Adopting a Zero Trust Model

Mark Harris

Solution Architect

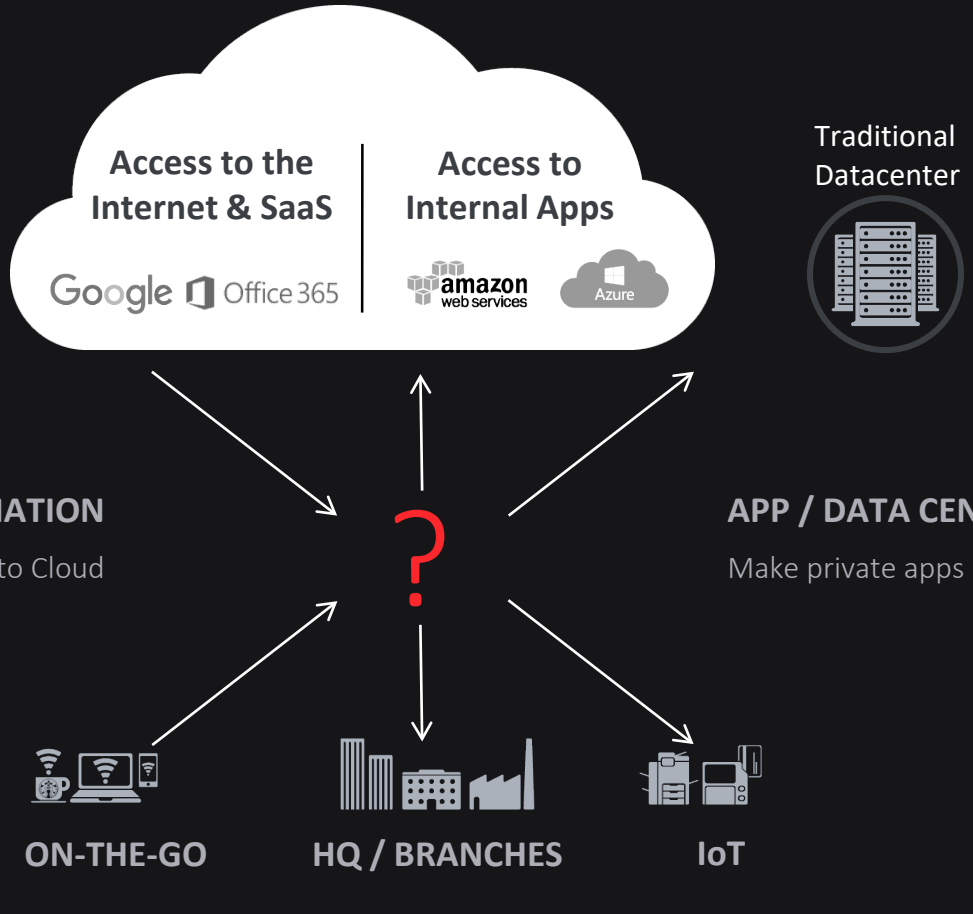
Zscaler Inc.

The Leader In Cloud Security

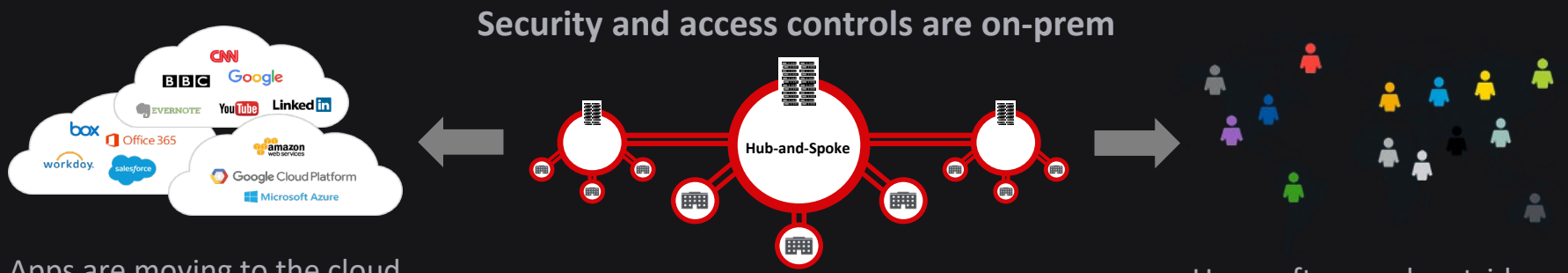
Zero Trust Networking may be interesting when thinking about:

