

# SASE 戰術策略邁向數位

Cato Networks. The Global SASE Leader.

Regional Sales Director

[Chris.shih@catonetworks.com](mailto:Chris.shih@catonetworks.com)

0938-967-952

# 什麼是SASE ?

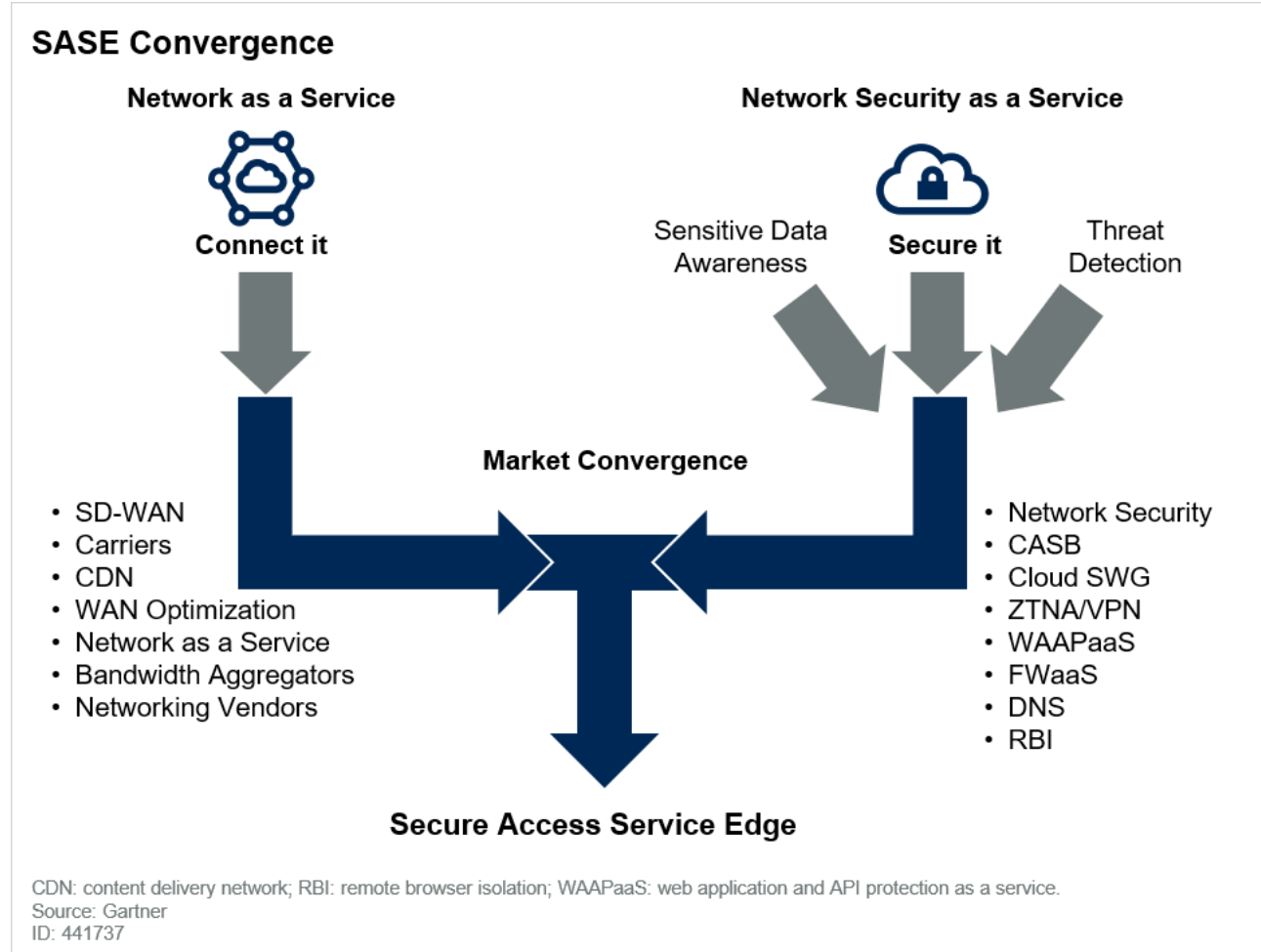
With the Secure Access Service Edge (SASE)

Gartner 認為SASE的網路架構能夠替企業帶來簡單、易於擴展、彈性、低延遲及安全性，這些優點應該擴展到企業每一個連結點上。

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

**Gartner**

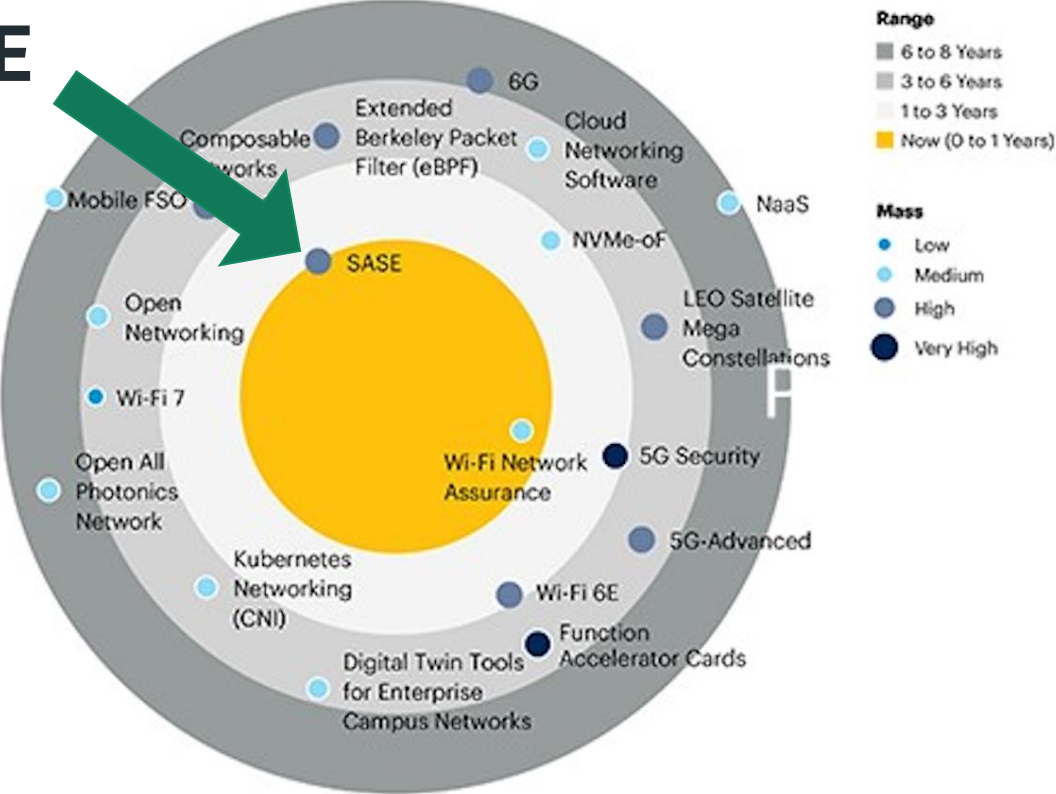
Market Trends: How to Win as WAN Edge and Security Converge Into the Secure Access Service Edge, 2019



# 未來的1年內將成為主流

## Impact Radar for Communications

SASE



Source: Gartner  
749438\_C

Published by:

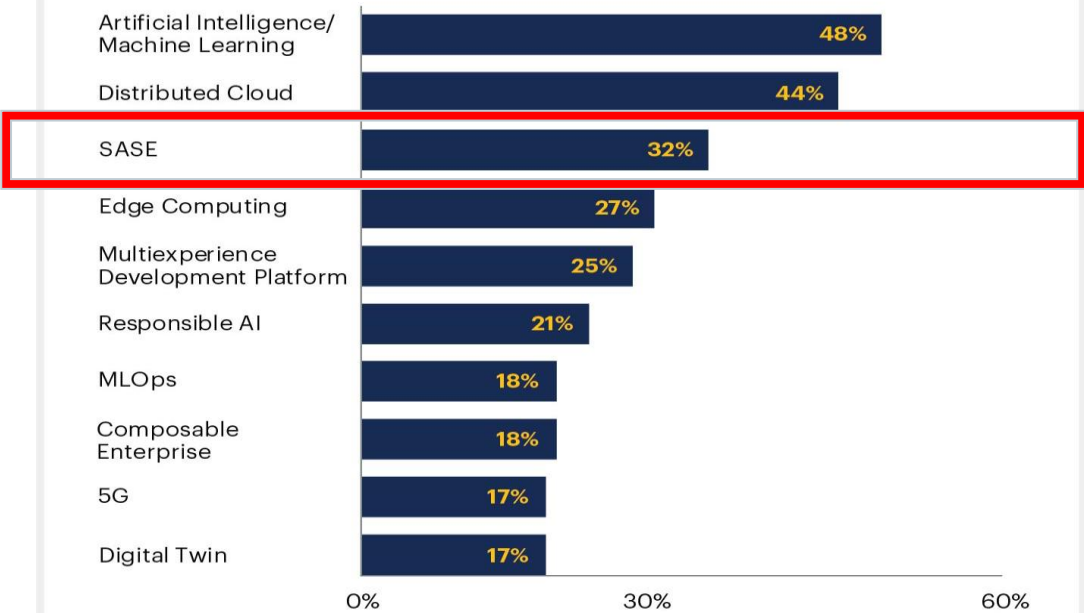
Gartner



# SASE已在CIO 心中計畫部署

## State of Deployment for Emerging Technologies

Percentage of Respondents Who Have Already Deployed or Plan to Deploy a Technology in Next 12 Months



