zscaler™

White Paper

# Whole of State Ecosystem Strategy

## How Independence and Collaboration Co-Exist in Zero Trust Architecture

# Contents

## Introduction

COVID challenged the government as a whole, requiring a massive technology pivot to accommodate remote access for the workforce as well as constituents accessing services. It was a heavy lift to make these significant changes in culture, process and service delivery – but agencies did it and the changes are here to stay. Digital transformation to the cloud is the new normal for users, workloads and IoT, and IT infrastructure must transform with it in order to stay ahead of sophisticated cyber threats while delivering a good user experience.

A Whole of State Strategy is intended to be a collaborative risk mitigating effort, leveraging state resources in building or strengthening local government entities cyber security defenses as well as sustaining them over time as the threat landscape continues to become more complex with increasing frequency. Why is Whole of State so important?

Zero Trust Architecture (ZTA) is at the center of this IT shift, as cybersecurity mandates and guidelines require changes to legacy systems and infrastructure to keep up with sophisticated cyber threats. The benefits of ZTA are proven, yet resources to continue the digital transformation at the state and local level are often limited or not available at all. From funding and skilled workforce to tools and training, collaborating to leverage resources can only help in the ongoing battle to stay a step ahead of cyber threats.

The cultural shift required for IT modernization that started with COVID still must navigate one obstacle: how to collaborate across state and local government without compromising independent policy setting and data privacy.

Zero Trust Architecture provides a path forward that not only improves the user experience and cyber threat protection, it enables collaboration across the public sector to maximize collective cybersecurity resources. Zscaler's multi-tenant architecture facilitates this approach to Whole of State while maintaining independent policies and data privacy at each individual agency.

## The Challenge for State and Local

State government traditional network and security architecture relies on hub and spoke networking and castle and moat security. This architecture worked well when all users were in the office and all applications were in the State data center. However, users today are everywhere, applications are moving beyond the datacenter, and the internet is the new connectivity layer. This new reality breaks legacy perimeter based security models and calls for a modernized Zero Trust Architecture.

In order to secure all government entities within a state and protect against modern cyber threats, a collaborative approach is required. IT modernization may be implemented by one agency, but the network is only as strong as its least protected link. Whole of State collaboration requires a forward thinking approach to cybersecurity – doing something different tomorrow to achieve a different and better result in the future. We must acknowledge the resistance from local government to be infiltrated by state policies, even when it means access to funds and other resources.

States currently have an opportunity to secure a share of the State and Local Cybersecurity Grant Program, U.S. Department of Homeland

Security's program for state and local governments to enhance their information systems. There is $1B in total grant funding over 4 years, however the program requires that 80 percent of the fund flow down to local governments, and 25% of that to rural areas. Most states struggle to find the appropriate audience and decision makers in local government to discuss grant opportunities when they have no cybersecurity budget, CIO or CISO. How can state and local governments collaborate to secure and deploy these funds?

