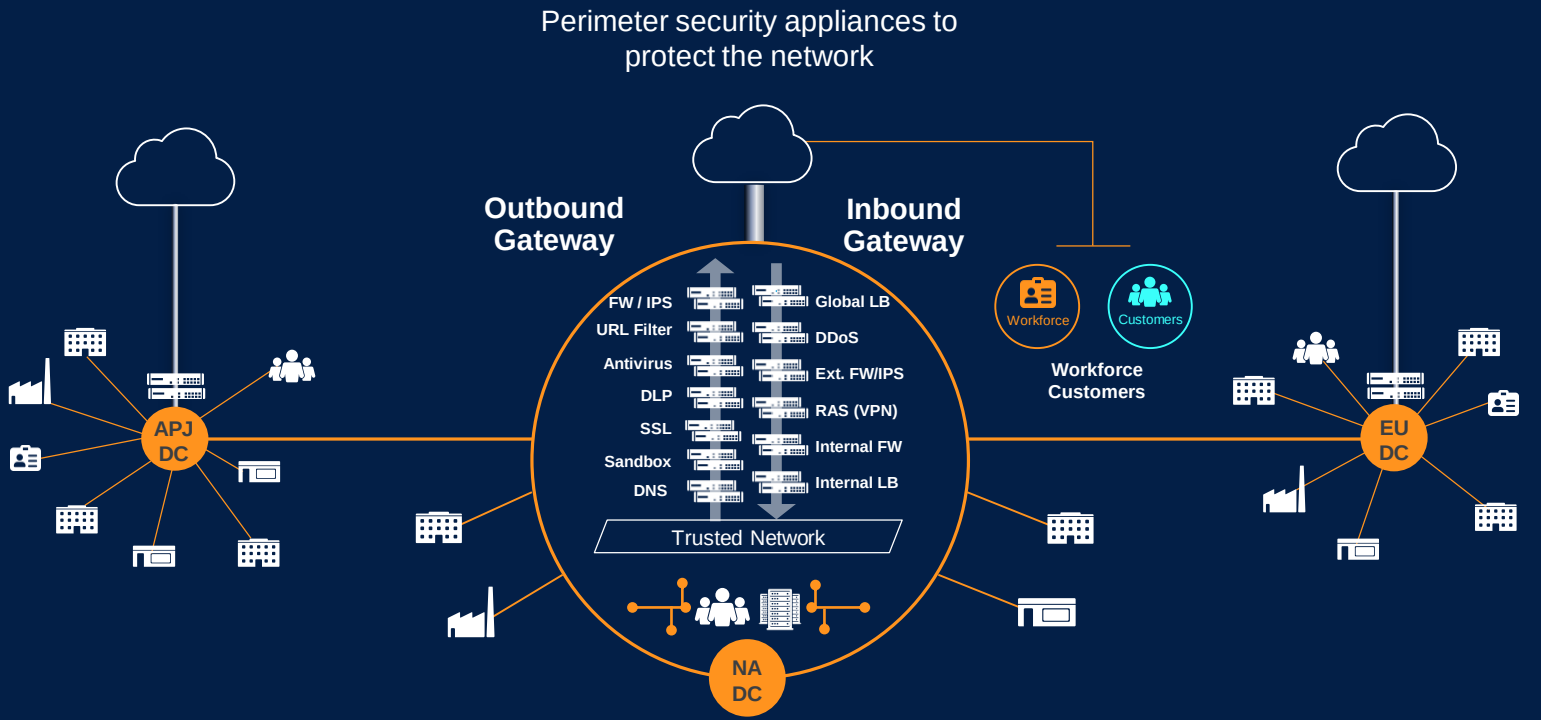
Security as a Service & Microsoft 365

Nils Ullmann

June 2020

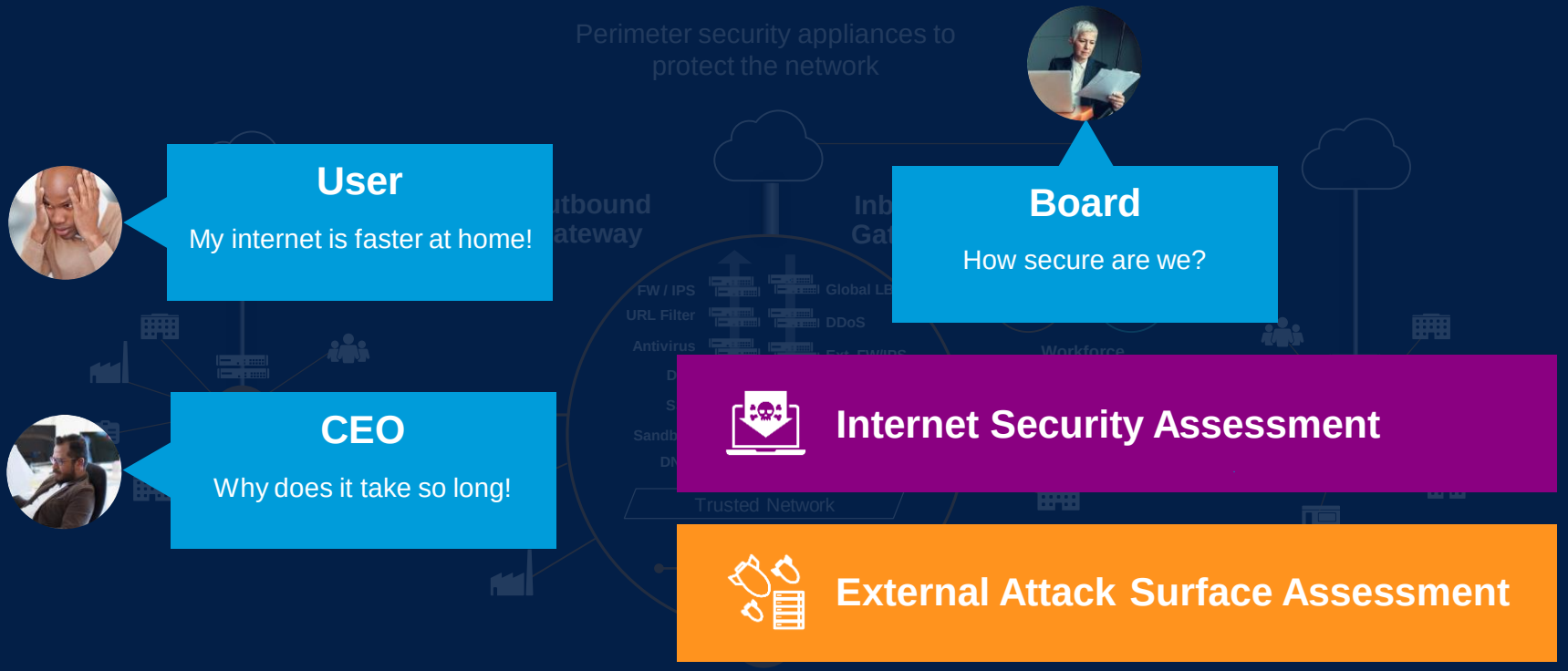
This model worked well in the old world

Internal networks were built and optimized to connect users to apps in the data center



This model worked well in the old world

Internal networks were built and optimized to connect users to apps in the data center



User

My internet is faster at home!

CEO

Why does it take so long!

Board

How secure are we?

