

Strengthen Your Security Program Combining Zero Trust with SASE

Bob Gilbert

VP Strategy & Chief Evangelist

Netskope

Circa 1985 – My first cyber experience

- I operated a Bulletin Board System (BBS) that hosted software
- My system was hacked, and data was deleted
- I developed a program (using assembly) to keep out hackers



Commodore 64, 300 baud modem, 1541 floppy storage, Color 64 BBS

```
System Defined Parameters
Maximum lines/msg (20-100) 100
Maximum cols/line (37-78) 37
Maximum # of msgs (25-99) 25
Maximum # of words (25-99) 25
Minimum bits/cyclic msg (25-75) 25
Minimum bits-allow upids (10-70) 10
Maximum downloads per call (1-20) 1
Download credits per upload (1-20) 1
New msg download credits (1-20) 1
Credit system exempt level (1-3) 1
Number of days to hold msg (1-30) 1
New caller access level (1-4) 1
Msgs expired access level (0-4) 1
Save caller log (y/n) y
Screen on Errors (y/n) y
Screen blanking (y/n) y
Normal/inverted hook (n/i) n
Use "B1" modem commands (y/n) n
Does your modem support B1 (y/n) n
Init command atzlx1s0=0s2=43r1q0v1m0
Is This Correct?
```

```
Disk Drive Assignments
Device,Drive,Command
Password File (8-15,0-1) 0 , 0 , i0
System Files (8-15,0-1) 0 , 0 , i0
Help Files (8-15,0-1) 0 , 0 , i0
Public Msgs (8-15,0-1) 0 , 0 , i0
Private Msgs (8-15,0-1) 0 , 0 , i0
Text Files (8-15,0-1) 0 , 0 , i0
Caller Log (8-15,0) 0 , 0 , i0
Prgm Files (8-15,0-1) 0 , 0 , ui
Max Files on Public Msgs Drv 0
```



Your Expanding Attack Surface

SaaS usage exploding

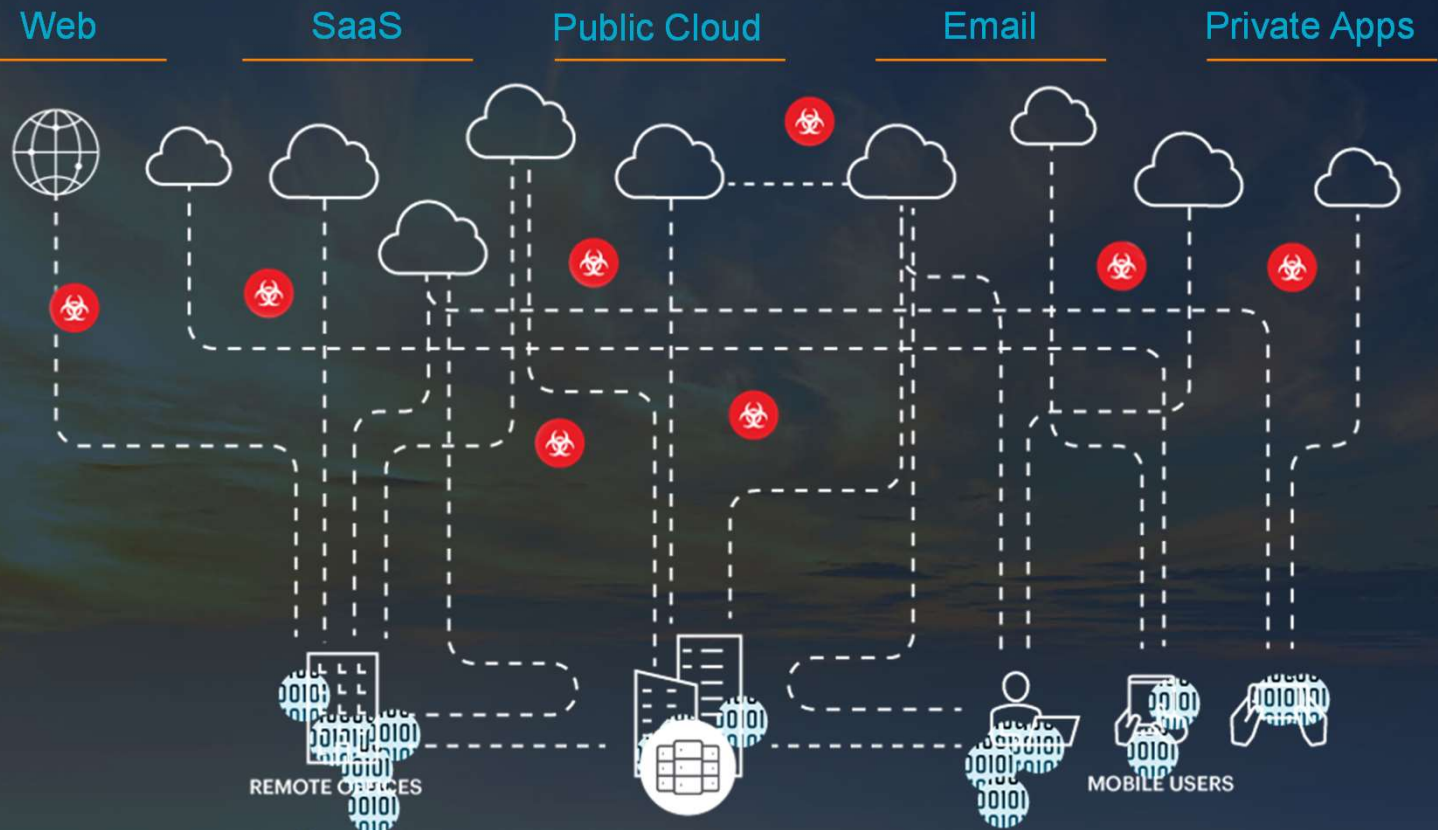
- 2,495 SaaS apps on average used by organizations and AI apps are seeing huge growth

