendor SASE MQ** report

“ Provides a **single**, **straightforward** UI that is delivered via a **unified platform**”

“ An early **pioneer** that helped **drive the market**, and its planned **innovations** are likely to continue to **shape the market**”

“ Delivers **above-average customer experience** compared to other vendors”

FORRESTER®

Leader in the **ZTE (SASE) Wave** Report

“ Cato Networks is the **poster child** for ZTE and SASE”

“ Cato has a **strong strategy** paired with a **truly unified** networking and security solution”

FROST & SULLIVAN

GIGAOM

CATO NETWORKS

Cato SASE 雲平台架構幫助 IT 打造清晰可見的數位化架構

Architecture	 **擁有完整的網路與資安事件可視性**	Know a lot (single context) and record everything
	 **透過 Cato SASE 將網路，使用者以及應用程式串連一起**	A single virtual network in the cloud, connecting all networks, users, and apps

CATO NETWORKS

Cato SASE 雲平台架構幫助 IT 打造清晰可見的數位化架構

Intelligence & Control	 **即時資安威脅防護**	Apply powerful inline controls, and use the cloud brain to quickly adapt to new threats
	 **降低資安攻擊層面**	Apply global policies and limit access
Architecture	 **擁有完整的網路與資安事件可視性**	Know a lot (single context) and record everything
	 **透過 Cato SASE 將網路，使用者以及應用程式串連一起**	A single virtual network in the cloud, connecting all networks, users, and apps

CATO NETWORKS

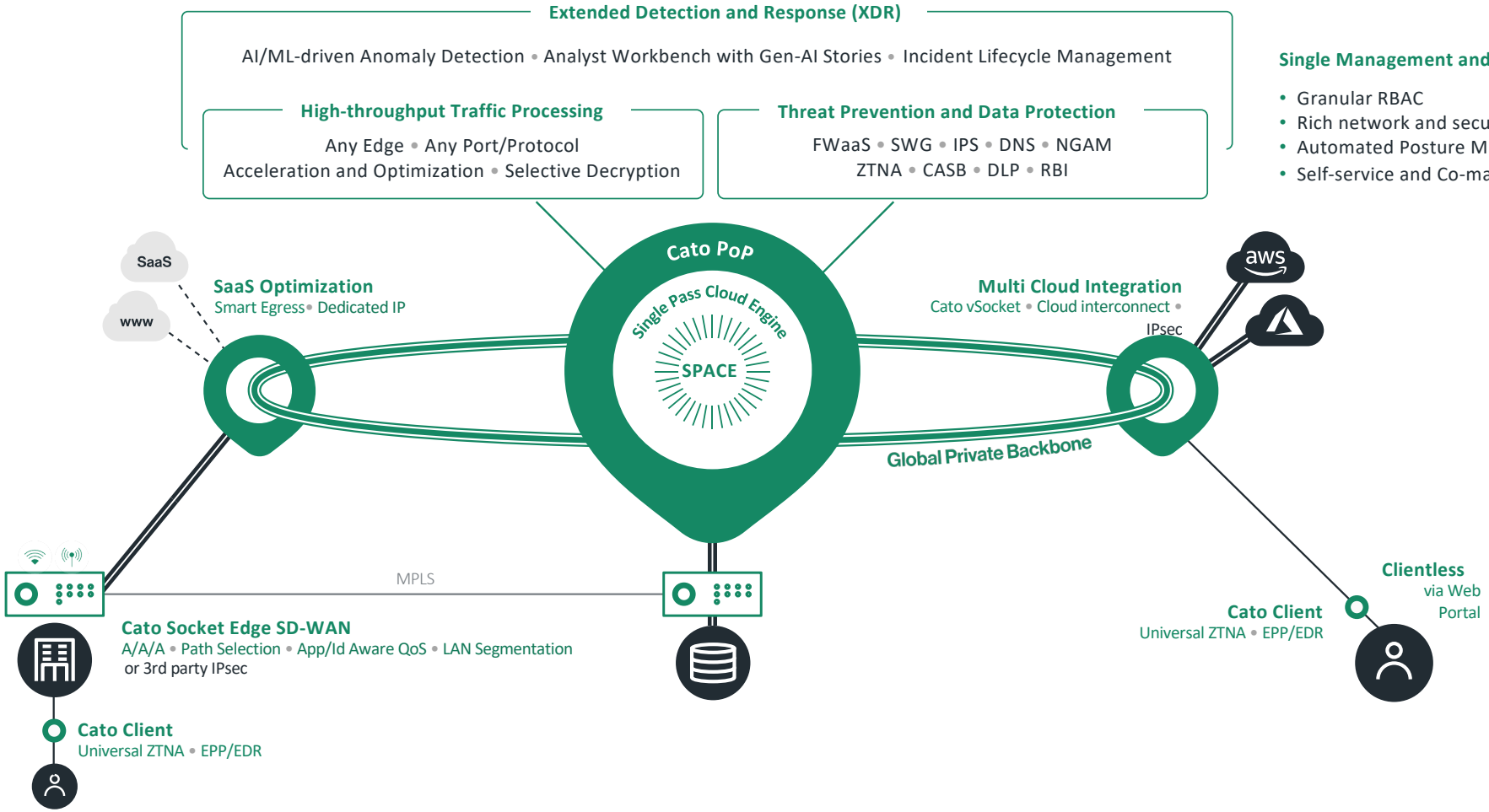
Cato SASE 雲平台架構幫助 IT 打造清晰可見的企業網路與資安基礎架構

Manage & Response	數位儀表板提供即時的多樣化資訊與建議	Provide a solution that works for every customer size, supporting complex enterprise environments
	集中的網路資安政策設定與資安防護更新	Use our data lake and network ownership to build a coherent detection to remediation flow
Intelligence & Control	即時資安威脅防護	Apply powerful inline controls, and use the cloud brain to quickly adapt to new threats
	降低資安攻擊層面	Apply global policies and limit access
Architecture	擁有完整的網路與資安事件可視性	Know a lot (single context) and record everything
	透過 Cato SASE 將網路，使用者以及應用程式串連一起	A single virtual network in the cloud, connecting all networks, users, and apps

