



Innovations Update with Investors

Jay Chaudhry
CEO and Founder

Amit Sinha
President & CTO

Patrick Foxhoven
EVP, Emerging Tech & CIO

Safe Harbor

Forward-Looking Statements

This presentation has been prepared by Zscaler, Inc. (“Zscaler”) for informational purposes only and not for any other purpose. Nothing contained in this presentation is, or should be construed as, a recommendation, promise or representation by the presenter or Zscaler or any officer, director, employee, agent or advisor of Zscaler. This presentation does not purport to be all-inclusive or to contain all of the information you may desire.

This presentation contains forward-looking statements. All statements other than statements of historical fact, including statements regarding our planned products and upgrades, business strategy and plans and objectives of management for future operations of Zscaler are forward-looking statements. These statements involve known and a significant number of unknown risks, uncertainties, assumptions and other factors that could cause results to differ materially from statements made in this message, including any performance or achievements expressed or implied by the forward-looking statements. Moreover, we operate in a very competitive and rapidly changing environment, and new risks may emerge from time to time. It is not possible for us to predict all risks, nor can we assess the impact of all factors on our business or the extent to which any factor, or combination of factors, may cause actual results or outcomes to differ materially from those contained in any forward-looking statements we may make, including but not limited to the duration and global impact of COVID-19 on our business, operations and financial results and the economy in general; our ability as an organization to acquire and integrate other companies, products or technologies in a successful manner. Additional risks and uncertainties that could affect our financial and operating results are included in our most recent filings with the Securities and Exchange Commission (“SEC”). You can locate these reports through our website at <http://ir.zscaler.com> or on the SEC website at www.sec.gov.

In some cases, you can identify forward-looking statements by terms such as “anticipate,” “believe,” “continues,” “contemplate,” “could,” “estimate,” “expect,” “explore,” “intend,” “likely,” “may,” “plan,” “potential,” “predict,” “project,” “should,” “target,” “will” or “would” or the negative of these terms or other similar words. Zscaler based these forward-looking statements largely on its current expectations and projections about future events that it believes may affect its business. Actual outcomes and results may differ materially from those contemplated by these forward-looking statements. All forward-looking statements in this message are based on information available to us as of the date hereof, and we do not assume any obligation to update the forward-looking statements provided to reflect events that occur or circumstances that exist after the date on which they were made.

Zscaler Innovation: Zero Trust Exchange Platform

Four pillars

User Protection and Experience

Zscaler Internet Access

Cyber protection
Data protection (DLP/CASB)
Local internet breakouts (O365/SD-WAN)

Secure Internet and SaaS access

User to Internet

Secure Private App Access

User to Private App

Zscaler Private Access

Remote app access without VPN
Zero trust from office to data center
B2B customer app access

Zscaler Digital Experience

Performance scores by user, app, location
Identify and resolve device and network issues

User Experience

User to App Experience

Secure Apps and Workloads

App to App

Zscaler Cloud Protection

Remediate cloud misconfigurations (CSPM)
Secure user-to-app and app-to-app access
App segmentation without network segmentation

Workload and Server Protection

Simplify IT and reduce costs by consolidating and eliminating point products

Securing cloud is fundamentally different than Data Center

Platforms

Distributed, multi-cloud, evolving
Growing configuration complexity

Workloads

User controlled, dynamic, ephemeral
DevOps moves faster than Infosec

Connectivity

Complex ingress/egress routes
Little east-west traffic controls

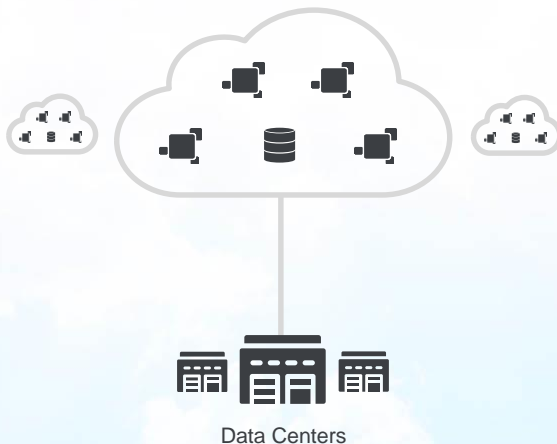
Security and operations challenges

Workload security posture

- Where are my workloads and what are they?
- Misconfigurations cause 99% of incidents

Risk of lateral movement

- Flat networks create lateral movement issues
- Network segmentation is not practical



Can apps talk to other apps securely?