Internet Security Assessment

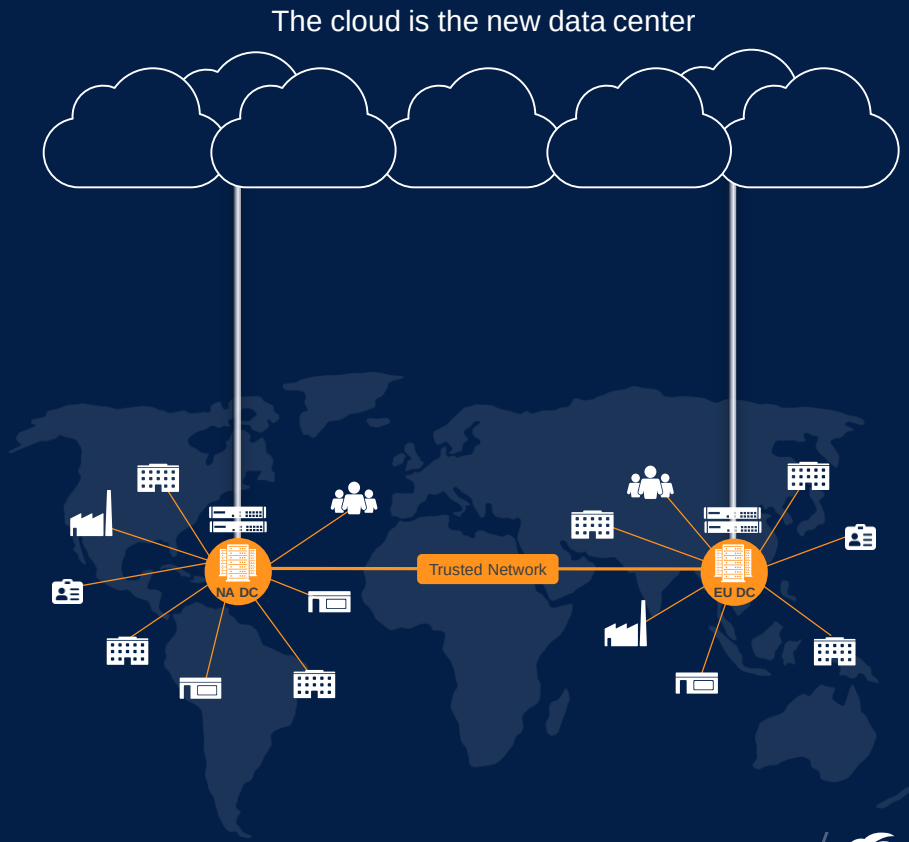
External Attack Surface Assessment

An opportunity for IT to empower the business

Application Transformation

Data Center to Cloud

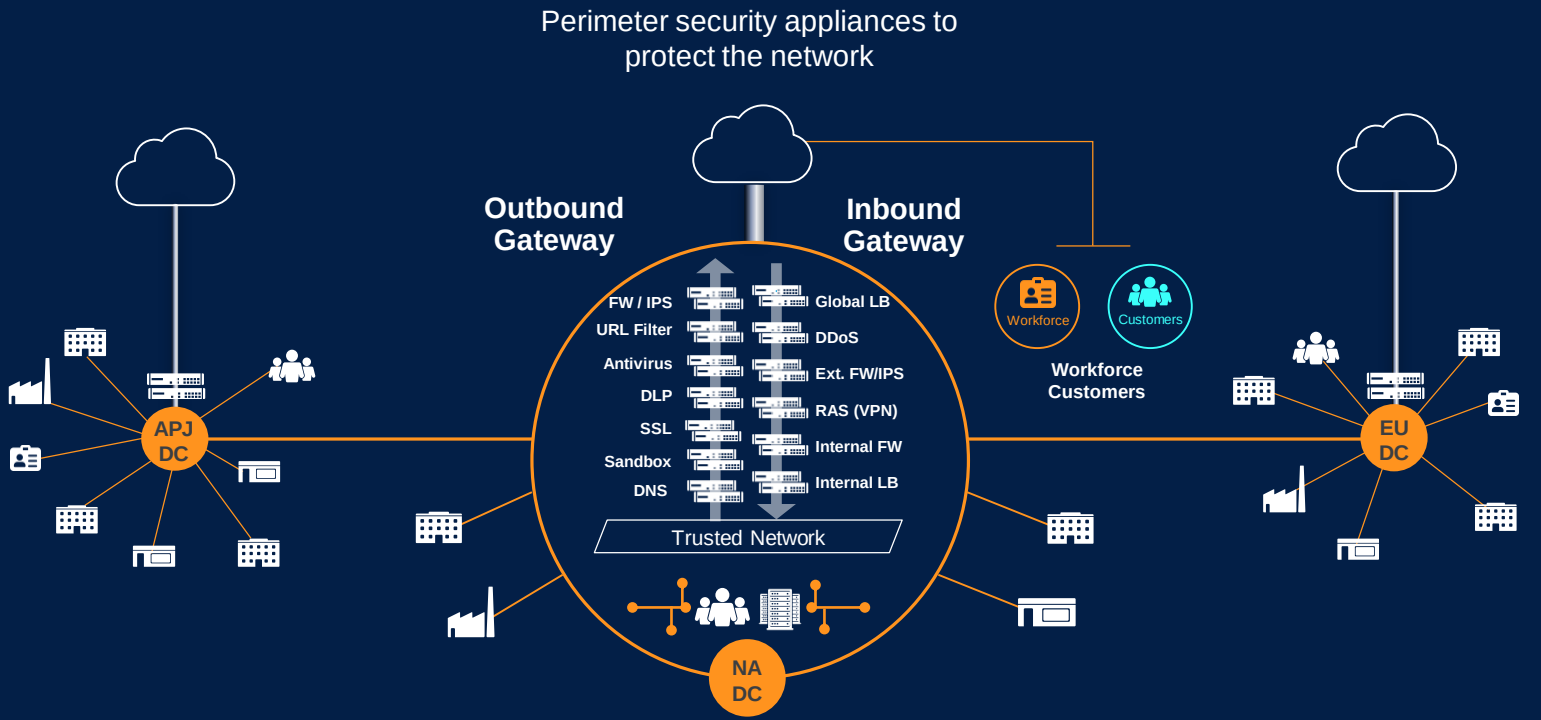
Facilitates collaboration
New business models
Simplifies IT



The Problem: Microsoft 365

This model worked well in the old world

Internal networks were built and optimized to connect users to apps in the data center



… the biggest megashift

MAINFRAME

1980s

CLIENT / SERVER

SIEBEL

PeopleSoft

1990s

INTERNET / MOBILITY

2000s

CLOUD

2010s

Default Route?

Public DNS?

Latency?

Dedicated Proxy Support?