CATO NETWORKS

Cato SASE 雲平台: 第一個雲原生 SASE 解決方案

SSE 360 and SD-WAN Converged



CATO NETWORKS

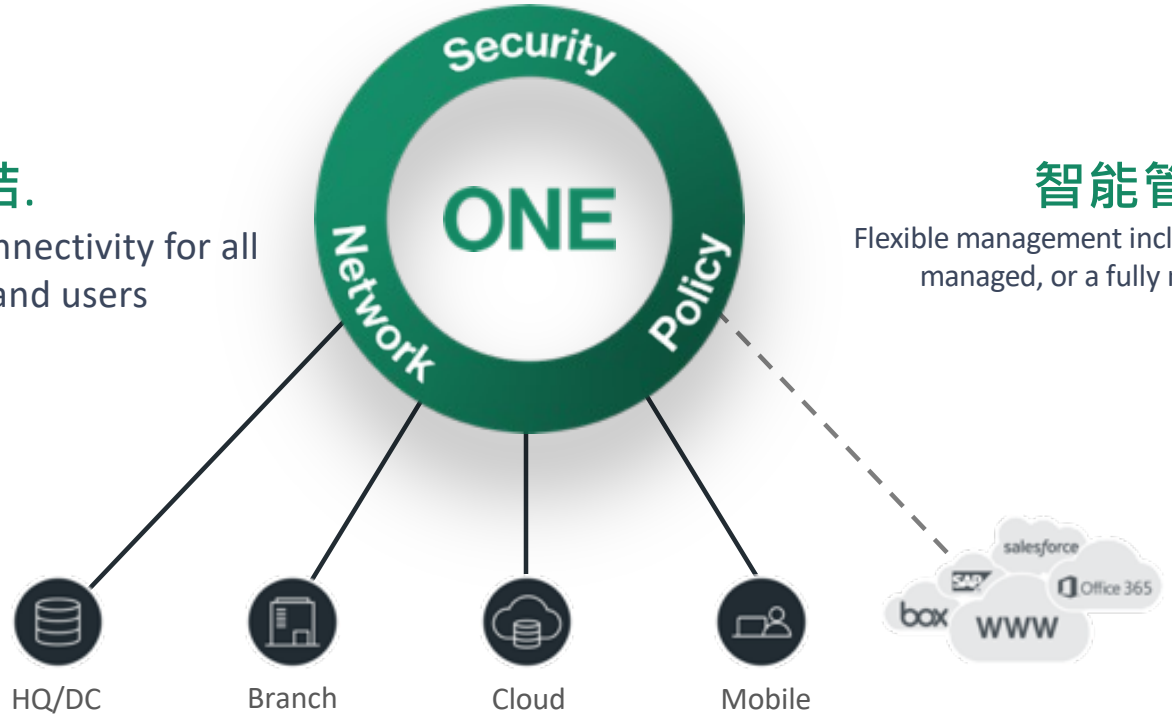
Cato 讓 SASE 更直覺簡單

資安防護.

Protect all traffic with built-in security as a service

雲地連結.

End-to-end optimized connectivity for all locations, clouds, and users



智能管理.

Flexible management including self-service, co-managed, or a fully managed service