- Application Migration
- Micro Segmentation
- Software-Defined Perimeter
- Security Transformation
- Mobility
- Network Transformation
- CARTA (Gartner)

Vision: Securely Enabling Transformation



Cloud and mobility are powerful enablers, but break perimeter security



Apps are moving to the cloud

Users often work outside the security perimeter

How do you securely enable this new world of IT?

❝ Digital businesses require more interconnections than ever before. When employees and partners need to interact externally with business applications in the corporate network or the cloud, managing secure access can be daunting. ❞ Gartner

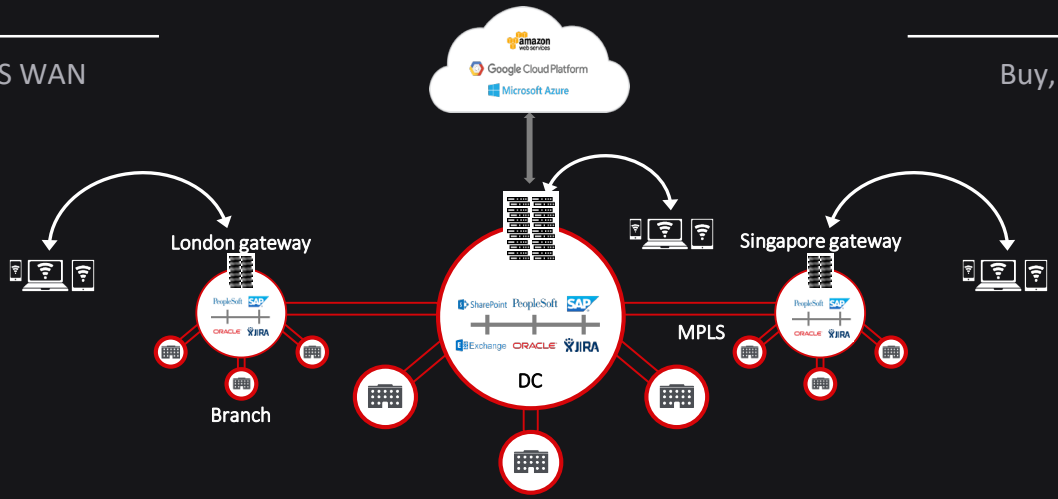
Hub & Spoke architecture with DMZ/VPN gateways

Complexity

Many gateways; MPLS WAN

High Cost

Buy, deploy, and manage



User Experience

Slow – depends on location of apps and number of VPN gateways

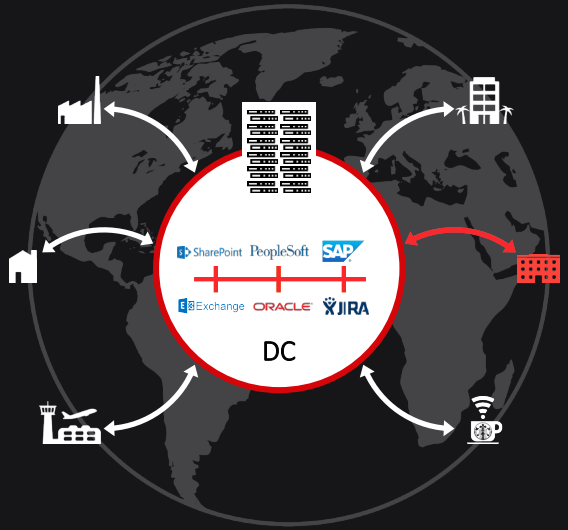
Inconsistent – different on-net and off-net