[gartner.com](https://www.gartner.com)

n = 2,363, CIOs and technology executives answering, excluding don't know  
Q. What are your enterprise's plans in terms of the following digital technologies and trends?  
Note: MLOps = machine learning operationalization; SASE = secure access service edge  
Source: 2022 Gartner CIO and Technology Executive Survey

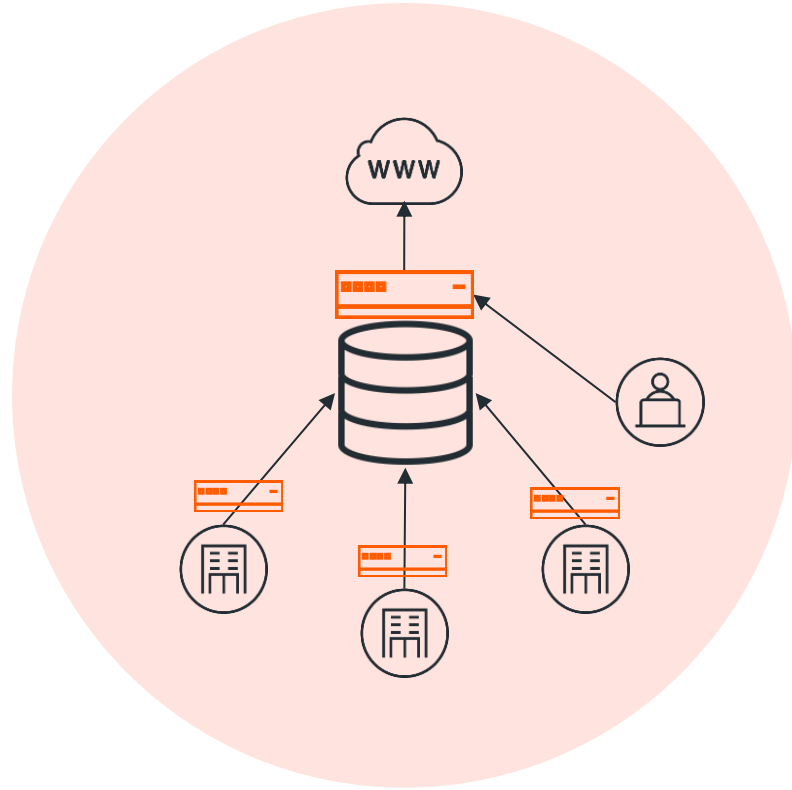
© 2021 Gartner, Inc. All rights reserved. CTMKT\_1548365

**Gartner**



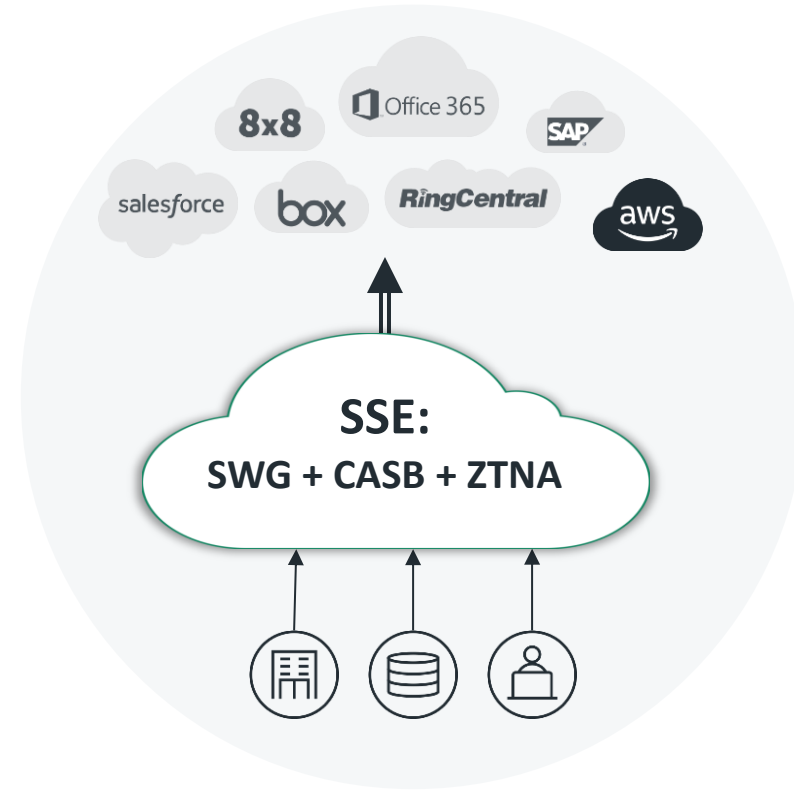
# 模糊的安全防護邊界

From **Security in Location** to **Security Everywhere**



## Security in Location

Applications in On-premises Datacenter  
Most Users in the Office



## Security Everywhere

Applications Everywhere  
Users Everywhere

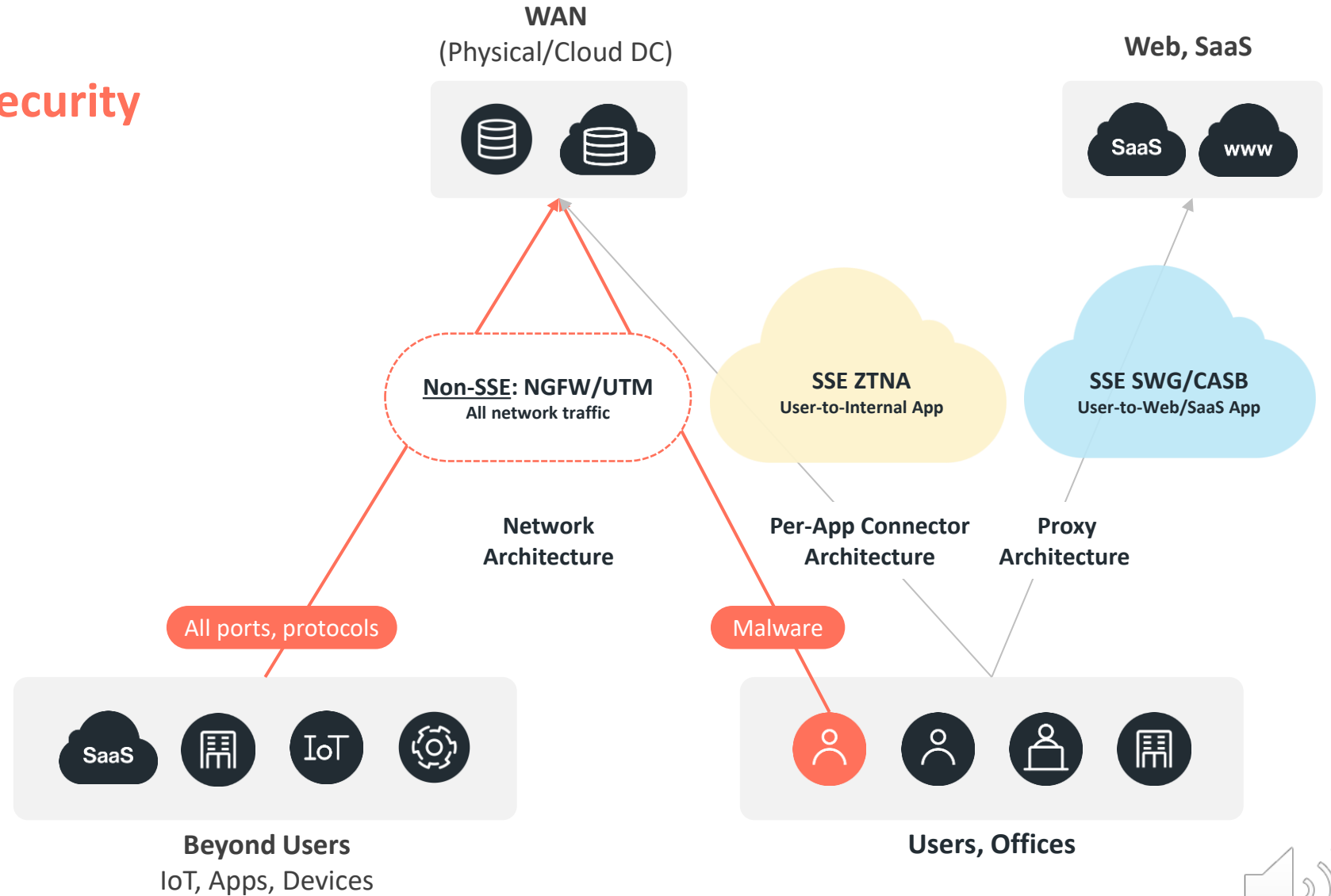


# 現今的網路環境如何達到無邊界的資安防護架構？

Blind spots and complexity

## Different Traffic, Different Security

- **Fragmented**  
multiple security architectures
- **Inconsistent**  
multiple policy engines
- **Limited Visibility**  
for WAN security
- **Unoptimized**  
public internet for global access



