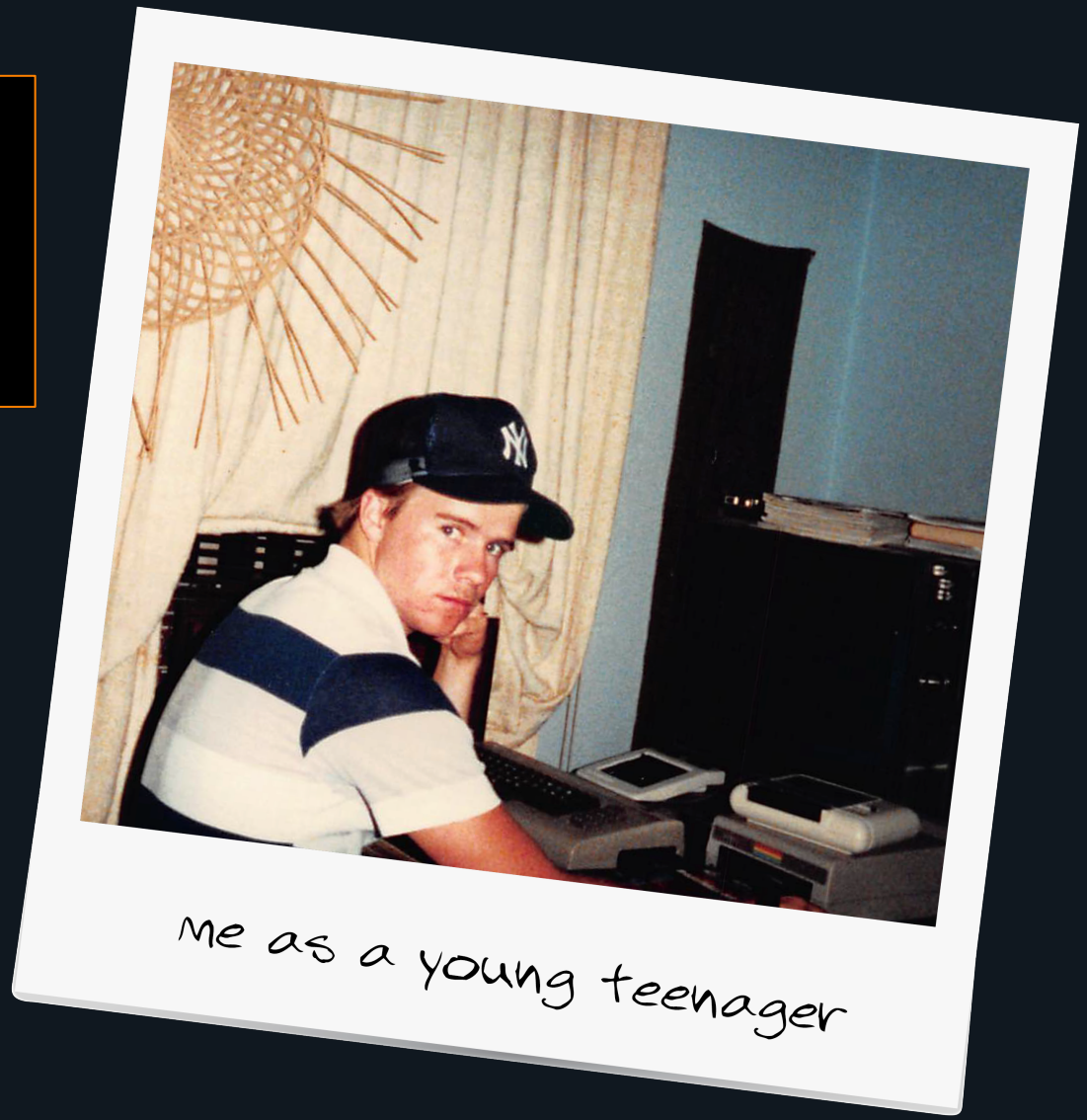
ZERO TRUST DATA PROTECTION

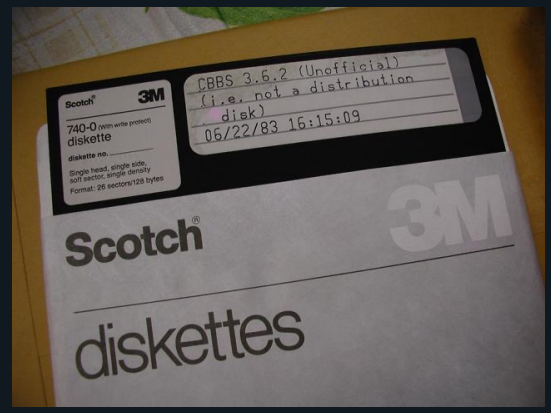
Bob Gilbert, VP & Chief Evangelist, Netskope

Circa 1983 – My first cyber security experience

Ran a Bulletin Board System (BBS) that hosted software

Developed a whitelist terminal program (assembly + Pascal) to keep out the hackers that wiped out my site

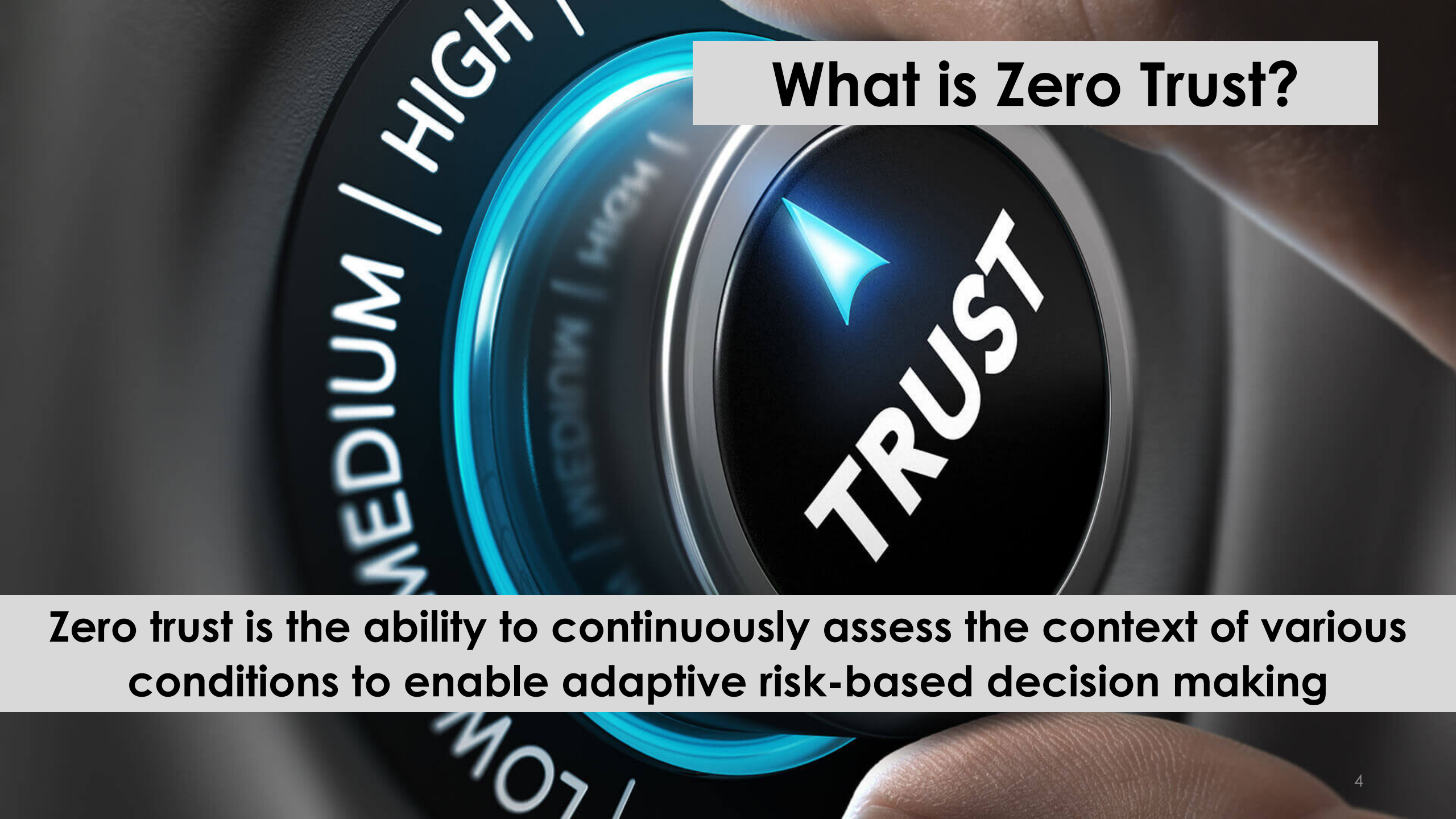




Commodore 64, 1200bps modem, 5.25in floppy storage


Charlie Ciso
We've implemented zero trust.
I don't believe you.
Exactly.
Powell/Amoroso

What is Zero Trust?



