netskope

PREPARING FOR THE RISE IN SUPPLY CHAIN RISK

Brian Zerafa, Regional Director, Netskope
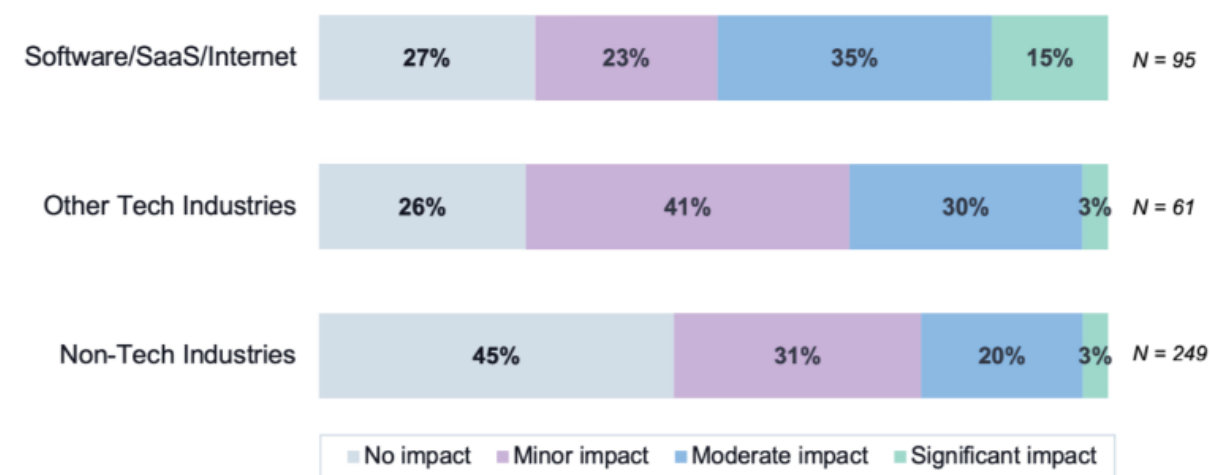
2022

Supply Chain Attacks by Industry Type
% of respondents

Industry	No impact	Minor impact	Moderate impact	Significant impact	N
Software/SaaS/Internet	27%	23%	35%	15%	N = 95
Other Tech Industries	26%	41%	30%	3%	N = 61
Non-Tech Industries	45%	31%	20%	3%	N = 249

■ No impact ■ Minor impact ■ Moderate impact ■ Significant impact

Anchore 2022 Software Supply Chain Security Report

Focus on Securing Software Supply Chain
% of respondents

- Not a priority: 3%
- Just starting to pay attention: 14%
- Top area of focus: 8%
- Significant area of focus: 46%
- Somewhat of an area of focus: 29%
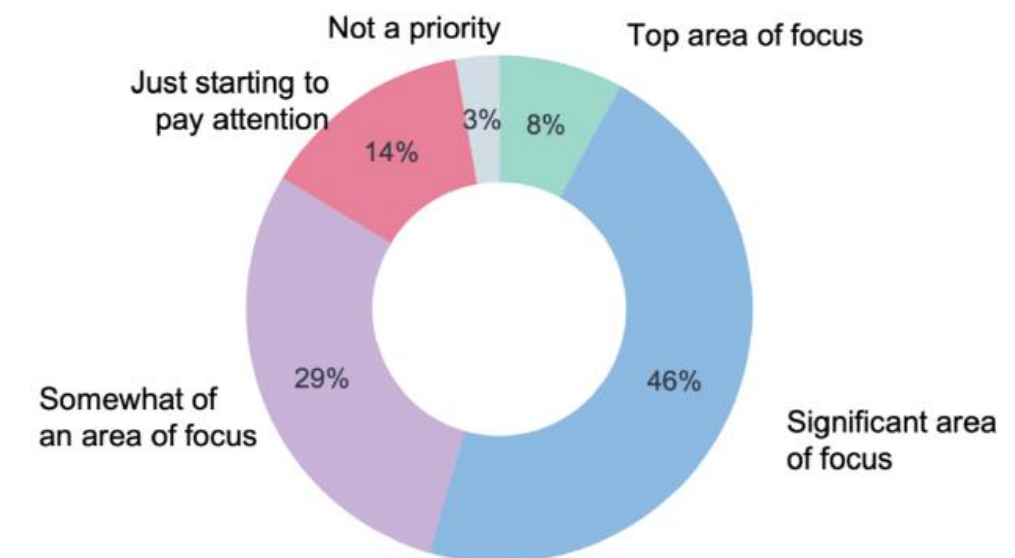
N=428

Anchore 2022 Software Supply Chain Security Report

12 OCT 2021 **NEWS**

Over 90% of Firms Suffered Supply Chain Breaches Last Year

Source : https://www.infosecurity-magazine.com/news/90-firms-supply-chain-breaches/

SUPPLY CHAIN ATTACKS…
THE ONES WE HEAR ABOUT

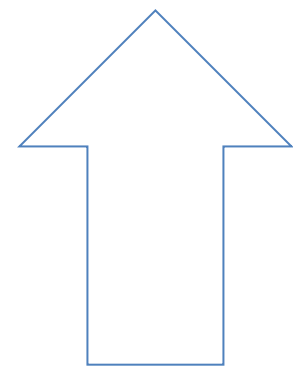| solarwinds	18,000+ customers
Kaseya®	50+ Managed Service Providers
LOG4J 🤯	35,000+ Java Packages Untold millions of Devices, Applications and Security Teams impacted

