netskope

NETSKOPE – Performance & Security Unified

Mid Atlantic CIO Forum

- Demystifying Zero Trust, SSE and SASE
- What is Continuous Adaptive Trust?
- Why the network matters
- Why SaaS control matters

What Trends Drive this Market

HYBRID WORK

The hybrid workforce requires a faster, easier, more reliable user experience

62% of global employees are working Hybrid[1]

18% are fully remote[1]

CLOUD SHIFT

Cloud is disrupting apps, workloads and network & security architectures

96% of companies use at least one public cloud[2]

70% of total software used by companies was SaaS in 2023[3]

CYBER CRIMINALS TAKING ADVANTAGE

Data sprawl across clouds & devices increases breach and compliance risk. Generative AI complex landscape.
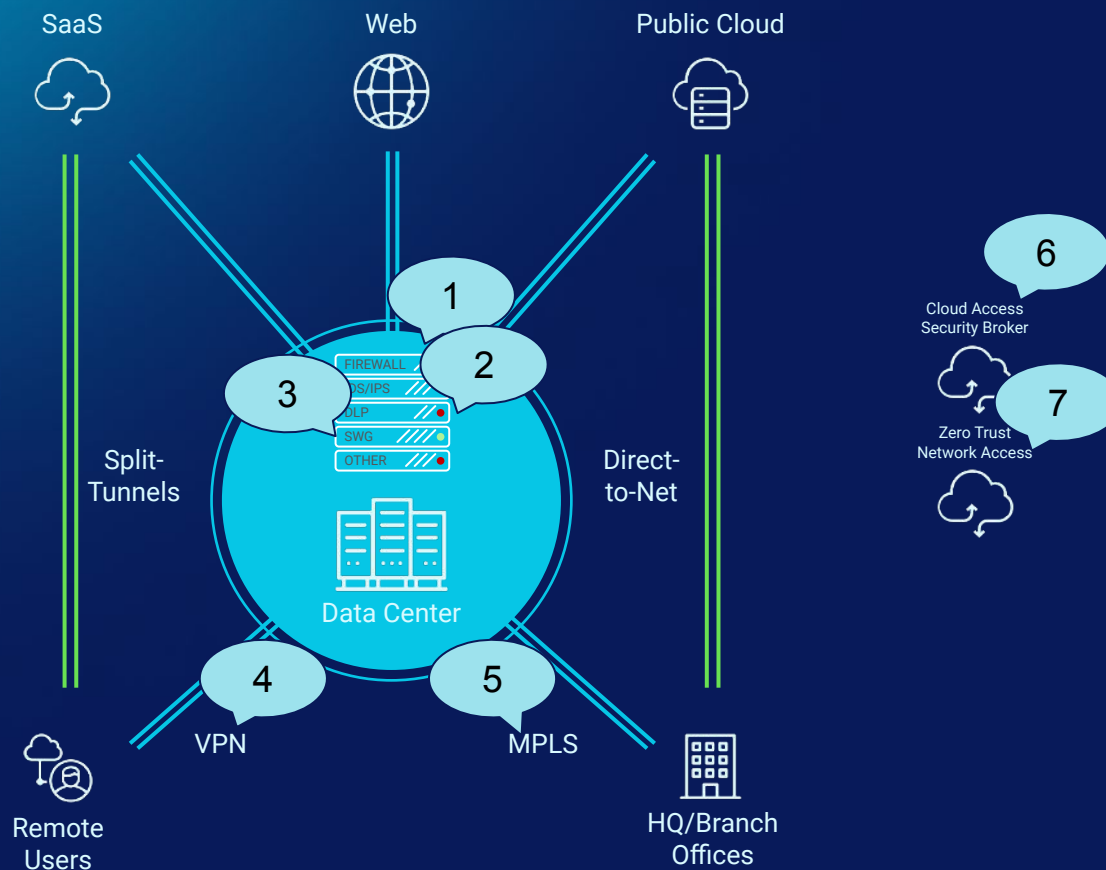
15x increase in cloud account-related attacks from 2022-2023[4]