Zero trust is the ability to continuously assess the context of various conditions to enable adaptive risk-based decision making

What is a Zero Trust concept?

Zero Trust is an Architectural principle with one main purpose:

Removal of Implicit Trust

Zero Trust is:

A business enabler

A marriage of process & technology

A reduction of complexity strategy

Data and context centric

Contextual and dynamic in nature

Zero Trust is not:

A quick win

A packaged product

Only for identity or network tech

An idea where all trust is removed

A one-off or IT only centric project

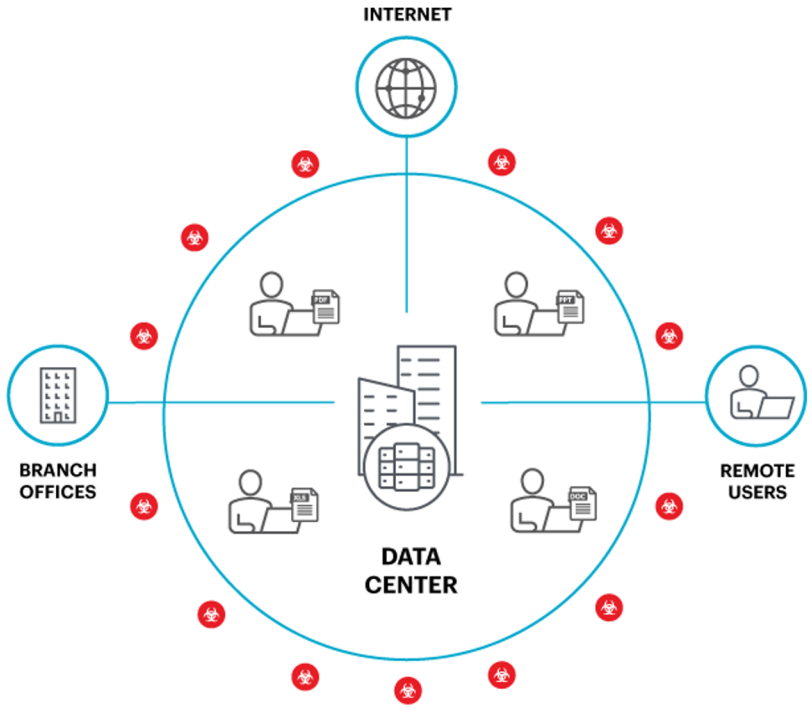
A Next-Gen perimeter

SASE (Secure Access Service Edge)