NETWORK & APP INVERSION
>70% OF TRAFFIC IS NOW CLOUD BASED
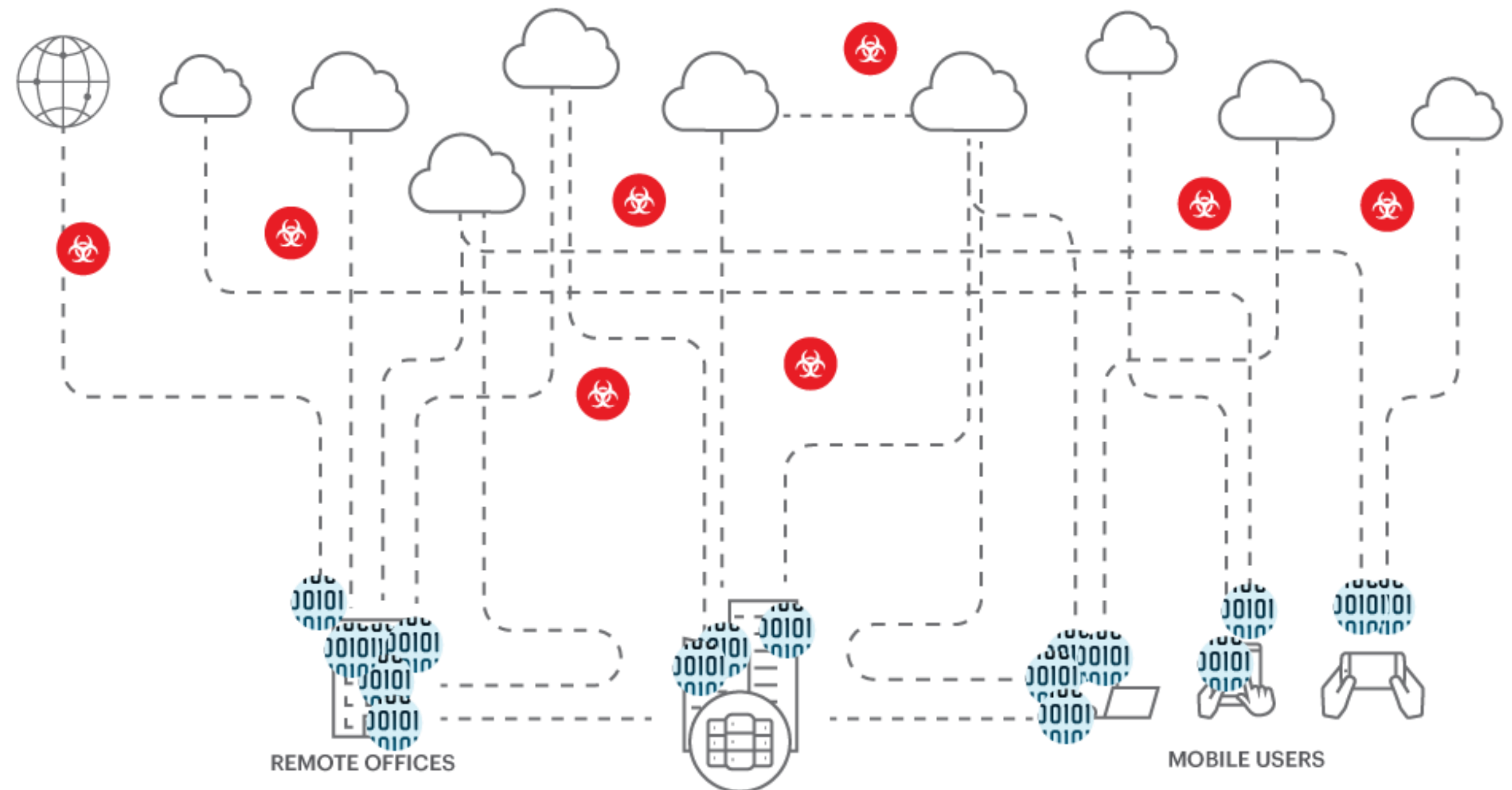
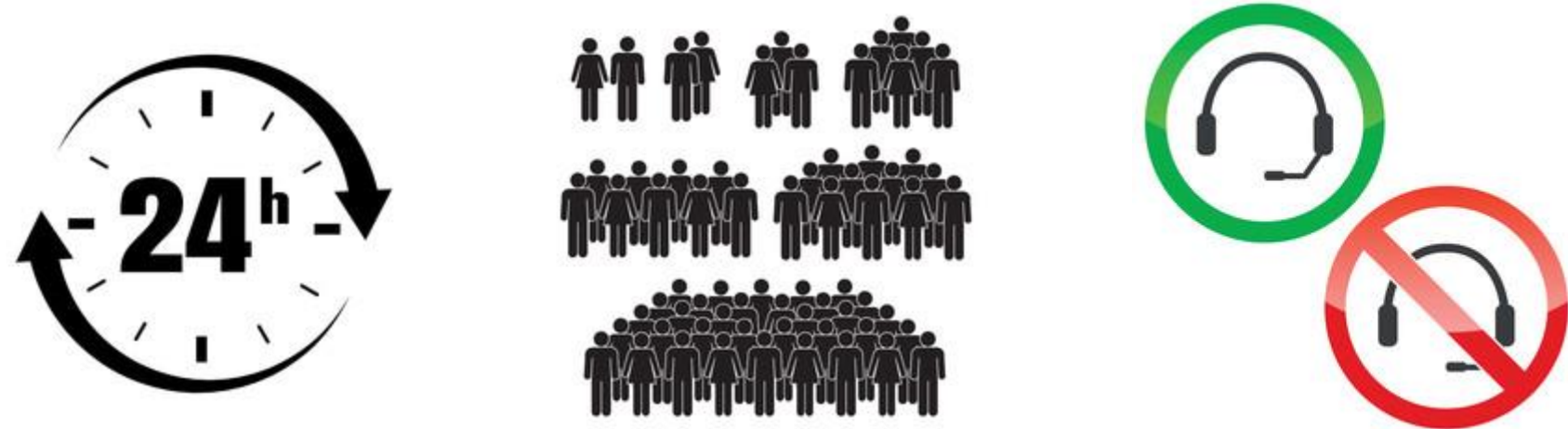Traditional Web   Public Cloud Apps and Services   Private Apps

Network Traffic

- **Digital transformation is shifting network load to internet**

- **Explosive growth in SaaS & IaaS adoption**

- **Controls need to follow the data and the Applications**

REMOTE OFFICES

MOBILE USERS

Australians 'worst in the world' for downloading dodgy apps, more than a quarter deemed risky

- Australia recorded 26.9 percent of app threats on a per-device basis worldwide
- Mobile security provider Lookout says Australians are complacent
- Users are advised to download from the official app store for added security

American Samoa 1.3 %

Australia 26.9 %

New Zealand 0.7 %

App Threat Encounter Rates (%)

0   5   7   10+

Platform
All
Android
iOS

Verticals
All Industries
Energy/Utilities
Financial Services
Government
Healthcare/Pharmaceutical
Manufacturing
Retail/Wholesale
Telecommunications
Other

Iceland 5.5 %
Finland 2.1 %
United Kingdom 2.8 %
Belarus 4.4 %
Spain 3.6 %
Albania 1.3 %
Azerbaijan 3.6 %
Algeria 2.9 %
Egypt 7.4 %
United Arab Emirates 3.8 %
India 4.0 %
Hong Kong 5.1 %
Cote d'Ivoire 3.9 %
Ethiopia 1.6 %
Guam 1.5 %
Malaysia 6.4 %
Angola 1.3 %
Malawi 3.8 %
South Africa 4.3 %
Mexico 2.7 %
Anguilla 5.6 %
Colombia 2.9 %
Peru 3.9 %
Brazil 2.2 %
Argentina 3.1 %

American Samoa 1.3 %
Australia 26.9 %
New Zealand 0.7 %

mapbox

Source : https://www.lookout.com/resources/app-threats-map

JUST HOW BIG IS YOUR 3RD PARTY SUPPLY CHAIN?

- Small organizations with <500 users
- Medium organizations with 500 – 2000 users
- Large organizations with 2000 – 4000 users
- X-Large organizations with >4000 users

The number of apps increases with organization size, w[...]
organizations averaging 1,265 apps in December 2020.