Data is everywhere

- By 2025 there will be 150 Zettabytes of data stored in the cloud

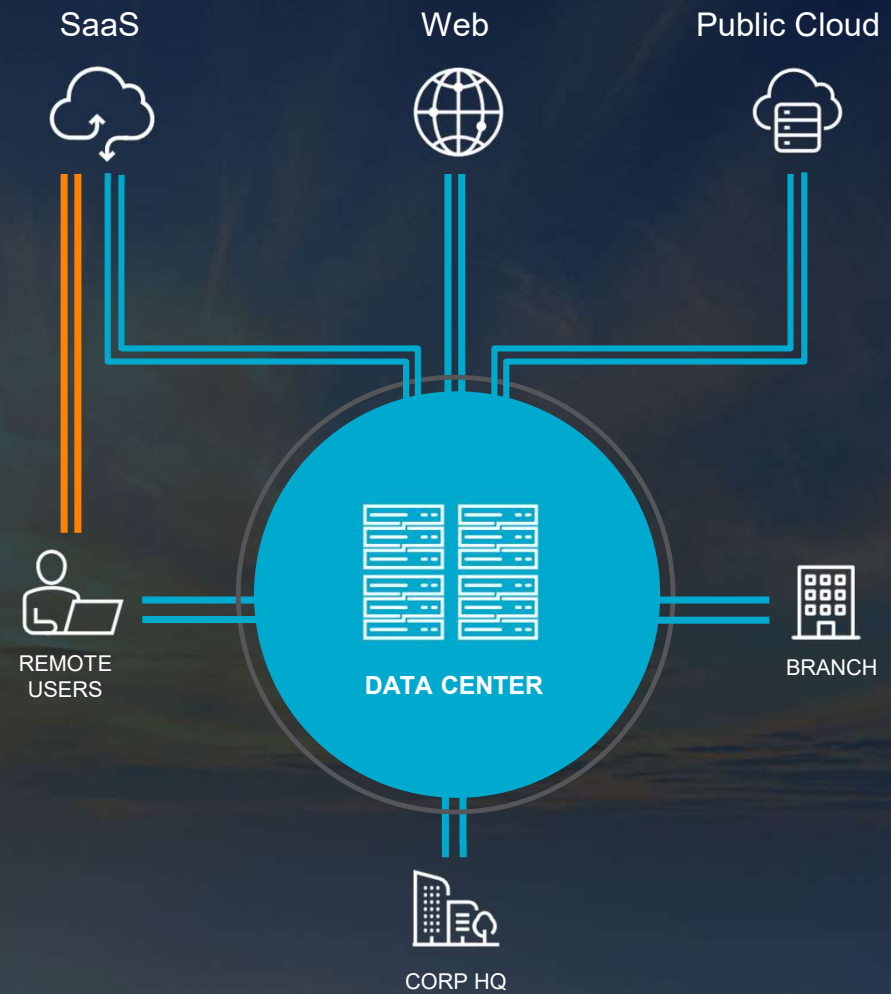
Rise of the remote worker

- Work-from-anywhere is the new norm



Current State

Hairpinning / Split Tunnel

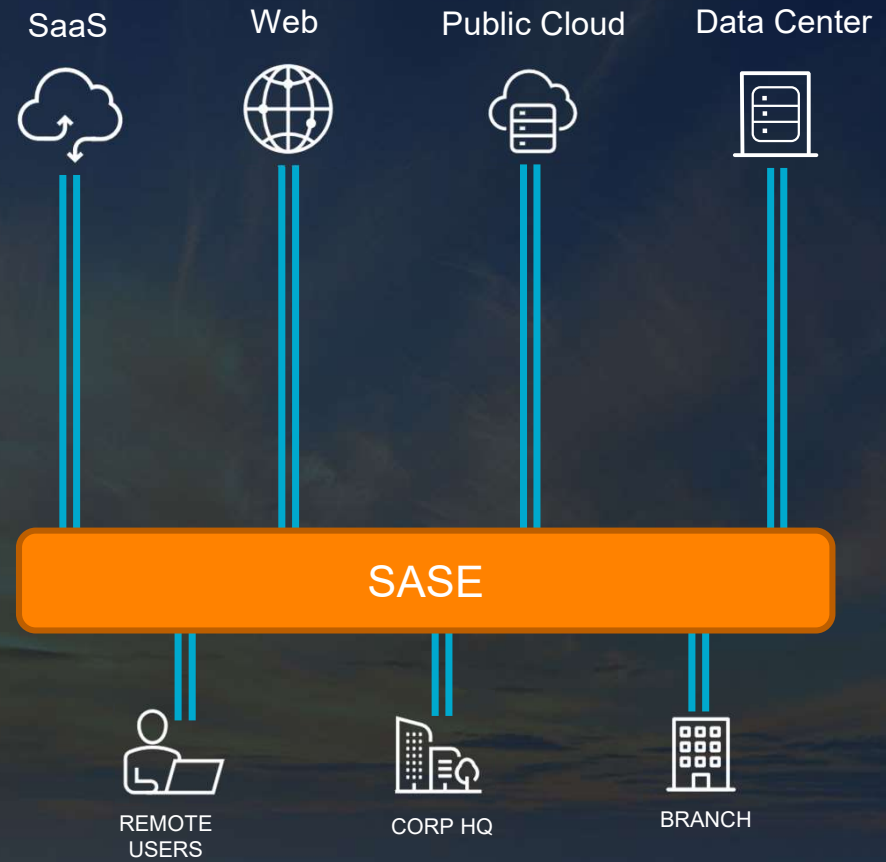




STRICTLY
NO
ACCESS

The Modern Way

Security Access Service Edge



SaaS

Web

Public Cloud

Data Center



Secure Access Service Edge (SASE)

- Unifies security as a service with networking as a service
- Quickly connects people safely to their destination
- Security controls follow the data and user