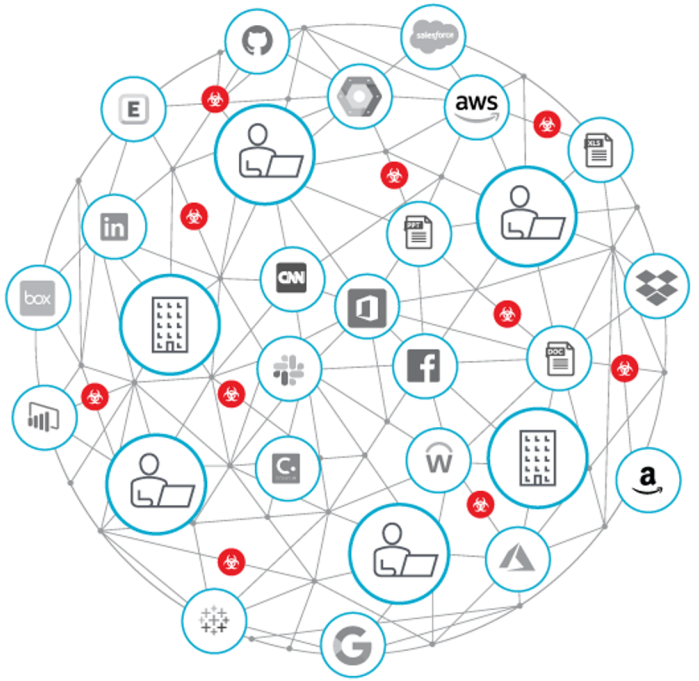
The delivery mechanism for Zero Trust

Digital Transformation Forcing a Tech Shift

Yesterday



Today



SaaS use has increased

2400+

cloud apps used by average enterprise

Data is everywhere

90%

of all data has been created within the past 2 years

Remote users will continue to work from anywhere

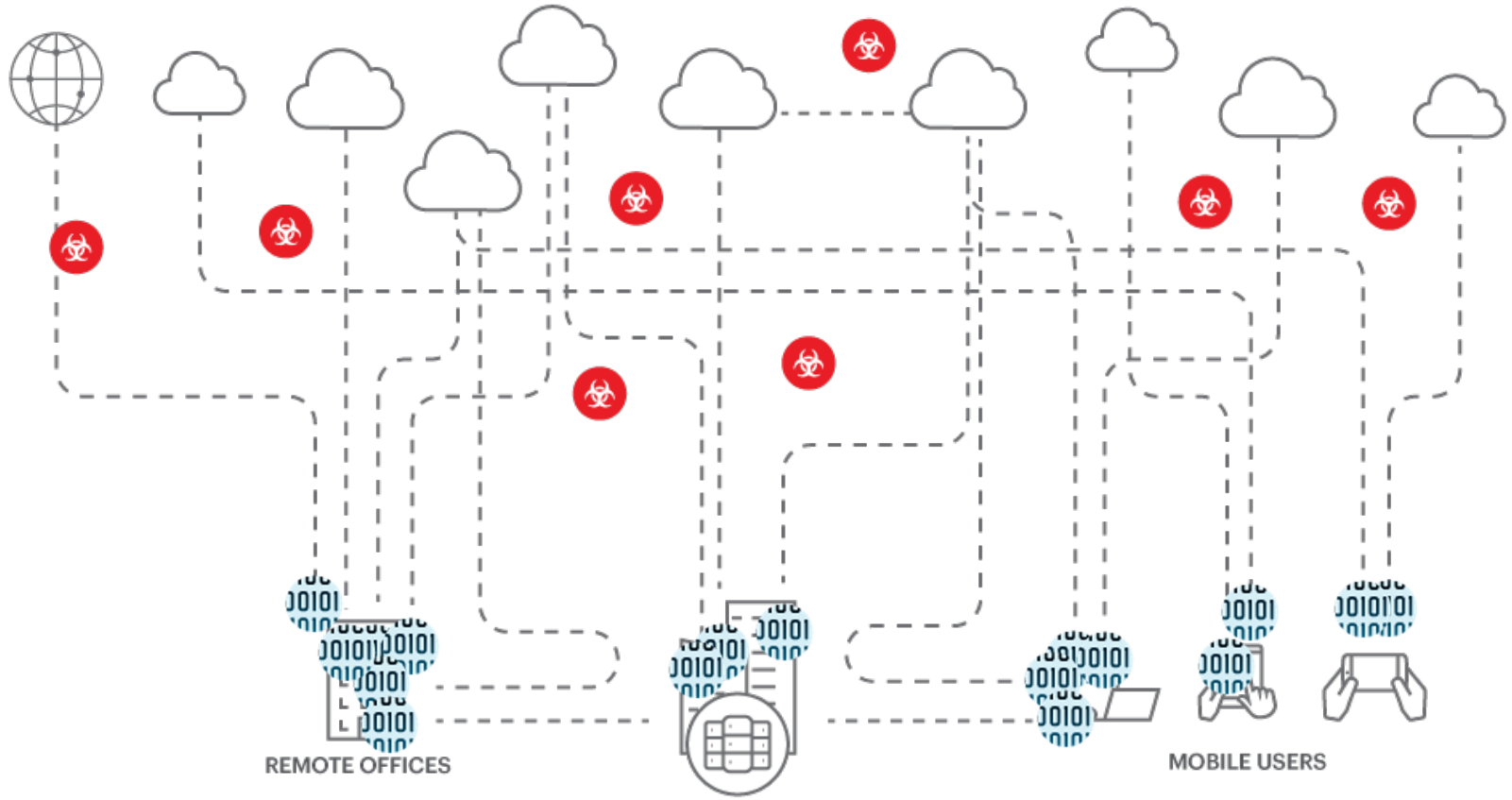
82%

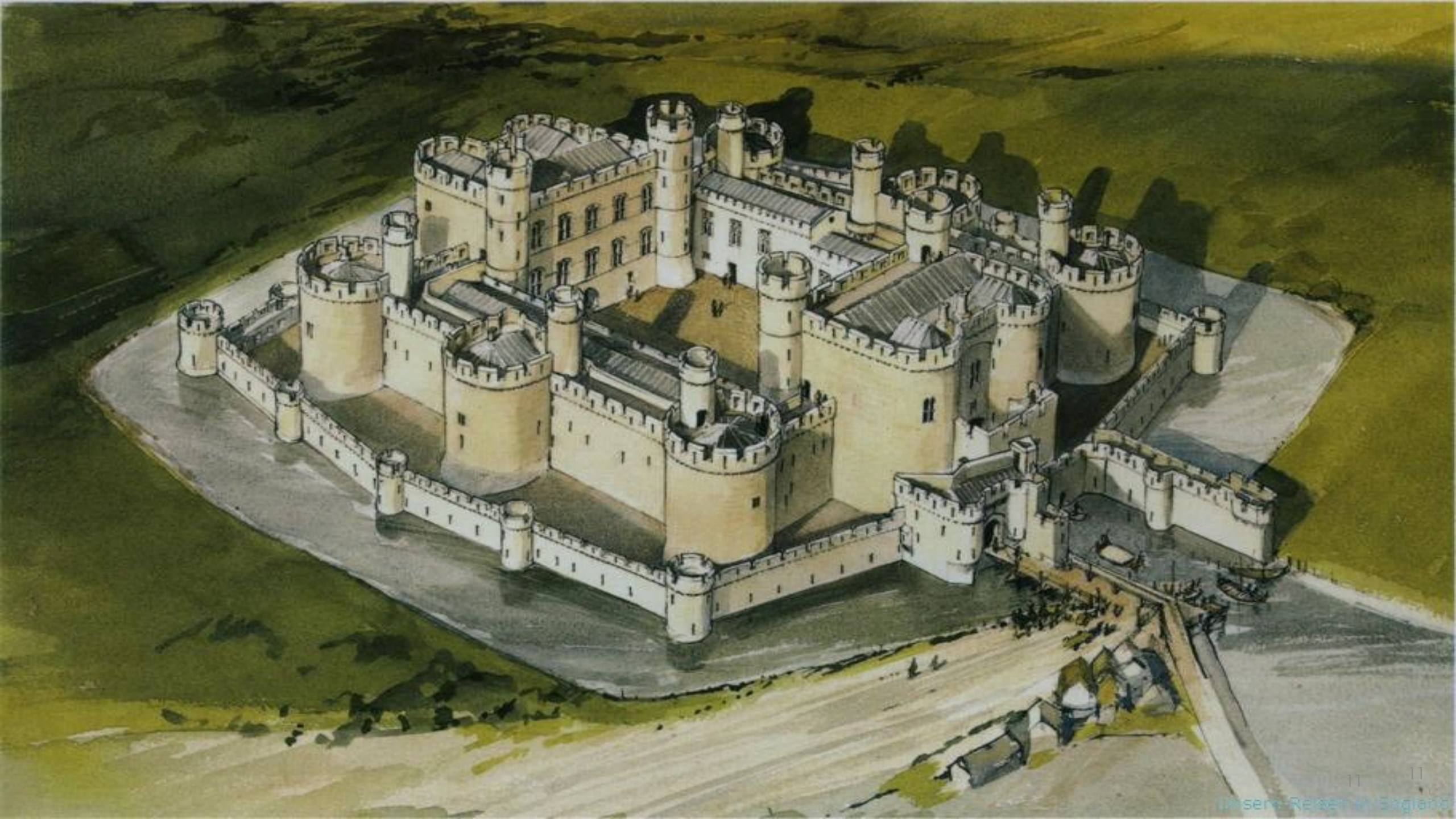
of company leaders plan to allow remote work some of the time

Digital Transformation and remote workers are driving major changes in network traffic leaving you blind to the network traffic