Windows-as-a-Service (aka Windows 10)

- first OS build from ground up for the Cloud
  - *many functions to improve Cloud usage, but also functionality based on the Cloud*

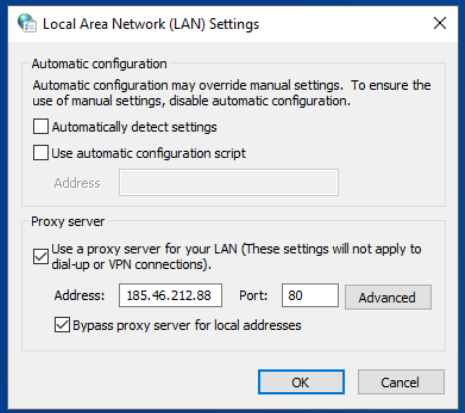
- breaks traditional software and hardware deployment cycles
  - monthly *Quality Updates* (~ 1 Gbyte)
  - semiannual *Feature Updates* (~ 3,5 Gbyte)
  - Roughly 20 Gbyte per client per year
  - *Application owner and delivery teams have to adopt agile development processes because of the frequency of the updates or shift the applications to the Cloud as well*

- Doesn't like proxies anymore / gardening for default route / direct Internet access recommend

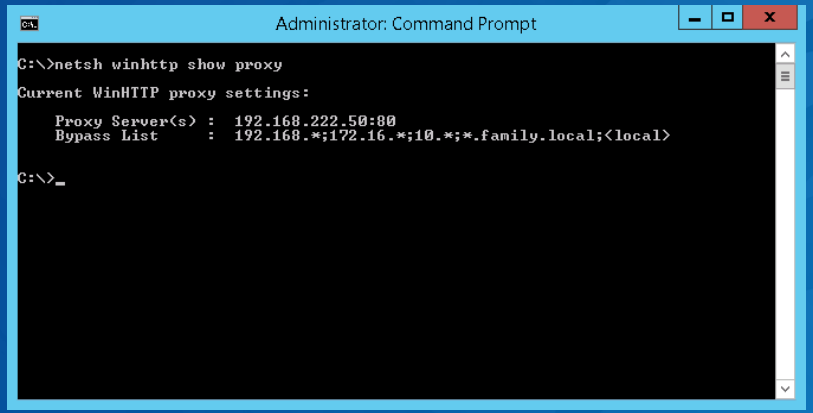
Windows 10 - Internet access

Microsoft offers two different APIs to access the Internet

WinINet



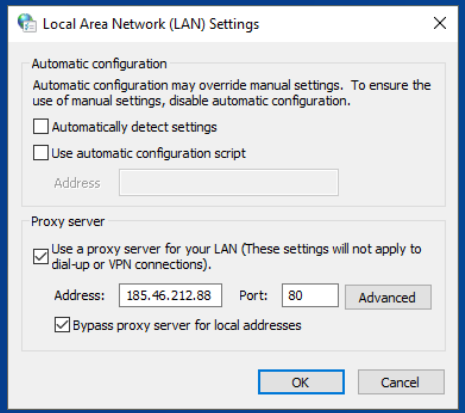
WinHTTP



Windows 10 - Internet access

Microsoft offers two different APIs to access the Internet

WinINet



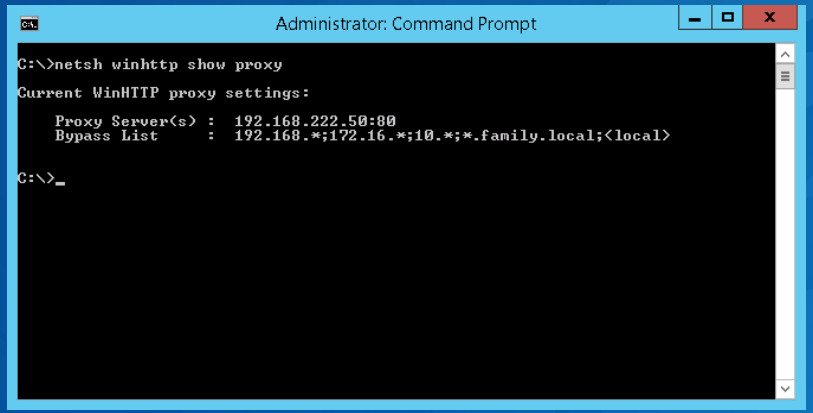
- for interactive user applications
- manual / gpo / proxy.pac / wpad / direct / auto-detect (default)

Windows 10 - Internet access

Microsoft offers two different APIs to access the Internet

- designed for services
- independent from WinINet
- different supported feature set
- manual / wpad / registry / **direct (default)**

WinHTTP



Windows 10 - Internet access

Application	WinINet	WinHTTP	3rd-party
Internet Explorer	X		
Edge Browser	X		
Google Chrome	X		
Firefox	(X)		X

Windows 10 - Internet access

Application	WinINet	WinHTTP	3rd-party
Internet Explorer	X		
Edge Browser	X		
Google Chrome	X		
Firefox	(X)		X
PowerShell		X	
Windows PKI		X	
Updates / Bits		X	
S4B Client		X	
Windows Store		X	
Store Apps		X	
Live Tiles		X	
Office 365 Lean Install		X	

Windows 10 - Internet access

Application	WinINet	WinHTTP	3rd-party
Internet Explorer	X		
Edge Browser	X		
Google Chrome	X		
Firefox	(X)		X
PowerShell		X	
Windows PKI		X	
Updates / Bits		X	
S4B Client		X	
Windows Store		X	
Store Apps		X	
Live Tiles		X	
Office 365 Lean Install		X	
Teams	X	X	X

Office 365 ProPlus

- first Office build from ground up for the Cloud
  - *many functions to improve Cloud usage, but also functionality based on the Cloud*

- breaks traditional software and hardware deployment cycles
  - initial deployment includes Microsoft CDN network (ca. 2 Gbytes)
  - multiple incremental updates each month (ca. 1 Gbyte / month)
  - *lean deployment strategy is the best option*

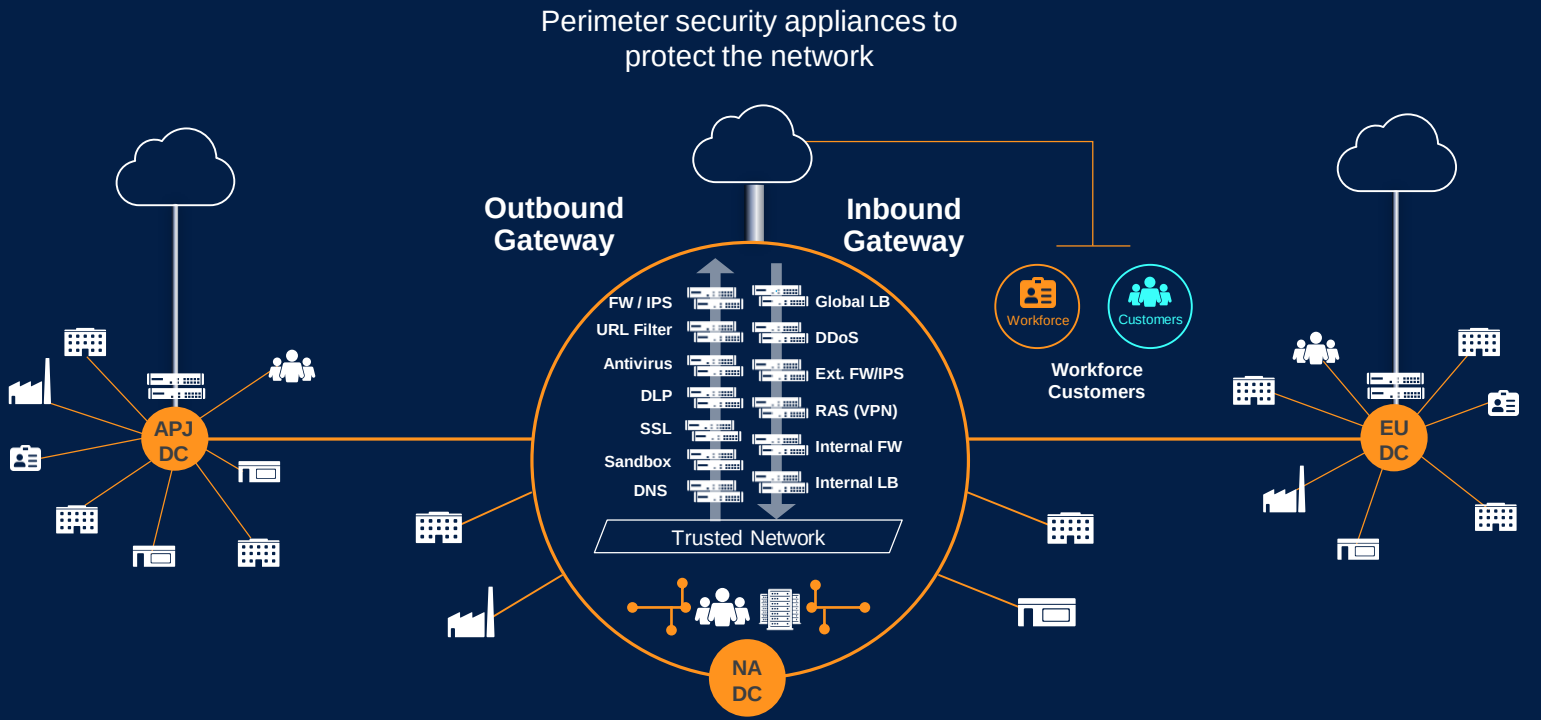
- Microsoft recommendation for good performance
  - Latency: 50ms from Client to Microsoft Edge
  - Latency: 30ms from Customer to Microsoft Edge
  - Direct-to-Internet
  - no dedicated proxies anymore