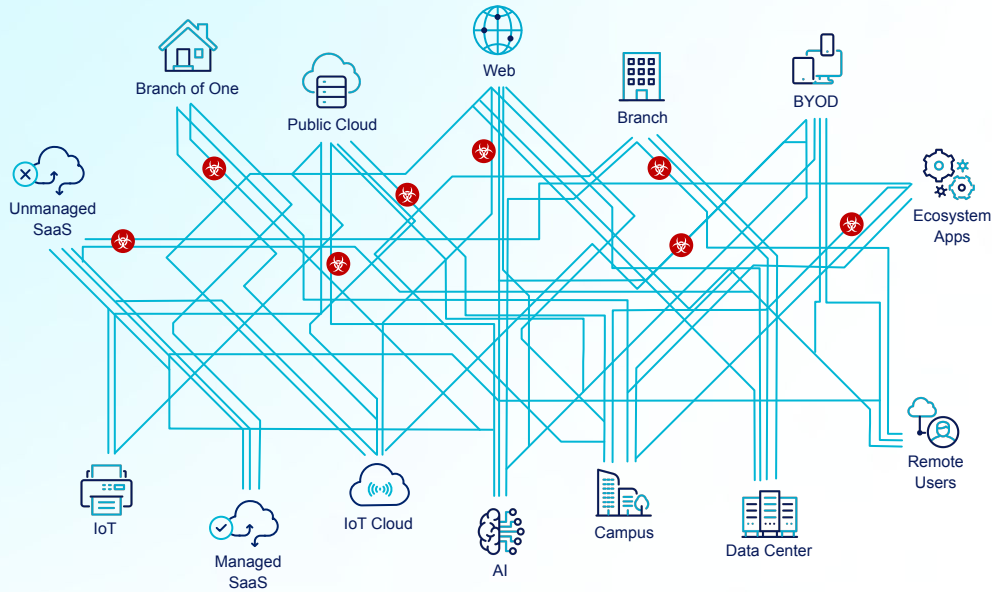78% of companies reported data exfiltration despite having data protection solutions in place[5]

1 - Owl Labs
2 - Spacelift
3 - McKinsey
4 - Red Canary
5 - HelpNet Security

Our New Reality Broke the Paradigm

SaaS

Web

Public Cloud

1. Complex
2. Costly
3. Ineffective
4. Less Secure

Split-Tunnels

Direct-to-Net

1

2

3

FIREWALL
IDS/IPS
DLP
SWG
OTHER

Data Center

4

5

VPN

MPLS

6

Cloud Access
Security Broker

7

Zero Trust
Network Access

Remote
Users

HQ/Branch
Offices

netskope

Evolution in Enterprise Internet Traffic

- **60%+** of traffic is SaaS and cloud delivering 50% of threats

- **2,400+** SaaS apps for average enterprise — most Shadow IT

- **95%** of traffic is **encrypted** where threats and data hide

Today's internet requires a different approach.
One that is cloud native and speaks the language of the modern internet.

netskope

Address Modern Security Gaps

IT LED
5% Apps managed by IT

BUSINESS LED
95% Apps unmanaged

USER LED
Choice of 40,000+ apps

WEB
1.5 Billion websites

2,400+
SaaS apps per enterprise

95%
Shadow IT

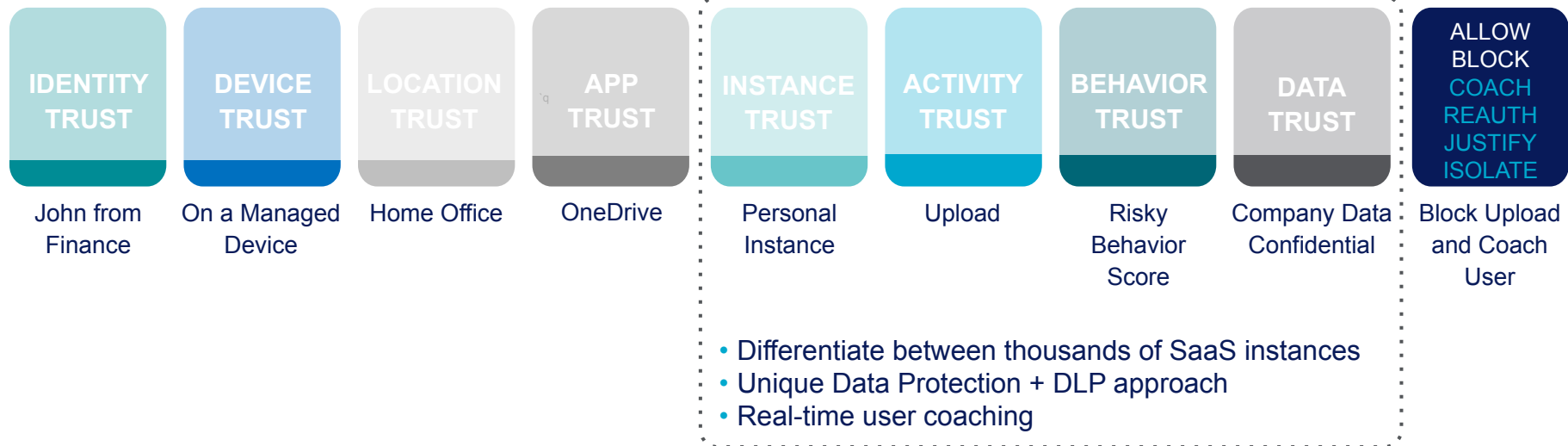Data Breach Risk & Cloud Delivered Malware