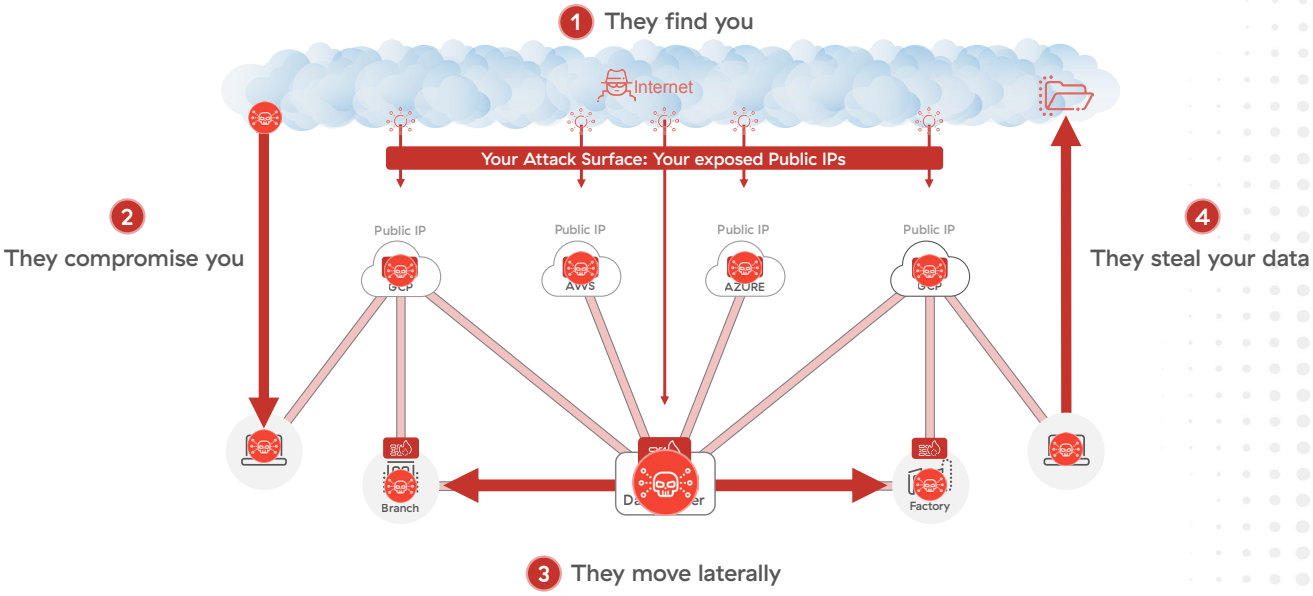
## Whole of State Strategy with Zero Trust Architecture

Secure digital transformation requires a zero trust architecture. Legacy architecture comes with increased cost, complexity, security risk, and compromised user experience.The legacy network–centric architecture has served us well for 30–plus years, but now our applications are moving everywhere, our users are becoming more mobile, and this architecture no longer works as adversaries are modernizing. That's where the Zero Trust Architecture comes in, and that's the architecture Zscaler pioneers. Let's dig deeper into why and how.

**Traditional architecture doesn't work anymore**

Over the past 30 years, organizations have built hub–and–spoke networks, connecting cloud, branches, employees, constituents, and all locations to a few data centers. The network was secured by building a perimeter around the ever–growing network. Inside the perimeter, everything is trusted, outside is untrusted.

**Why Firewall/VPN Architectures Create Issues**



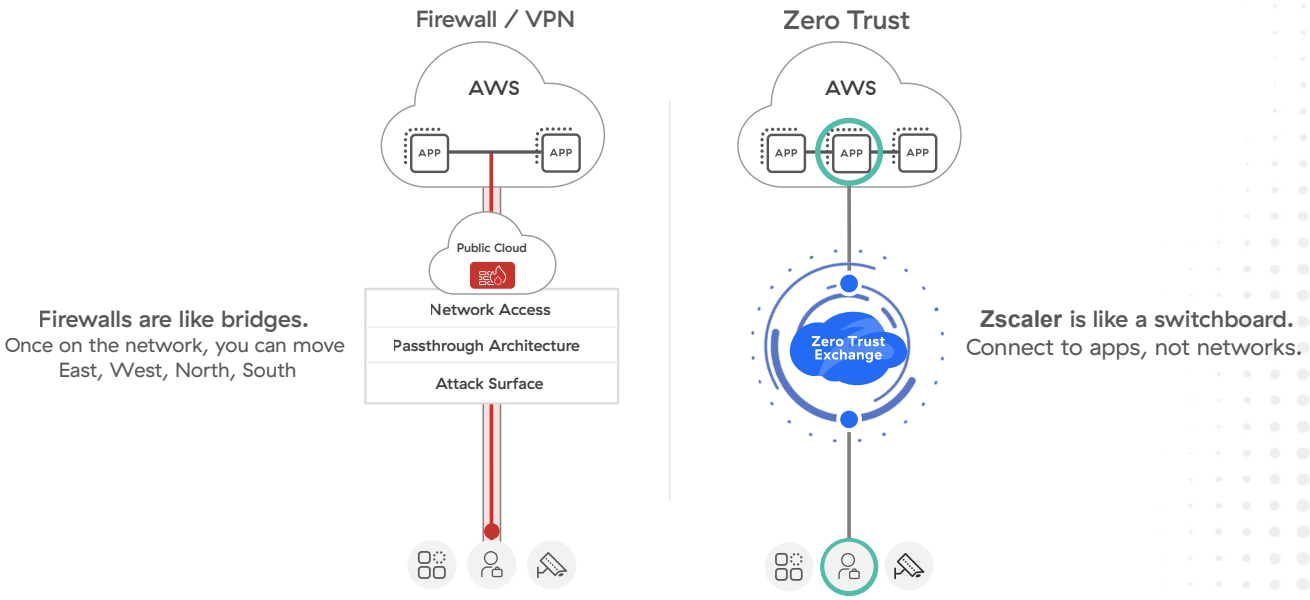
The issue with architecture that's based on firewalls and VPNs protecting a perimeter is that it functions like a bridge. Once the bridge opens, traffic starts flowing and you can go east, west, north, south. Your network is exposed to the internet and attackers exploit and penetrate entry points in your expanding attack surface. Once they find a vulnerabile entry point they compromise you, move laterally and steal your data. In today's borderless environment, where data is stored and accessed from various locations and devices, a perimeter network cannot be secured.