CATO NETWORKS

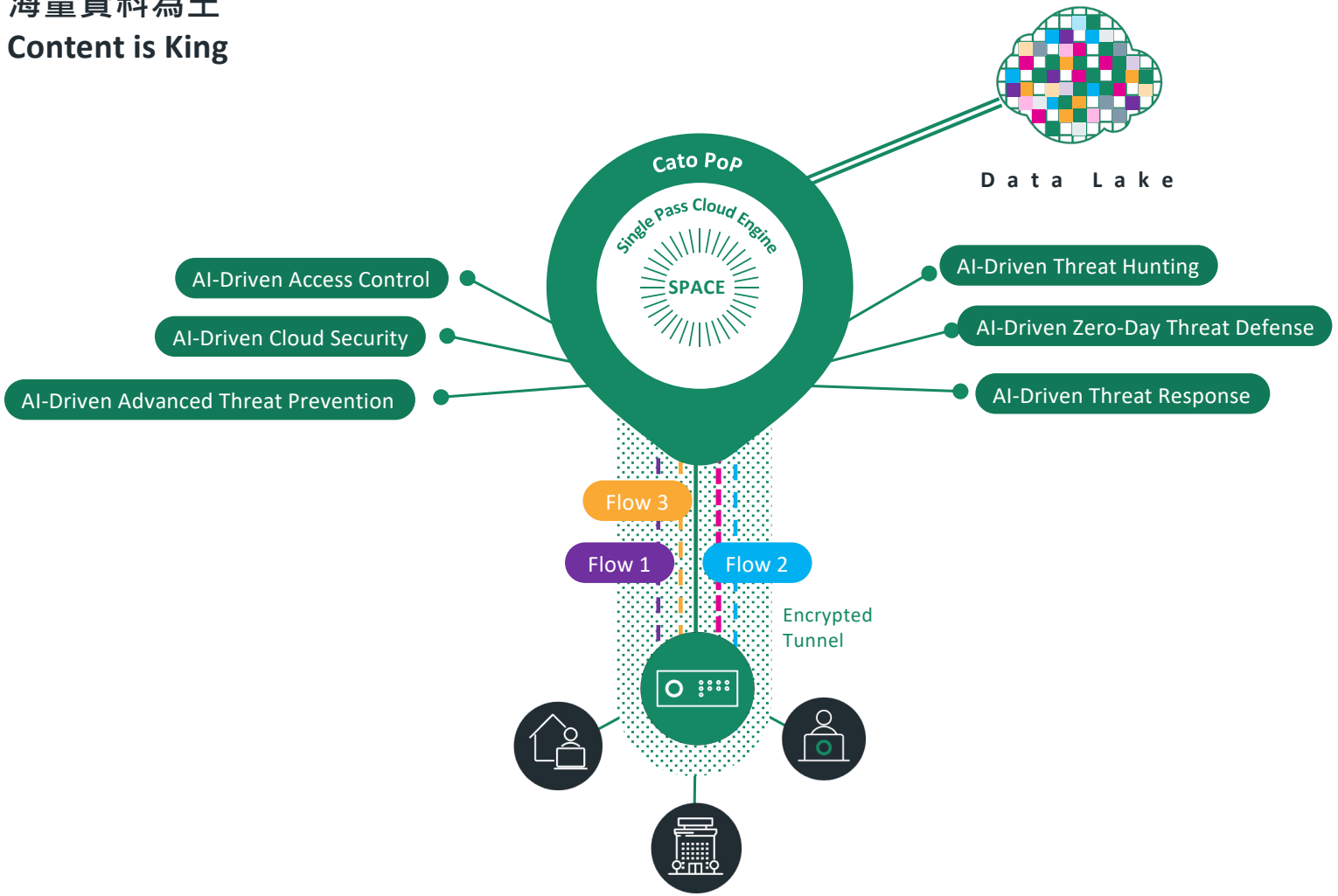
Cato 攜手 AI 技術
建構 SASE 雲平台

CATO
NETWORKS

SASE + AI + Zero Trust

海量資料為王
Content is King

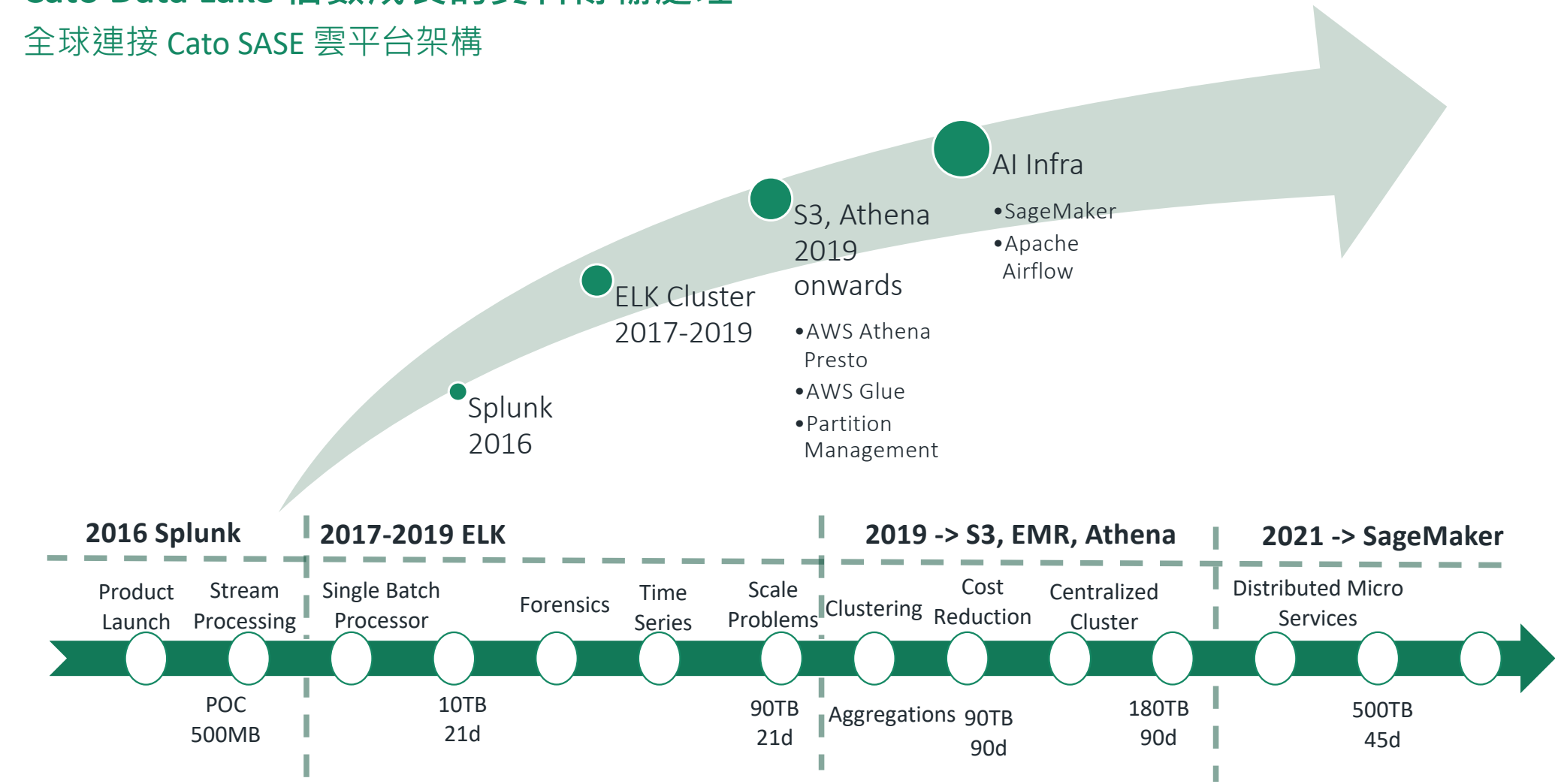
AI/ML + Cato 完美結合



CATO NETWORKS

Cato Data Lake 倍數成長的資料傳輸處理

全球連接 Cato SASE 雲平台架構



CATO NETWORKS

導入 AI 引擎的 Cato SASE 雲平台

提昇管理者使用體驗
Operations, Insights

- Copilot
- Storyteller

嚴實數位資安防護
Prevention, Detection

- Realtime prevention models
