Netskope Security Cloud Platform

✚ Secure connectivity that's ready for *anything*

Martin Nyman| Regional Sales Mgr Sweden

✚

Jan Lundberg | Solution Architect Sweden

Agenda:

- *Short Intro to Netskope Security Cloud Platform*
- *Demo*
  - *Netskope Private Access*
  - *Client Internet Access with CASB*

The Netskope Security Cloud Platform

Cloud-native security on a single platform for every user & every device - regardless of location
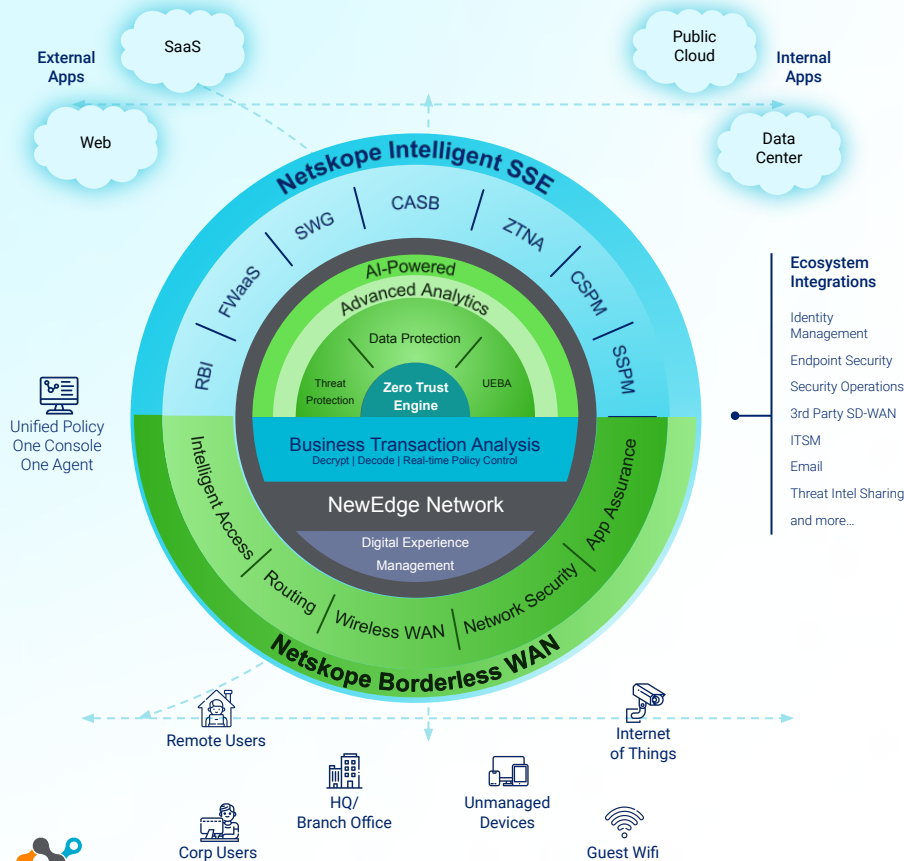

External Apps
SaaS
Web

Public Cloud
Internal Apps
Data Center

Netskope Intelligent SSE

CASB
SWG
ZTNA
FWaaS
CSPM
RBI
SSPM

AI-Powered Advanced Analytics

Data Protection

Threat Protection
Zero Trust Engine
UEBA

Business Transaction Analysis
Decrypt | Decode | Real-time Policy Control

NewEdge Network

Digital Experience Management

Intelligent Access
Routing
Wireless WAN
Network Security
App Assurance

Netskope Borderless WAN

Unified Policy
One Console
One Agent

Ecosystem Integrations

Identity Management

Endpoint Security

Security Operations

3rd Party SD-WAN

ITSM

Email

Threat Intel Sharing

and more...