Traditional cybersecurity architecture is often reactive, meaning that it logs events and if capable and configured, respond to threats after they occur. This approach is no longer sufficient as threats can now spread rapidly and cause significant damage before they are detected and mitigated. A more proactive, comprehensive and adaptive approach to cybersecurity architecture is needed to protect against the growing threat of cyber attacks.

**Zero trust network architecture – a switchboard versus a bridge**

Contrast legacy architecture that functions like a bridge with zero trust architecture, pioneered by Zscaler, that functions like a switchboard. A user connects with a switchboard, and based on the policy that user gets connected to a particular application and that application only, not to the network.

**Zero Trust Switchboard vs. Firewall/VPN Bridge**




While the Zero Trust term has been hijacked by many legacy companies because they're afraid of getting disrupted, here is a simple explanation of Zero Trust Architecture. In this architecture, your applications are merely destinations – applications managed by you in your data center or in public cloud or SaaS and the internet. How do users and devices connect? You do not need a trusted network connecting everything to everything, you simply have every party connecting to the internet, and Zero Trust Architecture (ZTA) sits in the middle like a switchboard.

**Context is the new perimeter**

With ZTA, the traffic comes to us and the first thing we do is say: Stop, who are you? Once we have verified Identify, we ask where are you going? This is app specific policy, you can restrict people to go to certain applications. ZTA checks a whole host of other policies and potential risks, such as device posture, and only when everything looks good is the go/no go decision made to pass the user through the switchboard to their requested destination.

For external applications, we can connect simply to the internet and SaaS with a normal outside–in connection that starts from your end device. For internal applications that are managed by you, we have a unique technique: An inside–out connection using a piece of software called a connector. This connector only makes that connection after all these policy criteria are met. By doing so, we are actually doing a number of things for you.

First, by completing SSL inspection of all traffic, we are providing better cyber and data loss protection. Adversaries are smarter now and encrypting their payloads which pass right through firewalls and VPNs.

Next, by connecting users to applications only – not to the network – we are preventing lateral threat movement. Stolen user credentials is the number one attack vector. By removing users from the network and removing the ability for an attacker to utilize those credentials (VPN login), agencies will see huge risk reductions.

Lastly, by opening an inside–out connection, we minimize your attack surface because your applications go invisible. If they can't find you, they can't attack you. Or as we like to say, "If you're not reachable, you're not breachable."

This is Zero Trust Architecture at Zscaler, which very closely follows the NIST model.