- Detection models

智能政策部署
Quality, Performance

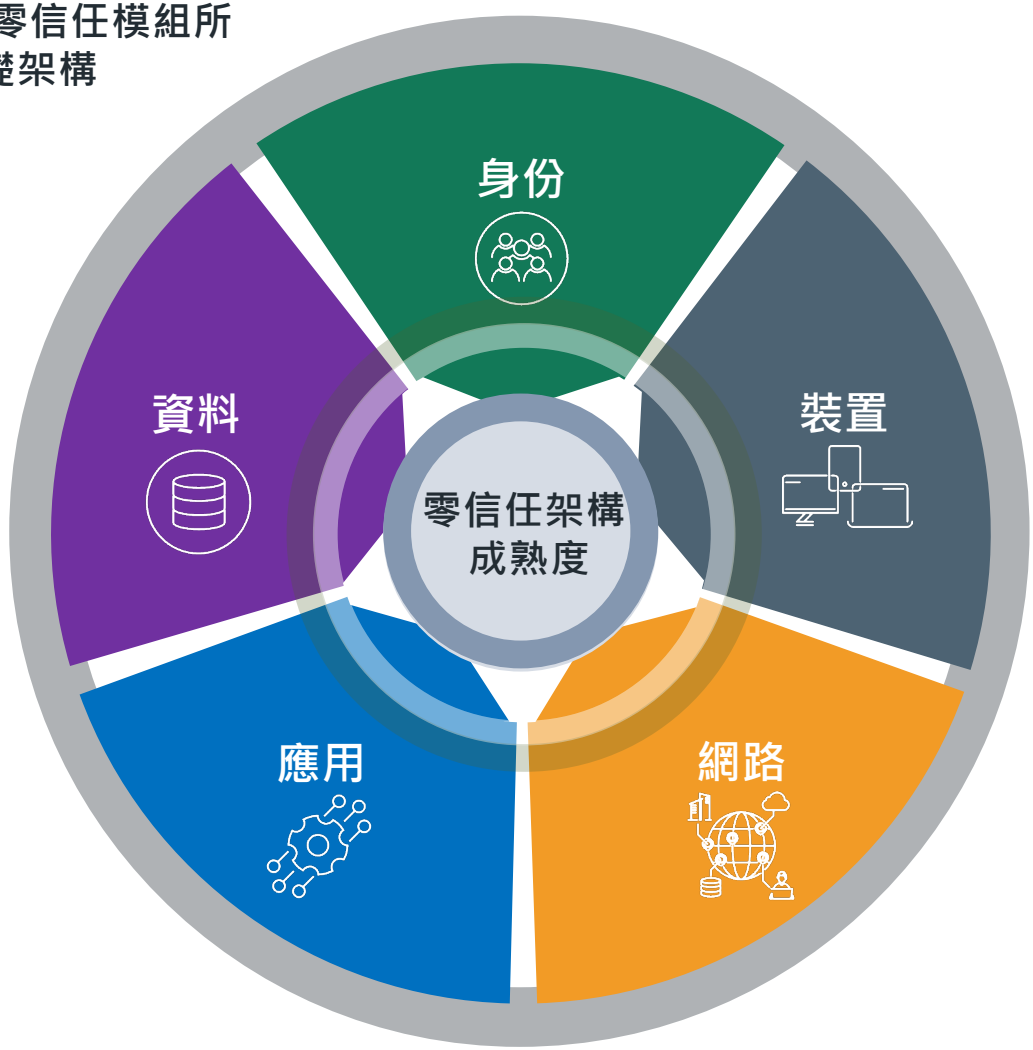
- Issues and Anomalies
- QOS policies

CATO NETWORKS

AI-Driven SASE Cloud

導入 AI 引擎的 Cato SASE 單一管理介面

根據 CISA 零信任模組所建構的基礎架構

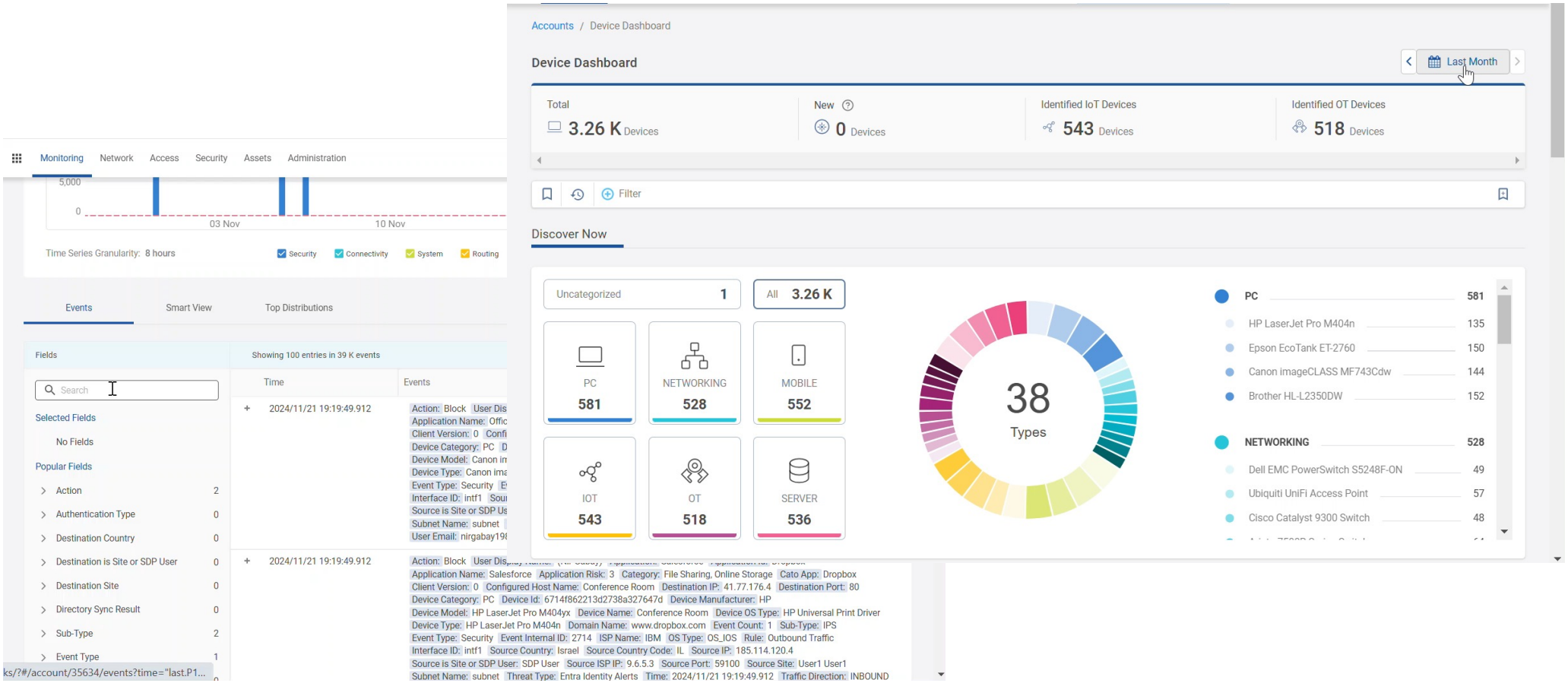


強化可見度分析，建立自動化機制，有效地編排及管理

CATO NETWORKS

Cato SASE 讓數位設備一目瞭然

Device Dashboard Unlocking IoT/OT Value with Cato



CATO NETWORKS

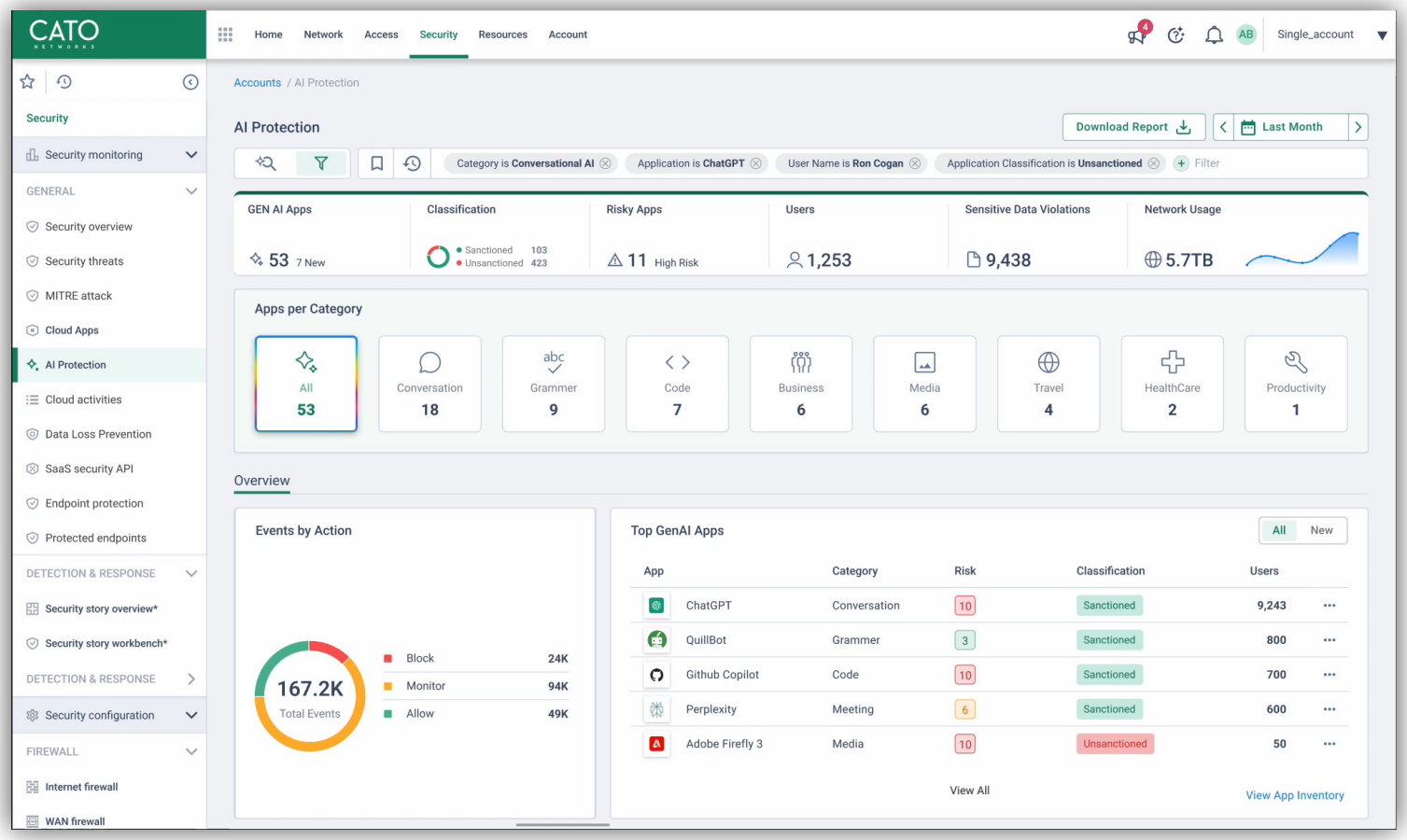