Remote Users
HQ/ Branch Office
Unmanaged Devices
Corp Users
Guest Wifi
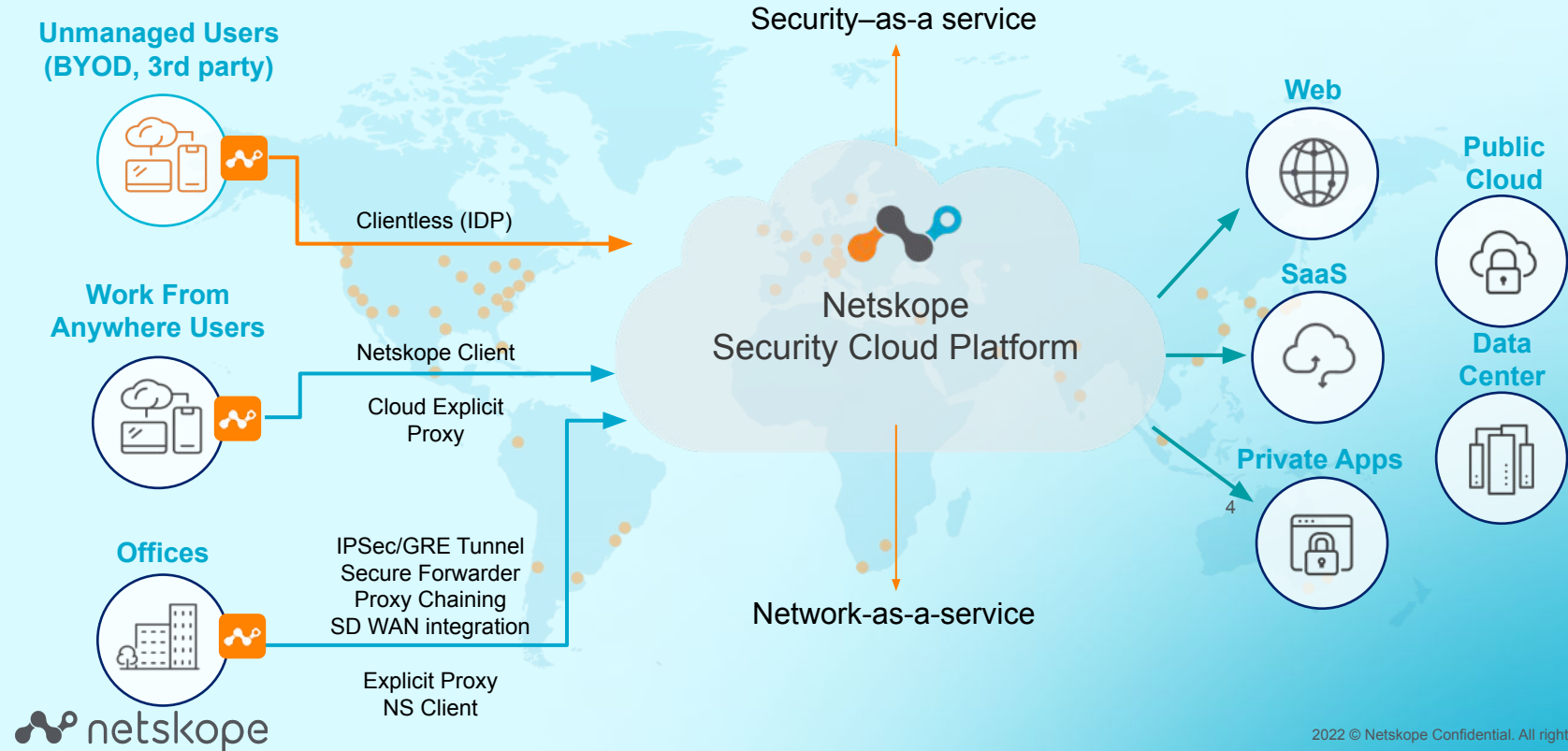Internet of Things

Figure 1: Magic Quadrant for Security Service Edge

Source: Gartner

Highest in Execution, Furthest in Vision.