## Continue to protect your people, your constituents and your data with a Whole of State Strategy.

## Whole of State Ecosystem

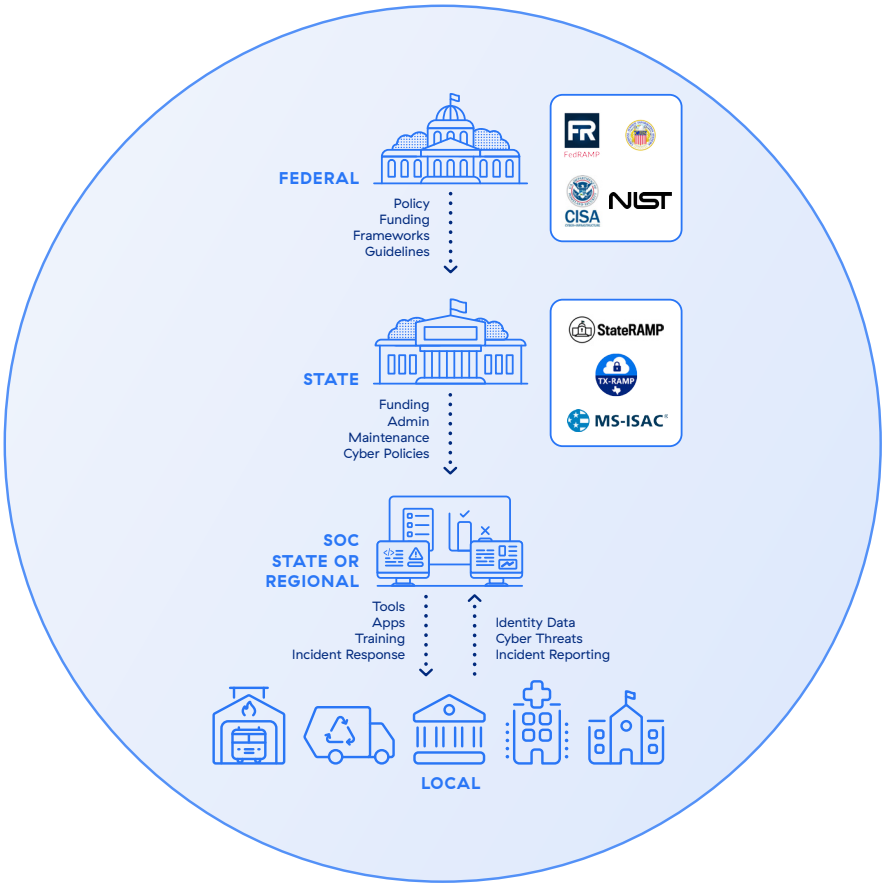
With Zero Trust Architecture, Zscaler is able to help government organizations build a Whole of State Ecosystem for cybersecurity. This symbiotic relationship between federal, state and local government strengthens security to protect and serve constituents as well as preserve national security for our country. Let's look at the contributions of each level of government in this ecosystem.

**Federal Government** – Creates federal level policies, frameworks and guidelines as well as funding for programs.

**State** – Receives federal funding and passes through to local government; also develops state level cyber policies, guidelines and collaborative committees.

**Local** – County, city and municipality determine local policies and manage public services for constituents. Each entity maintains its own data privacy

**SOC** – A State or Regional Security Operations Center sits in between the state and local levels.The State provides the administration of tools, applications, training and incident response while the Local level provides identity data, cyber threat notification and incident reporting. Together the State and Local governments are able to leverage federal funding and frameworks without compromising independent policy setting and data bifurcation.