CASB APIs (Reactive)   ←——— GAP ———→   NGFW and SWG (Limited)

Next-Gen SWG + Zero Trust Engine

netskope

Netskope Zero Trust Engine

Make continuous, adaptive trust-based policy decisions in real-time

IDENTITY TRUST	DEVICE TRUST	LOCATION TRUST	APP TRUST	INSTANCE TRUST	ACTIVITY TRUST	BEHAVIOR TRUST	DATA TRUST	ALLOW BLOCK COACH REAUTH JUSTIFY ISOLATE
John from Finance	On a Managed Device	Home Office	OneDrive	Personal Instance	Upload	Risky Behavior Score	Company Data Confidential	Block Upload and Coach User

- Differentiate between thousands of SaaS instances
- Unique Data Protection + DLP approach
- Real-time user coaching

60% of traffic is SaaS and cloud, delivering 50% of threats

95% of traffic is encrypted—where threats and data hide

netskope

Netskope NewEdge Network

World-class coverage to deliver security without performance trade-offs
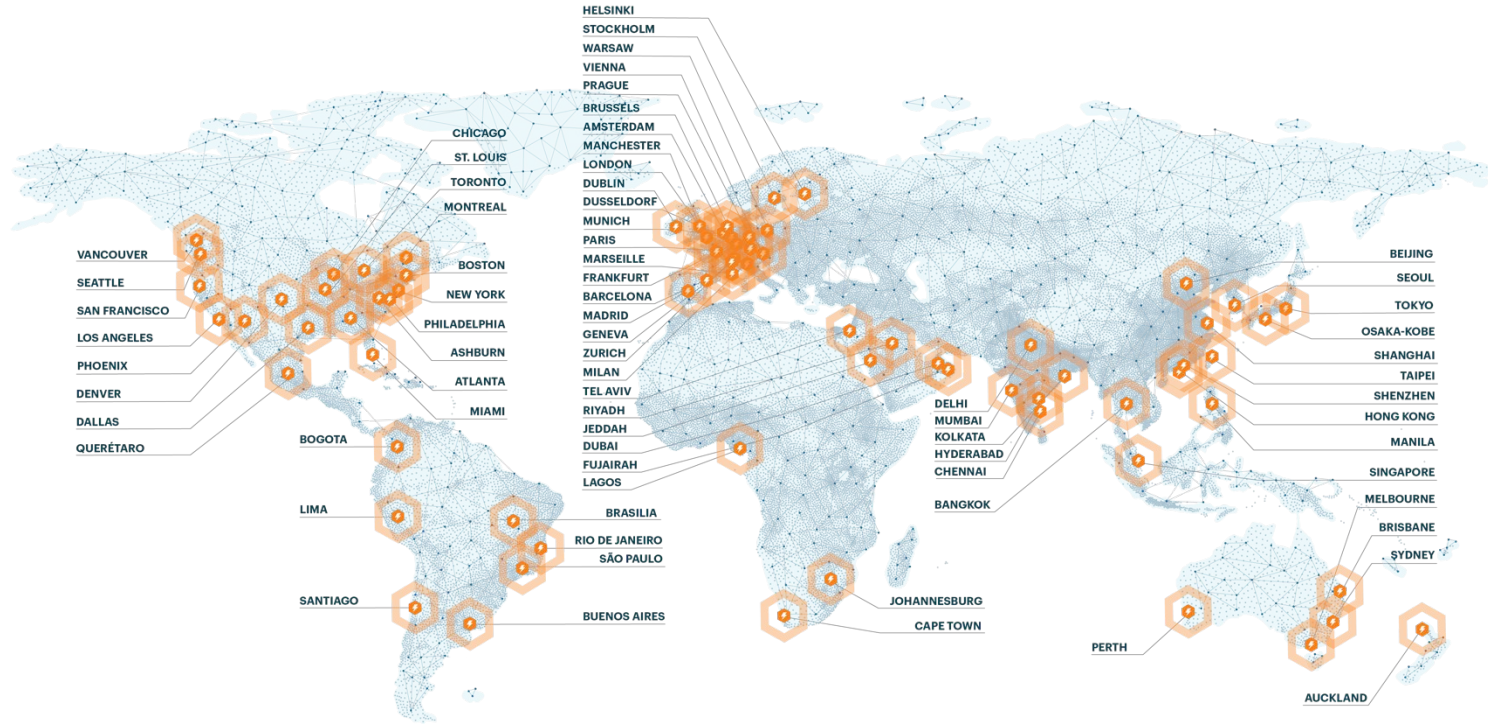
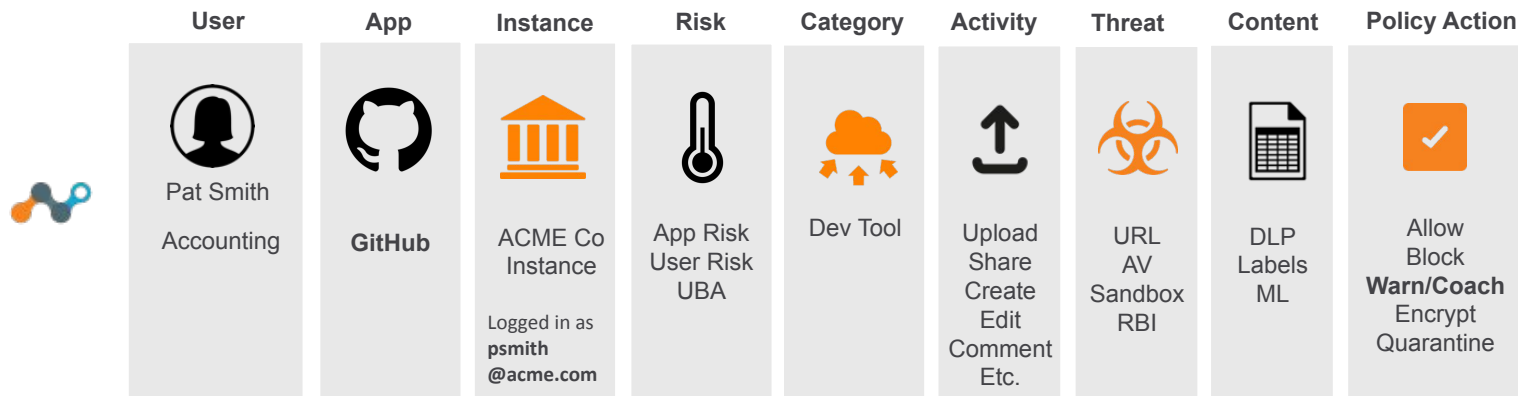**70+** Regions