❝ DMZs and legacy VPNs were designed for the networks of the 1990s and have become obsolete because they lack the agility needed to protect digital businesses. ❞ Gartner

Security problems with VPN technology

Broader attack surface = Higher risk

- App access requires a user to be on the network; corporate network extends to every location of a VPN user. This broadens the attack surface, exposing apps to attacks.
- Once on your network, a user can laterally scan other resources and exploit their vulnerabilities.



Over-exposed = Vulnerable

- VPNs are exposed to the Internet – a DDoS target, potential service disruption.
- Attackers will target any exposed surface, discover vulnerabilities, and attack them.

“ Attackers who discover services often find vulnerabilities in applications and in (APIs) that bypass firewalls and intrusion prevention systems (IPS). Attackers will target services, users of the services, or both. ” Gartner

bsi. International Cyber Resilience Exchange 2019

Software Defined Perimeter: better security, better experience

New Approach: Four key tenets for secure app access

1

Users not on the corporate network

App access shouldn't require network access

Policies are app-centric, not network IPs & ACLs

If users aren't on your network, your network isn't extended to thousands of locations and attack surface is minimized. Hence better security.

2

Apps invisible, not exposed to Internet

Internal apps can't be discovered or exploited

App access only after authentication & policy

No inbound connections, no public IP addresses. Darknet – apps are dark to the Internal and unauthorized users. Hence better security.

3

Use Internet as a secure network without a VPN

End-to-end encryption, double TLS tunnels

Bring your own keys, impossible to intercept

Customer-controlled client & server certificates. Cloud handles brokering, but traffic remains completely private.

4

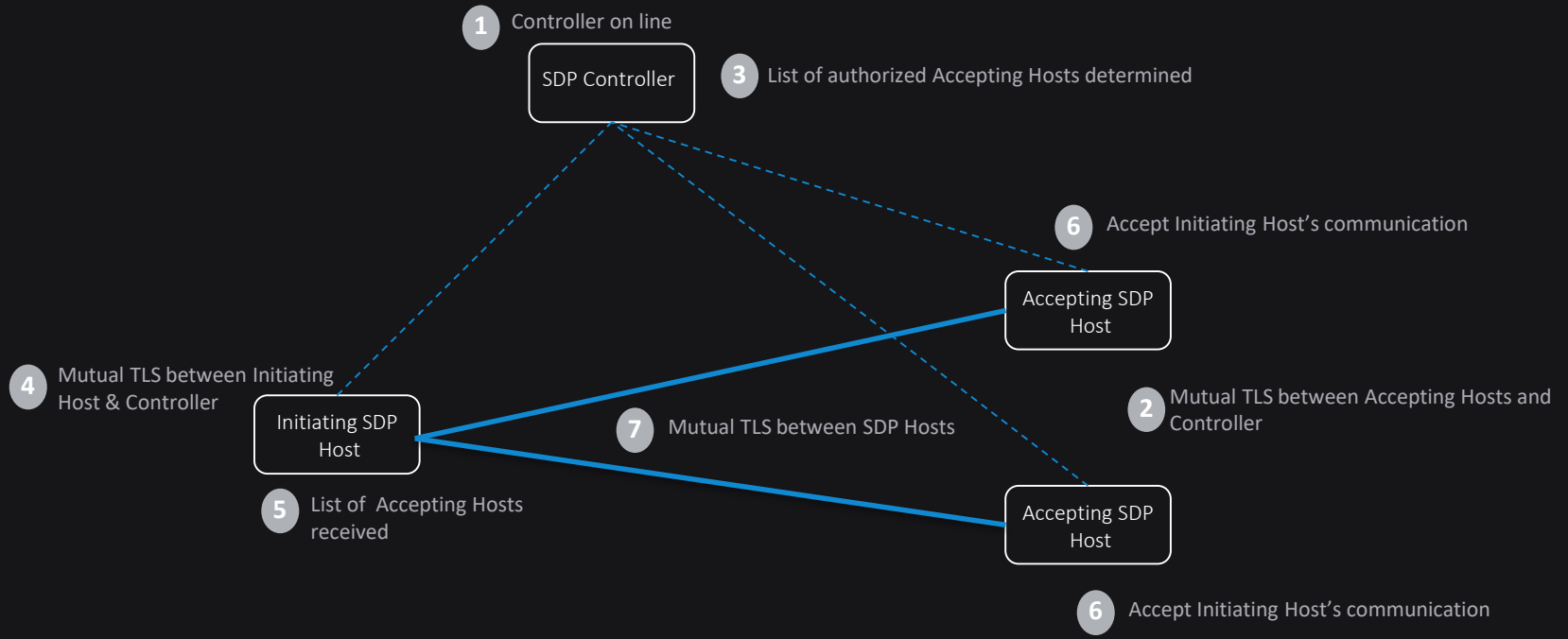
App segmentation without network segmentation