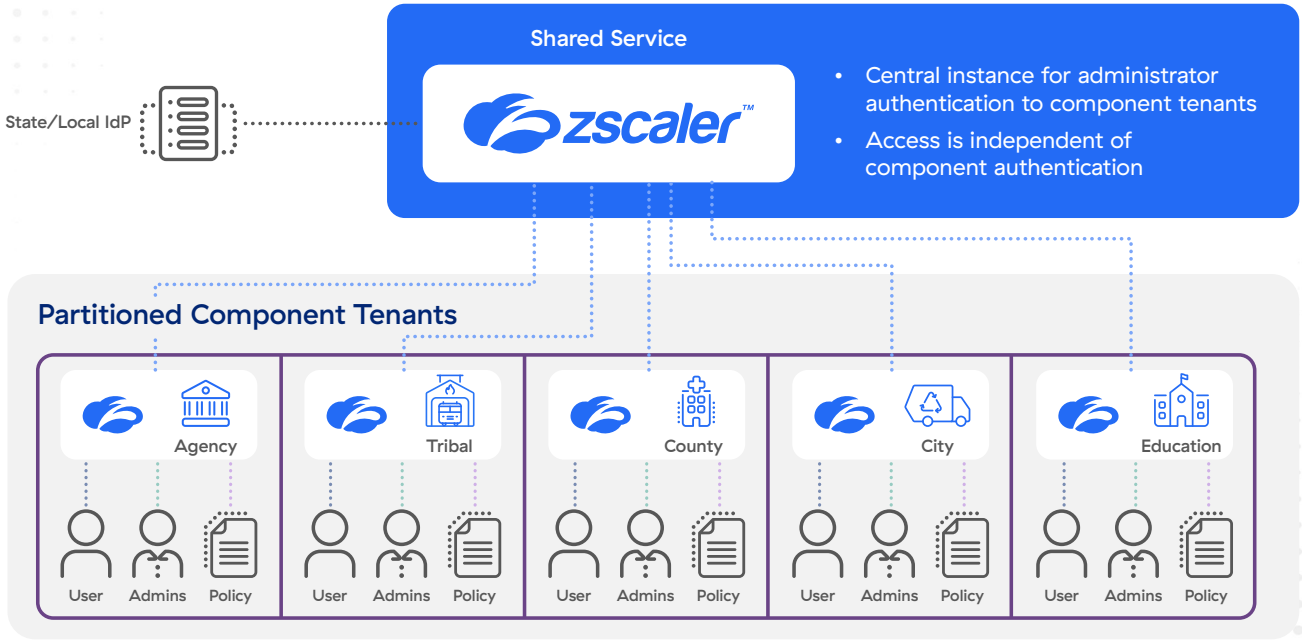


## Whole of State Built on Zero Trust Architecture

Zscaler's purpose-built multi-tenant architecture supports shared services, multi-agency environments and local governments. In a multi-tenant environment, customers share the same application, operating environment, hardware, and storage mechanism. This is distinct from virtualization, wherein every application runs on a separate virtual machine with its own operating system.

### Zscaler Internet Access

State administrative login and management; local government maintains independent policy setting.




A multi-tenant cloud is commonly likened to an apartment building—residents have keys to their own separate apartments, but they all share the infrastructure that delivers water and power. The provider sets overarching rules and performance expectations for customers, but the individual customers have private access to their data.

Utilizing multi-tenant architecture in a State or Regional SOC allows for each agency to set their own security policies and data privacy while sharing the infrastructure cost, burden and administration with other agencies. Multi-tenant clouds take advantage of their underlying architecture to achieve efficiency, flexibility, and scalability, achieve cost savings and maintain independent security policies to protect against cyber threats.

## How Zscaler can help

In partnership with state and local governments, Zscaler supports IT modernization and digital transformation in a number of ways.