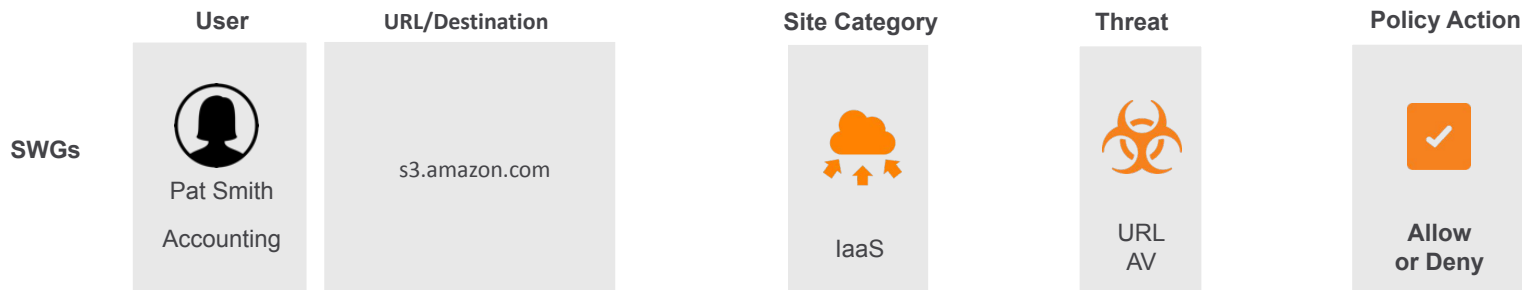**200+** Localization Zones

3K+ Network Adjacencies

FULL Compute

Industry's Best **SLAs**

Zero Trust SaaS Access

SWGs

User	URL/Destination		Site Category	Threat	Policy Action
Pat Smith Accounting	s3.amazon.com		IaaS	URL AV	**Allow or Deny**

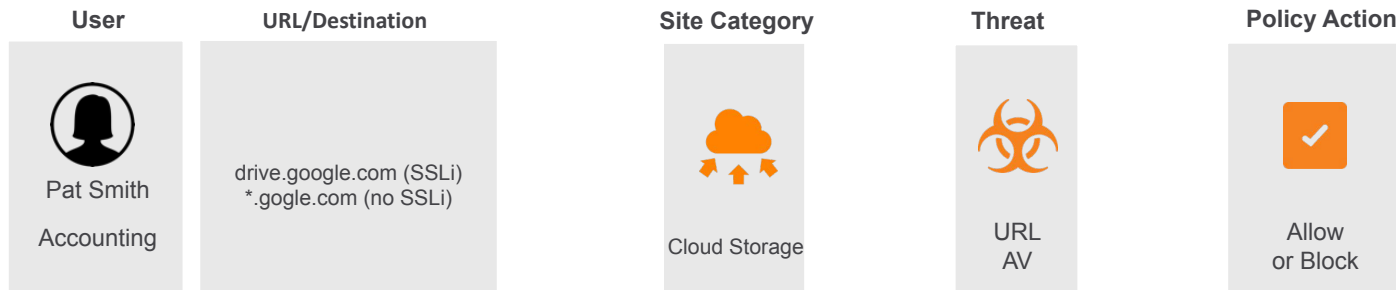| User	App	Instance	Risk	Category	Activity	Threat	Content	Policy Action
Pat Smith Accounting	**GitHub**	ACME Co Instance — Logged in as **psmith @acme.com**	App Risk User Risk UBA	Dev Tool	Upload Share Create Edit Comment Etc.	URL AV Sandbox RBI	DLP Labels ML	Allow Block **Warn/Coach** Encrypt Quarantine

netskope

8

Zero Trust SaaS Access

	User	URL/Destination		Site Category	Threat	Policy Action
SWGs	Pat Smith Accounting	drive.google.com (SSLi) *.gogle.com (no SSLi)		Cloud Storage	URL AV	Allow or Block

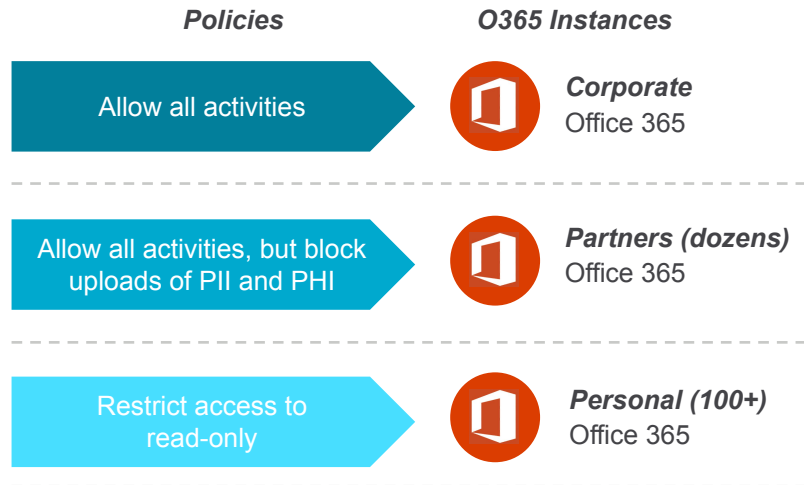|	User	App	Instance	Risk	Category	Activity	Threat	Content	Policy Action
	Pat Smith Accounting	Google Drive	Consumer bob@gmail.com	App Risk User Risk UBA	Cloud Storage	Upload Share Create Edit Chat Etc.	URL AV Sandbox RBI	DLP Labels ML	Allow Block **Warn/Coach** Encrypt Quarantine