Netskope recognized as a Leader in the 2023 Gartner® Magic QuadrantTM for SSE
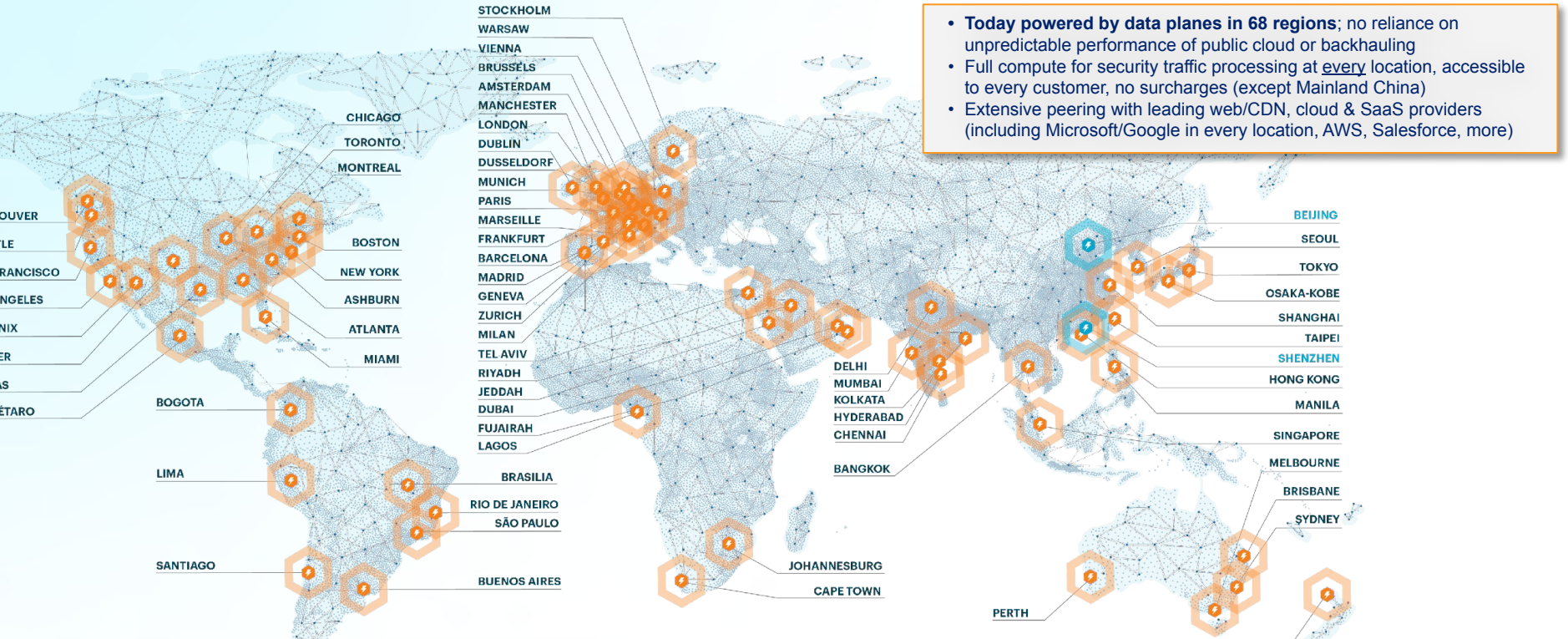
3

Secure Access to SaaS, IaaS, Web, and Private, Delivered through a SASE Architecture using the Netskope SSE Platform

Unmanaged Users (BYOD, 3rd party)

Clientless (IDP)