CLOUD ACCESS
SECURITY BROKER



SASE



ZERO TRUST
NETWORK ACCESS

Secure Access Service Edge



REMOTE
USERS

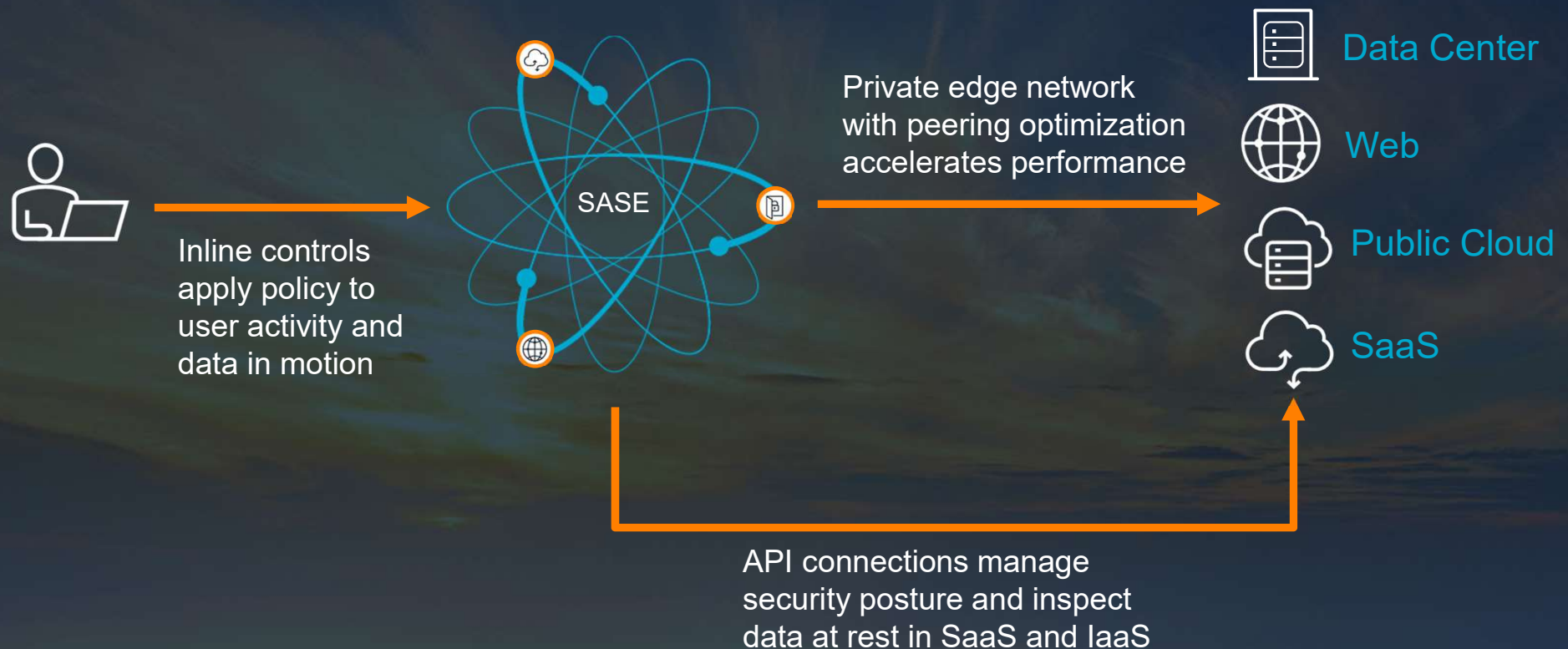


CORP HQ



BRANCH

SASE: Inline and Out-of-Band Controls



Charlie Ciso





ZERO TRUST



ZERO TRUST



ZERO TRUST



Granular Controls Using Signals

Remove Implicit Trust and Use Context to Continuously Verify

Criteria

Destination

Action

Identity

Device

Behavior

Browser

Location

Activity

Threat

Data

Cloud App

Website

Private App

Non-Web

Coaching



User
Group
OU



Managed
Unmanaged



Trust Score



Chrome
Safari
Edge
...



Geo
Network
Source
Destination



Browse
Login
Upload
Share to
Share from
Edit
Post
Create
...



Threat
Intel
AV
Analysis
Sandbox
UEBA



DLP Rules
AI/ML
Fingerprint
Data Match



Trust Score
App Instance
Category



URL
Category
Risk



FQDN
Ports
IP Address



Port
Protocol
IP Address

Allow
Deny
Warn
Justify
Isolate
Redirect
Step-Up

Active User Coaching Makes Granular Controls More Effective

Active User Coaching

Challenge

Traditional firewall and SWG methods of coarse-grained blocking users is disruptive and does not produce good behavior

Solution

Active User Coaching interrupts risky activities and coaches users to be good digital citizens



Zero Trust Scenarios

Scenario 1: Secure Access to Internal App

Traditional Way: VPN

Challenges:

- Bad user experience
- Complex
- Poor security

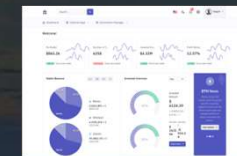
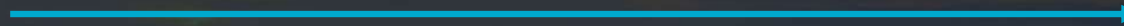
Modern Way: ZTNA

Advantages:

- Good user experience
- Simple
- Strong security based on zero trust

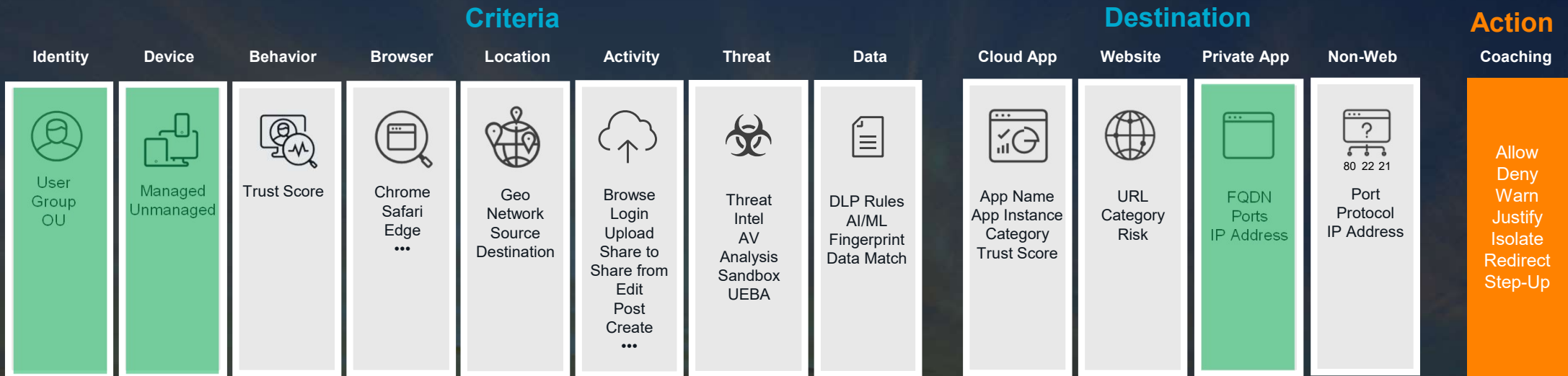


REMOTE
USER



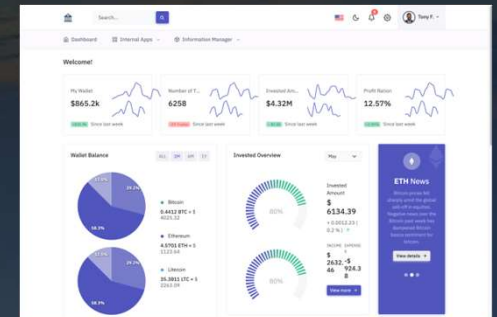
PRIVATE APP
HOSTED IN
DATACENTER
(Finance Portal)

Scenario 1: Secure Access to Private App



- ✓ fabio@bobsbank.net is in the 'finance' AD group
- ✓ Fabio is using his corporate-managed laptop

Fabio is granted access to his company's private app, Finance Portal



Scenario 2: Using Personal Cloud App Instance

Traditional Way: SWG, FW, CASB

Challenges:

- No instance-awareness
- Coarse-grained allow or block

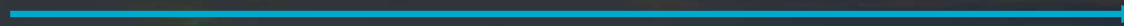
Modern Way: SASE

Advantages:

- App instance-aware
- Coach user to use corporate instance















Developer



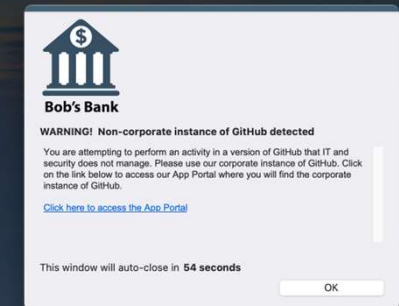
PERSONAL
CLOUD APP
(GitHub)

Scenario 2: Using Personal Cloud App Instance

Criteria								Destination				Action
Identity	Device	Behavior	Browser	Location	Activity	Threat	Data	Cloud App	Website	Private App	Non-Web	Coaching
 <p>User Group OU</p>	 <p>Managed Unmanaged</p>	 <p>Trust Score</p>	 <p>Chrome Safari Edge ...</p>	 <p>Geo Network Source Destination</p>	 <p>Browse Login Upload Share to Share from Edit Post Create ...</p>	 <p>Threat Intel AV Analysis Sandbox UEBA</p>	 <p>DLP Rules AI/ML Fingerprint Data Match</p>	 <p>App Name App Instance Category Trust Score</p>	 <p>URL Category Risk</p>	 <p>FQDN Ports IP Address</p>	 <p>80 22 21 Port Protocol IP Address</p>	<p>Allow Deny Warn Justify Isolate Redirect Step-Up</p>