netskope
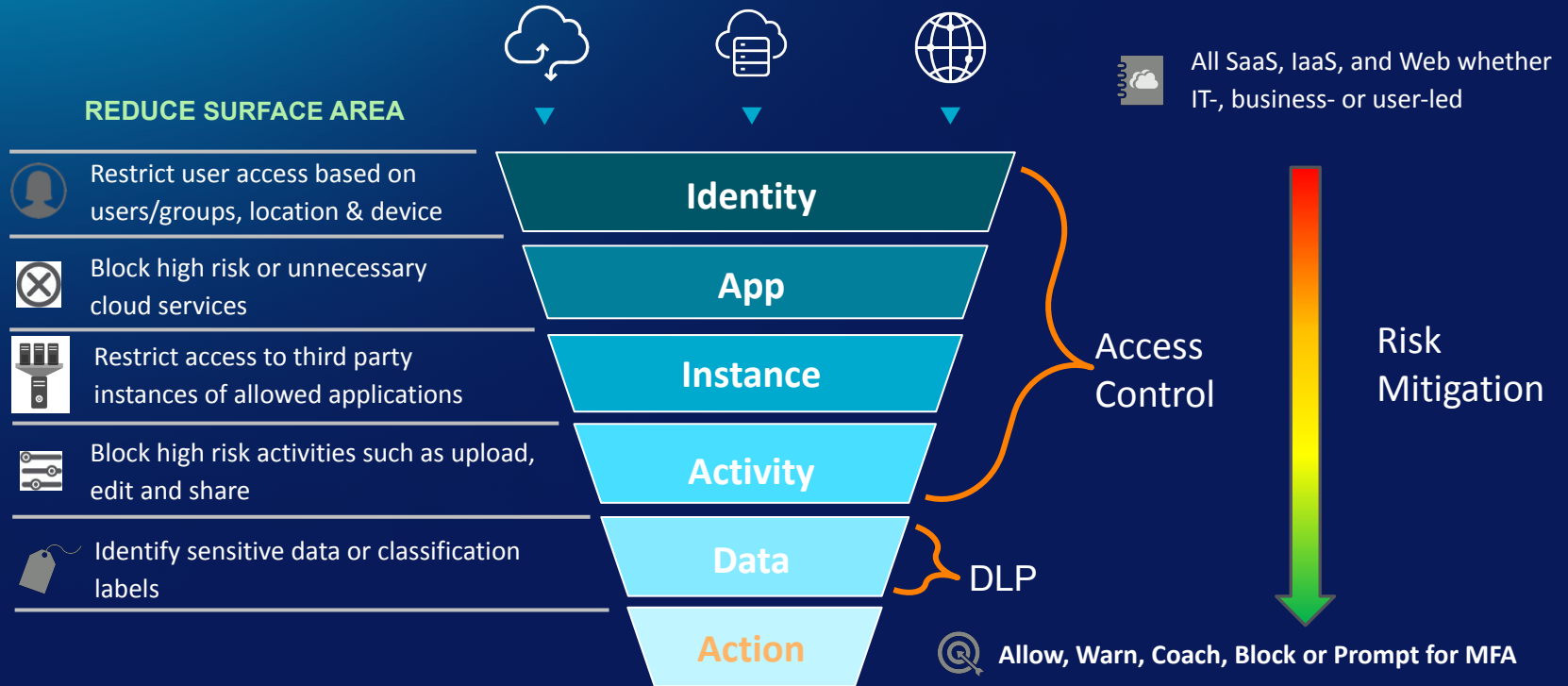
Example of Why Context Matters

Challenge

- Hundreds of unmanaged Office 365 instances in use
- Relying on tenant restrictions to block unmanaged O365 instances is too disruptive
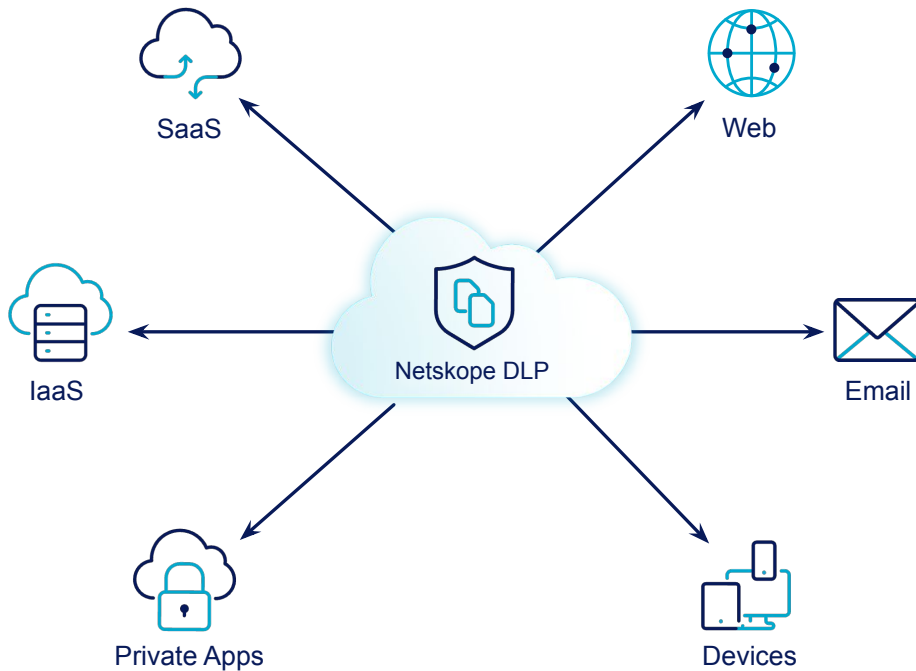
Solution

- Granular visibility and control of app instances
- Instead of blocking non-corporate instances, safely enable them by restricting activities and data movement

Policies   **O365 Instances**

Allow all activities → *Corporate* Office 365

Allow all activities, but block uploads of PII and PHI → *Partners (dozens)* Office 365

Restrict access to read-only → *Personal (100+)* Office 365

netskope

Data Protection Starts with Access Control

REDUCE SURFACE AREA

All SaaS, IaaS, and Web whether IT-, business- or user-led

Restrict user access based on users/groups, location & device

Block high risk or unnecessary cloud services

Restrict access to third party instances of allowed applications

Block high risk activities such as upload, edit and share

Identify sensitive data or classification labels