Work From Anywhere Users

Netskope Client

Cloud Explicit Proxy

Offices

IPSec/GRE Tunnel
Secure Forwarder
Proxy Chaining
SD WAN integration

Explicit Proxy
NS Client

Security–as-a service

Netskope
Security Cloud Platform

Network-as-a-service

Web

SaaS

Private Apps

Public Cloud

Data Center

netskope

World-class NewEdge global coverage today

More locations with full compute SSE services – *at the edge, closer to users* – than any other SASE vendor
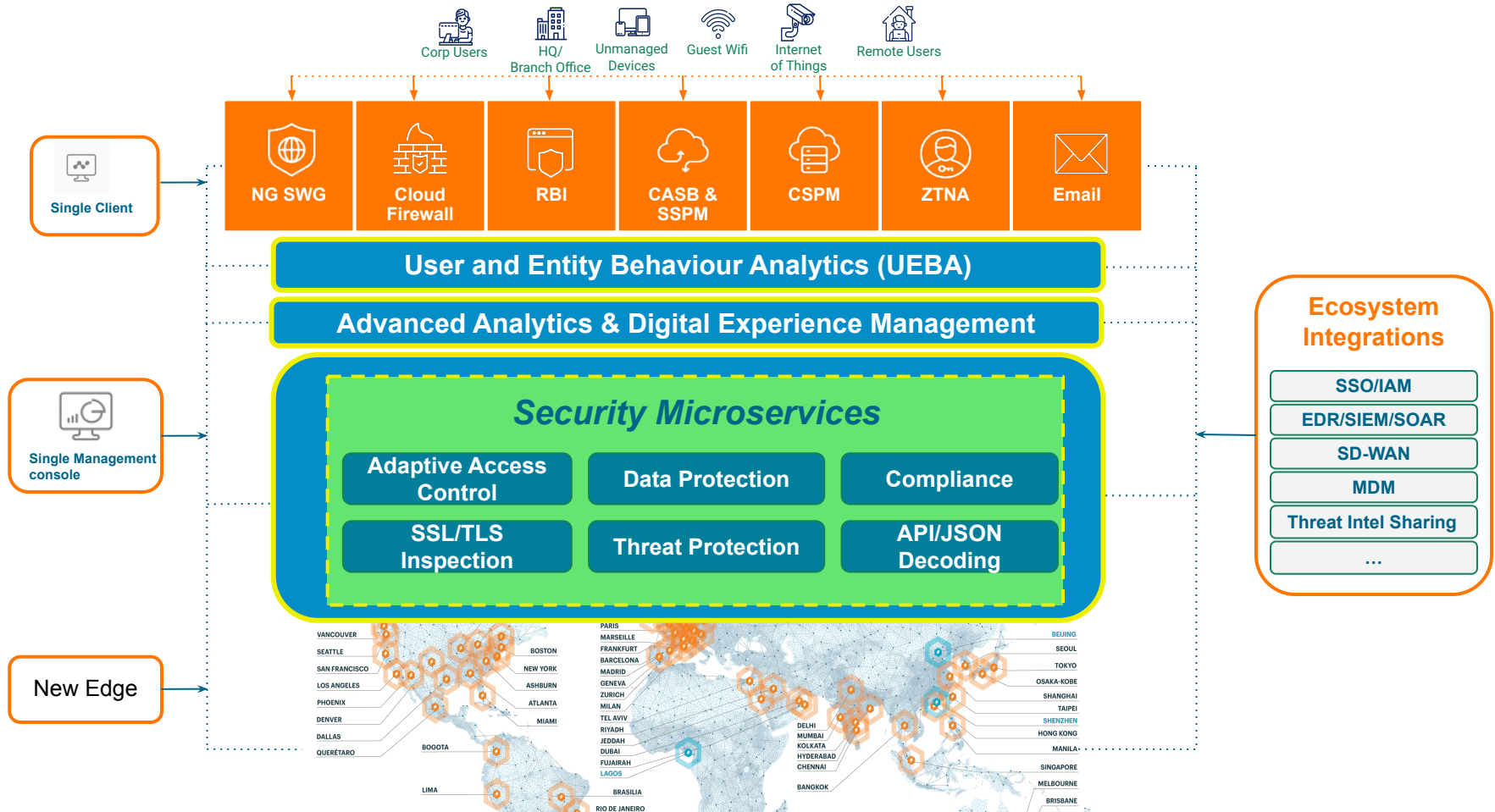
- **Today powered by data planes in 68 regions**; no reliance on unpredictable performance of public cloud or backhauling
- Full compute for security traffic processing at <u>every</u> location, accessible to every customer, no surcharges (except Mainland China)
- Extensive peering with leading web/CDN, cloud & SaaS providers (including Microsoft/Google in every location, AWS, Salesforce, more)

STOCKHOLM
WARSAW
VIENNA
BRUSSELS
AMSTERDAM
MANCHESTER
LONDON
DUBLIN
DUSSELDORF
MUNICH
PARIS
MARSEILLE
FRANKFURT
BARCELONA
MADRID
GENEVA
ZURICH
MILAN
TEL AVIV
RIYADH
JEDDAH
DUBAI
FUJAIRAH
LAGOS

CHICAGO
TORONTO
MONTREAL
VOUVER
LE
RANCISCO
BOSTON
NGELES
NEW YORK
ASHBURN
NIX
ATLANTA
ER
MIAMI
AS
ÉTARO
BOGOTA
LIMA
BRASILIA
RIO DE JANEIRO
SÃO PAULO
SANTIAGO
BUENOS AIRES