# Cato Networks SASE Solution



# 我們需要更簡單、安全及快速的網路環境

## 安全

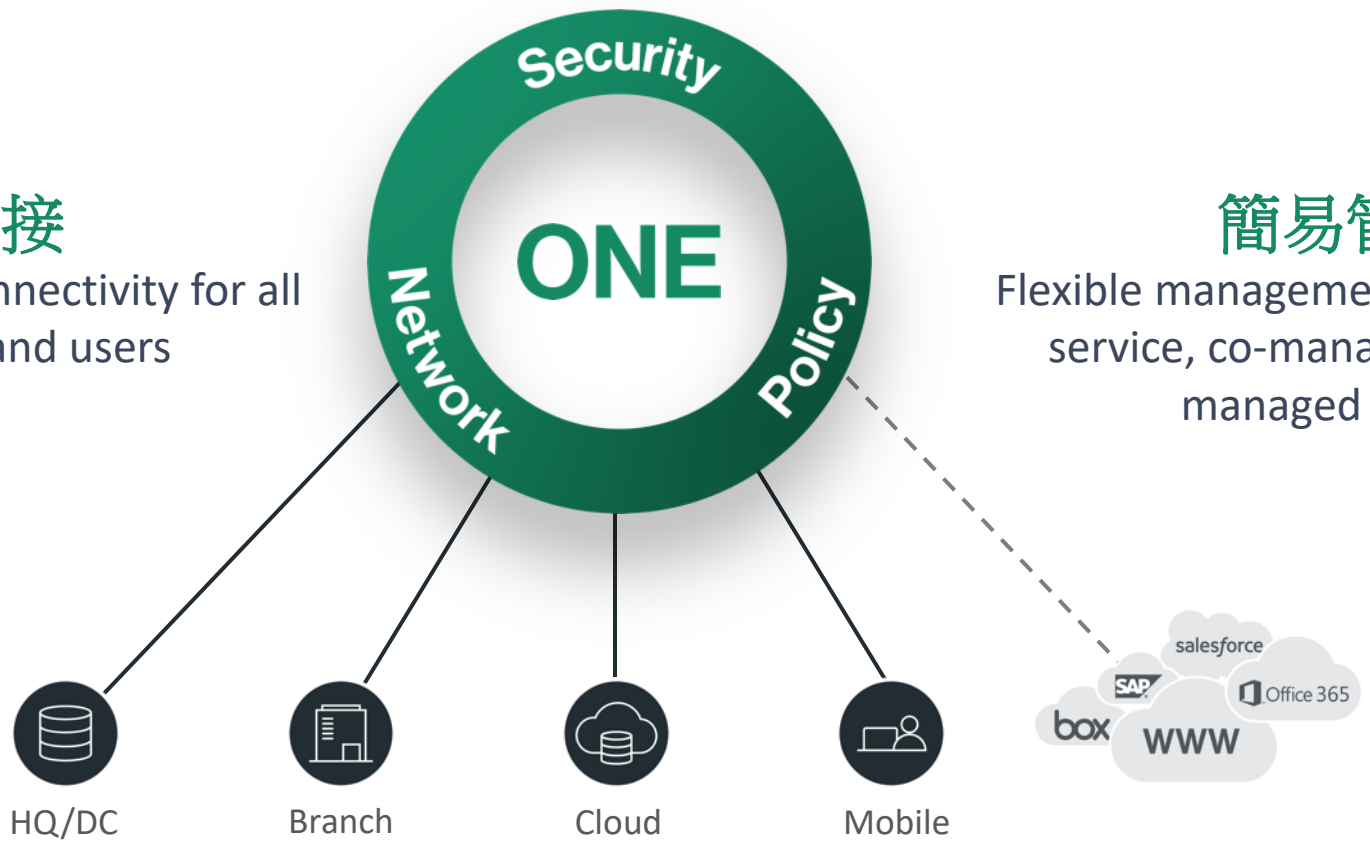
Protect all traffic with built-in security as a service

## 無邊界連接

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

## 簡易管理

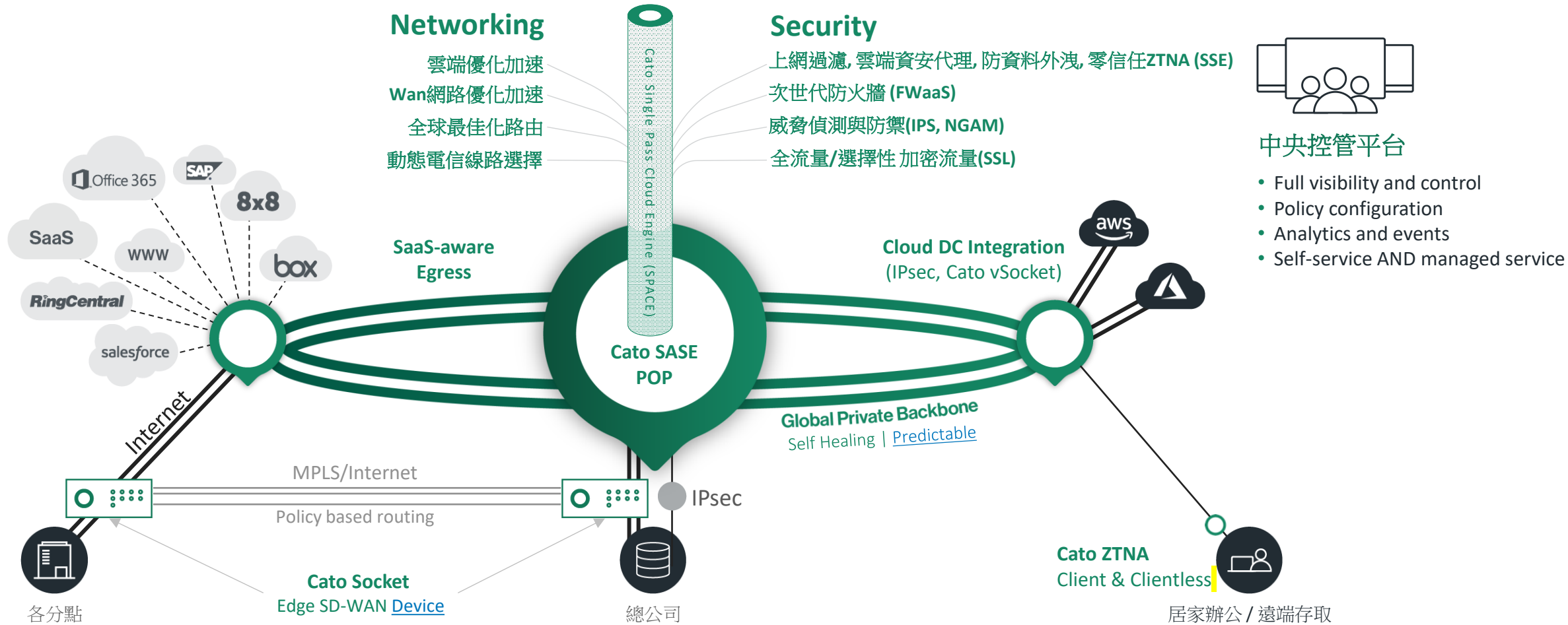
Flexible management including self-service, co-managed, or a fully managed service