Cato SASE 讓 GenAI 使用一目瞭然

AI Protection Dashboard

Shadow AI

Access Control

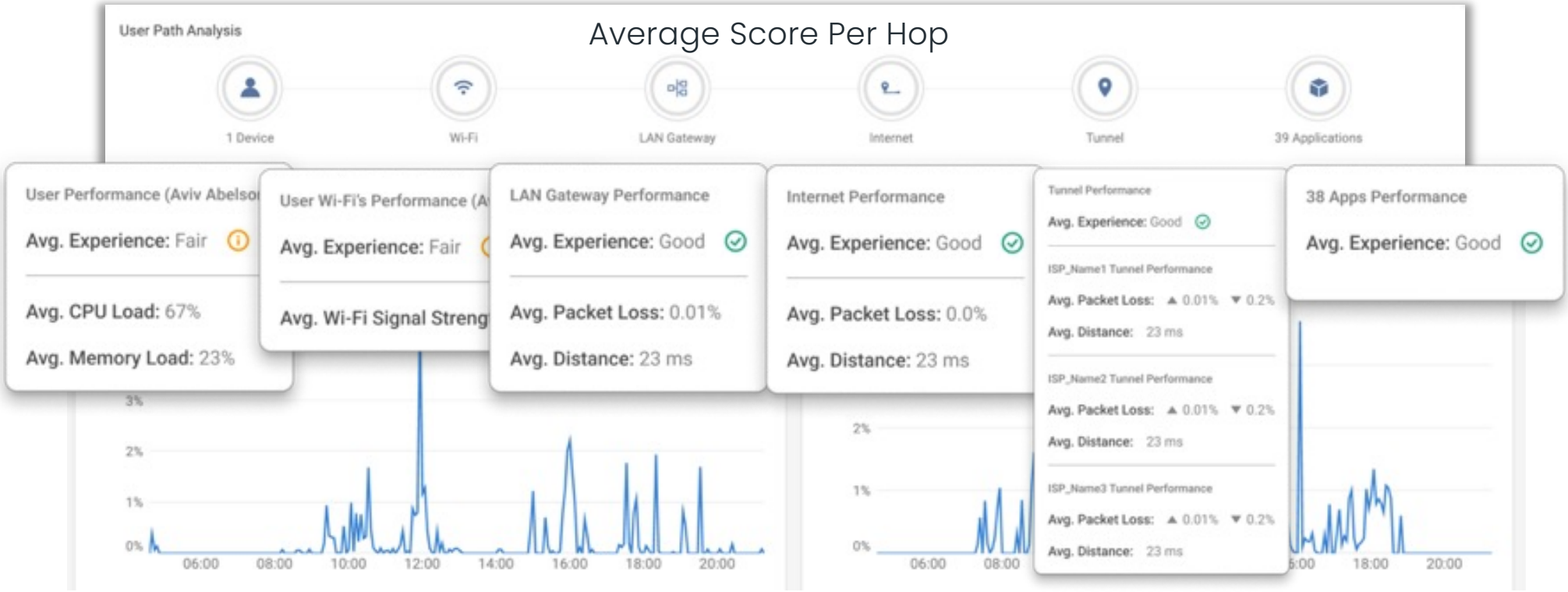
Data Protection



CATO NETWORKS

Cato DEM 檢視使用者數位化體驗

Gain Insight Into Digital Experience



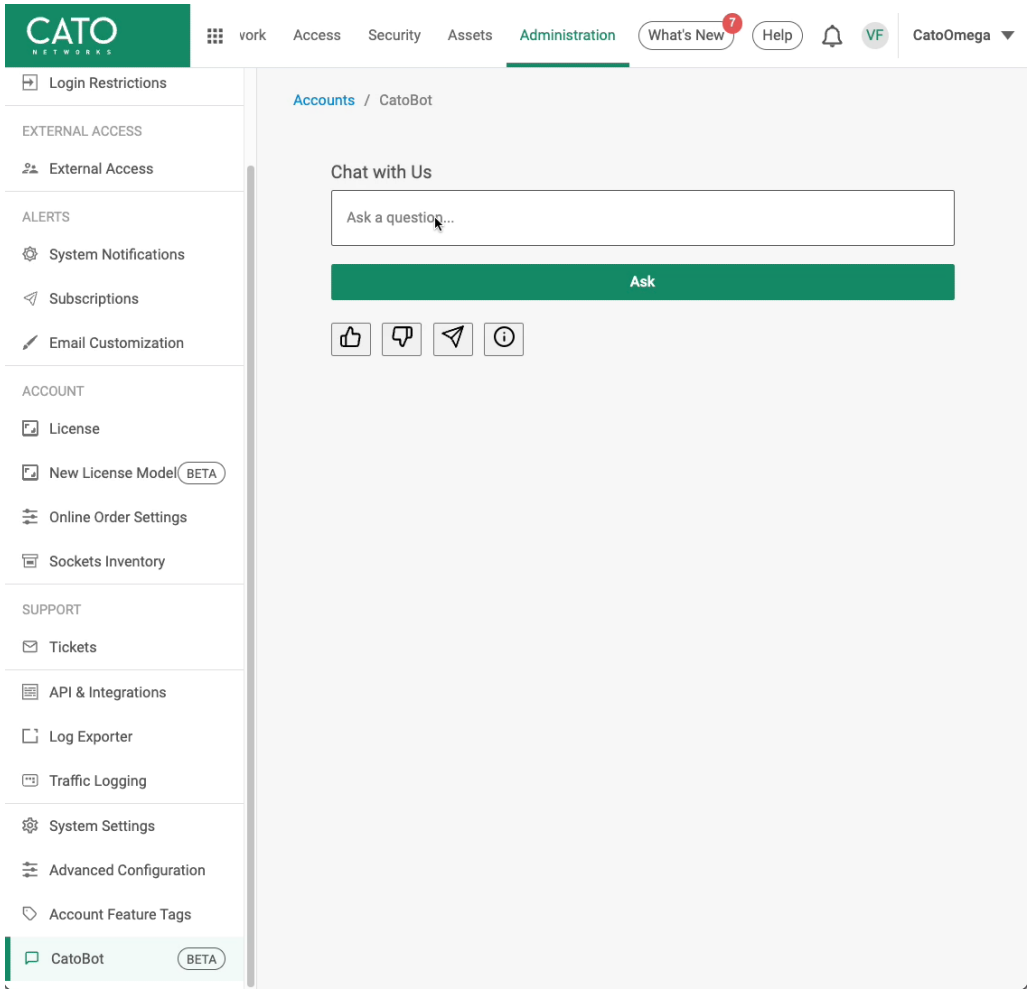
CATO NETWORKS

Cato CMA 智能化單一管理平台

導入LLM 模型的 GenAI 讓操作更直覺

CMA Co-Pilot

- Knowledge-base Q&A
- API code Reference
- Advanced search using NLP
- Policy / configuration