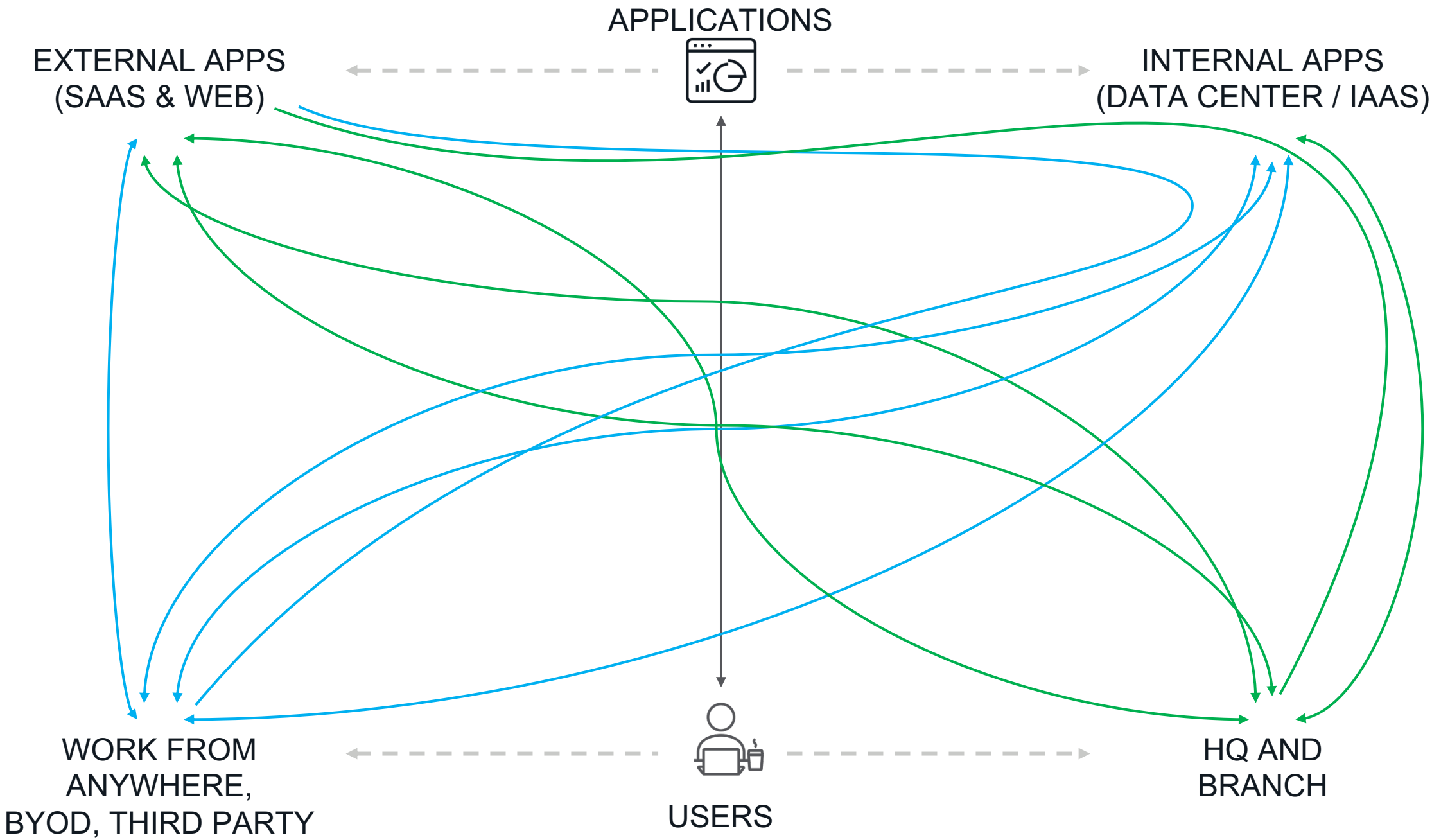
Network Traffic

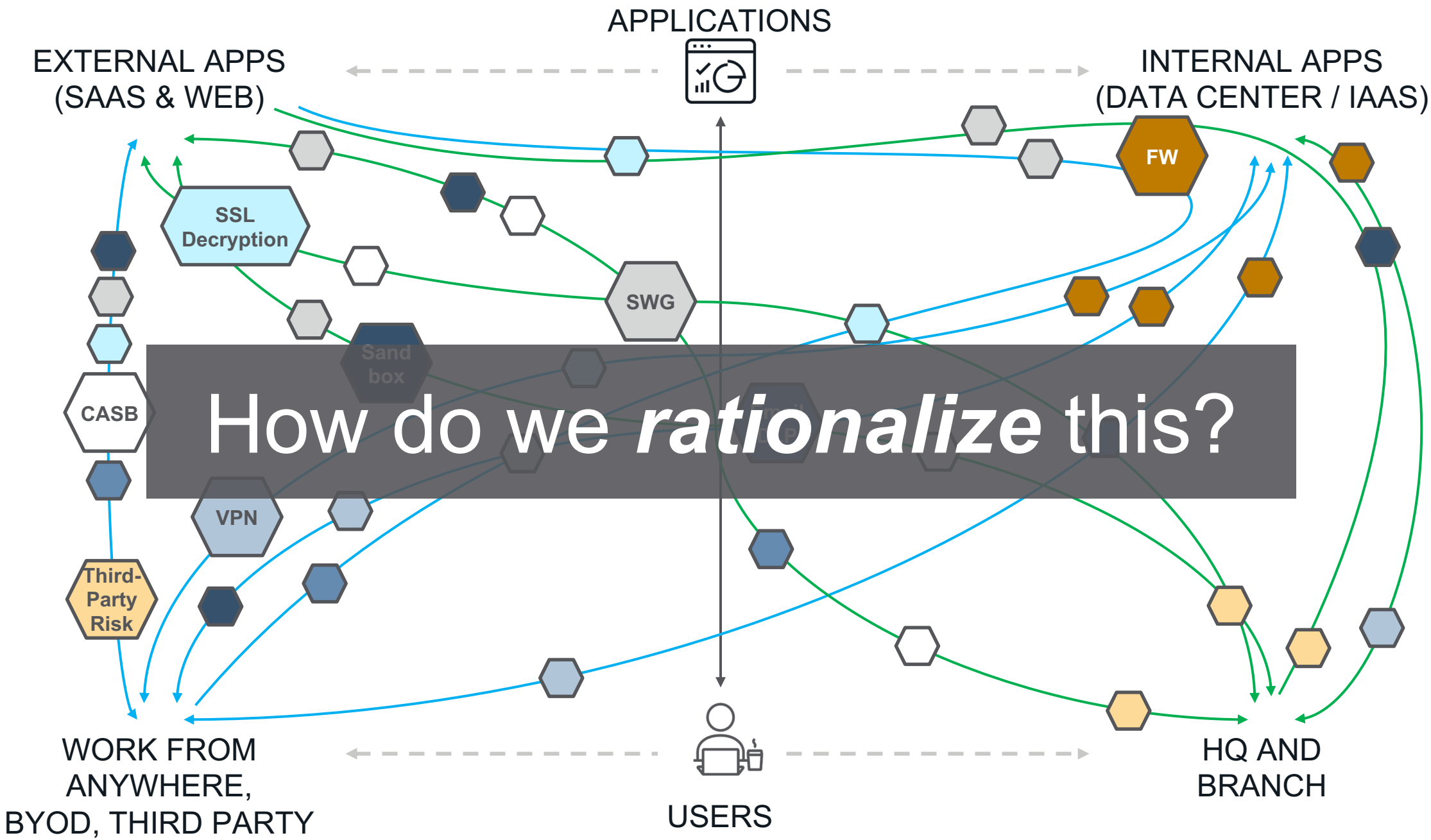
- Digital transformation is shifting network load to internet
- Remote workers change the pattern of network traffic
- Controls need to follow the data






STRICTLY
NO
ACCESS


APPLICATIONS
EXTERNAL APPS
(SAAS & WEB)
INTERNAL APPS
(DATA CENTER / IAAS)
WORK FROM
ANYWHERE,
BYOD, THIRD PARTY
USERS
HQ AND
BRANCH


APPLICATIONS
EXTERNAL APPS
(SAAS & WEB)
INTERNAL APPS
(DATA CENTER / IAAS)
FW
SSL
Decryption
SWG
Sand
box
CASB
VPN
Third-
Party
Risk
How do we *rationalize* this?
WORK FROM
ANYWHERE,
BYOD, THIRD PARTY
USERS
HQ AND
BRANCH

APPLICATIONS

EXTERNAL APPS
(SAAS + WEB)

INTERNAL APPS
(DATA CENTER / IAAS)

SECURE

DATA

ACCESS

Security Transformation

Requirements	Technology
• Data protection • Threat protection • Visibility / Risk • Compliance • Zero trust • Context	• CASB • SWG • EDR • DLP • AI/ML • UEBA