lean = SCCM with Office Content-Delivery-Network fallback

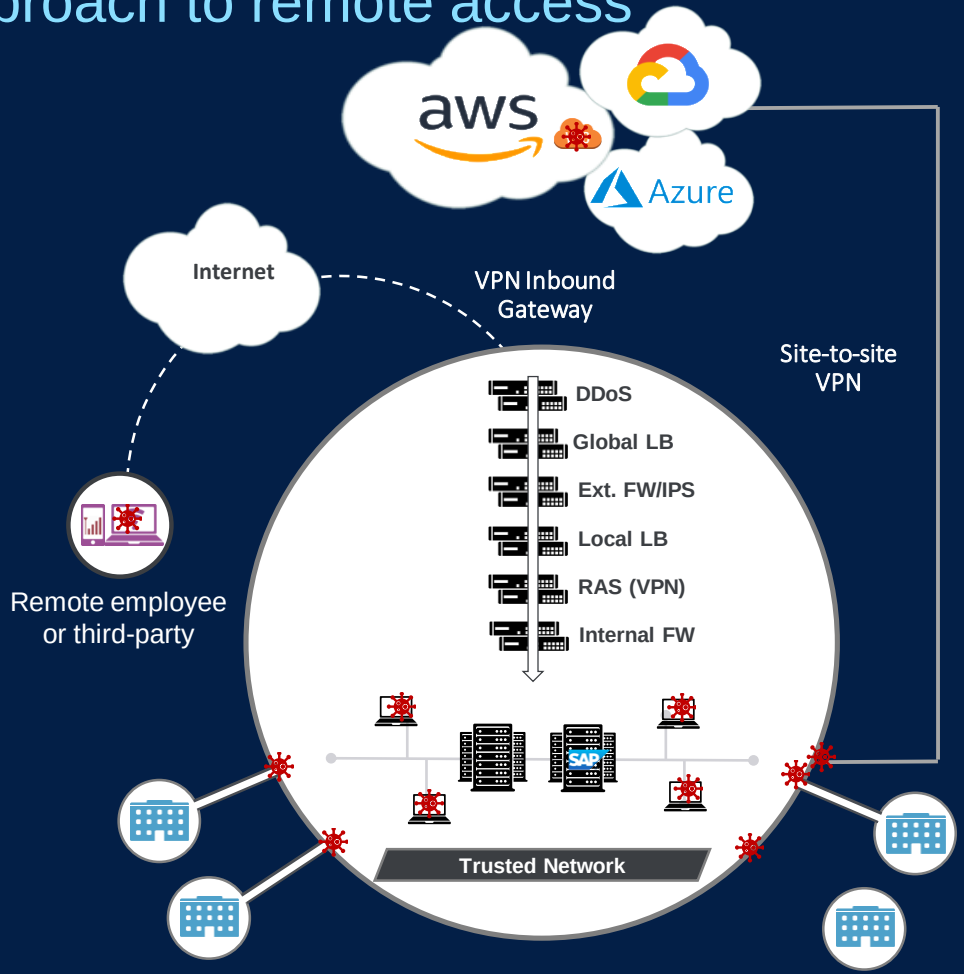
The Problem: Remote Access

This model worked well in the old world

Internal networks were built and optimized to connect users to apps in the data center



VPN: First approach to remote access



Remote users placed on network via IPsec tunnel

Traffic, including malware spreads laterally

Even as you move to cloud…

Back to Zscaler

An opportunity for IT to empower the business

Application Transformation
Data Center to Cloud

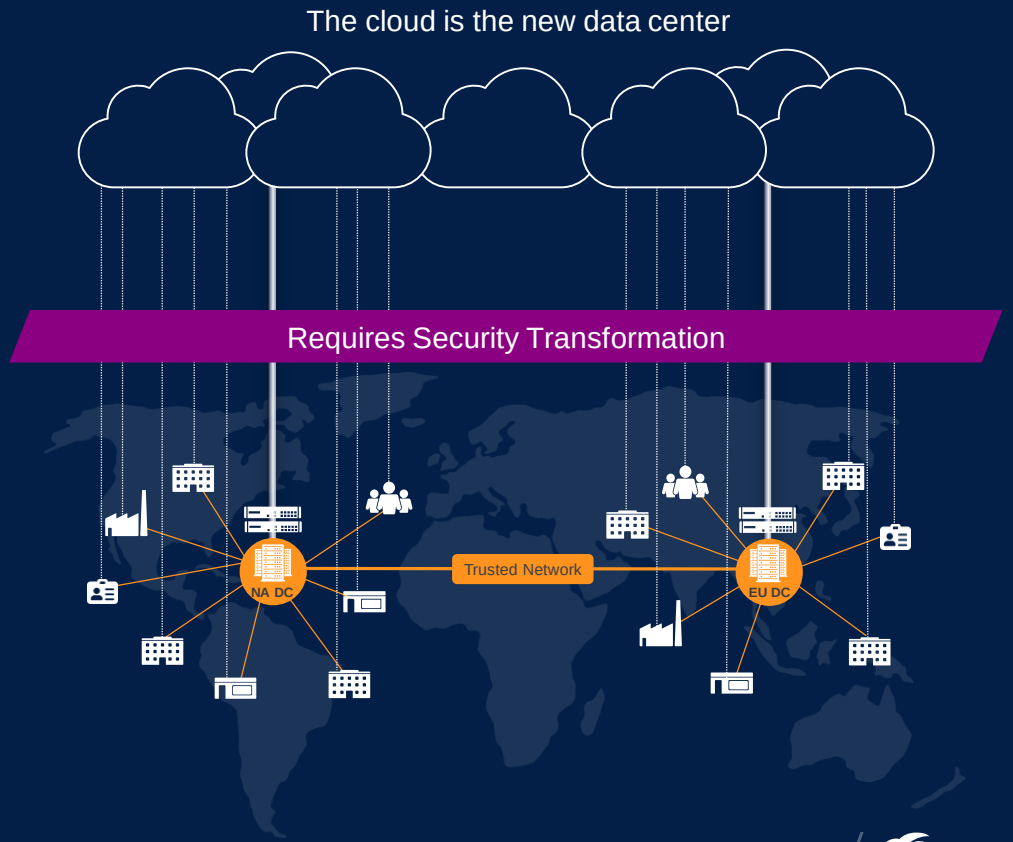
Facilitates collaboration
New business models
Simplifies IT