| Identity |
| App |
| Instance |
| Activity |
| Data |
| Action |

Access Control

Risk Mitigation

DLP

Allow, Warn, Coach, Block or Prompt for MFA

netskope

Data Protection + DLP

DATA PROTECTION

- Prevent risky data movement using Zero Trust context — no DLP required

ADVANCED DETECTION

- Leverage DLP for advanced detection using exact match, fingerprinting, AI/ML

PRECISE DETECTION

- Accurate and reliable via a broad set of advanced classification technologies

UNIFIED MODEL

- Cloud-delivered, centralized policy management, and always-on protections

netskope

Six High-Impact Use Cases

Discover and Protect Sensitive Information

PII
PCI
HIPA
GDPR
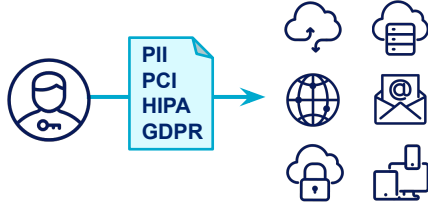
Govern Public Cloud

- Account visibility
- Redirect new account signup
- Govern specific services

Complete SaaS Visibility and Control

- SaaS app risk
- Instance awareness
- Control risky activities
- Shadow IT
- Personal apps

Real-time User Coaching

- Create good digital citizens
- Context-driven coaching
- Gently warn vs. block
- Redirect to suggested app
- Require justification