User connection to a specific app

Each app is segmented, no lateral movement

Not network-to-network connection, but user-to-app. Connection is made to a specific app with a per-session user-to-app micro-tunnel.

Software Defined Perimeter Overview



Digital Transformation Drivers & Use Cases

EMPLOYEE ACCESS / VPN REPLACEMENT

Is your VPN slow? Is it a security risk?

Users access to specific apps – users are never brought onto the network and apps are never exposed to the Internet – no hardware needed.

CLOUD FIRST / CLOUD MIGRATION

You moved private apps to a modern IaaS but your access is still legacy VPN.

Securely access private apps without requiring VPN or having to deploy infrastructure.

M&A AND DIVESTITURES

Do you feel comfortable connecting the two networks to access each company's apps?

Provide named users access to named apps without merging networks.

SECURE PARTNER ACCESS

Should partners/contractors be on your corporate network via VPN?

Only grant partners access to specific applications, not the network. (dev teams, contractors)

Unmatched security – Simplified IT – Better user experience

Benefits Across the Enterprise

Fast Response Time
(End-Users)

No need for “hairpin” traffic to get to cloud apps

Users are automatically connected to the app with the best performance

Reduced Risk
(CISO)

User is not on the network; no lateral movement

Applications are not on the Internet (DDoS protection)

Users can only access apps for which they are authorized; if they aren’t authorized, they cannot even see the app

IT Simplification
(CTO / IT Head)

No network segmentation required

No need to continually manage network segments

Move apps to Azure, AWS, or DC without any network changes or user impact

Impressive Value
(CIO / CFO)

No CAPEX, elastic subscription fee

Reduced OPEX, no box management

Reduce your global load balancers, DDoS protection; retire complicated VPN concentrators