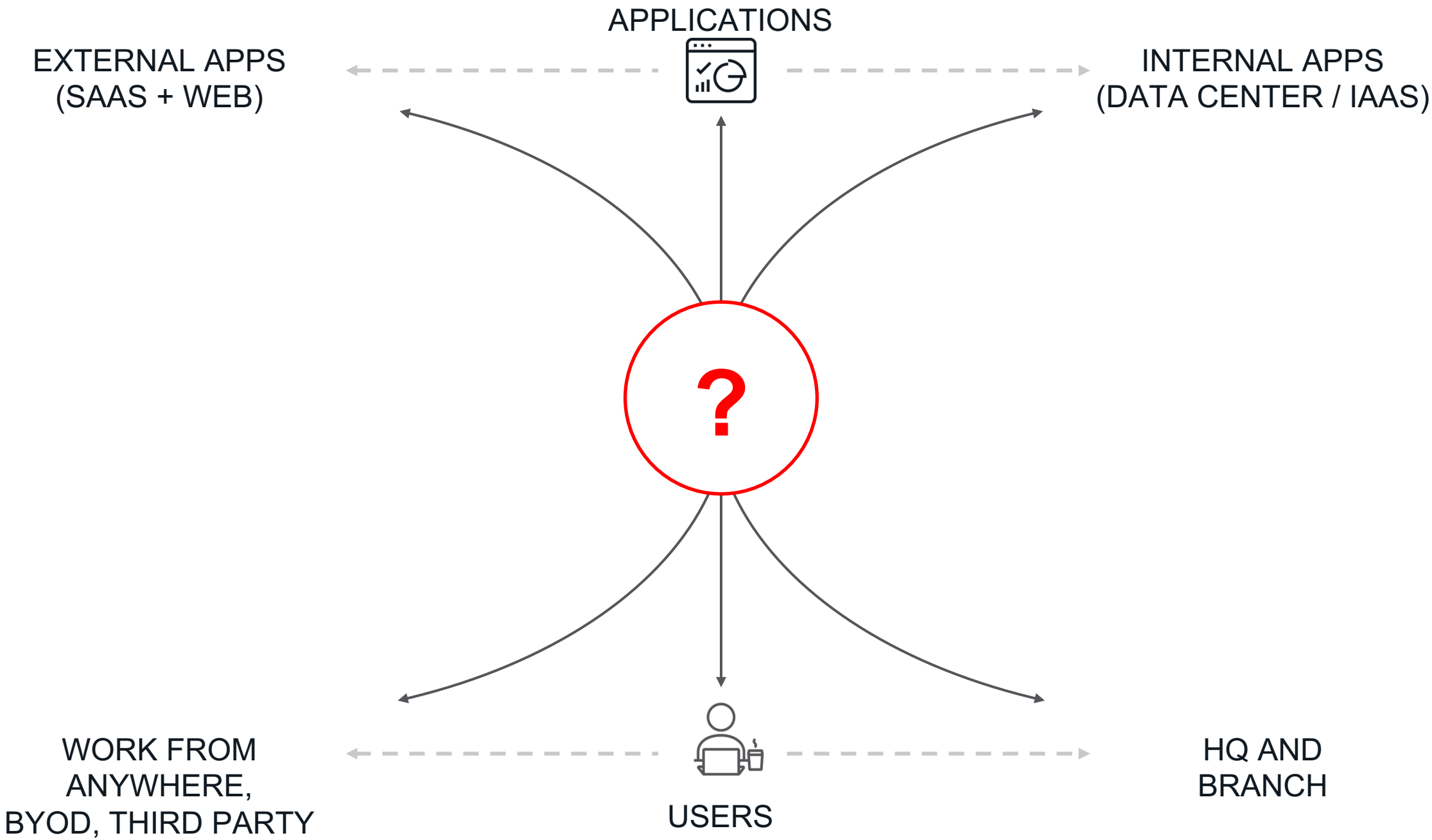
Network Transformation

Requirements	Technology
• App performance • 99.999% • Resilience • TCO • User experience	• ZTNA • SD-WAN • SWG • FW • Intelligent Routing

WORK FROM
ANYWHERE,
BYOD, THIRD PARTY

USERS

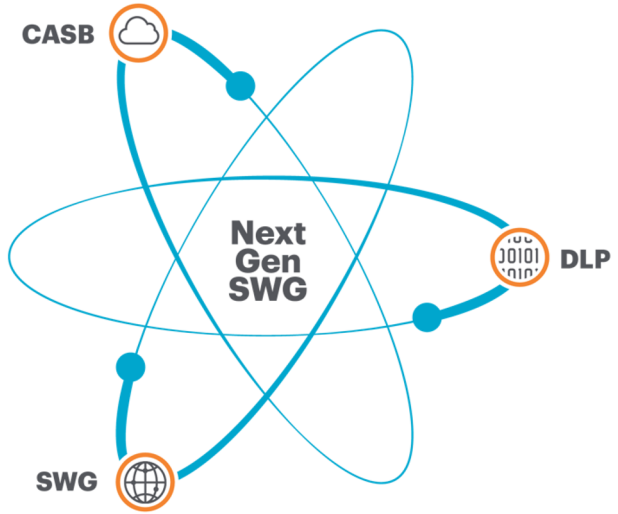
HQ AND
BRANCH


APPLICATIONS
EXTERNAL APPS
(SAAS + WEB)
INTERNAL APPS
(DATA CENTER / IAAS)
?
WORK FROM
ANYWHERE,
BYOD, THIRD PARTY
USERS
HQ AND
BRANCH

APPLICATIONS

EXTERNAL APPS
(SAAS + WEB)

INTERNAL APPS
(DATA CENTER / IAAS)



WORK FROM
ANYWHERE,
BYOD, THIRD PARTY

USERS

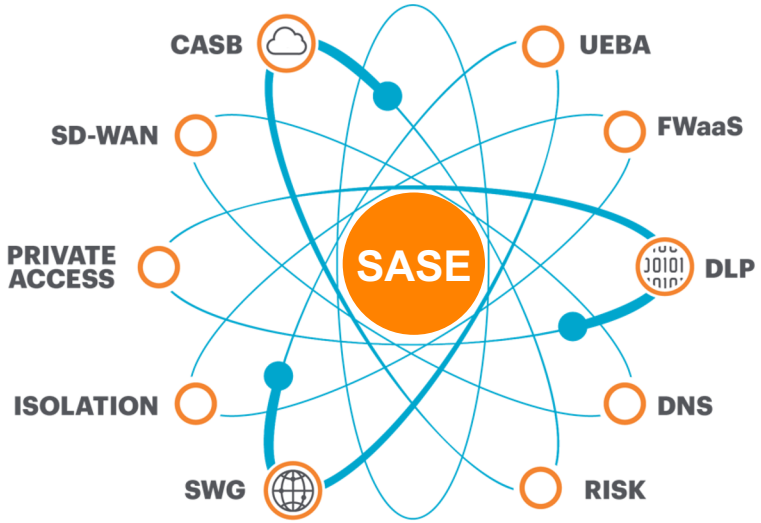
HQ AND
BRANCH

APPLICATIONS

EXTERNAL APPS
(SAAS + WEB)

INTERNAL APPS
(DATA CENTER / IAAS)

Single Agent, Single Console
Single Pass



Highly Performant, Peered Security
Cloud Network

WORK FROM
ANYWHERE,
BYOD, THIRD PARTY

USERS

HQ AND BRANCH
OFFICE LOCATIONS

Starting on a Zero Trust Journey

What to Consider Before Implementing Zero Trust:

You must architect with your business in mind first

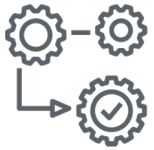
Understand your technology stack, process, and capability gaps

Understand your threats and risk

Understand your end user requirements (transparency, easy of use, availability, etc.)

A Path to Implement Zero Trust Principles:

Understand your information assets by both sensitivity and criticality



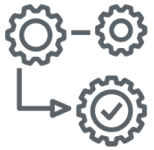
Understand the user population that requires access

Identify applications that you want to expose first - start with low risk applications and determine what will give the biggest value return

Understand and start grouping key business user populations and core application combinations

A Path to Implement Zero Trust Principles:

Begin defining business rules for access - Starting with coarse grained controls first using hierarchy of information asset ratings

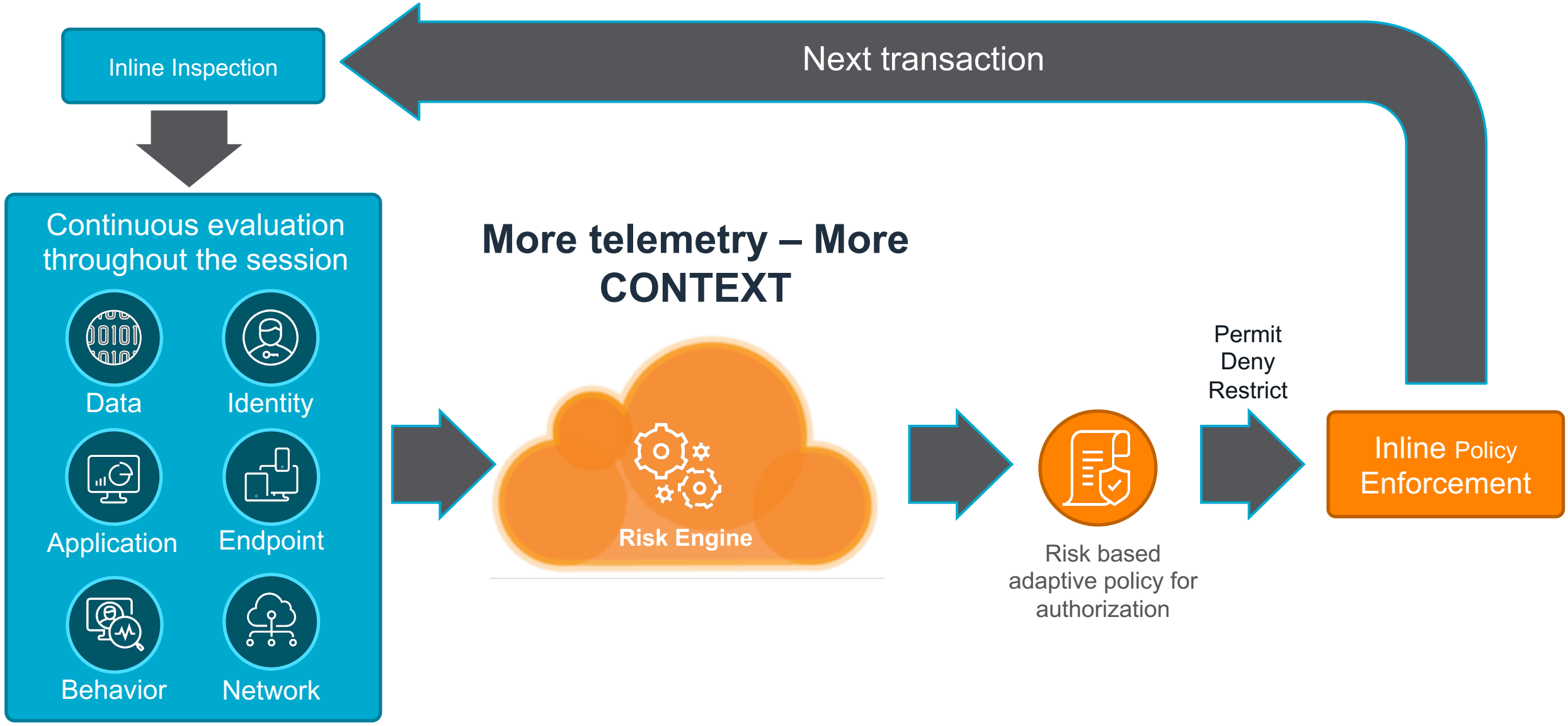


Define differentiated controls for high risk users – overlaying these additional controls as you work through the user population