DELHI
MUMBAI
KOLKATA
HYDERABAD
CHENNAI
BANGKOK

JOHANNESBURG
CAPE TOWN

BEIJING
SEOUL
TOKYO
OSAKA-KOBE
SHANGHAI
TAIPEI
SHENZHEN
HONG KONG
MANILA
SINGAPORE
MELBOURNE
BRISBANE
SYDNEY
PERTH

- **MPs:** San Jose (x3), Amsterdam, Frankfurt, Melbourne, Zurich, Riyadh, London
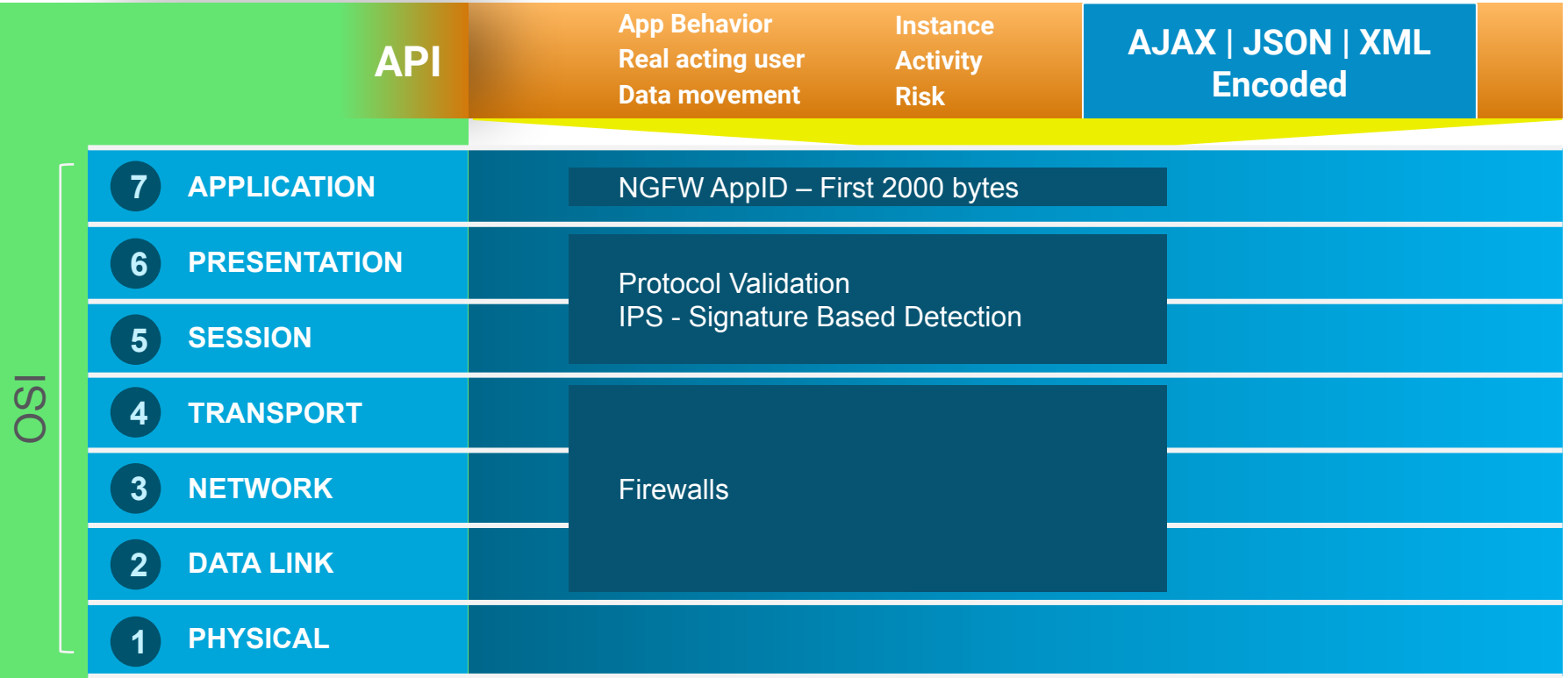- **For government:** US East/West FedRAMP, Melbourne IRAP