Security Transformation
Network Security to SASE

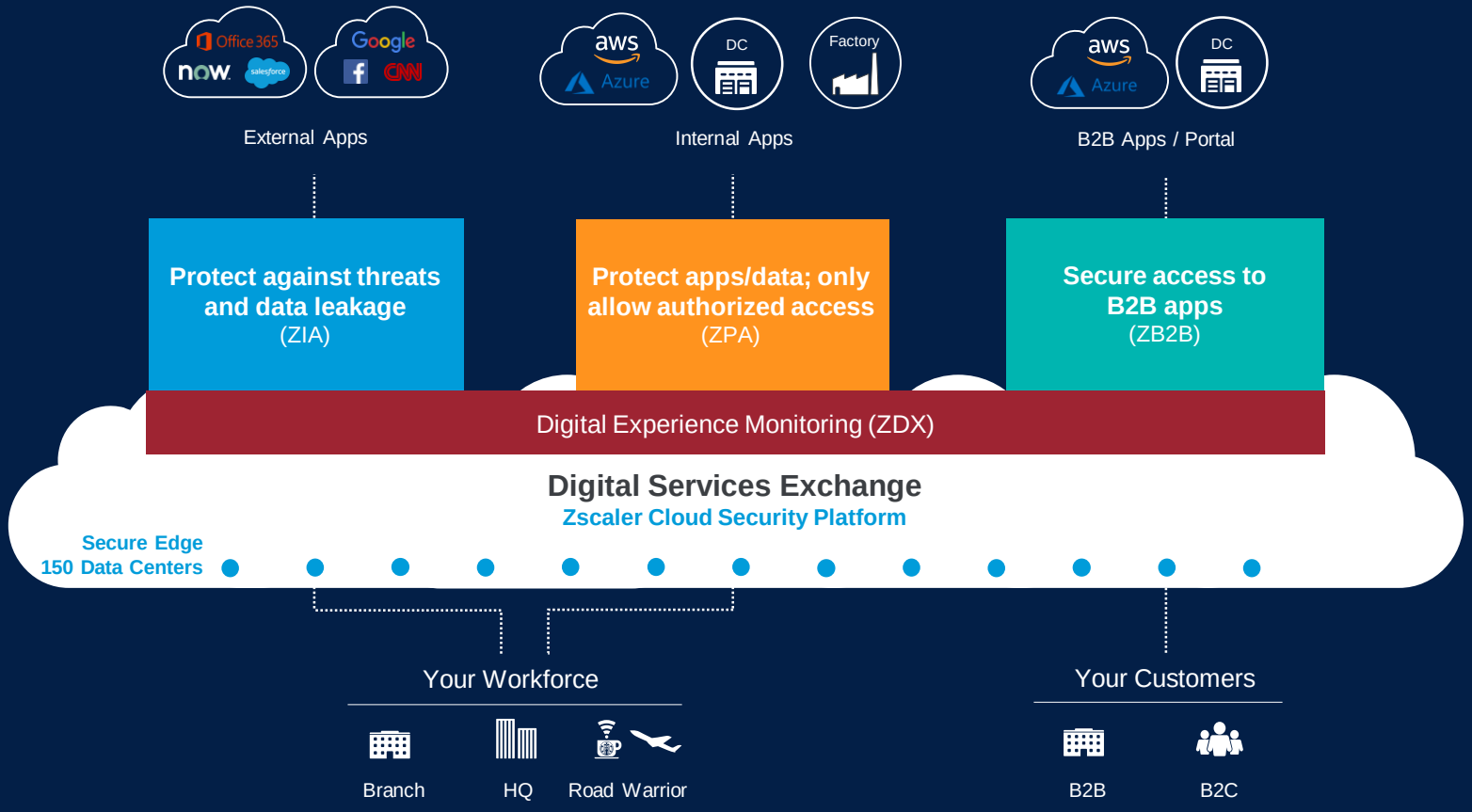
Policy-based
Transparent experience
Standardization

Network Transformation
WAN to Internet

Fast user experience
Network cost savings
Simplify IT (Agility)



Delivering secure, fast, and reliable access to apps/data



Global data center footprint brings security close to the user

150
Data centers across six continents

75B+
Requests processed/day

100M+
Threats blocked/day[1]

120K+
Unique security updates/day

Peering with content and service providers

Office 365 DC peering

Nestle, Company, and GE have users being secured by all Zscaler DCs

Cloud Insights: https://www.zscaler.com/threatlabz/global-internet-threats-insights

Peering: https://www.peeringdb.com

Securing your cloud transformation

zscaler

Four areas where Zscaler can help you deliver value

Make the business more agile and competitive

Accelerate cloud adoption

Remove network and security friction

Protect the company's increasing digital footprint

Policy-based access from anywhere

Inspect encrypted traffic at scale

Provide customers and end-users a better experience

Fast and direct access to apps – no backhaul

Security and policy at the edge in 150 data centers (SASE)

Reduce costs and ensure future cost avoidance

100% cloud service – per-user subscription

Consolidate and simplify IT

"It's a rare occasion in history where it got more secure, better, and cheaper all at once."

Blueprint for a cloud and mobile world

Better value: Easy deployment and operations

Identity Management

Microsoft okta Ping identity

Security Operations

splunk> IBM QRadar Microsoft ANOMALI SKYBOX SECURITY

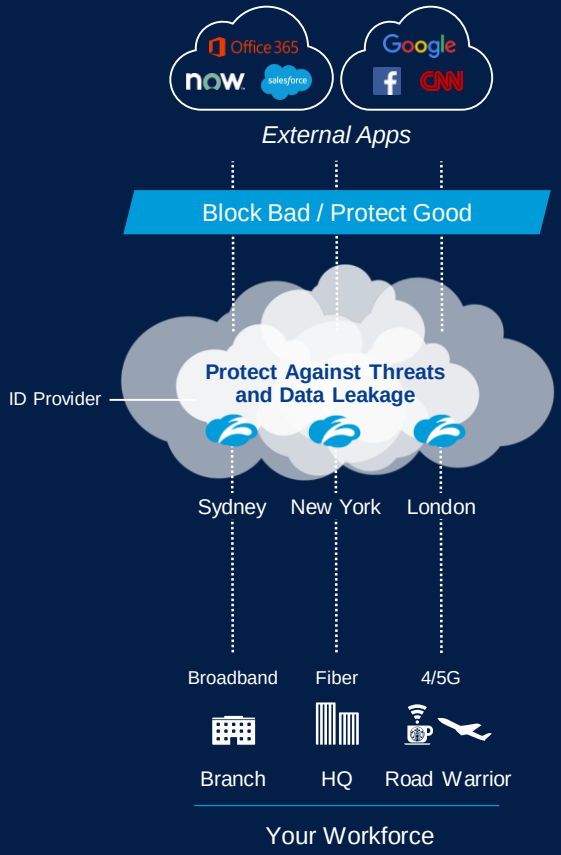
Endpoint Protection

Microsoft CROWDSTRIKE vmware airwatch mobileiron Carbon Black.