- Workers accessing the Internet safely?
- Across clouds?

Can right users access apps safely?

- Employees and B2B customers
- Workloads exposed to the internet can be exploited and DDoSed

Data center approach to security doesn't work for the cloud. A new approach is needed.

Zscaler Cloud Protection: Reduce risk of embracing the cloud

Protect multi-cloud workloads

1 Cloud Security Posture Mgt. (CSPM)

Ensure proper configuration and compliance of workloads

New – Built upon Cloudneeti

3 Workload segmentation

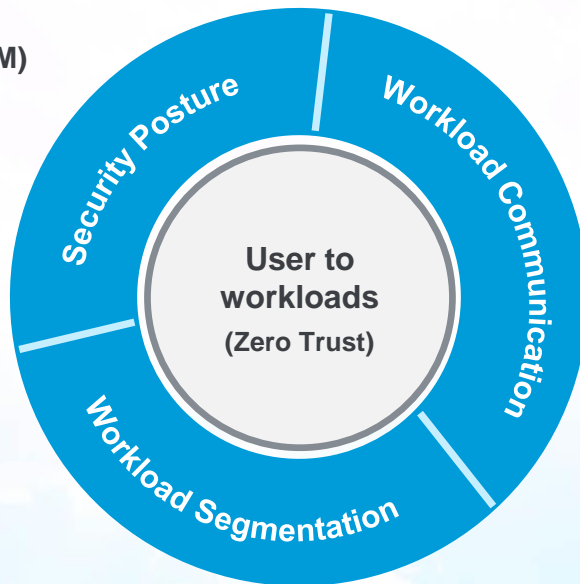
Eliminate the risk of lateral threat movement without having to do legacy network segmentation

New – Built upon Edgewise

2 Workload Communication

Secure workload and app-to-app cloud-cloud, cloud-internet and cloud-DC connectivity

New – Powered by Cloud Connectors. ZIA/ZPA used to do user protection. This expands it to net new ZIA/ZPA revenue for cloud workload protection



Provide secure user access

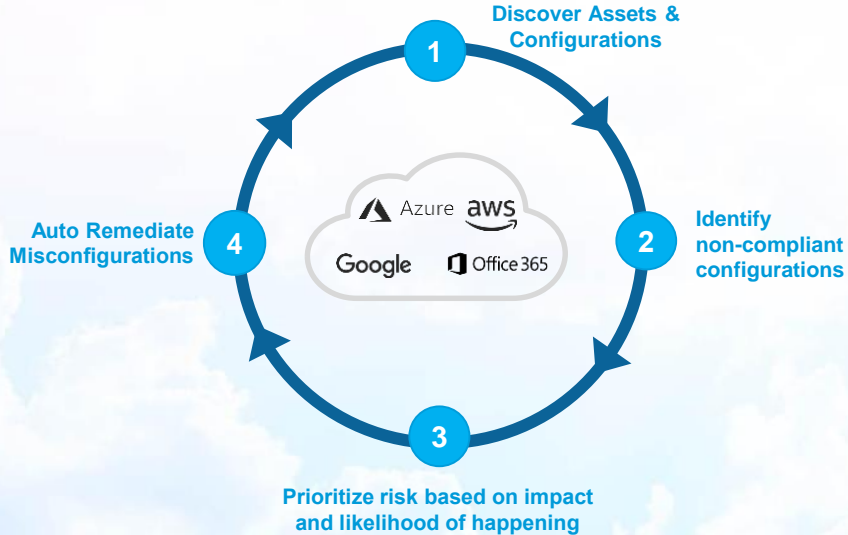
Secure user-to-app access (ZPA cross-sell)

Secure per app access by workforce and B2B customers without exposing apps to internet

1. Cloud Security Posture Management (CSPM)

“99% of cloud security incidents are the customer’s own fault. Implementing a CSPM offering will reduce cloud-related security incidents due to misconfiguration.” Gartner