Data centers coming soon

- **Future MPs:** Dallas, Frankfurt, Singapore

5

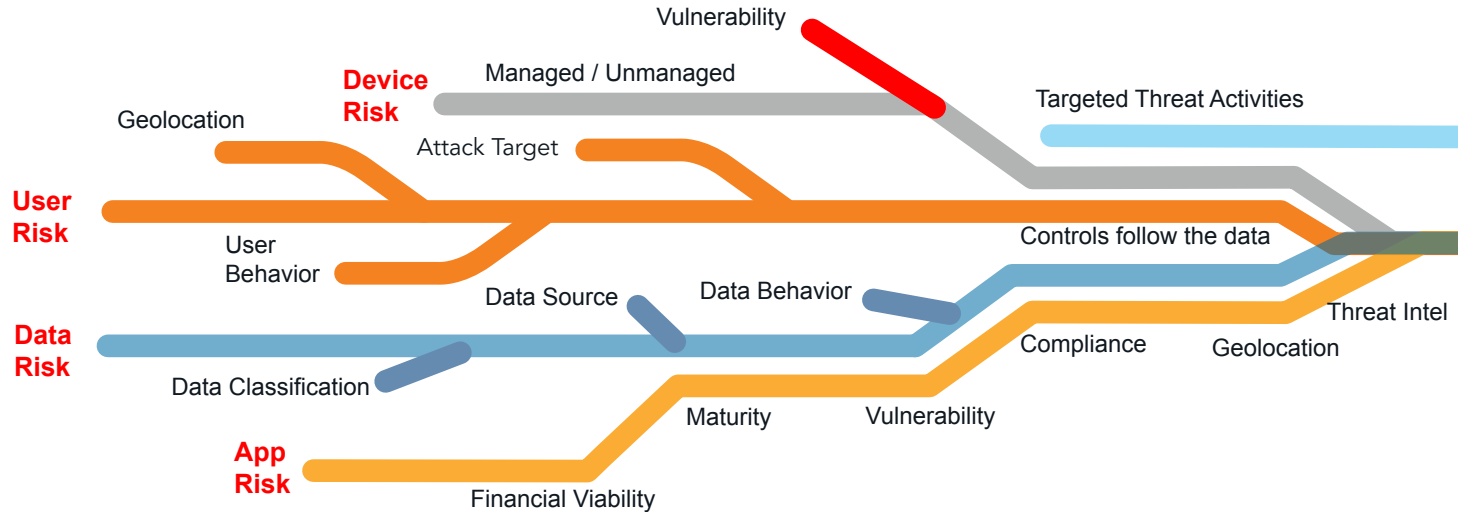# One platform. One goal. One MASSIVE Zero Trust Engine.

Corp Users | HQ/ Branch Office | Unmanaged Devices | Guest Wifi | Internet of Things | Remote Users

Single Client

| NG SWG | Cloud Firewall | RBI | CASB & SSPM | CSPM | ZTNA | Email |

User and Entity Behaviour Analytics (UEBA)

Advanced Analytics & Digital Experience Management

Single Management console

Security Microservices

| Adaptive Access Control | Data Protection | Compliance |
| SSL/TLS Inspection | Threat Protection | API/JSON Decoding |

Ecosystem Integrations

- SSO/IAM
- EDR/SIEM/SOAR
- SD-WAN
- MDM
- Threat Intel Sharing
- ...

New Edge

VANCOUVER, SEATTLE, SAN FRANCISCO, LOS ANGELES, PHOENIX, DENVER, DALLAS, QUERÉTARO, BOGOTA, LIMA, BRASILIA, RIO DE JANEIRO, BOSTON, NEW YORK, ASHBURN, ATLANTA, MIAMI

PARIS, MARSEILLE, FRANKFURT, BARCELONA, MADRID, GENEVA, ZURICH, MILAN, TEL AVIV, RIYADH, JEDDAH, DUBAI, FUJAIRAH, LAGOS, DELHI, MUMBAI, KOLKATA, HYDERABAD, CHENNAI, BANGKOK

BEIJING, SEOUL, TOKYO, OSAKA-KOBE, SHANGHAI, TAIPEI, SHENZHEN, HONG KONG, MANILA, SINGAPORE, MELBOURNE, BRISBANE

Netskope reads and understands the transmitted JSON instructions. We talk the cloud talk.

API	App Behavior Real acting user Data movement	Instance Activity Risk	AJAX | JSON | XML Encoded

OSI

7	APPLICATION	NGFW AppID – First 2000 bytes
6	PRESENTATION	Protocol Validation IPS - Signature Based Detection
5	SESSION	
4	TRANSPORT	Firewalls
3	NETWORK	
2	DATA LINK	
1	PHYSICAL	

Business Driven Zero Trust in Real Time

Identity	Device	SaaS App	App Instance	App Risk Rating	URL Category	Activity Controls	User Risk Rating	Threat	DLP	Policy Action
Pat Smith Accounting — Logged in as bob@ privatemail.com	Managed / Personal/BYOD	WeTransfer Drive — Sanctioned / UnSanctioned	Company / Personal	80 — High Risk rating — Breadth of 40K+ Apps	Cloud Storage — 130+ categories	Upload Share Create Post Login (Dozens)	User Behaviour & Anomaly Tracking (UEBA)	Threat Intel AV Sandbox IPS UEBA CTE	DLP Rules, ML, & OCR	Contextual: Allow Coach Block Encrypt Legal Hold Quarantine