- ✓ bob@bobsbank.net is in the 'engineering' AD group
- ✓ Bob is using his corporate-managed laptop
- ⚠ Bob attempts to upload source code to his personal GitHub

A coaching page is displayed, and Bob is redirected to use a corporate GitHub license



Scenario 3: Using Risky Cloud App

Traditional Way: SWG, FW, CASB

Challenges:

- No cloud app trust scoring
- Coarse-grained allow or block

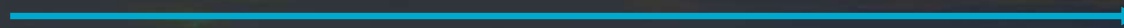
Modern Way: SASE

Advantages:

- Cloud app trust scoring
- Coach user vs block them















REMOTE
USER



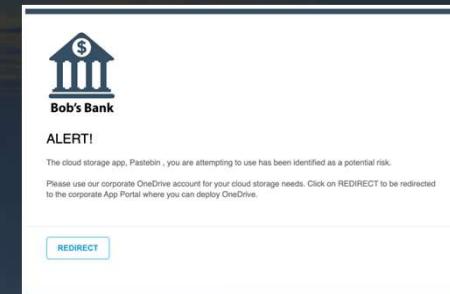
RISKY
CLOUD APP
(Pastebin)

Scenario 3: Using Risky Cloud App

Criteria								Destination				Action
Identity	Device	Behavior	Browser	Location	Activity	Threat	Data	Cloud App	Website	Private App	Non-Web	Coaching
 <p>User Group OU</p>	 <p>Managed Unmanaged</p>	 <p>Trust Score</p>	 <p>Chrome Safari Edge ...</p>	 <p>Geo Network Source Destination</p>	 <p>Browse Login Upload Share to Share from Edit Post Create ...</p>	 <p>Threat Intel AV Analysis Sandbox UEBA</p>	 <p>DLP Rules AI/ML Fingerprint Data Match</p>	 <p>App Name App Instance Category Trust Score</p>	 <p>URL Category Risk</p>	 <p>FQDN Ports IP Address</p>	 <p>80 22 21 Port Protocol IP Address</p>	<p>Allow Deny Warn Justify Isolate Redirect Step-Up</p>

- ✓ fabio@bobsbank.net is in the 'finance' AD group
- ✓ Fabio is using his corporate-managed laptop
- ⚠ Fabio attempts to access Pastebin with a poor app trust score

A coaching page is displayed, and Fabio is redirected to an app portal where he can use the corporate app instance



Scenario 4: Data Loss During Collaboration

Traditional Way: SWG, FW, CASB

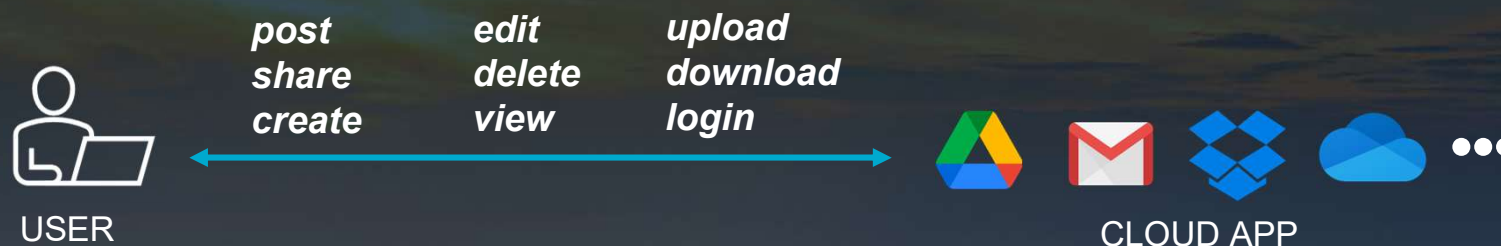
Challenges:

- Lacks activity-level visibility and control
- Lacks advanced DLP tied to activities











Modern Way: SASE

Advantages:

- 100+ activities across
- 1000's of cloud apps
- Advanced DLP tied to activities