Number of [...]
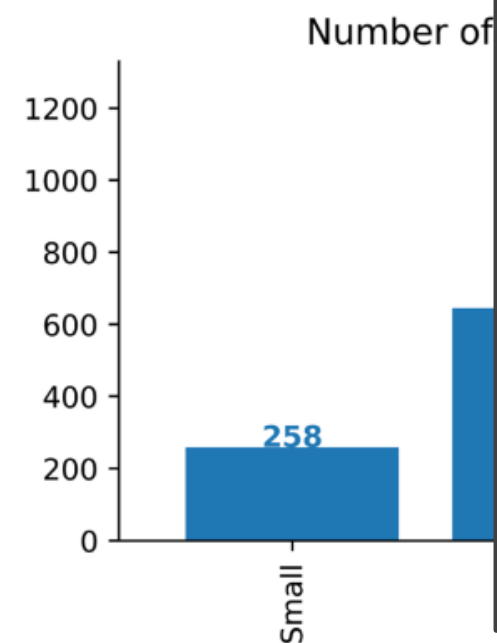
REAL EXAMPLE

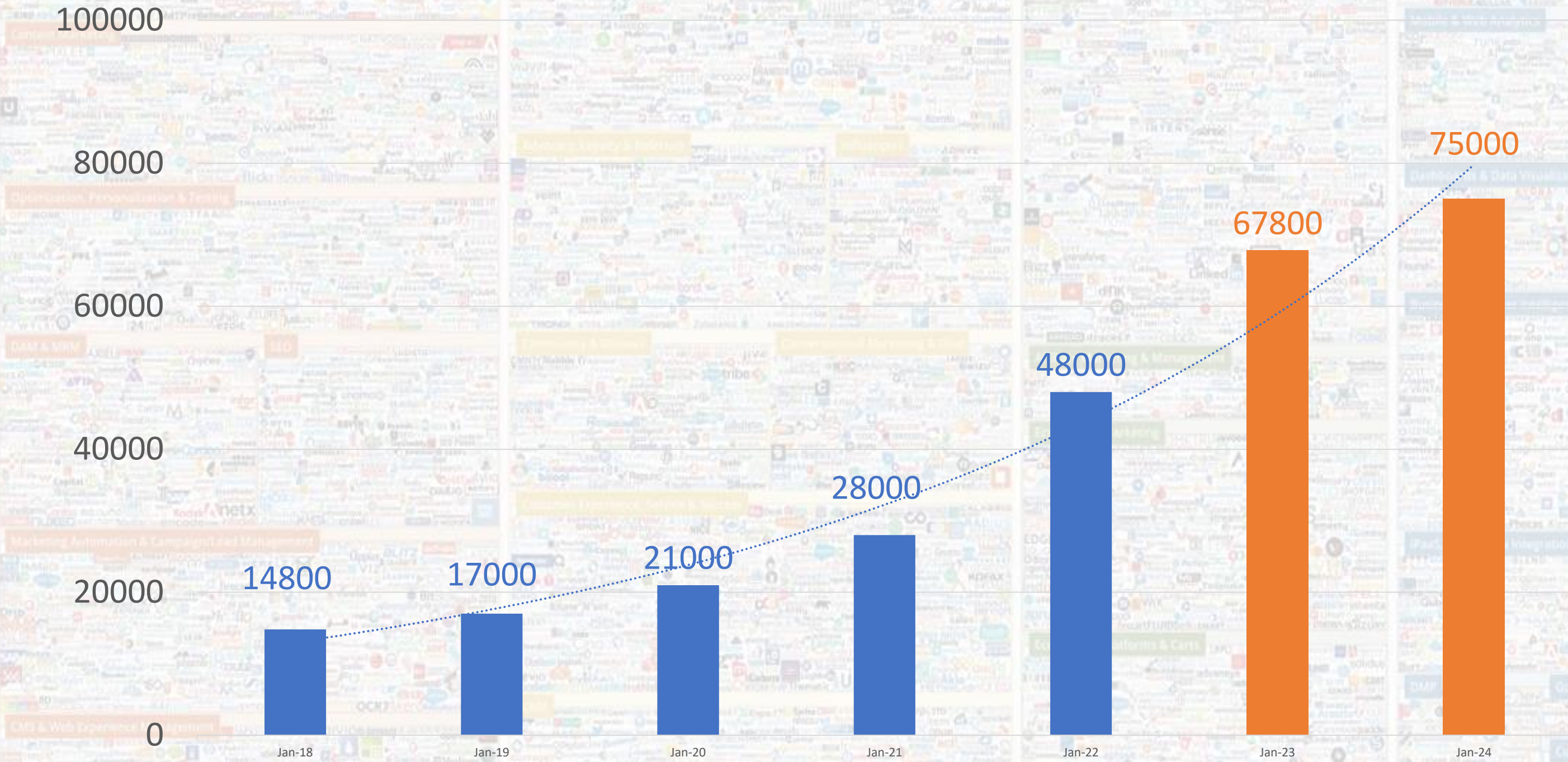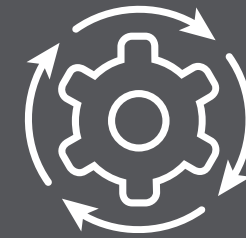| Visibility and control over unsanctioned SaaS Services	1,427 Cloud Apps discovered 61.18% Risky Apps 183 new apps discovered in the last 30 days
Visibility and control over data upload to cloud storage instances with non-approved vendor/party	713 Total Cloud Storage Instances Detected (21 instances with ABC Corp's instance IDs) 34,552 uploads to unsanctioned instances blocked
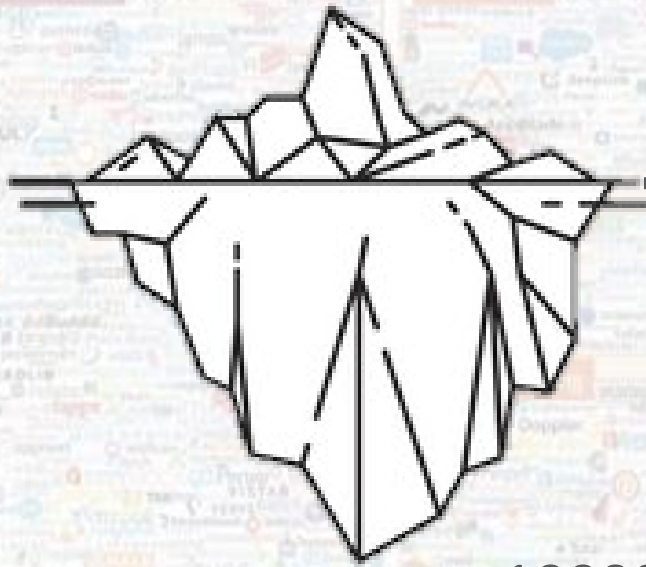
Actual and Projected Number of Cloud Apps

5%

95%

Date	Value
Jan-18	14800
Jan-19	17000
Jan-20	21000
Jan-21	28000
Jan-22	48000
Jan-23	67800
Jan-24	75000

Source : Netskope Cloud Confidence Index & Projected Analysis

TRADITIONAL 3RD PARTY RISK PROGRAM BUILDING BLOCKS

|	
Legal Risk	Operational Risk
Financial Crime Risk (e.g. ABC, CTF etc.)	ESG (e.g. Modern Day Slavery)
Technology Risk	Cyber Risk

SCHEDULED TIERED REASSESSMENTS
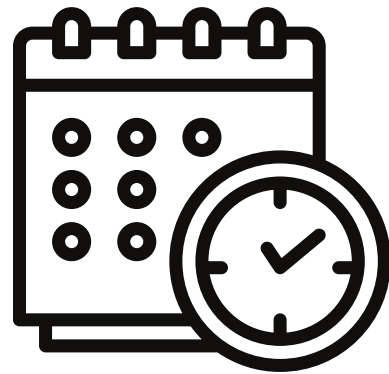
- **DETERMINE INHERENT RISK**
- **TIER BASED ON CRITICALITY**
- **REASSESS EACH TIER ON A SCHEDULE:**
  - **TIER 1 - ANNUALLY**
  - **TIER 2 - EVERY TWO YEARS**
  - **THE REST = RISK ACCEPTANCE**