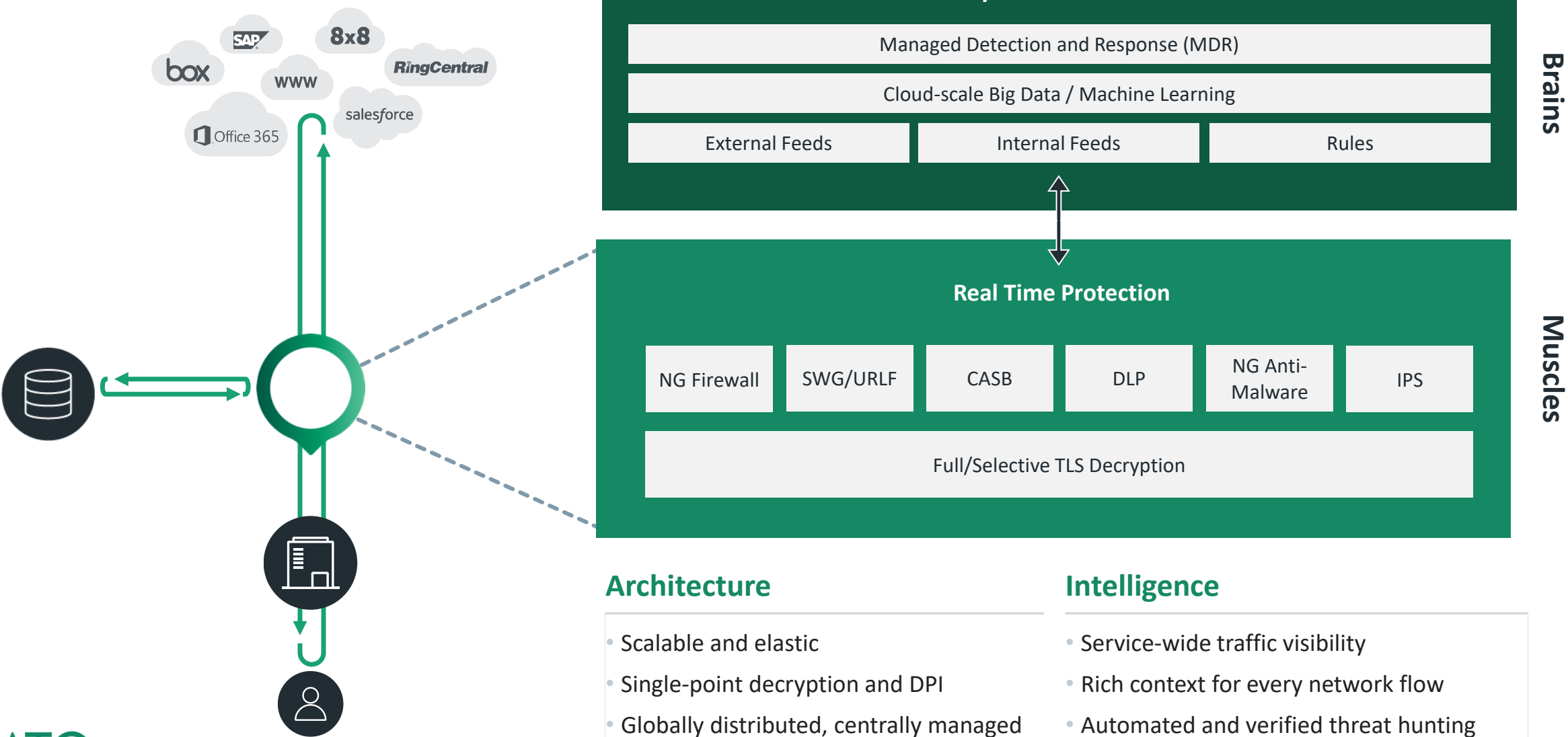
# Cato SASE Cloud

## The Power of Networking and Security Convergence



所有流量 All Ports/Protocols	所有方向 East/West, South/North	所有資料流 User-Apps, IoT, Apps-to-Apps, Machine-Machine, Service-to-Service	所有應用程式 Physical DC, Cloud DC, SaaS
檢查所有流量 Any source/destination	優化整體網路 Last mile, Middle Mile, Global		

# Security-as-a-Service Overview



# THREAT HUNTING – APACHE LOG4J VULNERABILITIES

Dec 10<sup>th</sup> - SEC team noticed  
CVE-2021-44228  
Friday, 07:00 am ILT  
first attack observed in Cato

“**Silent**” signature is  
released; KB is ready  
Dec 11<sup>th</sup> - 03:00 (TLV time)

**Blocking** signature is  
released – All Cato IPS  
customers are protected  
Dec 11<sup>th</sup> - 13:00 (TLV time)



**CATO NETWORKS**  
**Security Update**  
**CVE-2021-44228: Apache Log4j 2 Vulnerability**

Dear Customer,

As of the 9th December 2021, the Security community became aware of active exploitation attempts of a vulnerability in Apache Log4j. This vulnerability has been classified as CRITICAL, with a base CVSS score of 10.0. We are contacting you to make you aware of the Cato mitigation strategy.

**What is Cato doing to keep me protected?**

- Cato Networks identified the traffic signature associated with this exploit on the 10th December 2021, and was actively monitoring our customer base.
- As of 11th December 2021, we have implemented a global blocking rule within our IPS for all Cato Customers to mitigate this vulnerability.

**What do I need to do?**

- If you have the Cato IPS enabled, we will be actively blocking the traffic signature of this vulnerability automatically. No patching or updates to the Cato platform is required.
- We recommend that you follow continued vendor advisories to also mitigate the problem at the source.

**Where can I find more information?**

- More information regarding this exploit and Cato Networks' response can be found in this [Knowledge Base article](#).

**NIST**  
Information Technology Laboratory  
**NATIONAL VULNERABILITY DATABASE**  
**NVD**

**VULNERABILITIES**

**CVE-2021-45105 Detail**

**Current Description**

Apache Log4j2 versions 2.0-alpha1 through 2.16.0 (excluding 2.12.3 and 2.3.1) did not protect from uncontrolled recursion from self-referential lookups. This allows an attacker with control over Thread Context Map data to cause a denial of service when a crafted string is interpreted. This issue was fixed in Log4j 2.17.0, 2.12.3, and 2.3.1.

[View Analysis Description](#)

**Severity** CVSS Version 3.x CVSS Version 2.0

CVSS 3.x Severity and Metrics:

**QUICK INFO**

**CVE Dictionary Entry:**  
CVE-2021-45105

**NVD Published Date:**  
12/18/2021

**NVD Last Modified:**  
12/30/2021

**Source:**  
Apache Software Foundation

# Cato雲PoP全球分佈圖：75個PoP、“網路即是安全”



加拿大，卡爾加里  
加拿大，溫哥華  
華盛頓州，西雅圖  
俄勒岡州，波特蘭  
加利福尼亞州，聖約瑟  
加利福尼亞州，洛杉磯  
科羅拉多州，丹佛  
德克薩斯州，達拉斯  
墨西哥，瓜達拉哈拉

加拿大，多倫多  
佐治亞州，亞特蘭大  
伊利諾州，芝加哥  
加拿大，蒙特利爾  
麻塞諸塞州，波士頓  
紐約  
弗吉尼亞州，阿什本  
俄亥俄州，哥倫布  
佛羅里達州，邁阿密

愛爾蘭，都柏林  
英國，倫敦  
法國，巴黎  
西班牙，馬德里  
巴西，聖保羅  
瑞典，斯德哥爾摩

荷蘭，阿姆斯特丹  
捷克，布拉格  
羅馬尼亞，布加勒斯特  
德國，法蘭克福  
以色列，特拉維夫  
阿拉伯聯合酋長國

韓國，首爾  
日本，東京  
中國，上海  
香港  
越南，胡志明市  
珀斯  
墨爾本  
悉尼  
中國，北京  
印度，孟買  
泰國，曼谷  
馬來西亞，吉隆坡  
新加坡  
南非，約翰尼斯堡



**99.999%**  
Uptime SLA

**75+**  
PoPs

**1,100+**  
Enterprise Customers

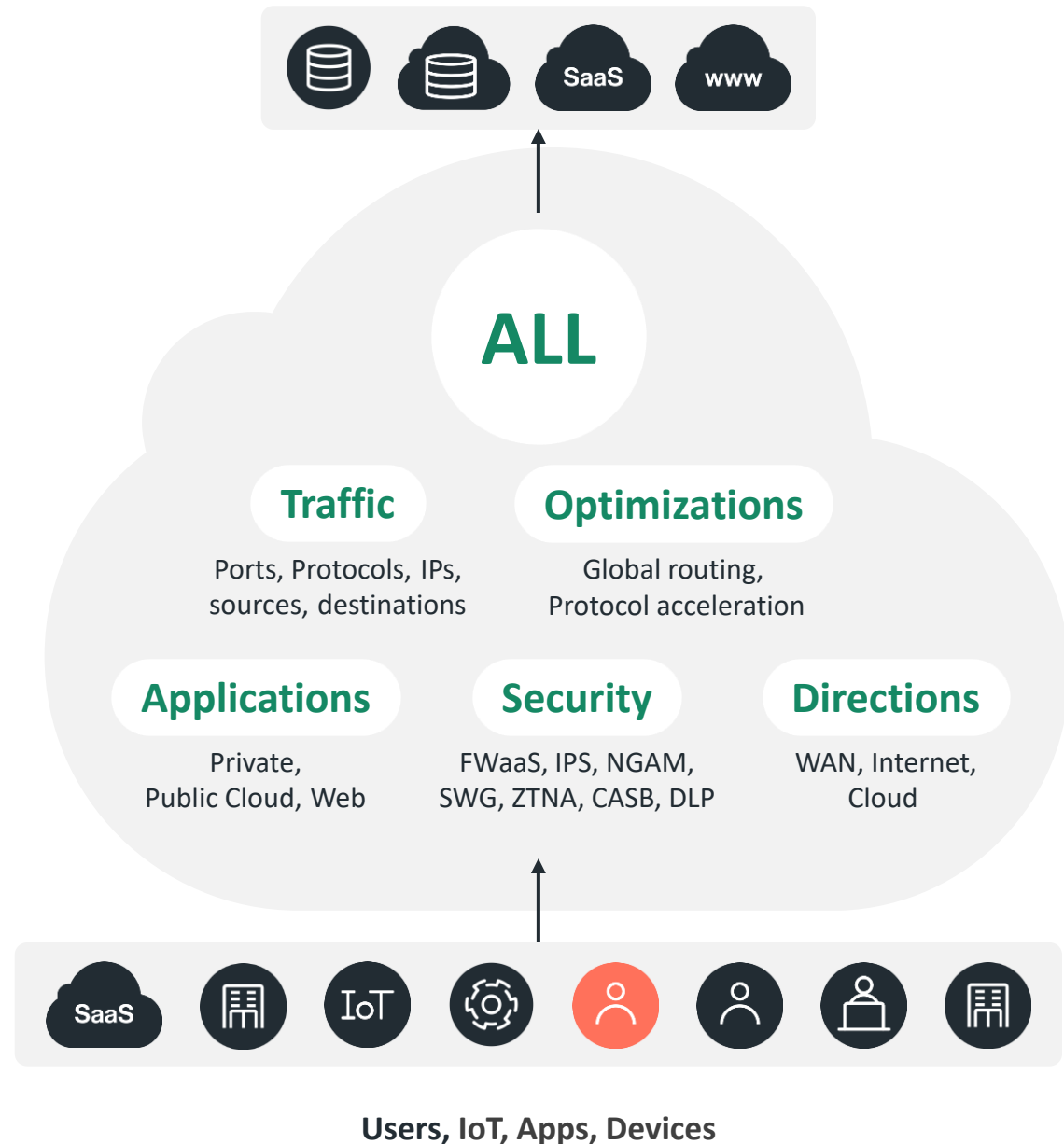
**24x7x365**  
Global NoC and SoC

# Cato SSE 360: 提供無邊界的資安防護架構

Beyond user-to-application access

## All Traffic, Same Security

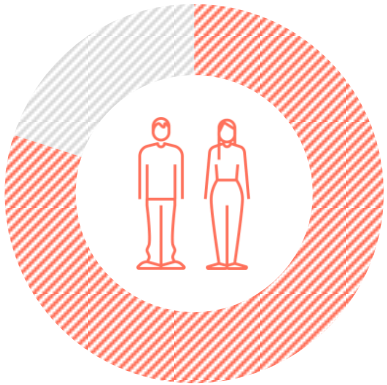
- **Converged**  
one architecture for all edges
- **Simple**  
one policy engine and rule base
- **Holistic**  
all traffic, all edges, all directions
- **Optimized**  
w/ global private backbone