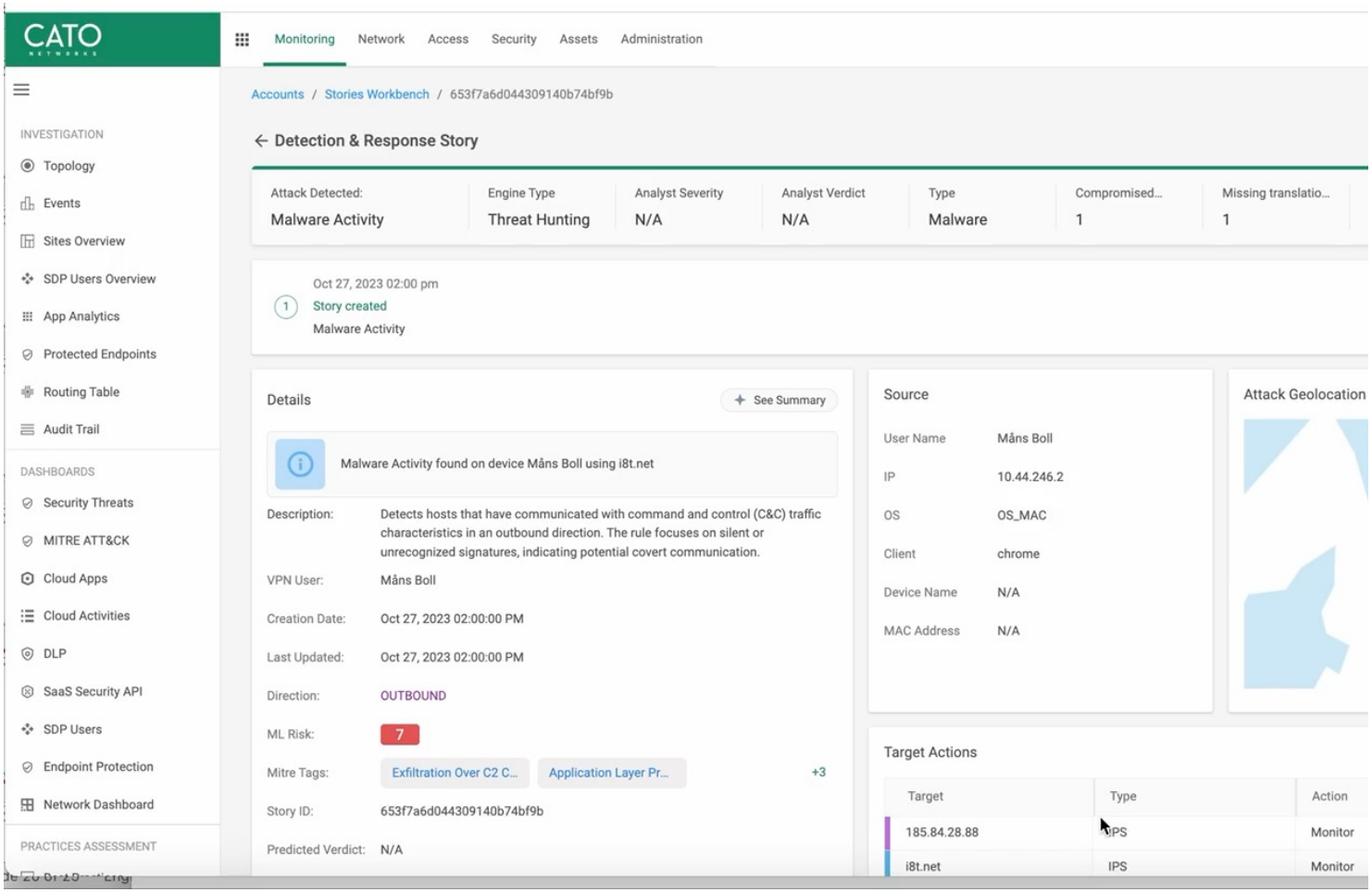


CatoBot: Using GenAI for Knowledge Q&A

CATO NETWORKS

Cato 完整詳實的網路與資安事件始末說明

XDR: Empowering Analysts with Storyteller



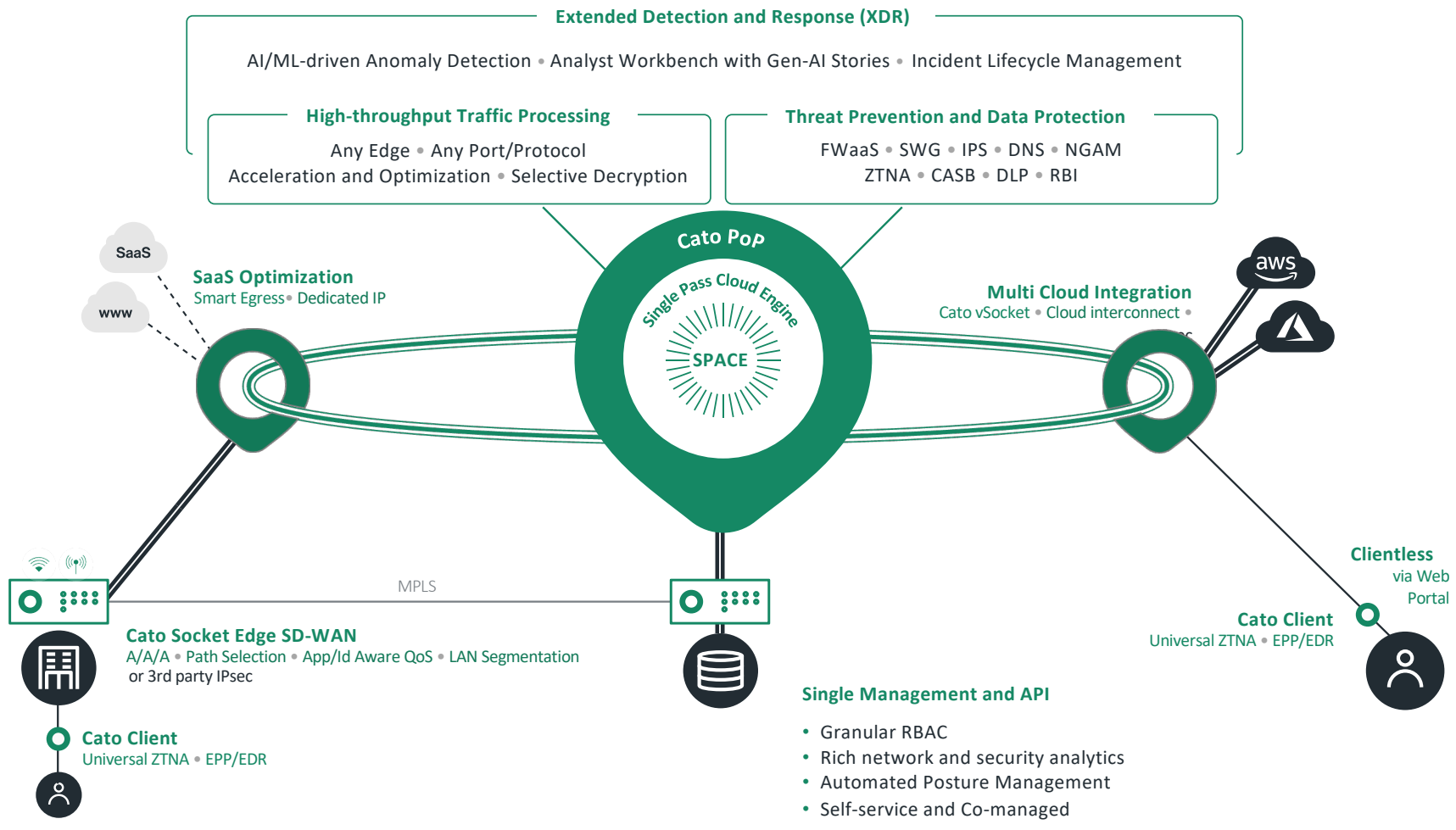
Using GenAI to produce natural language narratives in CMA