Branch Networking

cisco viptela vmware velocloud silver peak

Zscaler Internet Access: Secure and fast access to internet & SaaS



Use Cases

Office 365

- App prioritization/peering with Microsoft
- One-click deployment

Secure SD-WAN

- Local breakouts for branch internet
- API integration with SD-WAN vendors

Threat Protection

- Inspect encrypted traffic at scale
- Cloud-effect: Identify once, protect all

Data Protection

- Shadow IT discovery
- Protect IP / PII / Compliance

Standardization • Simplification • Identical Protection (mobile, branch, HQ)

Platform Services

Threat Prevention

Proxy (Native SSL)
Advanced Threat Protection
Cloud Sandbox
DNS Security

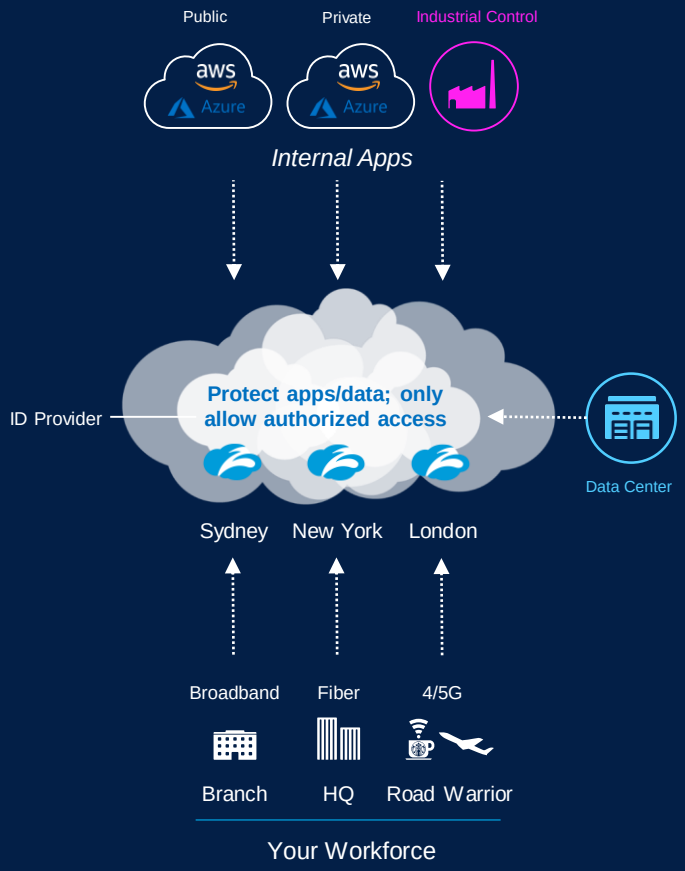
Access Control

Cloud Firewall
URL Filtering
Bandwidth Control
DNS Resolution

Data Protection

Cloud DLP
Exact Data Match
CASB
Browser Isolation

Achieve Zero Trust Network Access with ZPA



Use Cases

Replace Remote Access VPN

- Fast, direct access to apps – no backhaul
- Secure contractors' connectivity to data center

Direct Access to Multi-Clouds

- No data center-to-cloud direct connect required
- Eliminate the need for virtual DMZs

Accelerate M&A IT Integration

- Integrate companies w/out integrating networks
- Standardize security across companies

Secure Access to Industrial Systems

- Secure critical infrastructure (invisible)
- Policy-based access from anywhere

Zero Attack Surface • App Segmentation • Zero Trust Network Access

Platform Services

Zero Trust Network Access

Anti-VPN
Anti-Firewall
Anti-DDoS
Anti-network segmentation

Discovery/ Availability

GSLB
Optimal Path Selection
App Health Monitoring
App Discovery

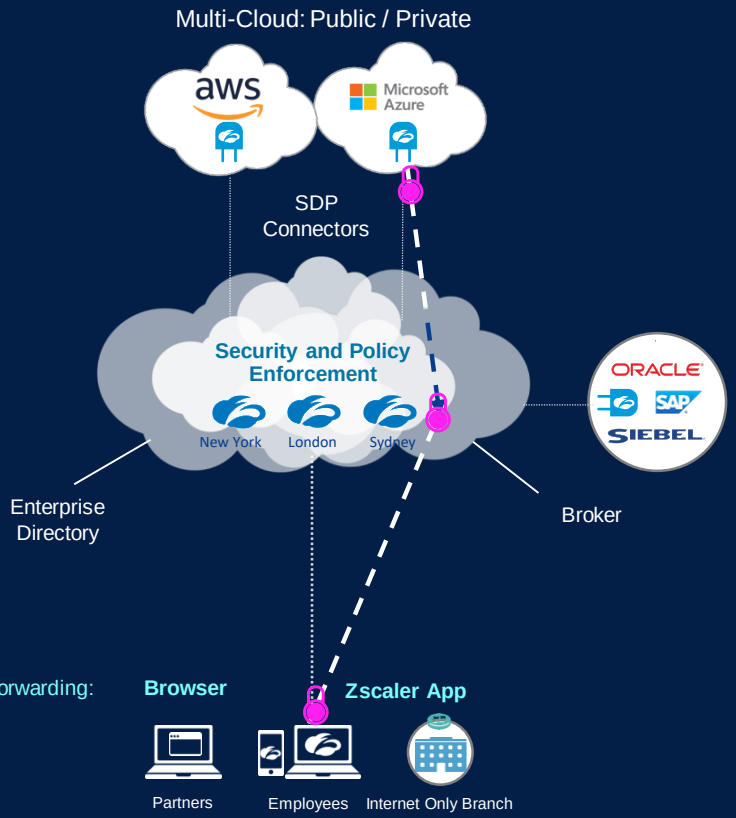
App/Device Access

Browser Access
Web Isolation
Private Service Edge

Zscaler Private Access: Fast and secure access to private apps

How it works….

1. A user requests access to an app
2. Policies determine if the user has access to the app
3. If allowed, the cloud establishes inside out connection from App Connector to ZEN and client to same ZEN



Zero Trust approach:

Remote users never brought on the corporate network

App access with out network access

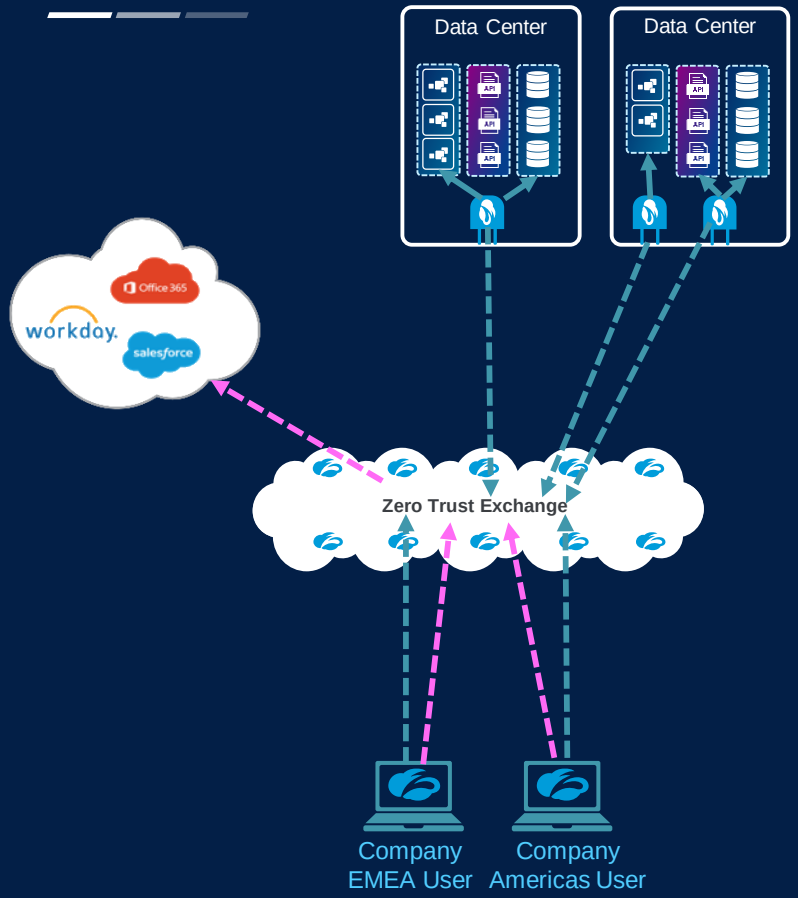
Apps are invisible

not exposed to the internet

Native app segmentation

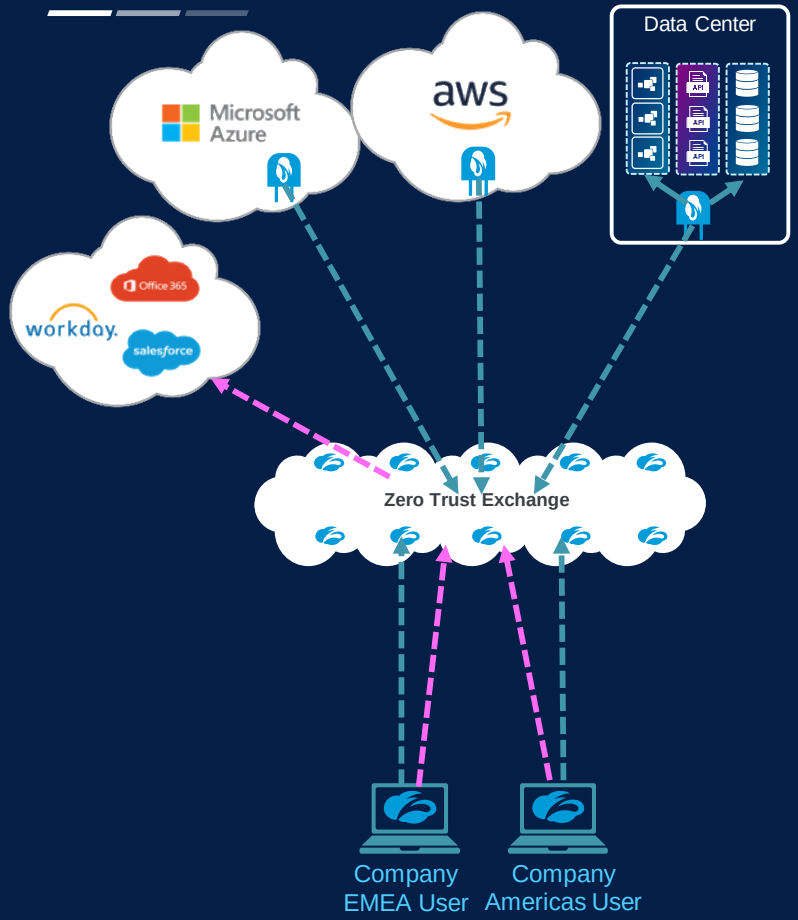
microtunnels that connect an authenticated user to an name app

A few ideas …



Employee Application Access

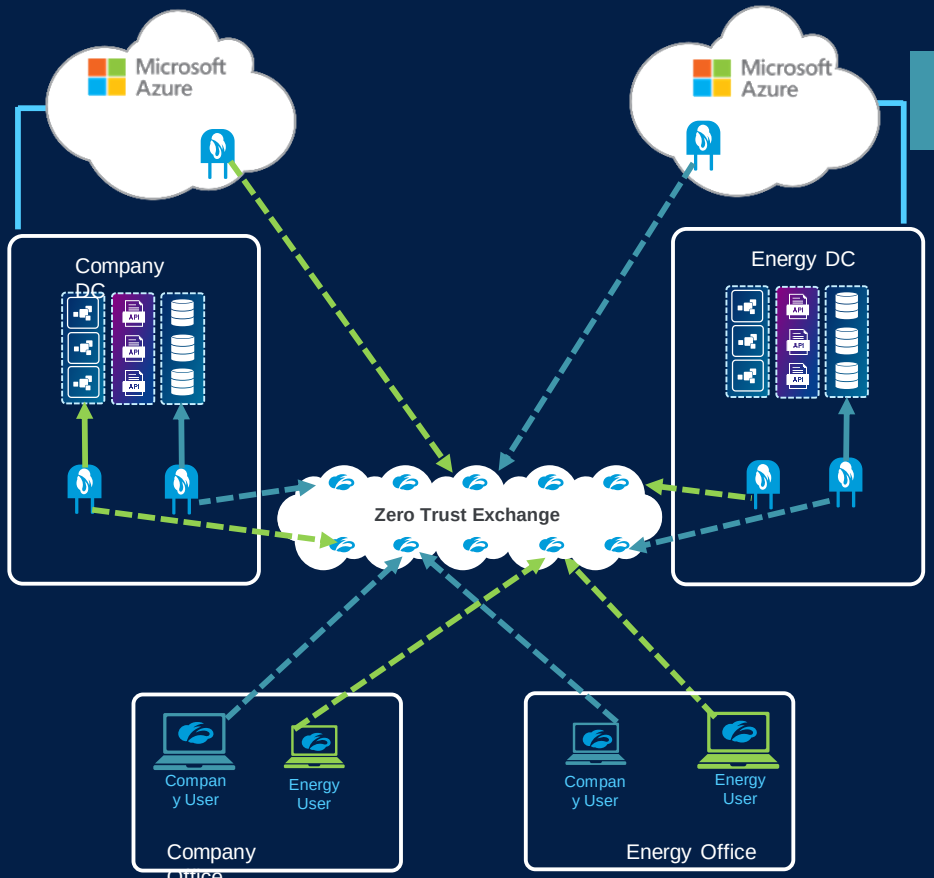
- Scale to demand is provided by the Zscaler cloud – no hardware requirements
- No exposed ecosystem to the Internet, turning infrastructure dark
- Single global access, user gets the same service, security and access, regardless of where they are
- Users can exist anywhere & are not tied to a physical location or network
- Outbound connections removes needs to “inbound controls”, e.g. VPN, FW, DDoS Protection”
- Single user experience with Zscaler Internet (ZIA) and Private Access (ZPA)