Implement controls into the form of policies that can be applied within the relevant technology platform(s)

Revoke access to previous VPN/RAS services when users have been fully on-boarded

Zero Trust Data Protection Architecture



Adaptive Trust

Trust	Level 1	Level 2	Level 3	Level 4	Level 5
Access Activity	Non-Sensitive Data (Read Only)	Non-Sensitive Data (Read & Write)	Limited Sensitive Data (Read)	Sensitive Data (Read & Write)	Sensitive Data (Read & Write & Store on Device)
Identity	Limited Access Validation	Multifactor Authentication	Multifactor Authentication	Time Based Multifactor Authentication	Event Based Multifactor Authentication
Endpoint	Unmanaged Device	Unmanaged Device	Unmanaged Device	Unmanaged Device	Managed Device
Application	Unsanctioned App	Unsanctioned App	Sanctioned App	Sanctioned App	Sanctioned App
Example	*Social Media*	*Google Drive, Box, Office365*	*Confidential Reports*	*Email*	*HR Data, Board Materials, Large Database*

Benefits of Zero Trust

Zero trust *drastically* decreases an organization's risk posture

Prevention of lateral movement

Predefined application/ resource access governance

Provide conditional/ least privileged access only

Gain massive visibility and control within your ecosystem

Enables the ability for risk-based decision making at scale

5-step Zero-Trust Implementation Strategy

Stages

1 Discover

Understand your unique organizational needs – assets, users, apps

2 Prioritize

Prioritize findings and align with business requirements

3 Protect

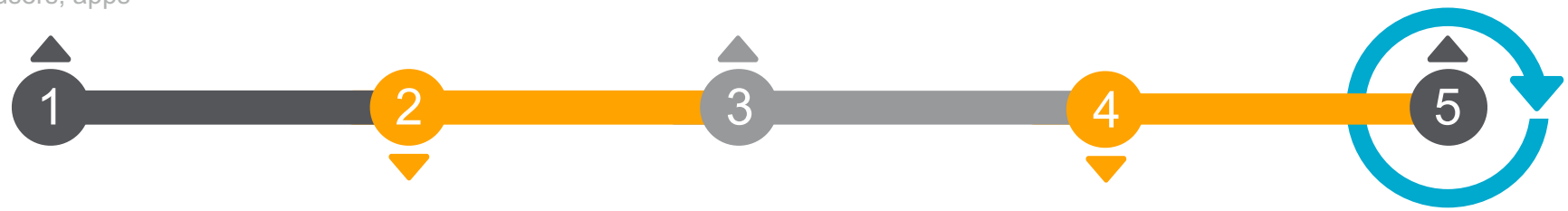
Implement technology and policies to enable continuous risk assessment

4 Educate

Safely enable services across the enterprise

5 Govern

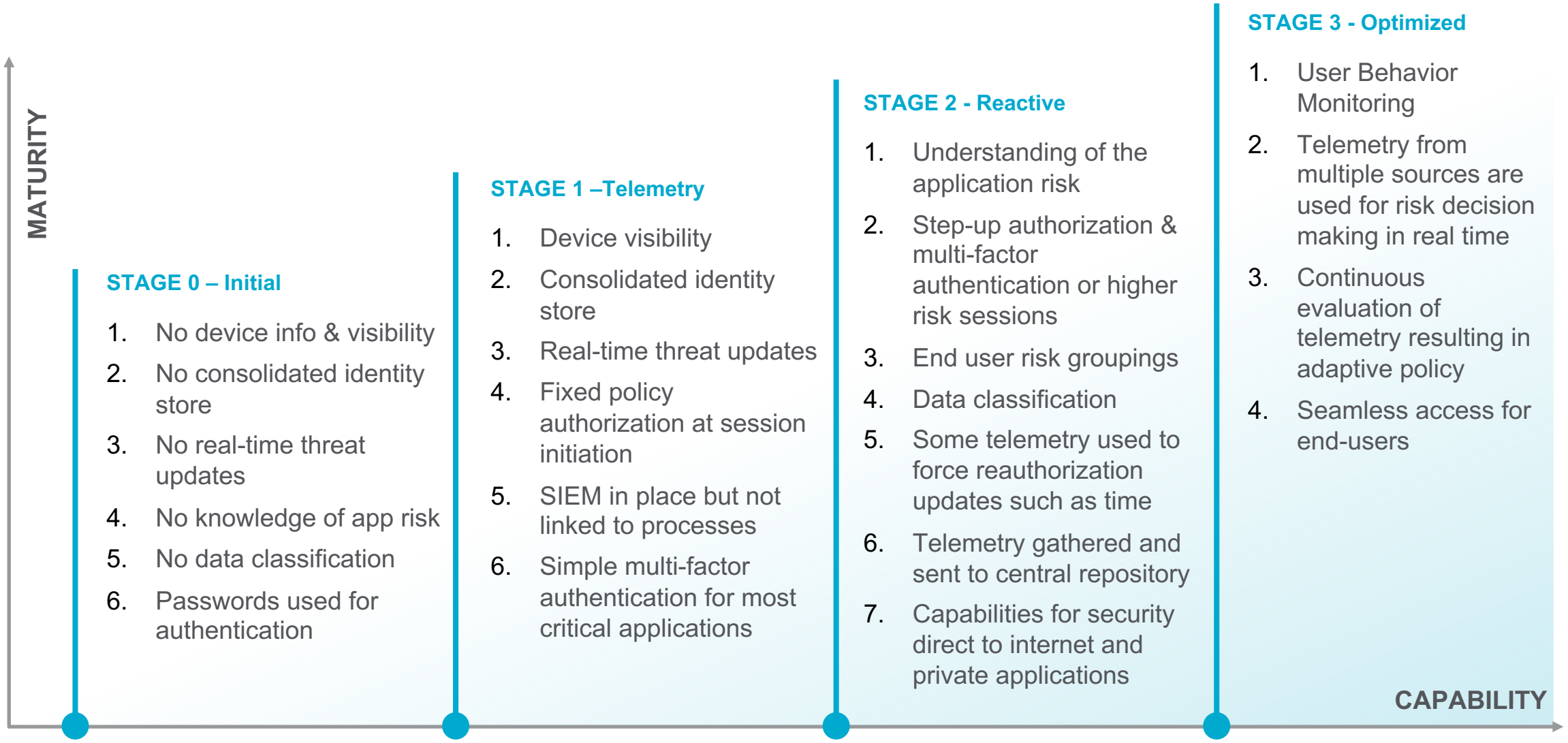
Govern services and data through continuous assessment