Cato SASE Cloud

The World's First SASE platform

Cato SASE 嚴實數位資安防護

整合 AI 科技的資安防護



CATO NETWORKS

Cato 進階資安威脅與防護

ML 強化與自動更新即時威脅防護模組

Anti Phishing: Cybersquatting

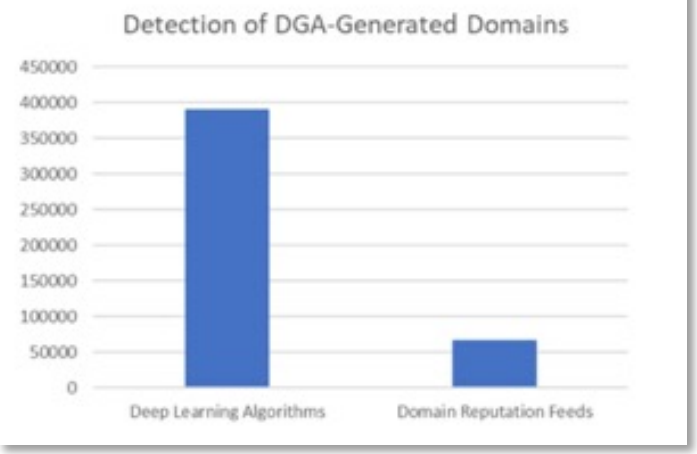
Figure 2- Example of homographsquatting targeting Facebook users

Combining **intel feeds** of leading legitimate domains with customers **popularity analysis** to eliminate cybersquatting false positives

Anti Bot: DGA Detection

Real-time Deep Learning Yields 6X Improvement in Threat Detection

Cato Research Labs routinely observes tens of millions of network connection attempts to DGA domains from across the 1700+ enterprises using the Cato SASE Cloud. For example, of the 457,220 network connection attempts to DGA domains made in a sample period, only 66,675 (15 percent) were listed in the 250+ threat intelligence feeds consumed by Cato. By contrast, Cato algorithms identified the rest, over 390,000 additional DGA domains, a nearly six-fold improvement.



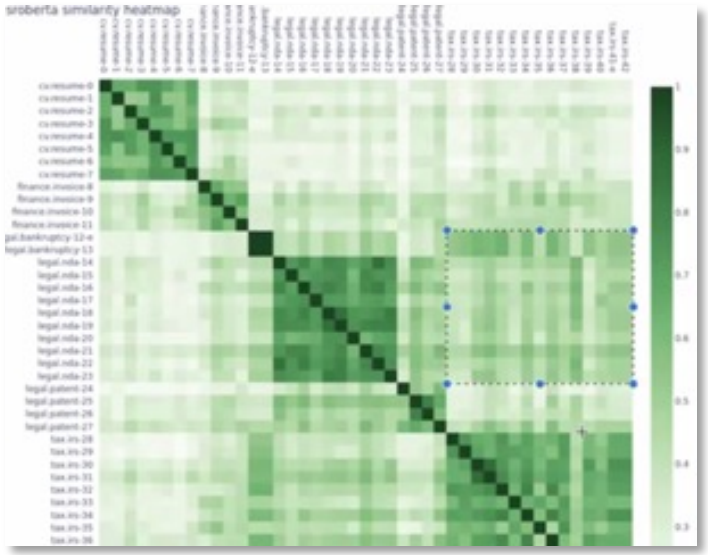
CATO NETWORKS

Cato 進階資安威脅與防護

ML 強化與自動更新即時威脅防護模組

ML Classifier for DLP

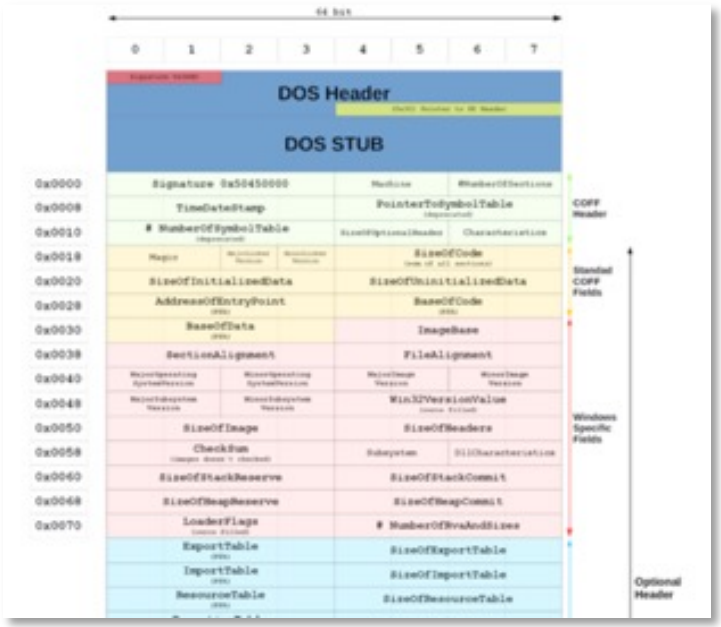
Utilize ML models for textual and graphic content classification



Pre-defined classifiers: legal, financial, HR

Custom classifiers: Allow customers to build custom models based on their specific data

ML-based Filescanning (NGAM)