# IT的陰影！



97% of cloud apps  
used in the enterprise are **shadow IT**<sup>1</sup>



80% of workers  
admit to using SaaS applications at work  
**without getting approval** from IT<sup>2</sup>



The average company has  
**975 unknown** cloud services<sup>3</sup>



Shadow IT is  
**50% or more**  
**of IT spending** at large enterprises<sup>5</sup>



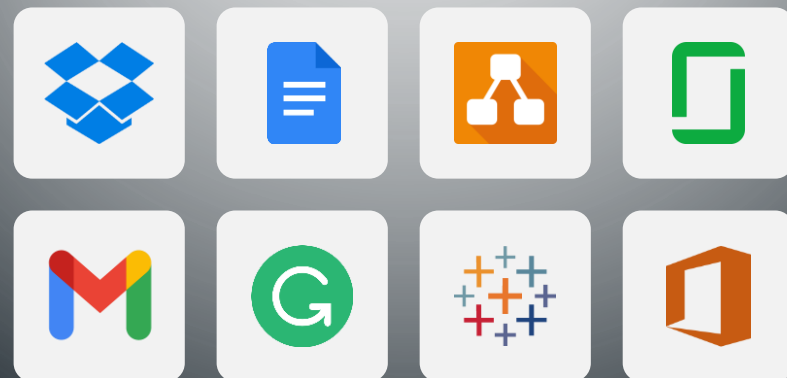
**67% of teams**  
have introduced their **own collaboration**  
tools into an organization<sup>4</sup>



**40% of organizations**  
have experienced a cloud-based data **breach** in  
the past 12 months<sup>6</sup>



受管制其及授權軟體



未授權之軟體

Shadow IT



# Predefined Data Sets for Profiling of Sensitive Data



## 350 Data Types

- Social security numbers [USA]
- Credit cards [Global]
- Bank account details [Germany]
- National identification numbers [Japan]
- ...



## 8 Compliance Categories

- PII
- PCI DSS
- HIPAA
- Financial Data
- ...



## 30 Countries

- Germany
- Italy
- UK
- US
- Japan
- ...



## 40 File types

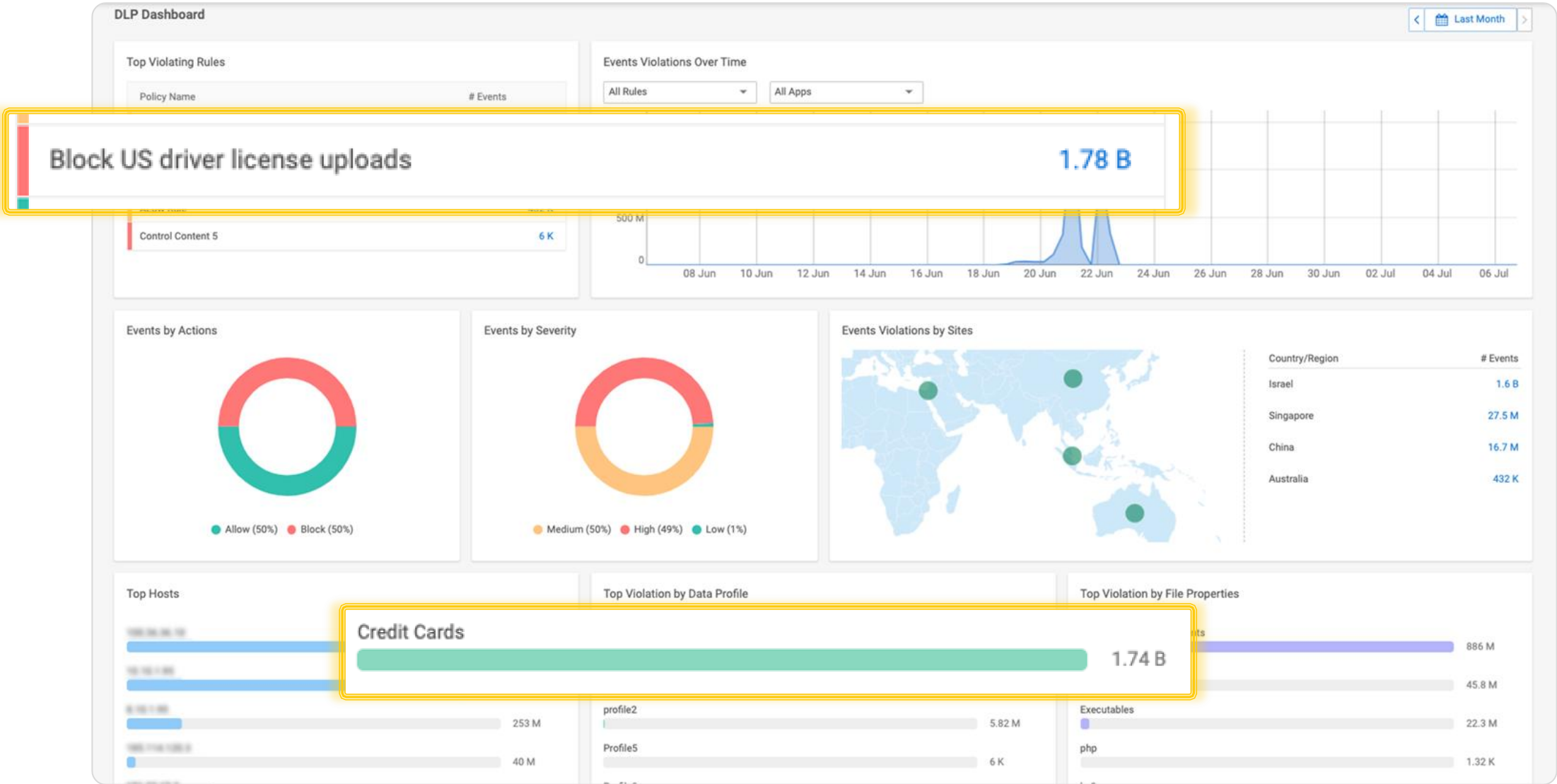
- Java
- PDF
- Excel
- Executable
- Microsoft Word
- ...

## A profile consists of a combination of data types

For example, the profile “PCI Germany” consists of:

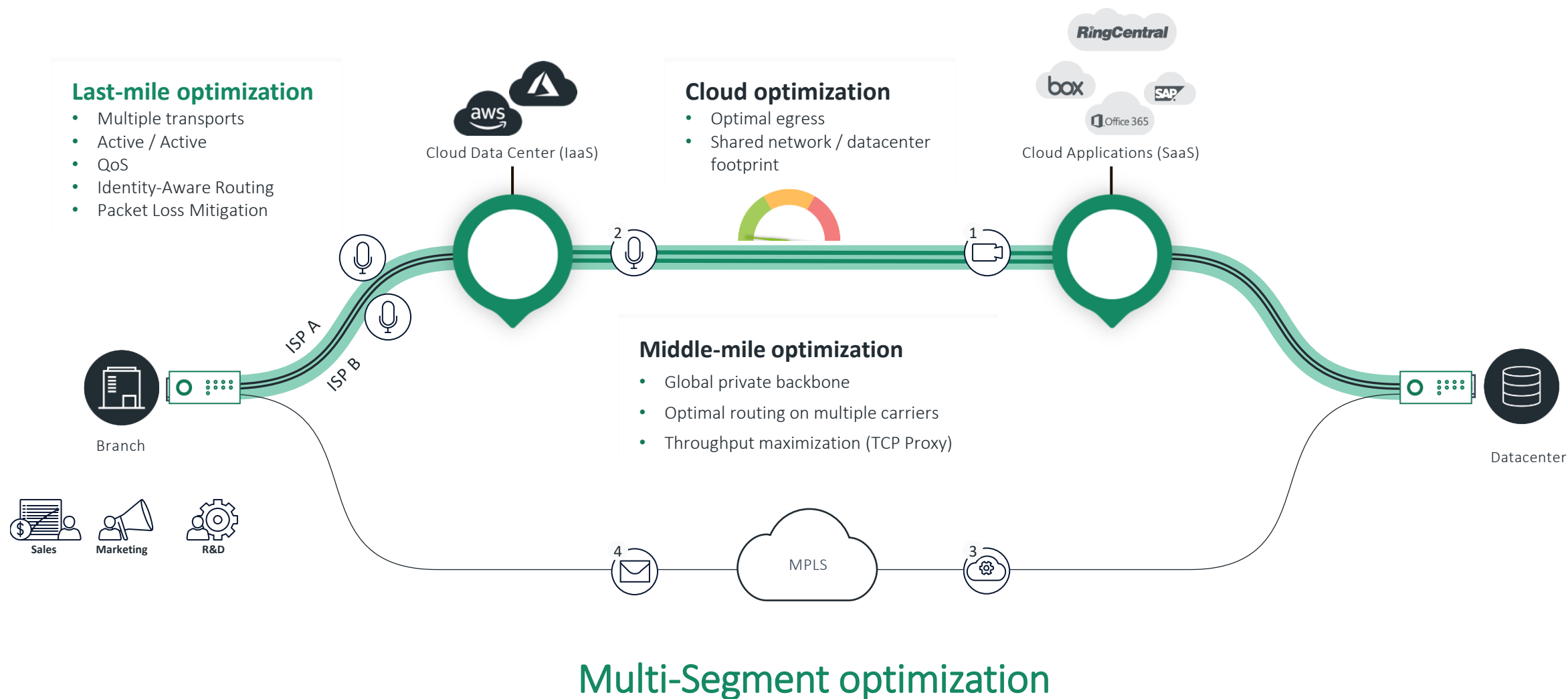
- International Bank Account Numbers [Germany]
- Bank account details [Germany]
- Credit card numbers [Universal]