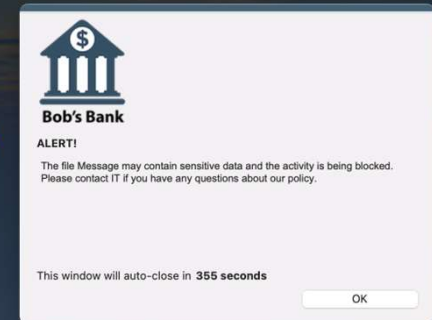


Scenario 4: Data Loss During App Usage

Criteria								Destination				Action
Identity	Device	Behavior	Browser	Location	Activity	Threat	Data	Cloud App	Website	Private App	Non-Web	Coaching
 User Group OU	 Managed Unmanaged	 Trust Score	 Chrome Safari Edge ...	 Geo Network Source Destination	 Browse Login Upload Share to Share from Edit Post Create ...	 Threat Intel AV Analysis Sandbox UEBA	 DLP Rules AI/ML Fingerprint Data Match	 App Name App Instance Category Trust Score	 URL Category Risk	 FQDN Ports IP Address	 80 22 21 Port Protocol IP Address	Allow Deny Warn Justify Isolate Redirect Step-Up

- ✓ bob@bobsbank.net is in the 'departing employee' AD group
- ✓ Bob is using his corporate-managed laptop
- ⚠ Bob posts confidential data to a public Slack channel
- ⚠ Bob edits a document in OneDrive and pastes PII data

The activities are blocked, and Bob is presented with a coaching page



Scenario 5: Risky User Downloading Data

Traditional Way: SWG, FW, CASB

Challenges:

- No behavior trust scoring
- No user coaching

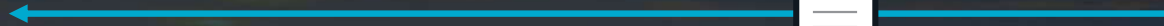
Modern Way: SASE

Advantages:

- Behavior trust scoring
- User coaching















RISKY
USER



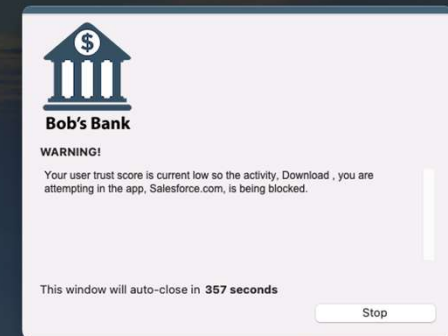
CORPORATE
CLOUD APP

Scenario 5: Risky User Downloading Data

Criteria								Destination				Action
Identity	Device	Behavior	Browser	Location	Activity	Threat	Data	Cloud App	Website	Private App	Non-Web	Coaching
 <p>User Group OU</p>	 <p>Managed Unmanaged</p>	 <p>Trust Score</p>	 <p>Chrome Safari Edge ...</p>	 <p>Geo Network Source Destination</p>	 <p>Browse Login Upload Share to Share from Edit Post Create ...</p>	 <p>Threat Intel AV Analysis Sandbox UEBA</p>	 <p>DLP Rules AI/ML Fingerprint Data Match</p>	 <p>App Name App Instance Category Trust Score</p>	 <p>URL Category Risk</p>	 <p>FQDN Ports IP Address</p>	 <p>80 22 21 Port Protocol IP Address</p>	<p>Allow Deny Warn Justify Isolate Redirect Step-Up</p>

- ✓ Bob@bobsbank.net is in the 'marketing' group
- ✓ Bob is using his corporate-managed laptop
- ✓ Bob has a good user trust score
- ⚠ Bob performs a number of activities, lowering his trust score
- ⚠ Bob attempts to download data from Salesforce

Bob's download is blocked, and a coaching page is displayed notifying Bob that as a risky user, his activity is non-compliant