CONTINUOUS RISK MONITORING
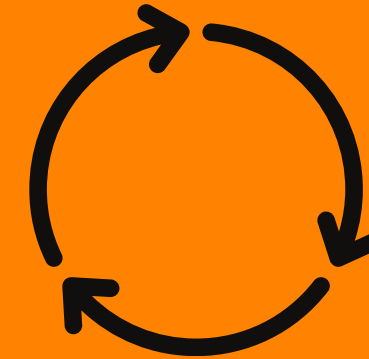
- **REAL TIME INFORMATION**
- **REAL TIME CONTROL**
- **INTELLIGENCE LED – DATA DRIVEN DECISIONS**
- **ADVANCED ANALYTICS**

SO WHAT DOES THE INHERENT RISK LOOK LIKE?
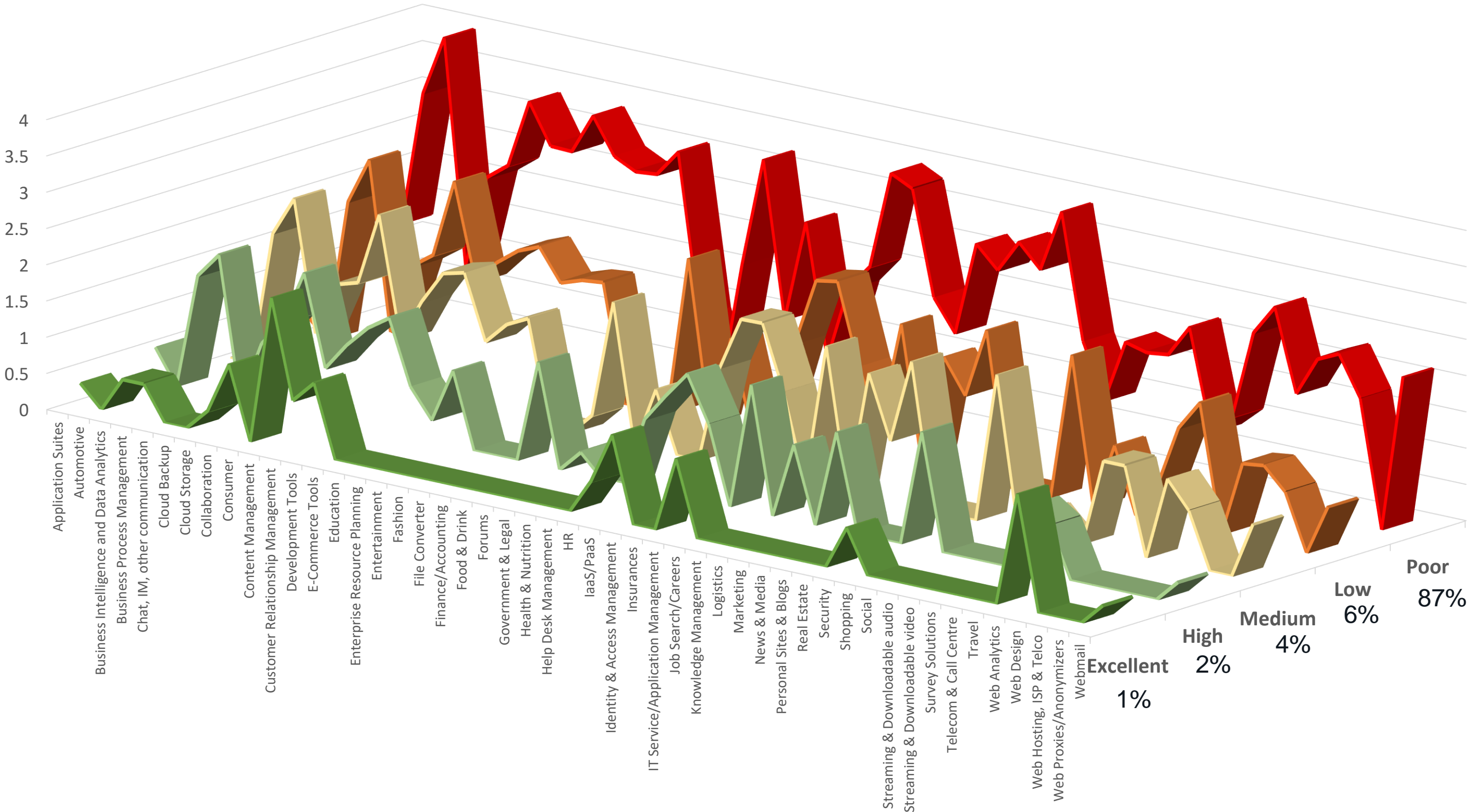
50,000 Cloud Apps – Ranked from Excellent (1%) to Poor (87%)