# DLP Dashboard



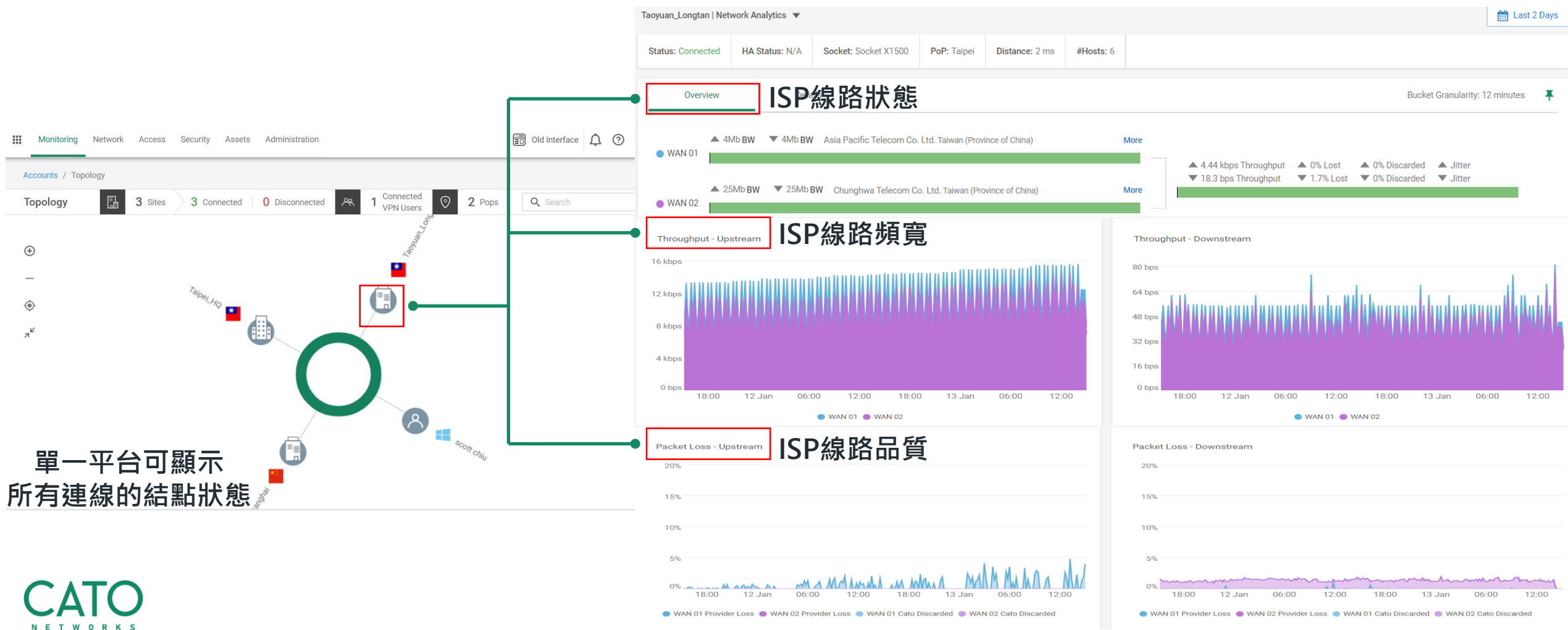
# Network Optimization

## Optimized WAN and Cloud Connectivity



# NoC網路流量分析機制-Network Analytics

➤藉由Cato SASE Cloud 功能介面上所提供的NoC網路流量分析機制，可讓網管人員統一旦快速得知集團內整體網路流量及相關應用分佈。



# NoC網路流量分析機制-Application Analytics

## Application Analytics

提供所有包含總部、各分點、VPN、  
內部User或IP的所有網路流量分析

Dec 01 15:42 - Jan 13 15:42



Custom

From

2022/01/12 上午 09:57



To

2022/01/14 上午 09:57



Recents

Last Hour

Last 2 Hours

Last Day

Last 2 Days

Longer

Last Week

Last 2 Weeks

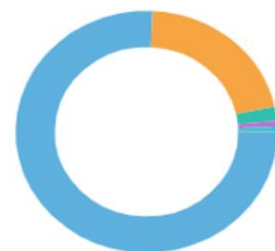
Last Month

OK

### Top Users

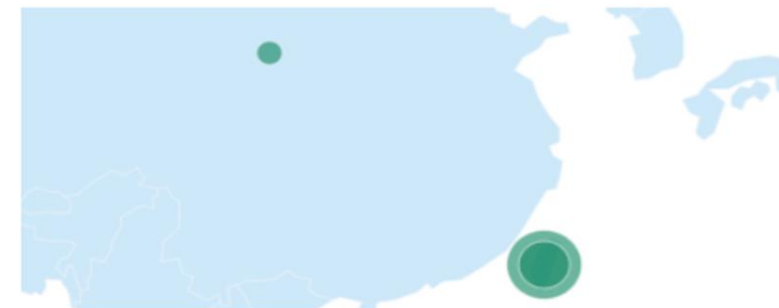
1	.104	368 GB
1	.4	19.7 GB
1	.2	9.1 GB
1	105.162	4.39 GB
1	1.3	2.44 GB

### Top Applications



UDP	306 GB	75.75%
SMBV3	84.6 GB	20.92%
Business apps	7.66 GB	1.89%
Windows Update	3.03 GB	0.75%
http_server	2.8 GB	0.69%

### Top Sites



Site	Country	Users	Flows	Download	Upload	Usage ↓
+ Taipei_HQ	TW	54	1.22 M	83 GB	114 GB	197 GB
+ Taoyuan_Longtan	TW	33	1.32 M	88.5 GB	82.1 GB	171 GB
+ China_Shanghai	CN	44	1.24 M	41.4 GB	1.77 GB	43.2 GB
+ Remote Users		7	450 k	696 MB	141 MB	837 MB

# SoC 日誌機制-Events Fields

Popular Fields		2021/12/29 15:47:35.035 何時		internalId: c96Goow1AF account id: 4620 src ip: 192.168.105.162 dest is site or vpn: Site device name: TEST001 pop name: Shanghai_DC3 src country: China event count: 1 ISP name: ChinaNet Shanghai Province Net... time: 19 days ago , 2021/12/29 event sub type: WAN Firewall src isp ip: 222.72.148.230 ip protocol: TCP rule id: 58565 src is site or vpn: Site os type: OS_WINDOWS dest ip: 192.168.0.141 event type: Security configured host name: Shanghai_PoC_PC dest port: 3200 subnet name: global_range application: SAP_DIAG action: Monitor rule name: Deafult Deny rule: Deafult Deny src site: China_Shanghai dest site: Taipei_HQ	
> Category	3				
> Destination IP	4				
> Sub-Type	4				
> Event Type	4				
> Source Site	4				
> SDP User Email	1				
Available Fields					
> Action	4				
Active Directory Name	0				
Application Activity	0				
> Application	4				
Application Class	0				
Application Risk	0				
Authentication Type	0				
BGP Cato ASN	0				
BGP Cato IP	0				
BGP Disconnect Error Code	0				
BGP Peer ASN	0				
BGP Peer Description	0				
BGP Peer IP	0				
BGP Router CIDR	0				
BGP Disconnect Sub-error Code	0				
> Category	3				
		internalId	c96Goow1AF		
		account id	4620		
		src ip	192.168.105.162 何人		
		dest is site or vpn	Site		
		device name	TEST001		
		pop name	Shanghai_DC3		
		src country	China 何地		
		event count	1		
		ISP name	ChinaNet Shanghai Province Network		
		time	19 days ago , 2021/12/29		
		event sub type	WAN Firewall		
		src isp ip	222.72.148.230		
		ip protocol	TCP		
		rule id	58565		
		src is site or vpn	Site		
		os type	OS_WINDOWS		
		dest ip	192.168.0.141 何物		
		event type	Security		
		configured host name	Shanghai_PoC_PC		
		dest port	3200		
		subnet name	global_range		
		application	SAP_DIAG 何事		
		action	Monitor		



打造自己的  
資訊安全監控中心



# Cloud Apps Security Risk Score-風險分析

➤ Cato給每個雲端應用分配一個風險分數，介於0（無風險）到10（非常高風險）之間，以協助客戶評估該應用是否符合企業的安全政策要求。Cato採用內部人工智能引擎來分析相關數據和指標並生成風險分數，包括：

- 一般性、合規性和安全性數據（顯示在雲端應用目錄中）。
- 基於最近有關該雲端應用提供或開發公司的新聞文章的情緒分析（機器學習技術）。
- 有關軟件漏洞和違規行為的訊息。
- 來自Cato研究實驗室內部威脅情報和領域相關訊息。

—



Zoom

Zoom is a software company that offers a communications platform that connects people through video, voice, chat, and content sharing.