bsi. International Cyber Resilience Exchange 2019

Zscaler : Zero Trust Implementation

Zscaler Private Access

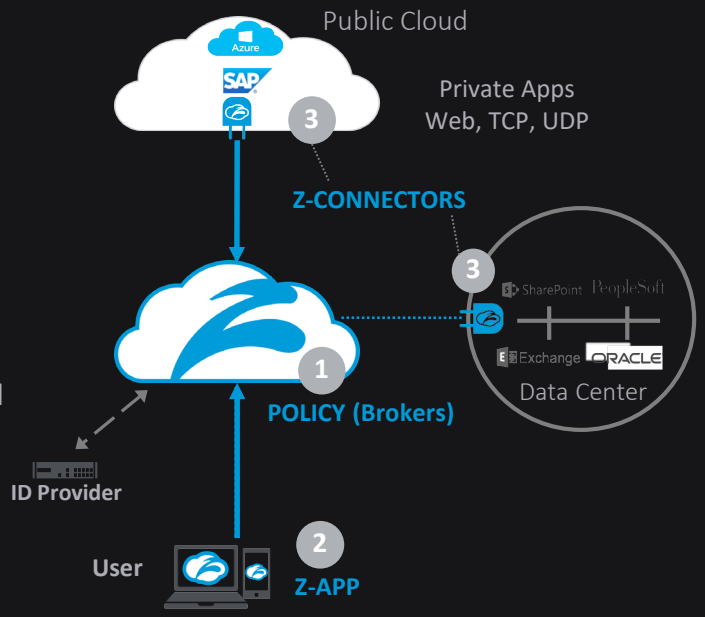
Secure and fast policy-based access to private apps on Azure, AWS, or your DC

Connect a named user to a named app, not a network. Direct path to cloud apps without hair-pinning through DC. No VPN needed.

ZPA: Innovative Design

1. Cloud-based policy engine – who can access what apps
2. Z-App – runs on user endpoint, intercepts requests for apps
3. Z-Connector – sits in front of apps, outbound connection only

Zscaler cloud brokers a secure connection between the Z-Connector and Z-App



Policy-Based Access

- Device: Windows/Mac/mobile
- User location: office or remote
- App location: data center or cloud
- App type: all TCP & UDP ports

ZPA replaces the entire inbound gateway/DMZ - not just a VPN replacement

Reduced cost and complexity; better security and user experience

Unmatched Security: Strong authentication, context-aware policy

Strong Authentication

Critical as users get ubiquitous access to apps

- Integration with your directory
- SAML-based; multi-factor auth
- Device fingerprint & your company certificate
- Device posture checking

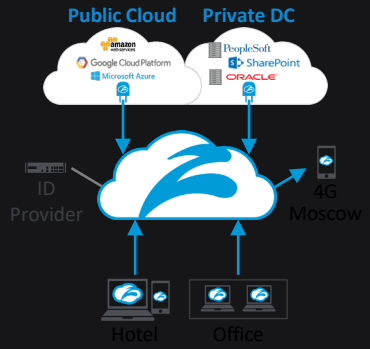
Four Contexts for Policy

App context

Access to a specific app or app groups
Each app can be its own segment

Location context

Understand where user access originates
Restrict apps to be accessed from road



Device context

John can access a specific app, only from a company-owned PC (with cert)

User context

John can access only a specific app
Marketing can access a group of apps

Example

HVAC consultants can only access the HVAC app

Granular access policy by user and application, not by network

POLICY ENGINE

Rule Order	Name	Description	Attribute	Criteria	Permission
1	All employees	Access for all employees	SAML: employee = true	APPLICATION GROUP(S) Intranet	Allow
2	HVAC contractor	Contractor access for HVAC contractors	SAML: contractor = hvac	APPLICATION GROUP(S) HVAC Control Apps	Allow
3	IT access	Access for IT to SCCM servers	SAML: group = it	APPLICATION GROUP(S) SCCM Apps	Allow
4	Finance access	Access for finance employees	SAML: group = finance, exec	APPLICATION GROUP(S) Finance Apps	Allow