CLOUD APP CATEGORIES WITH THE POOREST SCORES

APPLICATIONS

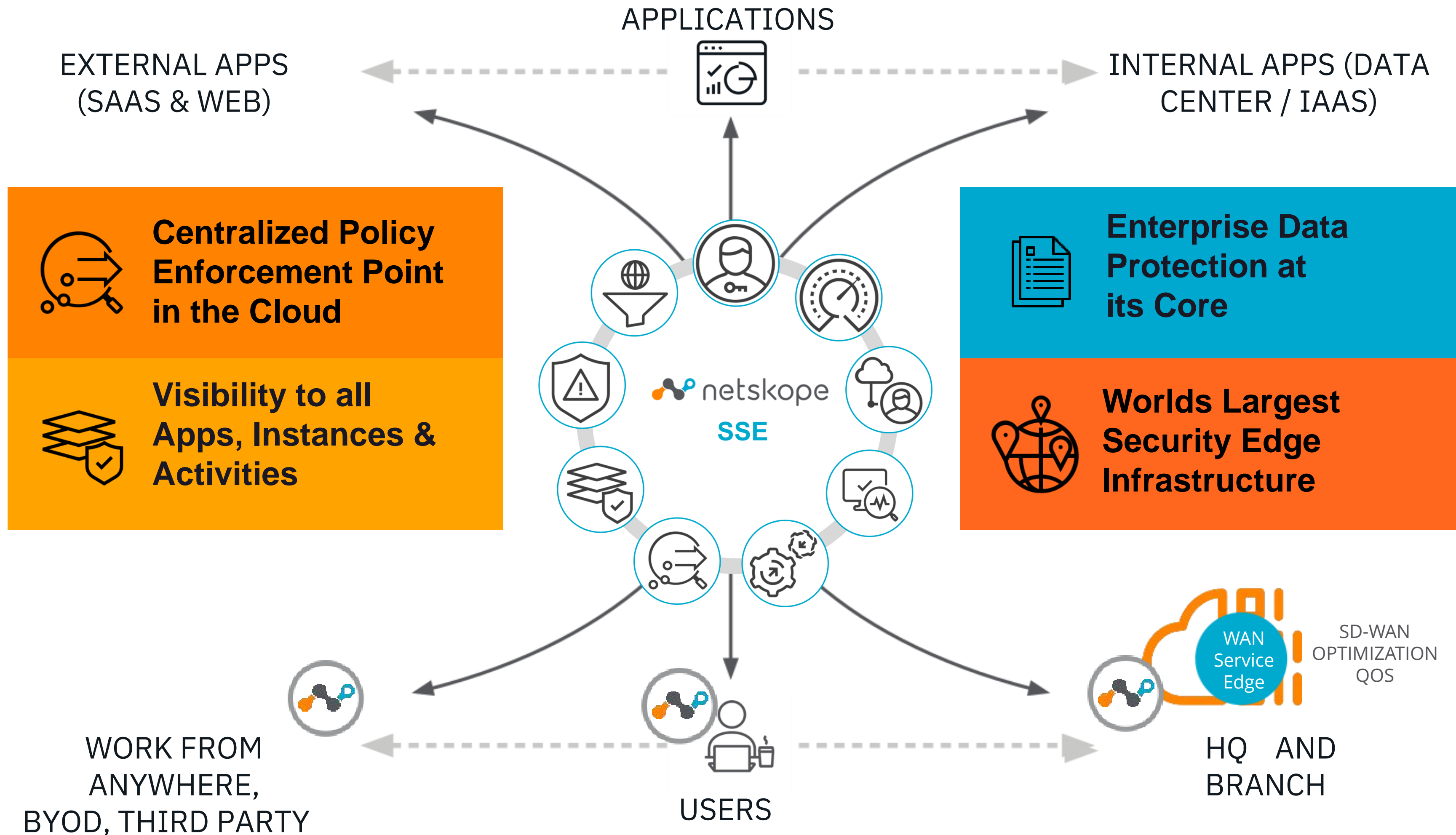EXTERNAL APPS
(SAAS & WEB)
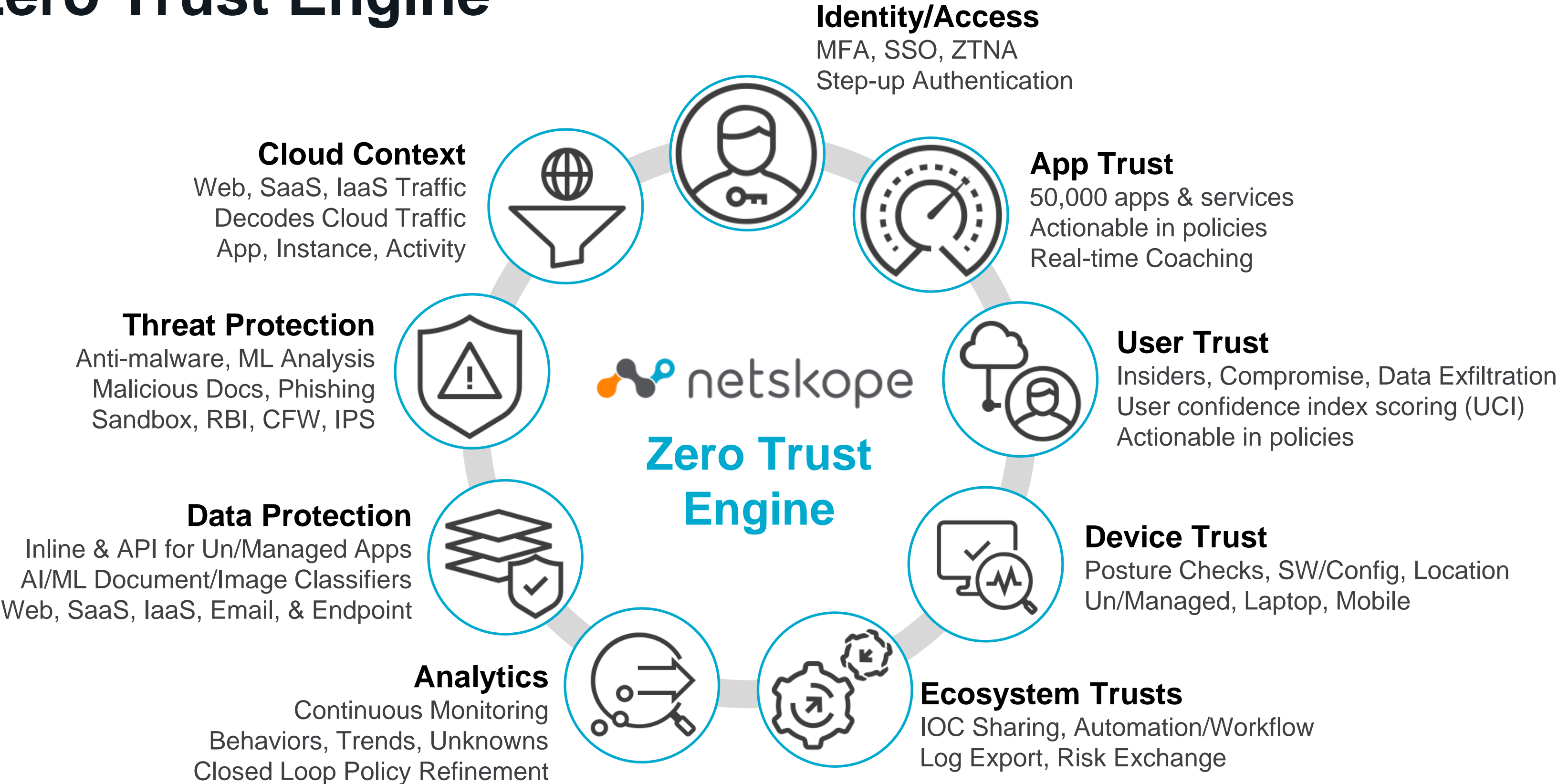
INTERNAL APPS (DATA
CENTER / IAAS)

Security
Service Edge

WORK FROM
ANYWHERE,
BYOD, THIRD PARTY

USERS

HQ   AND
BRANCH

netskope

APPLICATIONS

EXTERNAL APPS
(SAAS & WEB)

INTERNAL APPS (DATA
CENTER / IAAS)

**Centralized Policy
Enforcement Point
in the Cloud**

**Enterprise Data
Protection at
its Core**

**Visibility to all
Apps, Instances &
Activities**

**Worlds Largest
Security Edge
Infrastructure**

netskope
SSE

WAN
Service
Edge

SD-WAN
OPTIMIZATION
QOS

WORK FROM
ANYWHERE,
BYOD, THIRD PARTY

USERS

HQ   AND
BRANCH

netskope

Zero Trust Engine

Identity/Access
MFA, SSO, ZTNA
Step-up Authentication

Cloud Context
Web, SaaS, IaaS Traffic
Decodes Cloud Traffic
App, Instance, Activity

App Trust
50,000 apps & services
Actionable in policies
Real-time Coaching

Threat Protection
Anti-malware, ML Analysis
Malicious Docs, Phishing
Sandbox, RBI, CFW, IPS

User Trust
Insiders, Compromise, Data Exfiltration
User confidence index scoring (UCI)
Actionable in policies

netskope

Zero Trust Engine

Data Protection
Inline & API for Un/Managed Apps
AI/ML Document/Image Classifiers
Web, SaaS, IaaS, Email, & Endpoint

Device Trust
Posture Checks, SW/Config, Location
Un/Managed, Laptop, Mobile

Analytics
Continuous Monitoring
Behaviors, Trends, Unknowns
Closed Loop Policy Refinement

Ecosystem Trusts
IOC Sharing, Automation/Workflow
Log Export, Risk Exchange

netskope

Cloud Confidence Index (CCI)

All Apps ▾

RESET SCORES	CANCEL

CCI LEVEL

☁️ ☁️ ☁️ ☁️ ☁️ ☁️ ☁️

CUSTOM APP TAGS

All Custom Tags

IT-Dept Sanctioned Only

CorporateSanctionedApp

APPLICATION CATEGORIES

All Categories

Advocacy Groups & Trade Associations

App Admin Console

Application Suite

Arts

Auctions & Marketplaces

Automotive

Business

Business Intelligence and Data

Search App Name ▾

🔍 Sear

49,518 matches found.

aws — 96
Amazon Database

Amazon Database provides managed database services that includes relational databases for...