Internet Conferencing, Voip Video

## General

Zoom is a software company that offers a communications platform that connects people through video, voice, chat, and content sharing. It has an easy, reliable cloud platform for video and audio conferencing, collaboration, chat, and webinars across mobile devices, desktops, telephones, and room systems. Zoom unifies cloud video conferencing, simple online meetings, and group messaging into one easy-to-use platform. The company's mission is to create a people-centric cloud service that transforms the real-time collaboration experience and improves the quality and effectiveness of communications. Zoom was founded in 2011 and is headquartered in San Jose, California, United States.



San Jose, California, United States



<http://zoom.us>



1001-5000



IPO



## Compliance



ISAE 3402



PCI-DSS



ISO 27001



SOX



HIPAA



SOC 1



SOC 2



SOC 3

## Security



MFA



Encryption At Rest



Audit Trail



RBAC



Remember Passwords



SSO



Trusted Certificates



HTTP Security Headers



TLS Enforcement



# Single Pass Cloud Engine (SPACE): Just-in-time Contextual Policy Enforcement

The building block of the Cato SASE backbone architecture

## Policy

- Bandwidth Management
- Quality of Service
- Risk-based Access Control
- Application Acceleration
- Threat Prevention
- Data Protection\*

## Context

- Account
- Device
- Authentication
- Identity
- Network
- Application
- Data

## Flows

- Branches
- Users
- Applications
- Clouds
- Systems
- IoT



## Access

- Zero Trust Network Access
- Single Sign-On
- Multi Factor Authentication
- Risk-Based Application Access

## Network

- Traffic shaping
- Global Route Optimization
- WAN & SaaS Acceleration
- Multi-Cloud Networking

## Security

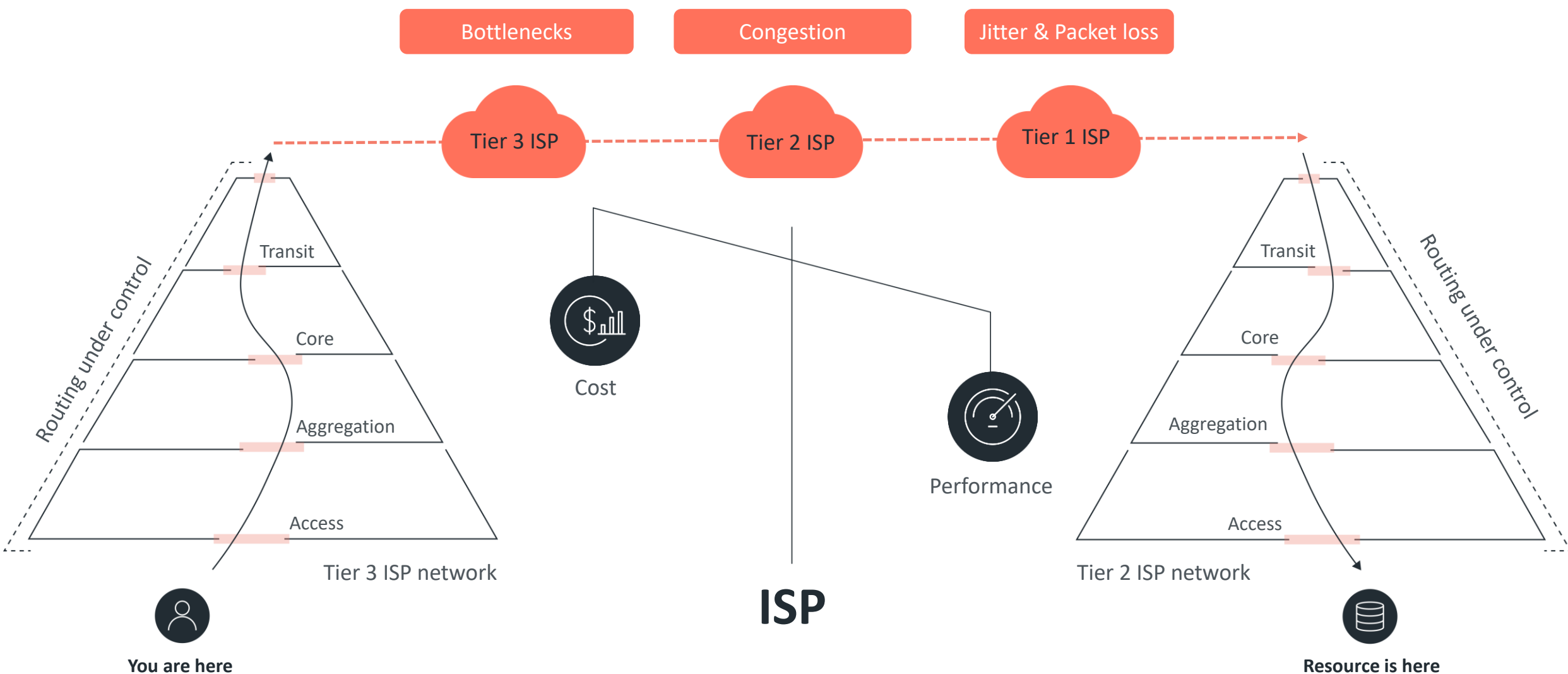
- Next Generation Firewall
- Secure Web Gateway
- Next Generation Anti Malware
- Intrusion Prevention System
- Cloud Access Security Broker\*
- Data Loss Prevention\*
- Remote Browser Isolation\*

## High Performance

- Up to 2 Gbps from a single edge
- W/ Full decryption
- W/ All security engines on