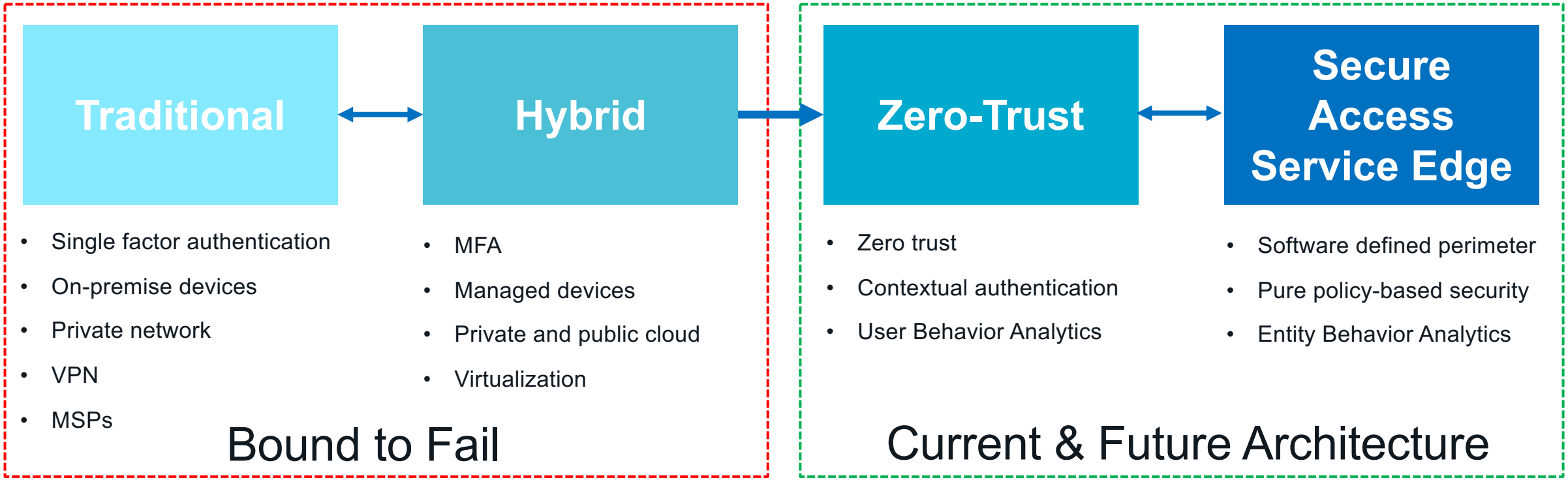
Deliverables

- 1. Understand your assets by criticality and sensitivity
- 2. Understand the user population access needs
- 3. Identify priority applications – risk or consumption driven
- 4. Understand and start grouping key user populations and core application combinations
- 5. Start with coarse grained controls first and refine over time
- 6. Implement these into enforceable policies that can be applied
- 7. Add differentiated controls to the user population
- 8. Revoke access to previous VPN/RAS services when users have been on-boarded into above
- 9. Report exposure to data owners
- 10. Identify broken business processes
- 11. Report on cloud security program and measure risk buy-down improvements
- 12. Continually look for changes to profile or new high-risk issues – continuous policy refinement

Zero Trust Maturity



Our Next “New Normal” in Cyber Security



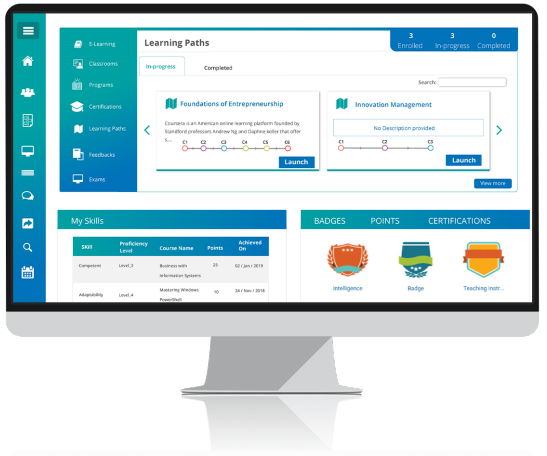
How are you transitioning back and what is your new normal?

Live Demo of 10 Common Zero Trust Scenarios

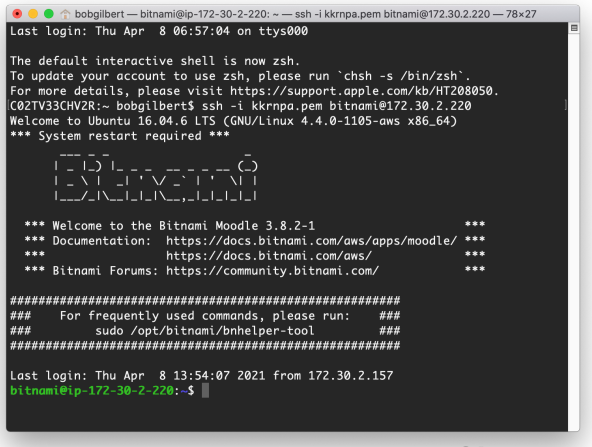
Zero Trust access to Internal App Hosted in AWS

Concern: Bad actors gain access and move laterally

Bob in marketing needs browser access to internal LMS app



Frank, a sysadmin, needs SSH access to internal LMS app



Scenario 1: A member of the marketing team, Bob needs browser access to his company's internal Learning Management System that is hosted in AWS

Access Requested	Identity ✓	+	Device ✓	+	Port/ Protocol ✓	=	Contextual Response (Allow/Deny Access)
Browser access to LMS app	bob@bobsbank.net is in the marketing group		Bob is using a managed laptop with encryption and CrowdStrike endpoint enabled		Access to port 80,443		**Bob is granted browser access to the internal LMS app**

Old way: *Make app publicly accessible or provide VPN access, enabling Bob to move laterally*

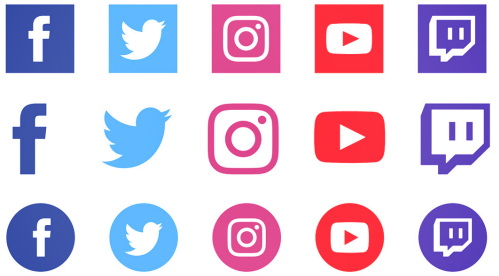
Scenario 2: A member of the Sysadmin team, Frank needs SSH access to his company's internal Learning Management System that is hosted in AWS

Access Requested	Identity ✓	+ Device ✓	+ Port/ Protocol ✓	= Contextual Response (Allow/Deny Access)
SSH access to LMS app	frank@bobsbank.net is in the sysadmin group	Frank is using a managed laptop with encryption and CrowdStrike endpoint enabled	SSH, requiring access to port 22	**Frank is granted SSH access to the internal LMS app**

Old way: *Make app publicly accessible or provide VPN access, enabling Frank to move laterally*

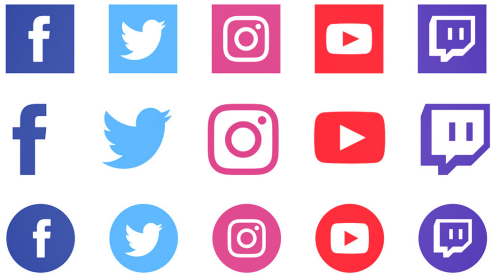
Zero Trust data protection when using social media

Finance team needs access to social media so they can follow companies



Concern: FINRA compliance

Marketing team needs full access to social media so they can post, retweet, and comment as part of social campaigns



Scenario 3: Social media is blocked company-wide because of FINRA compliance, but Finance team needs view-only access to get their job done

Access Requested	Identity	+	Device	+	App	+	Activity	=	Contextual Response (Allow/Deny Access)
Adele in finance is attempting to view social media posts	✓ adele@bobsbank.net is a member of the finance group		✓ Adele is using a managed laptop with encryption and CrowdStrike endpoint enabled		✓ **App:** Twitter **Cat:** Social **App Risk:** Low		✓ Login View		**Adele is granted view access to social media apps**
Post to Twitter	✓ •••		✓ •••		✓ •••		? Post		**Adele is blocked from posting to Twitter**

Old way: *Block social media outright or face risk of FINRA violation*

Scenario 4: Social media is blocked company-wide because of FINRA compliance, but Marketing team needs full access to get their job done.

Access Requested	Identity	+	Device	+	App	+	Activity	+	Data	=	Contextual Response (Allow/Deny Access)
Bob in Marketing is attempting to post to Twitter	✓ bob@bobsbank.net is a member of the marketing group		✓ Bob is using a managed laptop with encryption and CrowdStrike endpoint enabled		✓ **App:** Twitter **Cat:** Social **App Risk:** Low		✓ **Post**		✓ Opinion about NCAA bracket		**Bob is granted access to social media apps and can post to Twitter**
Bob in Marketing is attempting to post sensitive data to Twitter	✓ •••		✓ •••		✓ •••		✓ **Post**		? stock recommendation		**Bob is blocked from posting FINRA violations to Twitter**

Old way: *Block social media outright or face risk of FINRA violation*

Zero Trust data protection when using risky cloud apps

Bob in marketing wants access to a popular cloud storage app so he can quickly upload and share data

Concern: Data loss and malware

Scenario 5: Bob wants to access a popular cloud storage app so he can quickly upload and share data.