Safely Enable Generative AI

- Show acceptable use policy
- Protect sensitive data
- Enable innovation

Stop Threats and Ransomware

- Ransomware
- Phishing
- Malicious websites
- Risky SaaS apps
- Insider threats

netskope

Netskope Enables Seamless Integrations

Open platforms eliminate point solutions and allow for vendor consolidation and automation
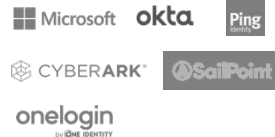

Cloud Providers
Cloud Onramp

SaaS
100's of Integrations and Partnerships

SIEM & SOAR
Incidents, Logs, and Threat

Azure Sentinel

Identity Management
MFA User Access

Netskope Cloud Exchange

EMAIL SECURITY
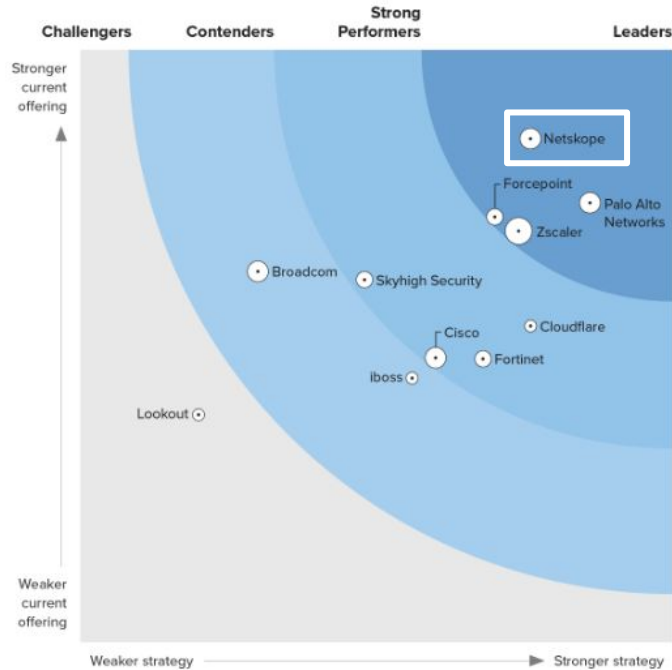Threats, IoCs, Data

Endpoint Management
App Updates

Endpoint Security / XDR
Device Posture and Threat
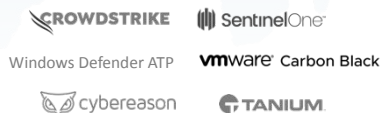
Branch Router / SD-WAN
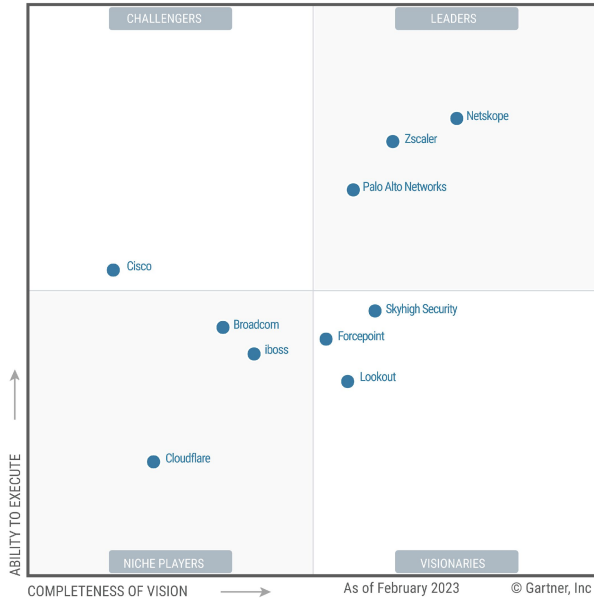Network Routing

Forrester Wave Security Service Edge Solutions, Q1 2024

Netskope has <u>the Strongest Current Offering</u> of <u>any</u> SSE player in the space.

"Netskope should be <u>at the top of this list</u> for enterprise clients looking to secure the remote workforce and provide comprehensive data protection."

Figure 1: Magic Quadrant for Security Service Edge

Source: Gartner

Netskope named the **Leader** in the 2023 Gartner MQ for Security Service Edge

- Netskope ranks *highest* versus any other leader in 2023 Gartner Critical Capabilities for SSE across *all* use cases

- Netskope has been named a *Leader* by Gartner *seven years* in a row