A...
RD...

Google — 96
google-docs

docs.google.com

Google Docs brings your documents to life with smart editing and styling tools to help you easily...

salesforce — 96
Work.com

work.com

Work.com is a corporate performance management platform for sales representatives...

Mic... Azu...
Microsoft A...

windowsazure.c...

Microsoft Azure is... infrastructure, crea...

amazon DynamoDB — 96
Amazon DynamoDB

dynamodb.amazonaws.com

Amazon DynamoDB is a fully mana... database service that provides fast a...

Amazon Elastic Container Service — 95
Highly secure, reliable, and easy to run containers

Amazon EC2 Container Service...

AWS Lambda
Amazon Lambda...

NETSKOPE CLOUD CONFIDENCE INDEX™
CONTINUOUS REAL-TIME ASSESSMENT OF APP RISK

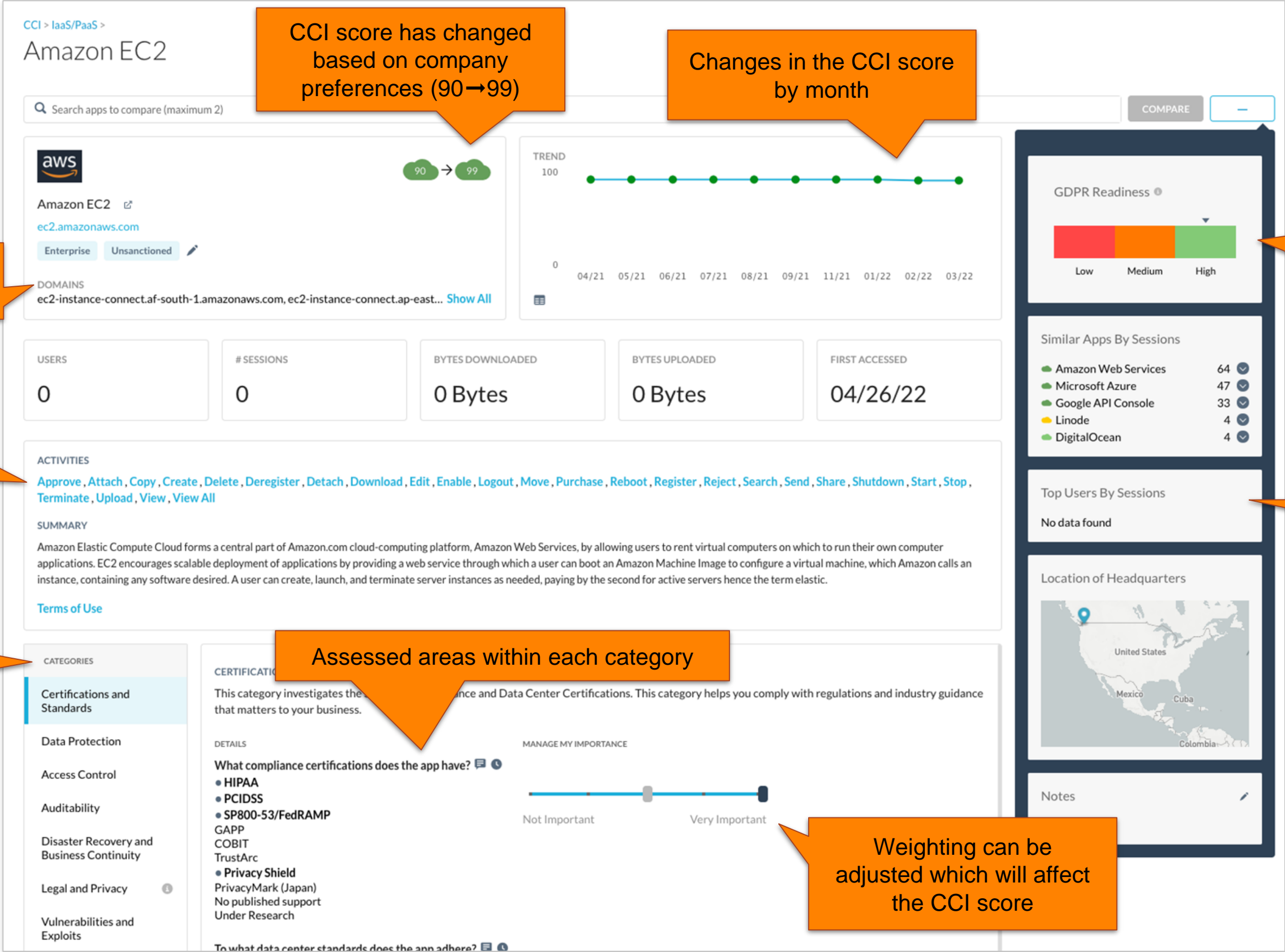**50,000+ CLOUD SERVICES, AND COUNTING; REVIEWED EVERY TWO WEEKS**

CSA CCM AS A BASE WITH VULNERABILITIES, BREACHES AND TERMS AND CONDITIONS ADDED

RISK SCORES CAN BE USED IN POLICIES

netskope

Application Trust

Cloud Confidence Index (CCI) - Sample Entry for *Amazon Web Services EC2*

CCI score has changed based on company preferences (90→99)

Changes in the CCI score by month

GDPR readiness of the app as assessed by Netskope

All domains used by the app.

The user activities that can be tracked and controlled in policy.

The users consuming the application (if any).

The categories the CCI score is calculated across

Assessed areas within each category

Weighting can be adjusted which will affect the CCI score

CONTEXTUALISE THE RISK TO YOUR ORGANISATION

Cloud Confidence Index (CCI)

All Apps ▼	RESET SCORES	CANCEL

CCI LEVEL

☁️ ☁️ ☁️ ☁️ ☁️ ☁️ ➡️

Search App Name ▼

49,518 matches found.

CUSTOM APP TAGS

All Custom Tags

IT-Dept Sanctioned Only

CorporateSanctionedApp

APPLICATION CATEGORIES

All Categories

Advocacy Groups & Trade Associations

App Admin Console

Application Suite

Arts

Auctions & Marketplaces

Automotive

Business

Business Intelligence and Data Analytics

Business Process Management

Chat, IM & other communication

aws
Amazon Database
Amazon Database provides managed services that includes relational datab...

Google
google-docs
docs.google.com
Google Docs brings your documents t smart editing and styling tools to help...

salesforce
Work.com
work.com
Work.com is a corporate performance management platform for sales repres...

Amazon Elastic Container Service
Highly secure, reliable, and scalable way to run containers
Amazon EC2 Container Service
ecs.eu-west-3.amazonaws.com
Amazon Elastic Container Service (An a managed container orchestration service....

Cloud Confidence Index (CCI)

Discovered Apps ▼	RESET SCORES	CANCEL

CCI LEVEL

☁️ ☁️ ☁️ ☁️ ☁️ ☁️ ➡️

Search App Name ▼

358 matches found.