Zscaler CSPM provides continuous assurance in 4 key areas



Key Functionality

- Only vendor covering cloud workloads (Azure, AWS, GCP) and apps (Office 365)
- Deep security policy coverage with 2500+ policies.
- Broad out-of-box compliance automation – 16+ different frameworks
- Enables cloud governance across multiple teams -DevOps, InfoSec, GRC, SOC)

**Accelerates cloud adoption
and reduce risks across the spectrum**

2. Secure workload communication

Zero Trust architecture – direct to cloud

Cloud connector provides simplified, flexible traffic forwarding
ZIA or ZPA policy engines enforce policies that are easy to manage

Workload to internet

Cloud Connector forwards traffic
Enforces policy, security and data protection

Cloud-to-Cloud: multi-cloud

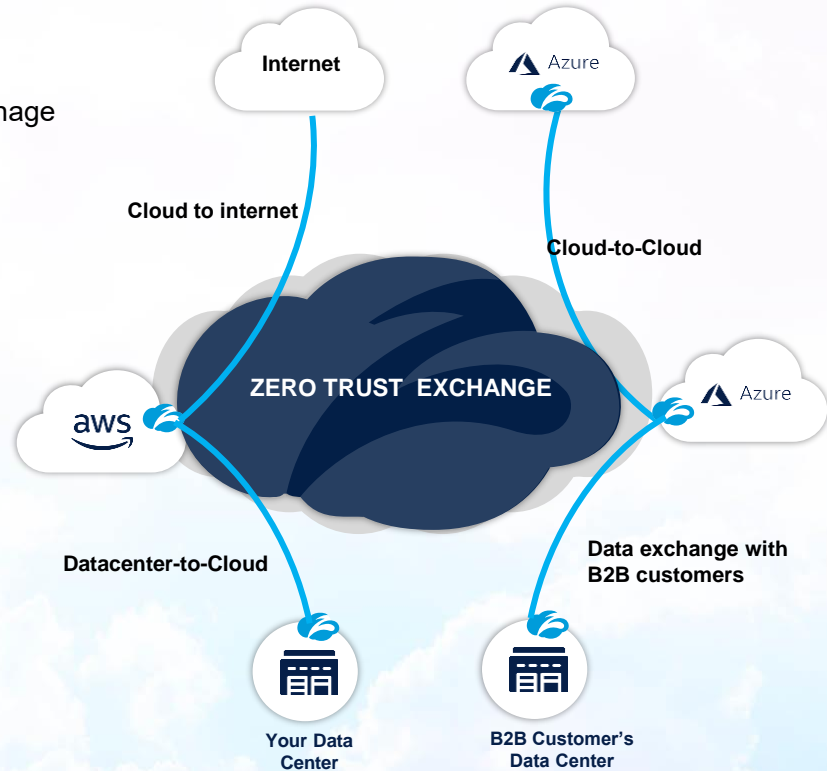
Cloud Connector forwards traffic, ZPA connects app to app

Data Center-to-Cloud

Cloud Connector forwards traffic, ZPA connects app to app

Data/File exchange with 3rd parties

Cloud Connector forwards traffic
Customer certificate authenticates. ZPA connects app-to-app



Enhanced security.
Reduced complexity and operational overhead.