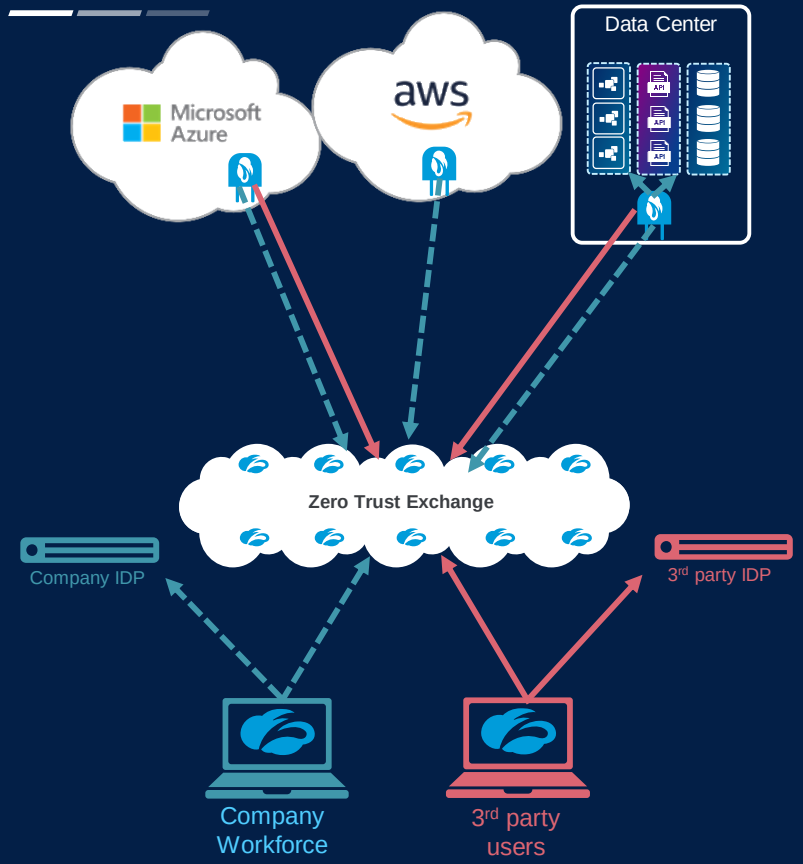
Multi-Cloud Access

- Users access apps directly. There is no backhaul over MPLS links
- Apps exist in any location, user access apps in parallel, no network connection
- Single global access, user gets the same service, security and access, regardless of where they are
- Optimization of network interconnects – server to server connections
- Single user experience with Zscaler Internet (ZIA) and Private Access (ZPA)

Divestiture / M&A



- Connection path is **not** dependent on user or app location:
  - No need for network interconnect (MPLS/VPN/Etc.)
  - Users can be at any location
  - No doubling up of NAT/FW/DNS
- Access control is managed for both sets of users (company A&B), globally.
- Single global access, user gets the same service, security and access, regardless of where they are



3rd Party User Access

- 3rd parties get direct access to only what is allowed and nothing more, protecting your infrastructure
- No need to integrate or manage 3rd parties on IDP, leverage 3rd party IDP for authenticated
- Single global access, user gets the same service, security and access, regardless of where they are

What you should consider

User “networks” are pointless

- Substantial Hardware Requirements
- Useless when your users are mobile
- Multiple user networks means multiple spots for ingress to occur
- Limit your ability to consume external services

Use the Internet

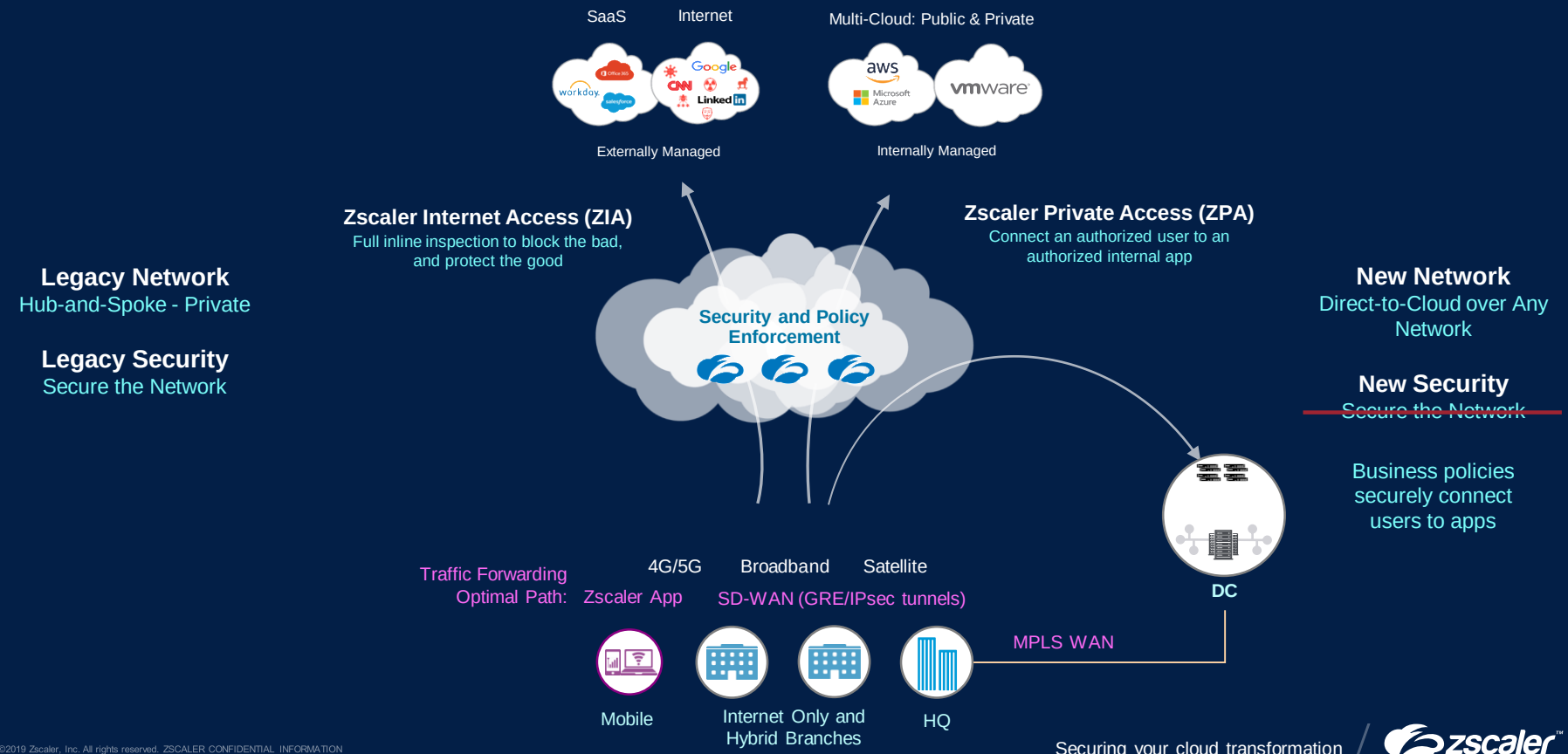
- Access from anywhere
- Cloud goes direct – it is native to the Internet
- Faster User Experience
- Global Protection regardless

Host Apps Anywhere

- On Premise
- Cloud Locations
- Simplified user access
- Policy is enabled granularly, but globally

Zscaler: Securely transforms IT for a world of cloud

Fast, secure, and reliable access to your apps – to any cloud, over any network, on any device



Next Steps

Architecture Workshop • Executive Briefing • San Jose, CA