CUSTOM APP TAGS

All Custom Tags

IT-Dept Sanctioned Only

CorporateSanctionedApp

APPLICATION CATEGORIES

All Categories

Advocacy Groups & Trade Associations

App Admin Console

Application Suite

Arts

Auctions & Marketplaces

Microsoft Azure
Microsoft Azure
windowsazure.com
Microsoft Azure is a cloud computi infrastructure, created by Microsof...

amazon S3
Amazon S3
s3.amazonaws.com
Amazon Simple Storage Service (A provides developers and IT teams w...

Google Sites
Google Sites
sites.google.com
Google Sites is a structured wiki- ar creation tool offered by Google as p...

computing platform. It is a computing service tha...

Cloud Confidence Index (CCI)

Sanctioned Apps ▼	RESET SCORES	CANCEL	APPLY CHA

CCI LEVEL

☁️ ☁️ ☁️ ☁️ ☁️ ☁️ ➡️

Search App Name ▼	🔍 Search for apps by name

14 matches found.

CUSTOM APP TAGS

All Custom Tags

IT-Dept Sanctioned Only

CorporateSanctionedApp

APPLICATION CATEGORIES

All Categories

Advocacy Groups & Trade Associations

App Admin Console

Application Suite

Arts

Auctions & Marketplaces

Google Drive — 91
Google Drive
drive.google.com
Google Drive provides a single place to store, access, create, edit and share documents, files, an...

Microsoft 365 — 89
Microsoft Office 365 Suite
login.microsoftonline.com
The Microsoft Office 365 Suite listed in Netskopes application suite category tracks user...

OneDrive for Business — 87
Microsoft Office 365 OneDrive for Business
officeapps.live.com
OneDrive for Business is Microsoft's cloud storage offering. Users can store, sync, and share their...

SharePoint Online
Microsoft Office 365 Sharepoint Online
sharepoint.com
Microsoft Office SharePoint Online is a cloud-based service that helps organizations share an...

zoom
Zoom
zoom.us
Zoom unifies cloud video conferencing, online meetings, group messaging, and software-defin...
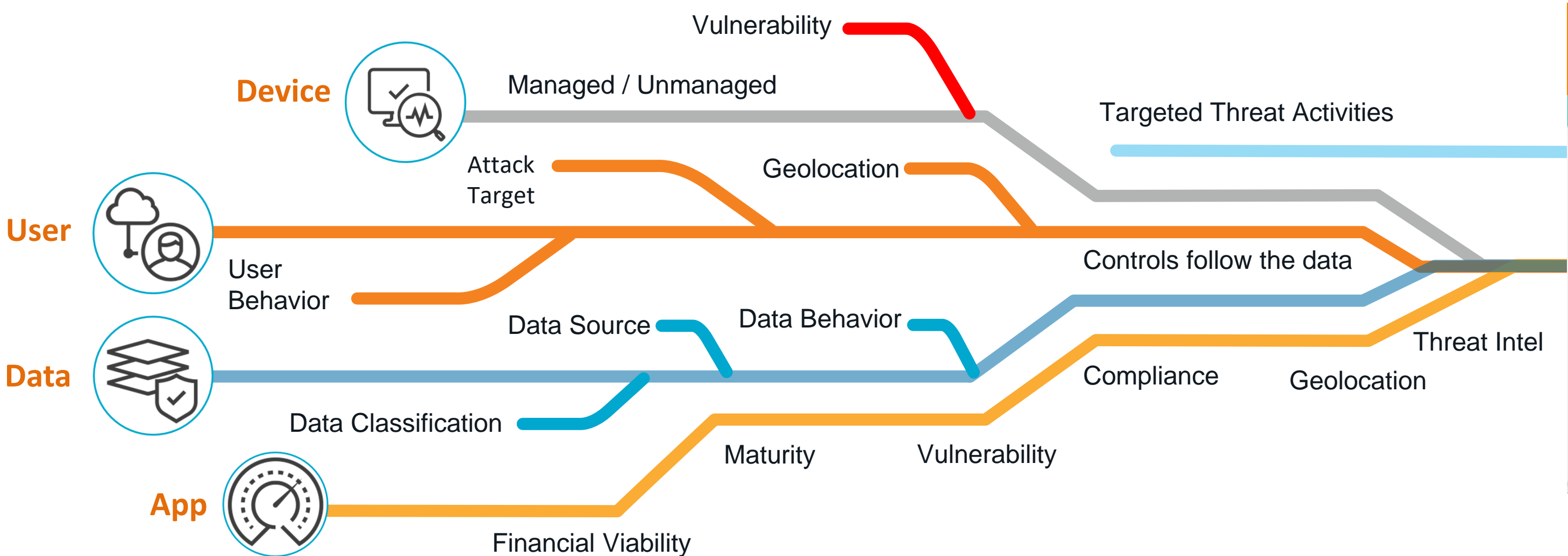
slack
Slack
slack.com
Slack is a team communication application providing services such as real-time messaging...

Continuous Assessment of App Risk feeding your *adaptive* & *context-driven* security controls

COLLABORATE DON'T RESTRICT

GOOGLE DRIVE = https://drive.google.com

Personal   **Corporate**   **Partner**
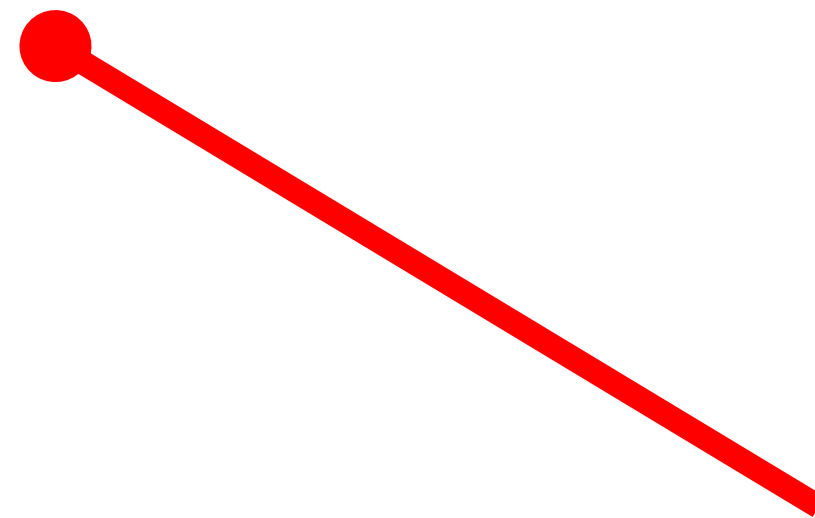
DATA

USE RISK TO ENABLE THE BUSINESS

Proceed
10%

Stop
90%

Providing Risk Associated Guardrails educates the end users in real time.