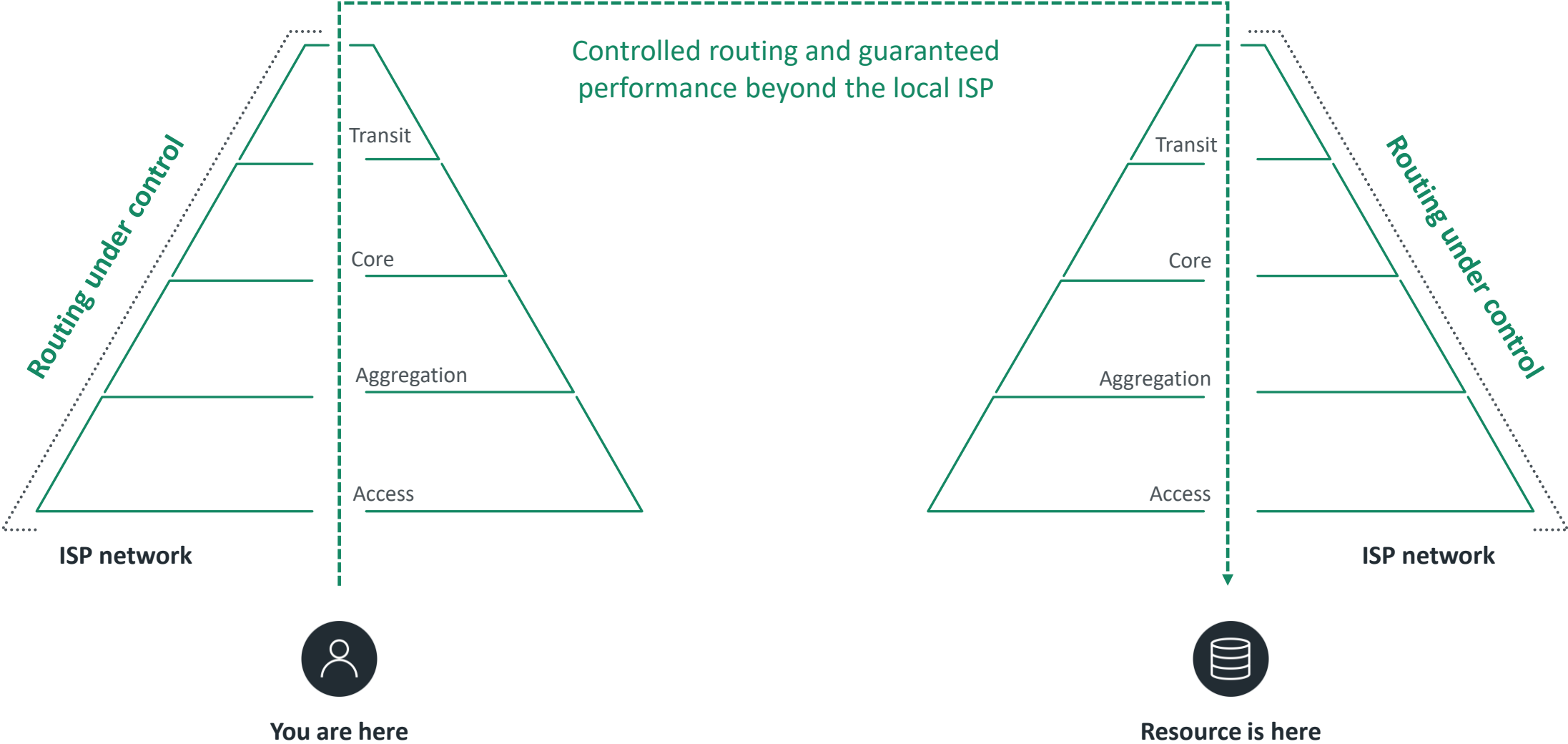
# The Problem

## Unpredictable Routing and Unreliable Performance



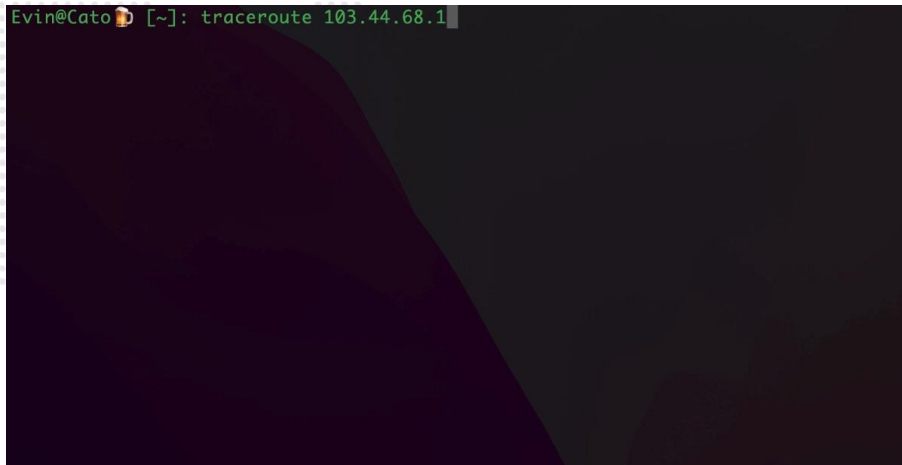
# The Solution

## Private Backbone

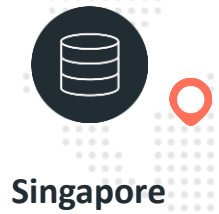


# Real world example: Public Internet (3x Playback)

Trace Route to 103.44.68.1



Without CATO



# Real world example: Public Internet

Trace Route to 103.44.68.1

With CATO

```
Last login: Tue Dec 14 13:46:58 on ttys000  
Evin@Cato 🍌 [~]: traceroute 103.44.68.1
```

Global Private Backbone



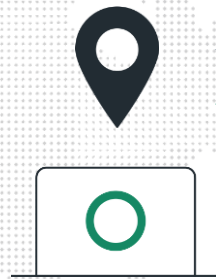
The Woodlands,  
Texas



Singapore

## Demo: Global File Transfer

SMB Transfer: 3.18GB



Primary Transport: CATO  
Interfaces: Automatic

✓ Active TCP  
Acceleration

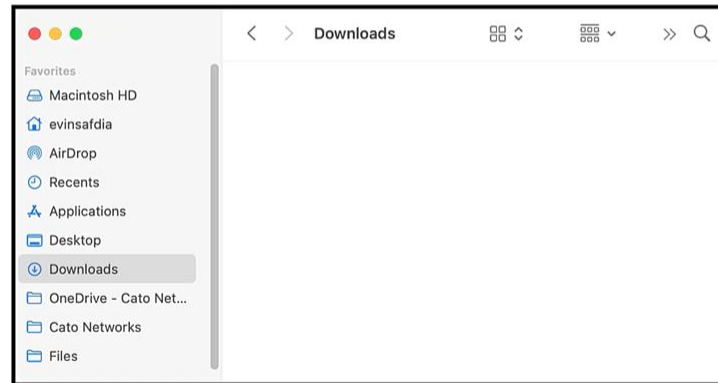
Secondary  
Transport: Automatic

# Demo: Global File Transfer

(90x Playback Speed)

CATO  
NETWORKS

 Public  
Internet



00:00.00



00:00.00



# Cato Networks 公司簡介

# Company Facts



**Shlomo Kramer, CEO**  
(Check Point, Imperva)



**Gur Shatz, President & COO**  
(Imperva, Incapsula)



**\$532M**

\$2.5B Valuation



**500+**

Employees



**70+**

PoPs



**1,100+**

Customers



**17,000+**

Branches and clouds



**300,000+**

Remote Users



**150+**
















Countries



**246%**

ROI & Payback <6 months according to **FORRESTER**

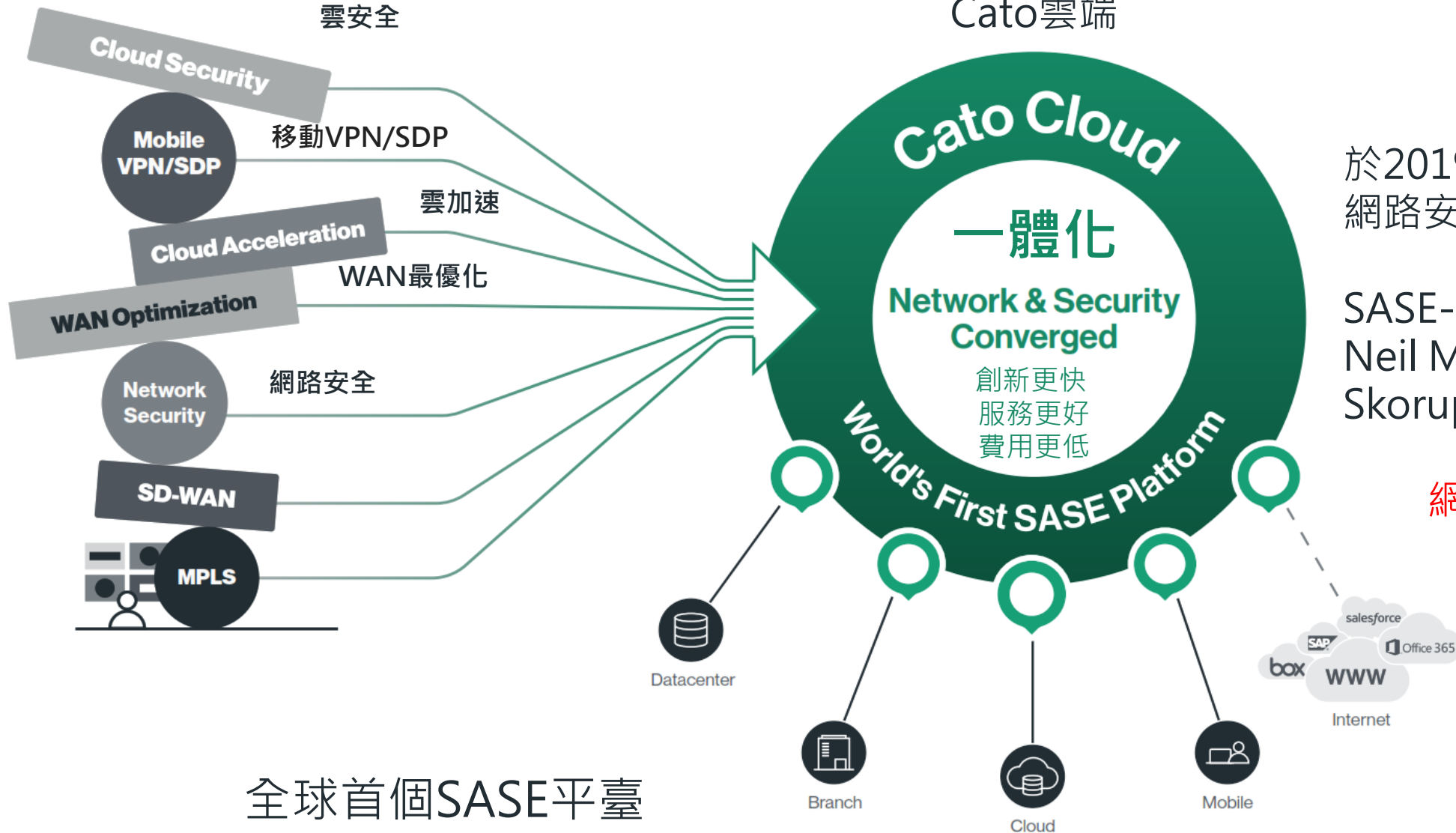
# Selected Customers by

Employees	Sites	Countries	Bandwidth	Remote Users
 <b>50,000</b> Communications	 <b>1,001</b> Retail	 <b>33</b> Chemicals	 <b>25 Gbps</b> Hospitality	 <b>21,000</b> Automotive
 <b>45,000</b> Transportation	 <b>547</b> Services	 <b>28</b> Manufacturing	 <b>20 Gbps</b> Manufacturing	 <b>5,400</b> Holding
 <b>43,000</b> Food & Beverage	 <b>254</b> Manufacturing	 <b>23</b> Manufacturing	 <b>18 Gbps</b> Construction	 <b>5,100</b> Manufacturing

# 全球首推SASE平台 -- Gartner SASE架構是未來的趨勢

雲安全

Cato雲端



於2019年8月30日發佈  
網路安全的未來在雲端

SASE-由Gartner的分析師  
Neil McDonald 和Joe  
Skorupa 所定義的新類別

網路即是安全！！

全球首個SASE平臺

**Secure Access Service Edge (SASE)**

**Cato is the convergence of networking and security in the cloud**



## 導入Cato Networks 客戶所帶來的效益

降低資安/網路設備的投資成本

降低跨國線路成本

簡化管理網路所耗的人力成本

增強網路  
資訊安全防護邊界

加速雲端應用程式存取效能

大幅降低  
人力成本



Cato SASE. Ready for Whatever's Next.