Access Requested	Identity ✓	+ Device ✓	+ App ?	+ Activity ?	= Contextual Response (Allow/Deny Access)
Bob in Marketing is attempting to access Zippyshare	bob@bobsbank.net is a member of the marketing group	Bob is using a managed laptop with encryption and CrowdStrike endpoint enabled	**App:** Zippyshare **Cat:** Cloud Storage **App Risk:** High	**Login**	**Bob is blocked from accessing Zippyshare and is redirected to OneDrive install page**

Old way: *Blunt force blocking of cloud apps*

Zero Trust data protection for risky users

Adele's contract with the company is ending and she wants to download data from the company OneDrive

OneDrive for Business

Concern: Data loss/theft

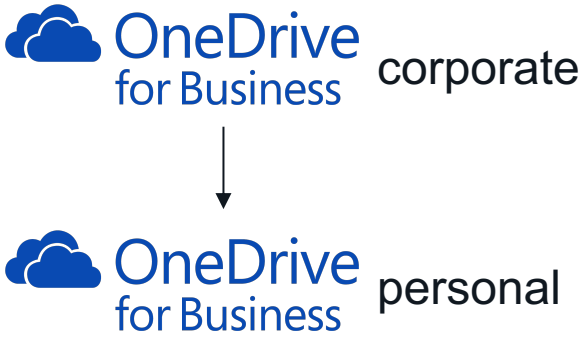
Scenario 6: Adele's contract with the company is ending and she wants to download data from the company OneDrive

Access Requested	Identity ?	+	Device ✓	+	App ?	+	Activity ?	=	Contextual Response (Allow/Deny Access)
Adele, a contractor, is attempting to download and share data in OneDrive	adele@bobsbank.net is a contractor **User Risk:** High because of past behavior		Adele is using a managed laptop with encryption and CrowdStrike endpoint enabled		**App:** O365 OneDrive **Cat:** Cloud Storage **App Risk:** Low		**Download**		**Adele is blocked from downloading data from OneDrive**

Old way: *Coarse-grained access controls*

Zero Trust data protection for unintentional or unapproved data movement between cloud apps

Bob wants to download data from the corporate Office 365 OneDrive account and upload it to his personal instance of O365 OneDrive



Concern: Data loss

Scenario 7: Bob wants to download data from the corporate Office 365 OneDrive account and upload it to his personal instance of O365 OneDrive

Access Requested	Identity	+	Device	+	App	+	Activity	+	Data	=	Contextual Response (Allow/Deny Access)
	✓		✓		✓		✓		✓		
Bob in marketing is attempting to download data from OneDrive	bob@bobsbank.net is a member of the marketing group		Bob is using a managed laptop with encryption and CrowdStrike endpoint enabled		**App:** O365 OneDrive **Instance**: Corporate **Cat:** Cloud Storage **App Risk:** Low		**Download**		confidential data		**Bob's download from the corporate OneDrive is allowed**
	✓		✓		?		?		?		
Bob in marketing is attempting to upload confidential data to OneDrive	•••		•••		**App:** O365 OneDrive **Instance**: Personal **Cat:** Cloud Storage **App Risk:** Low		**Upload**		confidential data		**Bob's upload to unmanaged OneDrive is blocked**

Old way: *Block Office 365 instances!*

Zero Trust data protection when sharing, posting, creating, editing data in cloud apps

Bob wants to share his credit card info in Slack and in the company's O365 OneDrive account so his team can use it to buy marketing schwag

OneDrive for Business

slack

Concern: Data loss

Scenario 8: Bob wants to share his credit card info in Slack and in the company's O365 OneDrive account so his team can use it to buy marketing schwag

Access Requested	Identity	+	Device	+	App	+	Activity	+	Data	=	Contextual Response (Allow/Deny Access)
Bob in marketing is attempting to post credit card data to a public Slack channel	✓ bob@bobsbank.net is a member of the marketing group		✓ Bob is using a managed laptop with encryption and CrowdStrike endpoint enabled		✓ **App:** Slack **Instance**: Public **Cat:** Collaboration **App Risk:** Low		✓ **Post**		? PCI		**Bob's Post activity in Slack is blocked**
Bob in marketing is attempting to edit content in OneDrive and paste in credit card data	✓ •••		✓ •••		✓ **App:** O365 OneDrive **Instance**: Corporate **Cat:** Cloud Storage **App Risk:** Low		✓ **Edit**		? PCI		**Bob's edit activity in O365 OneDrive is blocked**

Old way: *Block Slack*

Zero Trust data protection for unmanaged devices

Adele, a contractor, wants to download data from the company's Box account to her personal laptop

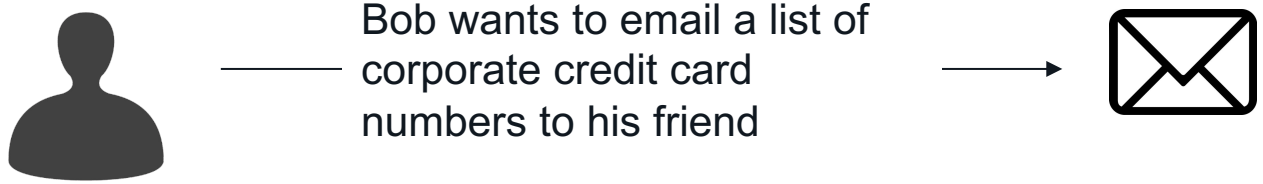
Concern: Data loss via device not managed by IT and malware coming from unmanaged device

Scenario 9: Sensitive data downloaded from the corporate Box account to a device not managed by IT

Access Requested	Identity	+	Device	+	App	+	Activity	+	Data	=	Contextual Response (Allow/Deny Access)
Adele is a contractor and is attempting to download the latest presentation from Box to her personal device	✓ Adele is a contractor		✓ Adele is using a device not managed by IT		✓ **App:** Box **Cat:** Cloud Storage **App Risk:** Low		✓ **Download**		✓ benign pptx		**Adele's download of the benign data is allowed**
Adele is a contractor and is attempting to download confidential data from Box to her personal device	✓ •••		? •••		✓ **App:** Box **Cat:** Cloud Storage **App Risk:** Low		✓ **Download**		? PCI		**Adele's download of the PCI data is blocked**

Old way: *Block unmanaged devices*

Zero Trust data protection for email



Concern: Data loss via email

Scenario 10: Sensitive data sent via email to a recipient outside of the company

Access Requested	Identity	+	Device	+	App	+	Activity	+	Data	=	Contextual Response (Allow/Deny Access)
	?		✓		✓		✓		?		
Bob in marketing is attempting to send an email containing credit cards data, to his friend's Gmail address	From user is Bob in marketing To user is frank@gmail.com		Bob is using a managed laptop with encryption and CrowdStrike endpoint enabled		**App:** Gmail **Cat:** Email **App Risk:** Low		**Send**		PCI		**Bob's email containing PCI data is blocked**

Old way: *Enable DLP and block sensitive data without to user context*

Key Takeaways

Zero trust is the ability to continuously assess the context of various conditions to enable adaptive risk-based decision making

1

Zero Trust Model

The Zero Trust Model is changing to a continuum of trust levels to support a user from any location, to any device, using any application and contextual sharing of information.

2

Zero Trust Data Protection

Zero trust is more than granting secure access. It is about using context to continuously verify trust when activities are being performed. Data protection is the #1 goal.

3

SASE is a Requirement for Successful Zero Trust

SASE enables you to move the control and zero trust decision point wherever the user and data goes as they access websites, cloud apps, and internal apps.

Thank You!

Connect with me:

https://www.linkedin.com/in/bobegilbert

@bobegilbert

bob@netskope.com

Must-read zero trust white paper:

https://resources.netskope.com/cloud-security-solution-white-papers/zero-trust-leading-practice

Authors: Vladimir Klasnja
David Fairman