ACME COLLEGE
BUSINESS SCHOOL

Temporary Access Allowed - Justify Access

If you have a business reason for performing this action provide an explanation

Hi, mferguson@netskopeacmeinc.onmicrosoft.com, the activity you are trying to perform is not authorised.
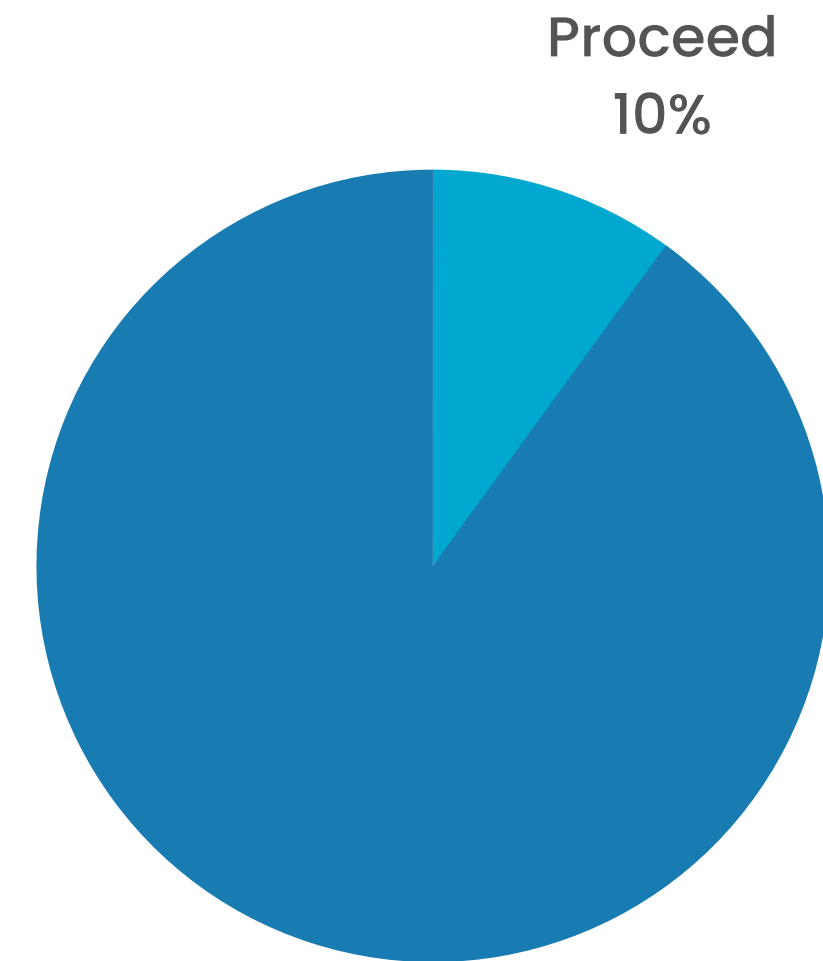
Diagnostic Information:
- Application: Microsoft Office 365 OneDrive for Business
- Activity: Delete

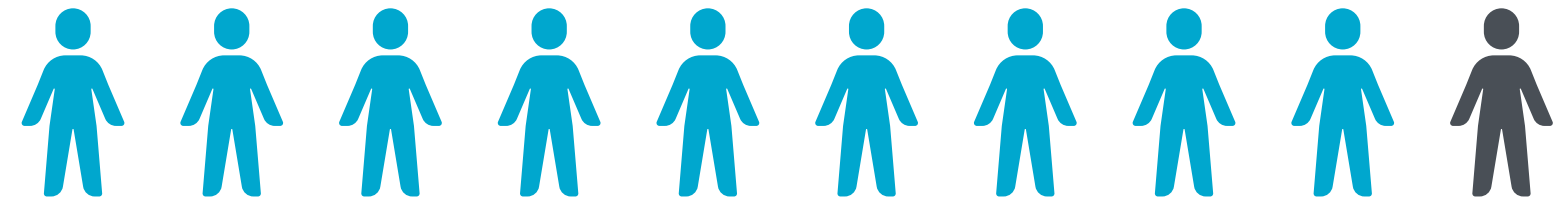⦿ Justify Usage
◯ Report False Positive

Please close this tab.

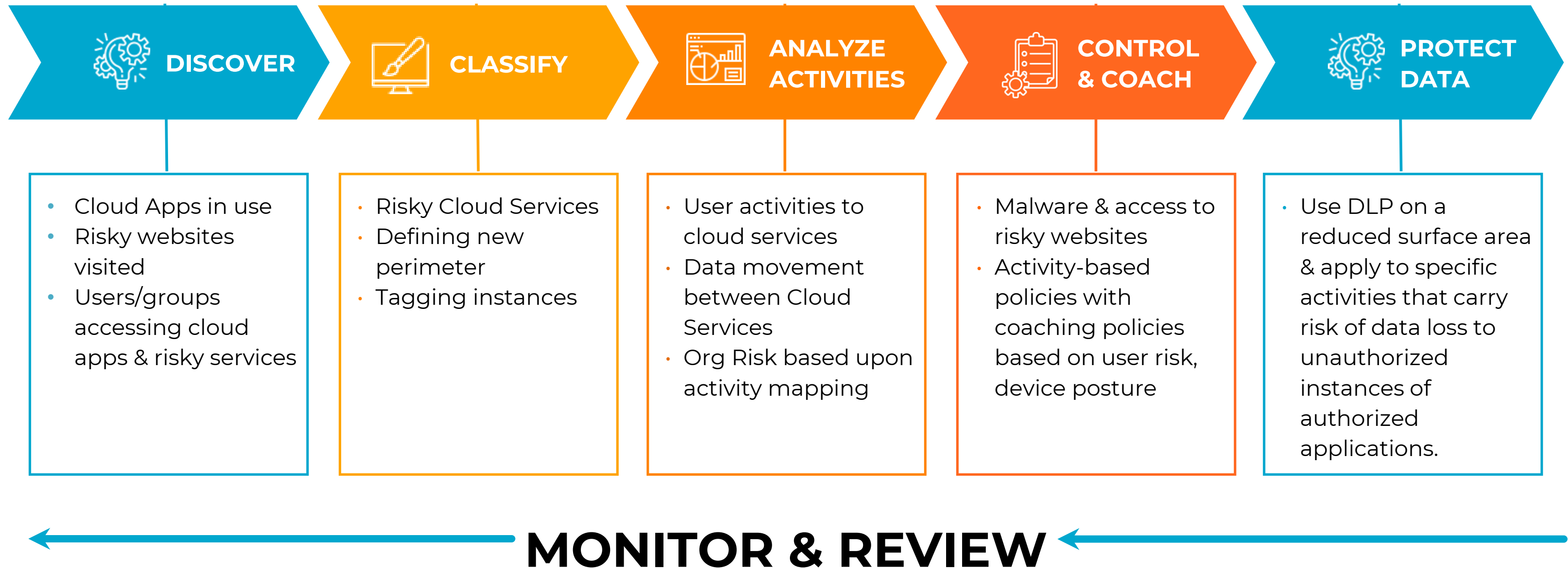This window will auto-close in **59 seconds**

Exit   Proceed

RISK POLICY FRAMEWORK

3rd PARTY RISK IDENTIFICATION

RISK MITIGATION

DISCOVER	CLASSIFY	ANALYZE ACTIVITIES	CONTROL & COACH	PROTECT DATA

DISCOVER
- Cloud Apps in use
- Risky websites visited
- Users/groups accessing cloud apps & risky services

CLASSIFY
- Risky Cloud Services
- Defining new perimeter
- Tagging instances

ANALYZE ACTIVITIES
- User activities to cloud services
- Data movement between Cloud Services
- Org Risk based upon activity mapping

CONTROL & COACH
- Malware & access to risky websites
- Activity-based policies with coaching policies based on user risk, device posture

PROTECT DATA
- Use DLP on a reduced surface area & apply to specific activities that carry risk of data loss to unauthorized instances of authorized applications.

← MONITOR & REVIEW ←

THANK YOU