Operationalizing Data Protection

Granular Controls Using Signals to Reduce Risk Surface Area

Implement DLP Policies



IDENTITY

- Strong Auth
- Device Trust
- Behavior Trust



APPLICATIONS

- Application Trust
- App Instance Trust
- Activity Trust



DATA

- Data in motion and at rest
- AI-powered DLP
- AI-powered auto-classification

SASE and Zero Trust – A Phased Approach

PHASE 1

PHASE 2

PHASE 3

PHASE 4

PHASE 5

Zero Trust Access

Adaptive Access

Flexible Actions

AI-powered DLP

Use Analytics to
Continuously Refine



Establish a zero-trust access baseline for internal apps

Implement continuous adaptive trust policies for SaaS

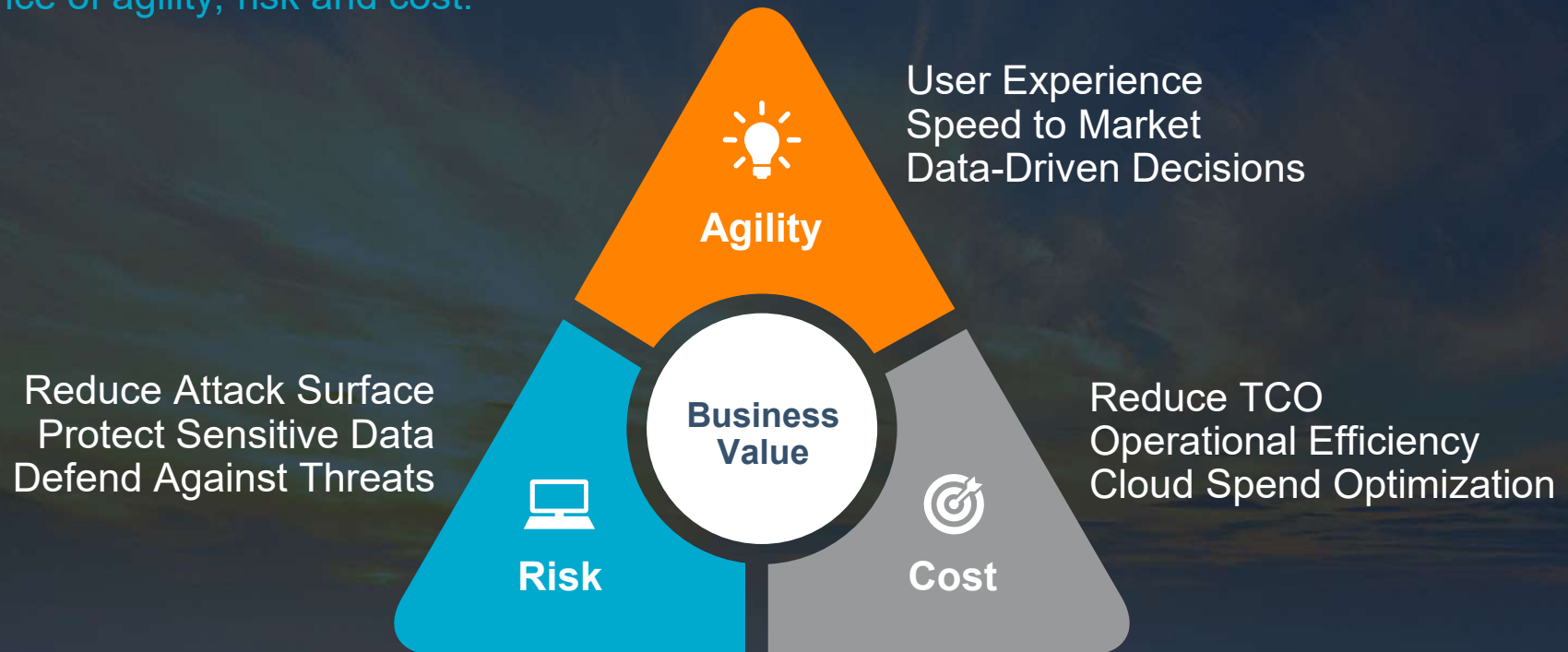
Implement actions such as block, coach, force step-up, based on use case.

Implement AI-powered DLP as part of adaptive access controls or apply to the reduced surface area after controls are in place

Use analytics to refine policy and strengthen security and trust posture

Business Value Benefits: SASE + Zero Trust

Business value is optimized by finding the right balance of agility, risk and cost.



Source: ESG; <https://www.netskope.com/lp-esg-economic-validation>

Summary

SASE combines networking and security as-as-service

Security controls follow the data and app performance follows the user

Continuous Adaptive Trust is key for aligning SASE to zero trust principles

Risk-based context applied to every transaction enables better alignment with zero trust principles

SASE + Zero Trust

Combining SASE + Zero Trust results in a much stronger and more effective security program

Thank You!



www.linkedin.com/in/bobegilbert



bob@netskope.com



[@bobegilbert](https://twitter.com/bobegilbert)