Vulnerability
Managed / Unmanaged
Targeted Threat Activities

Device Risk
Geolocation
Attack Target

User Risk
User Behavior

Data Risk
Data Source
Data Behavior
Controls follow the data
Threat Intel

Data Classification
Compliance
Geolocation

App Risk
Maturity
Vulnerability

Financial Viability

Netskope provides CONTEXT-driven Conditional Controls

Real-time, Customizable User Coaching

netskope

RISK Violation!
You are attempting to Login Attempt at a HIGH RISK SaaS application WeTransfer that violates our company RISK policy. IF you believe this activity should be allowed, enter your justification below and click on Proceed.

Please provide your justification

Policy: TCO-[CASB]-Internet-RISK-SCORE--HIGH

This window will auto-close in **50 seconds**

STOP   Proceed

8

- *Demo*
  - *Netskope Private Access*
  - *Inline Internet Access with CASB*

NPA: Connect to an Application

Remote Users

Netskope Client

Private Apps in Public Cloud

Microsoft Azure

Google Cloud Platform

amazon web services™

Atlassian JIRA

Atlassian Confluence

Windows Server 2012

Netskope Security Cloud

Security Microservices

| Adaptive Access Control | Data Protection | Compliance |
| Third-Party Risk | Threat Protection | API/JSON Decoding |

NewEdge

Publisher

Private Apps in Corporate Data Center

SAP

ORACLE DATABASE

Offices

Legend: Netskope Client | Netskope Publisher

Guacamole Server

netskope

ZTNA with Netskope Private Access

Netskope provides CONTEXT-driven Conditional Controls

Netskope Private Access

Unmanaged Users (BYOD, 3rd party)

Clientless (IDP)

Work From Anywhere Users

Netskope Client

Cloud Explicit Proxy

Offices

IPSec/GRE Tunnel
Secure Forwarder
Proxy Chaining
SD WAN integration

Explicit Proxy
NS Client

Security–as-a service

Netskope
Security Cloud Platform

Network-as-a-service

Web

SaaS

Private Apps

12

Google Drive

SaaS

Instance: Netskope

Instance: Company 2

Instance: Company 3

Instance: Company 4

netskope

Zero Trust aligned with Your Business Needs

Netskope provides CONTEXT-driven Conditional Controls

Zero Trust aligned with Your Business Needs

⠿	3.1	**Allow for sanctioned google instances**	Any	⊞ Google Drive:GDriveNetskope, Google Gmail:Netskope ⌁ Post, Send, Upload	☁ POPITOPP	🔔 Alert
⠿	3.2	**Block for unsanctioned google instances**	Any	⊞ Google Drive, Google Gmail ⌁ Post, Send, Upload	☁ POPITOPP	⊘ Block Upload Activity Denied
⠿	3.3	**UNSANCTIONED CLOUD STORAGE WITH LOW or MEDIUM RISK SCORE**	Any	▤ Cloud Storage ⌁ Download, Upload, Login Attempt ☁ Low, Medium	None	👤 User Alert Activity To Poor Applicat...
⠿	3.4	**Blocked activity to HIGH Risk Cloud storage**	Any	▤ Cloud Storage ⌁ Download, Upload, L Attempt ☁ Unknown, Poor		

Netskope Policies navigation:
- ← Policies
- SSL Decryption
- Endpoint Protection
- **Real-time Protection**
- API Data Protection
- Security Posture
- Behavior Analytics

PROFILES
- DLP
- DNS
- Threat Protection
- Web
- App Instance
- HTTP Header

- Settings
- Help
- Account

RISK Violation!

You are attempting to Login Attempt at a HIGH RISK SaaS application WeTransfer that violates our company RISK policy. IF you believe this activity should be allowed, enter your justification below and click on Proceed.