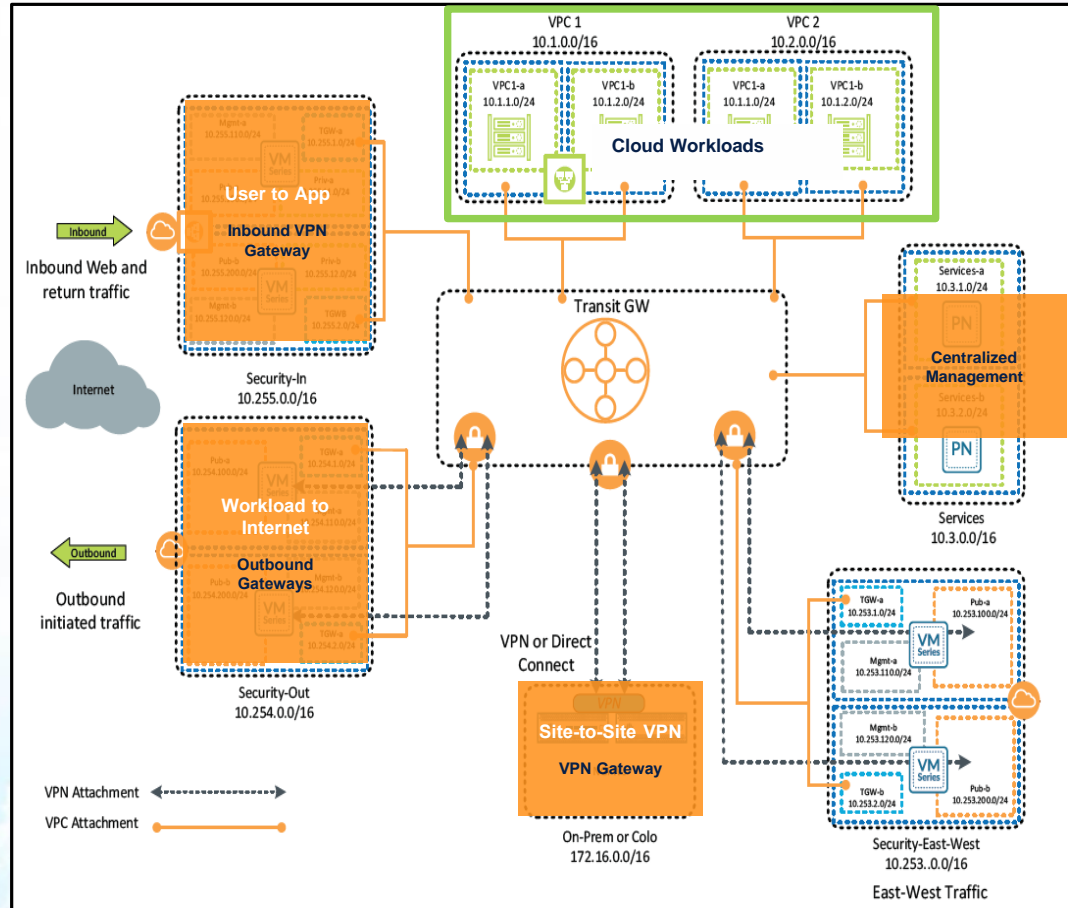
Legacy firewall-based network segmentation is complex

Legacy – Virtual firewalls with network policies


Deploy virtual firewalls with network centric policies

With limited ability for traffic inspection, poor cyber and data protection

Poor security. Complexity and management overhead.



3. Identity-based Workload Segmentation

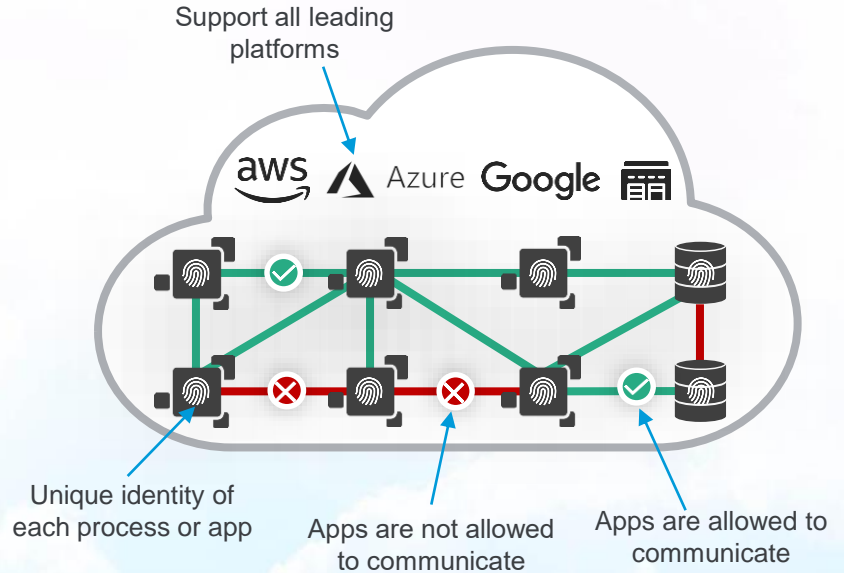
 IP-based network segmentation is not pragmatic for dynamic and ephemeral cloud workloads. Most deployments default to open, flat networks