Only execs and Finance can access financial apps

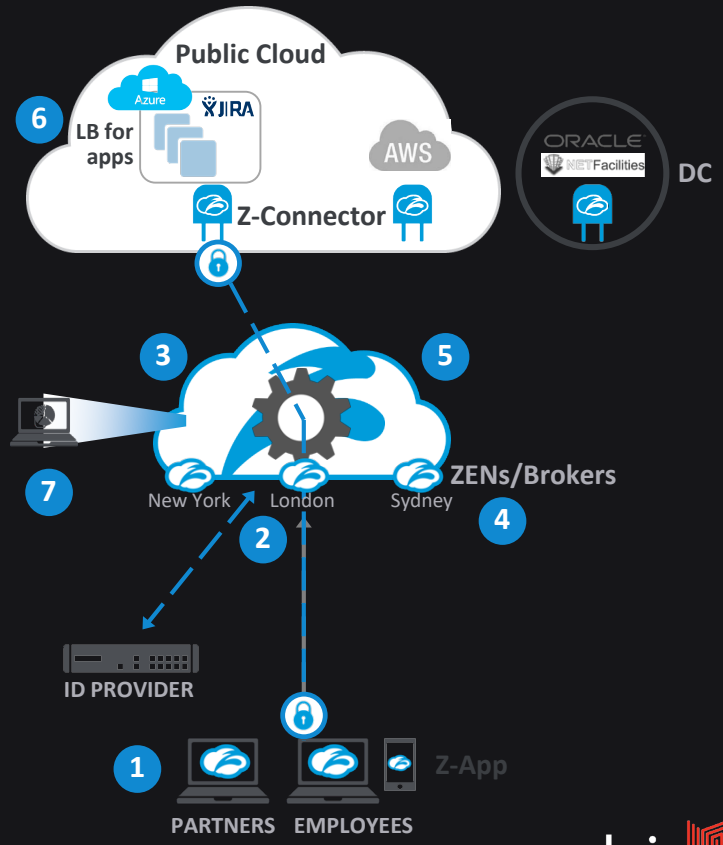
Zscaler Private Access – how it works

GETTING STARTED

- Deploy Z-App on endpoints
- Deploy Z-Connectors in front of your apps
- Define user and app access policies

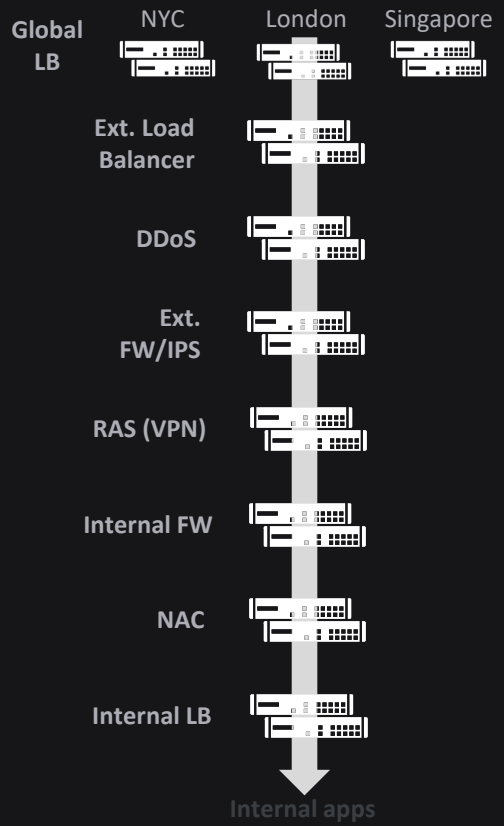
HOW IT WORKS

1. User attempts to access an app
2. User identity/role is verified (before DNS)
3. Policy is checked to determine if access is permitted
4. Optimal path to app is determined
5. If allowed:
   - Z-Connector initiates outbound connection
   - Z-App initiates a connection (per app)
   - Zscaler cloud broker stitches connection together
6. Z-Connector provides app load balance across VMs/servers
7. Monitor app usage – anomaly detection



Comparing Strategies

Legacy On-Prem VPN/DMZ Stack



Cloud Service

Global Platform

Provides dynamic best-path discovery for applications

No inbound connections / apps are invisible, eliminating attack surface and DDoS threat

Outbound connections only - better security than a traditional FW

Connects named user to named app

Not needed as users are never on the corporate network

App segmentation native to Cloud, so no network access by user

Best-path discovery load-balances across internal app instances, too

bsi.

International
Cyber Resilience
Exchange 2019

Thanks for listening. Any questions?