Please provide your justification

Policy: TCO-[CASB]-Internet-RISK-SCORE--HIGH

This window will auto-close in **50 seconds**

STOP   Proceed

Netskope provides CONTEXT-driven Conditional Controls

Application instance, log example SLACK:

APPLICATION

Application: Slack
Instance Name: Netskope ✏
Instance Tags: Untagged
Instance ID: netskope
App Category: Collaboration
URL: netskope.slack.com/api/chat.postMessage
CCI: 82 ⬀
CCL: high
Activity: Post
Website: Slack
Object Type: Message
AppSession ID: 7481586213762061037
Domain: netskope.slack.com
Page: netskope.slack.com
Category: Collaboration
Other Category: Technology, Collaboration

APPLICATION

Application: Slack
Instance Name: DemoTenantSlack ✏
Instance Tags: Untagged
Instance ID: demo-tenant-slack
App Category: Collaboration
URL: demo-tenant-slack.slack.com/api/chat.postMessage
CCI: 82 ⬀
CCL: high
Activity: Post
Website: Slack
Object Type: Message
AppSession ID: 7481586213762061037
Domain: demo-tenant-slack.slack.com
Page: demo-tenant-slack.slack.com
Category: Collaboration
Other Category: Technology, Collaboration

APPLICATION

Application: Slack
Instance Name: TRBS ✏
Instance Tags: Untagged
Instance ID: trbs-se
App Category: Collaboration
URL: trbs-se.slack.com/api/chat.postMessage
CCI: 82 ⬀
CCL: high
Activity: Post
Website: Slack
Object Type: Message
AppSession ID: 7481586213762061037
Domain: trbs-se.slack.com
Page: trbs-se.slack.com
Category: Collaboration
Other Category: Technology, Collaboration

Netskope provides CONTEXT-driven Conditional Controls

10 Critical Use Cases Covered by Netskope

✦ All within ONE Centralised Platform & Management Console

1

Protect Against Advanced Threats
Stop threats *before* they get to the endpoint

‣ Sandboxing & Browser Isolation
‣ Cloud IPS
‣ Insider Threats
‣ Phishing & Ransomware
‣ Risk Score & Intel Sharing

2
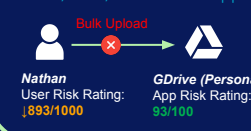
Control Sensitive Data Propagation
Understand the *context* of user actions in relation to your data

Download
Share
Send

3

Visibility & Control Over Shadow IT
Control *usage & risk* across SaaS, IaaS, and Private Apps

Bulk Upload
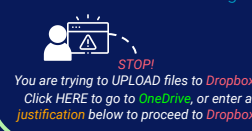
Nathan
User Risk Rating:
↓893/1000

GDrive (Personal)
App Risk Rating:
93/100

4

Control Access & Coach Users
Provide *risk-based* Conditional Access with user warnings
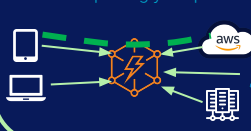
STOP!
You are trying to UPLOAD files to Dropbox.
Click HERE to go to OneDrive, or enter a
justification below to proceed to Dropbox.
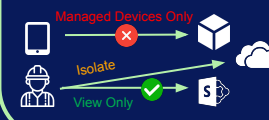
5

Zero Trust Network Access (ZTNA)
Provide access to *internal apps* without exposing your perimeter

6

Provide Secure Access to BYOD & 3rd Parties
Real-time security & access controls in a *clientless* manner

Managed Devices Only
Isolate
View Only

7

Secure Internet Breakouts, & WAN Orchestration
Orchestrate your WAN; secure your internet breakouts

8

Track SaaS & IaaS Standards Compliance
Continuous *assessment* of your IaaS environments & SaaS apps

ISO 27001
PCI DSS
NIST

9

Digital Experience Management (DEM)
End-to-end *performance monitoring* to ID & triage issues

Poor Performance!
Why?
Where is the issue?

10

Integrate with & Facilitate Intel Sharing b/w Vendors
Ensure your *vendor ecosystem* works together

mimecast · Microsoft · aws
Jira
now · W
vmware · aruba · okta
RAPID7 · CROWDSTRIKE

netskope

Thank You!

SASE Summit Sweden

Special Guest speaker from the FBI

+

May 16, 2023
Stockholm

netskope **Orange Cyberdefense**

Propose calls to action:

1. **Review** independent reports from Analysts such as Gartner and IDC

2. **Schedule** time with your OCD team to discuss your SASE Journey

3. **Plan** a follow-up session with Netskope for a demo and deep-dive in the solution

4. **Sign up** for the SASE FBI DAY May 16