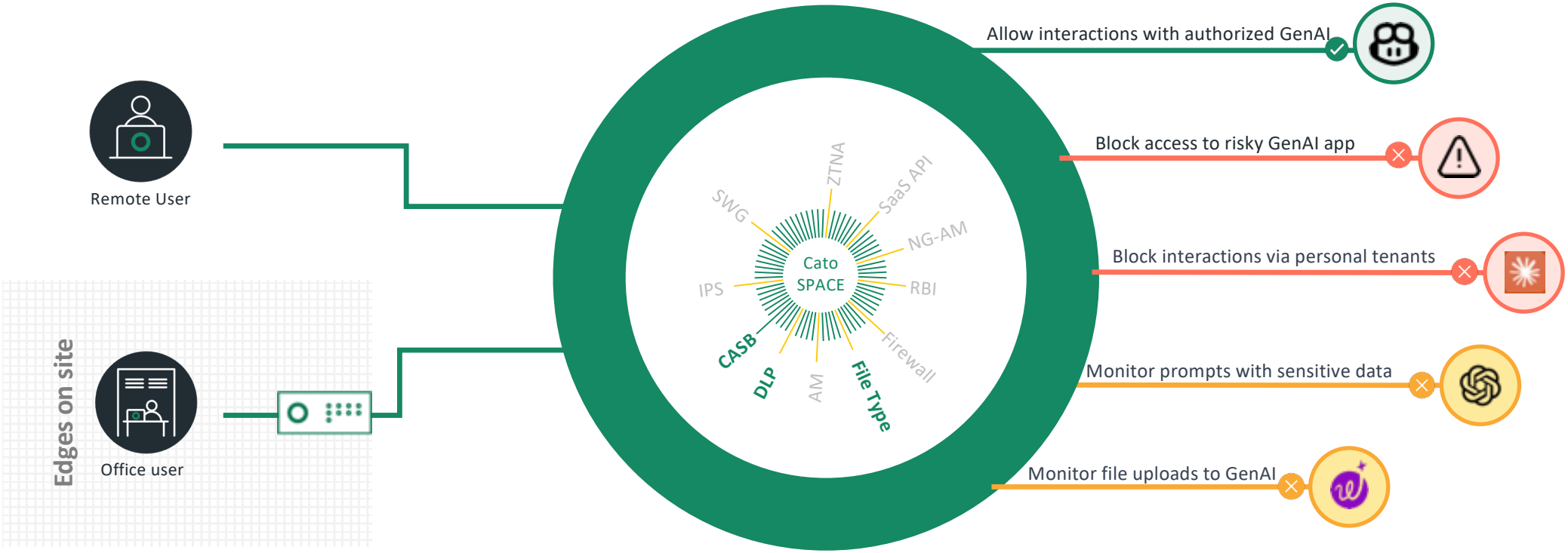


Pre-execution classifiers to detect malicious files using machine learning, powered by Sentinelone engine.

CATO NETWORKS

Cato 落實 GenAI 資安防護

保障企業對 GenAI 使用與防護



CATO NETWORKS

Mitigat
e Risk

使用 AI 模型協助組態設定評估與優化

Cato SASE 智能化政策風險評估

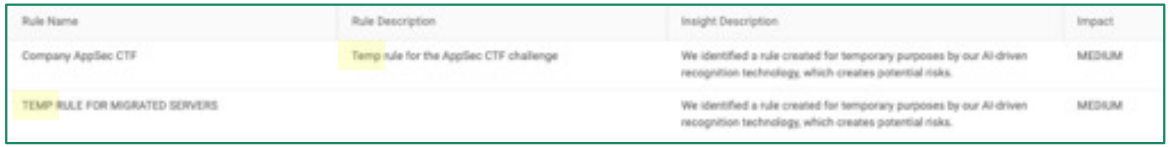
- **識別風險** – 預先評估潛在的風險用戶和設備
- **評估風險** – 確定風險狀況並做出相應定義
- **控制風險** – 全面執行適當的存取政策
- **審查風險** – 持續的風險評估和即時調整

CATO NETWORKS

Cato 資安政策部署檢視與建議

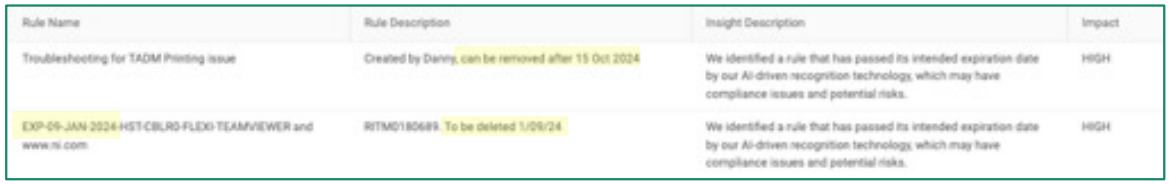
資安政策規則檢視與建議

- **Temporary Rules**
  - Introduced as a short-term solutions to address immediate, often business-related need. These rules are mostly created to function temporarily while a proper or permanent solution is being deployed or developed
- **Testing Rules**
  - Rules explicitly created for validating, debugging, or experimenting with a specific feature or scenario
- **Expired Rules**
  - Rules created to address a specific need and have a desirable cutoff date that has already passed.
- **Future Expiration Hinting**
  - Rules created to address a specific need and have a desirable cutoff date that has not yet been reached or cannot be proven/evaluated.

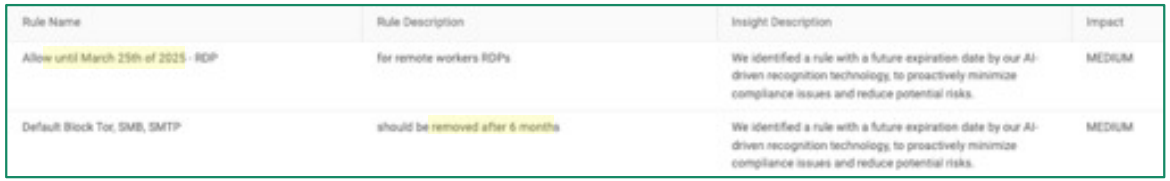


Rule Name	Rule Description	Insight Description	Impact
Company AppSec CTF	Temp rule for the AppSec CTF challenge	We identified a rule created for temporary purposes by our AI-driven recognition technology, which creates potential risks.	MEDIUM
TEMP RULE FOR MIGRATED SERVERS		We identified a rule created for temporary purposes by our AI-driven recognition technology, which creates potential risks.	MEDIUM

Rule Name	Rule Description	Insight Description	Impact
TAG - Rule for Network Troubleshooting (PING & Tracert tests)	Created by Joey - For network issue troubleshooting (10.10.2.2 & 10.5.4.x for Conan)	We identified a rule created for testing purposes by our AI-driven recognition technology, which creates potential risks.	MEDIUM
Test - block unfimiliar port	from CISO ticket	We identified a rule created for testing purposes by our AI-driven recognition technology, which creates potential risks.	MEDIUM



Rule Name	Rule Description	Insight Description	Impact
Troubleshooting for TADM Printing issue	Created by Danny, can be removed after 15 Oct 2024	We identified a rule that has passed its intended expiration date by our AI-driven recognition technology, which may have compliance issues and potential risks.	HIGH
EXP-09-JAN-2024-HST-CBLR0-FLEXI-TEAMVIEWER and www.ni.com	RITM0180689. To be deleted 1/09/24	We identified a rule that has passed its intended expiration date by our AI-driven recognition technology, which may have compliance issues and potential risks.	HIGH



Rule Name	Rule Description	Insight Description	Impact
Allow until March 25th of 2025 - RDP	for remote workers RDPs	We identified a rule with a future expiration date by our AI-driven recognition technology, to proactively minimize compliance issues and reduce potential risks.	MEDIUM
Default Block Tor, SMB, SMTP	should be removed after 6 months	We identified a rule with a future expiration date by our AI-driven recognition technology, to proactively minimize compliance issues and reduce potential risks.	MEDIUM

CATO NETWORKS

Cato SASE 攜手 IT 夥伴邁向 AI 時代

Cato 內建 AI 技術的 SASE 解決方案

企業使用者

- True Agility
- Increased Speed to market
- Increased Speed to value
- Increased Visibility & Control
- Optimum user experience
- Reduced Security Risk

企業 IT

- No Capex Financial Risk
- Increased Speed to revenue
- Increased Operational Margins
- Reduced Management Resource
- Compete against Telcos
- Operational Simplicity & Upsell

CATO NETWORKS

CATO
NETWORKS


CATO
NETWORKS
WE ARE SASE™
We challenge old concepts.
We lead to a better tomorrow.

CATO NETWORKS

Cato SASE. Ready for Whatever's Next.

Thank You