Zscaler delivers micro-segmentation by enforcing policies for east-west traffic:

- Software identity is created for each process or app
- Machine learning models app communication patterns
- Segmentation policies automatically generated

Benefits

- Easy to deploy and manage, no change to network or apps required
- 90%+ reduction in policy rules
- Quantified risk reduction



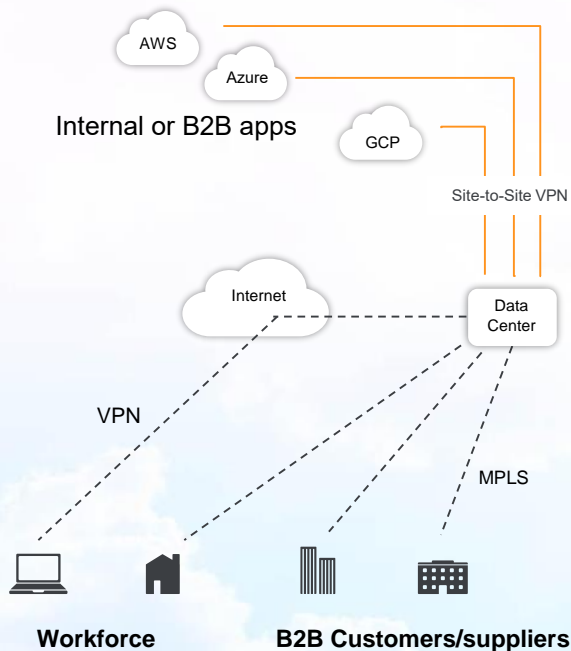
ZCP enables secure user-to-app access

Secure per app access by workforce and B2B customers without exposing apps to internet

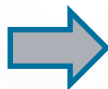
Legacy approach – thru the data center

Connect data center-to-cloud via site-to-site VPN

All users backhaul thru the DC to your public cloud apps



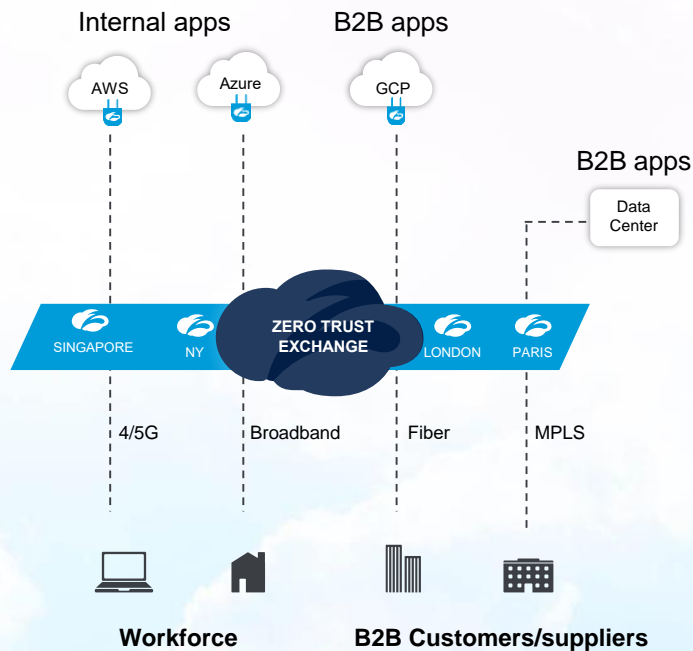
Expensive network, Operational overhead,
Poor user experience, Lateral movement risk



Zero Trust architecture – direct to cloud

No data center-to-cloud direct connect required

Go direct over the Internet. No need for virtual DMZs for each cloud



Reduces network cost, Lower operational overhead,
Great user experience, Enhanced security

Summary

- Customers continue to accelerate the move to the Public Cloud
- Traditional security approaches can't meet Cloud-Native requirements
- Zscaler is a leader in offering a comprehensive, platform approach to Zero Trust which:
 - Secures Internet and SaaS access
 - Secures private application access
 - Monitors user and app experience; and,
 - Can now secure apps and workloads in the Public Cloud
- Extending Zero Trust innovations to the Public Cloud with the introduction of **Zscaler Cloud Protection**
- Zscaler Cloud Protection is available today



Thank You