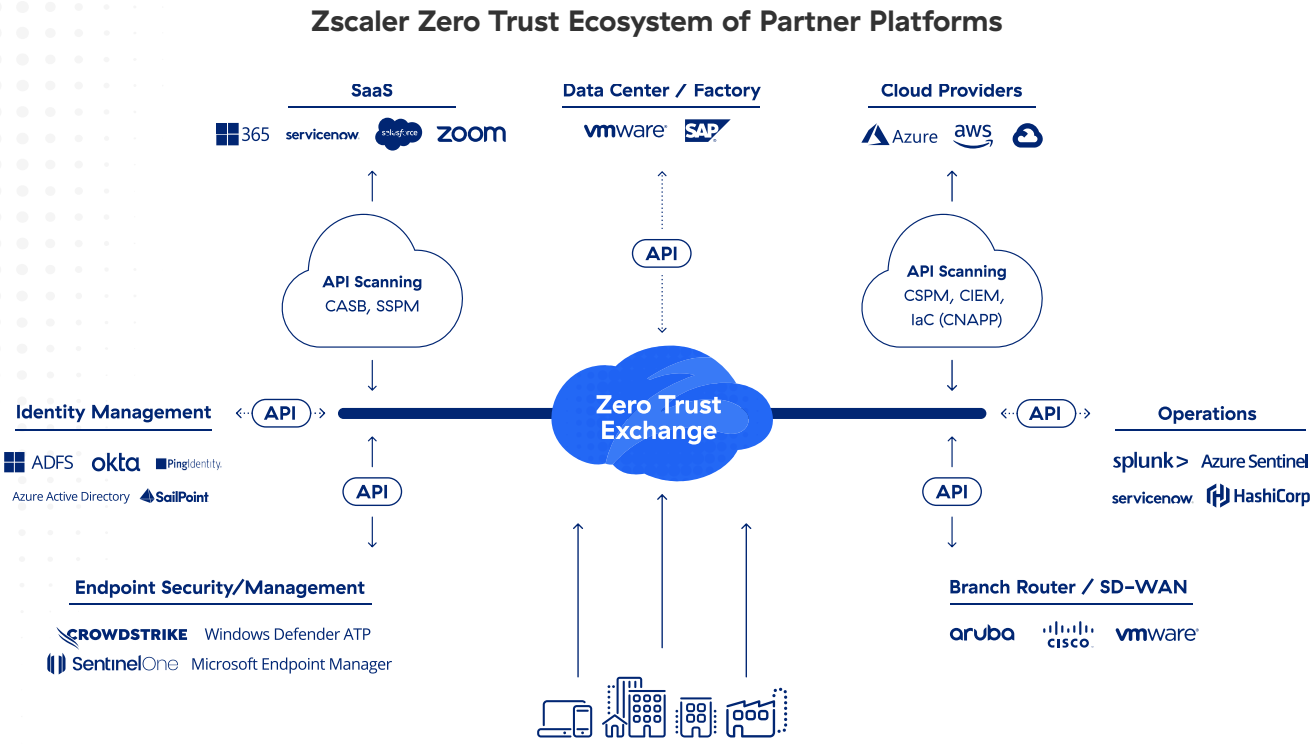
**Architectural Workshops** – We have worked with thousands of architects specializing in infrastructure, networking and security to help them understand how a cloud-hosted security architecture enables their cloud transformation journey. You and your team can schedule a private, interactive workshop with our zero trust experts to share insights and best practices during a whiteboarding session. We'll map out your current state and transform that into a digital strategy that better prevents cyberattacks, protects users and data, and reduces IT costs and complexity. Seeing a demonstration of the power of a zero trust architecture is believing.

**Hands-On Workshops** – One of the best ways to explore how zero trust architecture can benefit your agency is to experience zero trust for yourself. Zscaler regularly hosts hands-on workshops and demos for the public sector community. These events bring together public sector IT leaders, including current Zscaler customers, to discuss their first-hand experiences and unique deployment strategies. Join us for an interactive session on Zscaler Internet Access (ZIA), Zscaler Private Access (ZPA) and Zscaler Digital Experience (ZDX), to network and interact with the Zero Trust Exchange to experience the functionality and benefits of zero trust.

**State/Regional SOC Participation** – Zscaler currently works with government entities in over half of the states across the U.S. As part of a Whole of State Ecosystem strategy, we are partnering with state and local IT leaders to stand up state and regional SOCs, and we want you to be a part of this initiative. Reach out if you have interest in SOC participation.

**SLTT Grant Program** – With over 6 million users from State, Local, Tribal and Territorial customers on Zscaler's Zero Trust Exchange, we have worked with agencies on their State and Local Cybersecurity Grant Program. Zscaler assists with cybersecurity plans, zero trust architecture solution language for the application process, and mapping out a multi-year transition plan including the pass through of funds awarded to local units.

**Vendors Who Inter-Operate** – Whole of State strategies should leverage provider partnerships in deploying enterprise solutions that build and strengthen cyber defenses. Zscaler focuses on building ecosystems, including partner platforms that have already been successfully integrated in the field. We share this information with state and local governments to provide insights into how top-tier providers are working together to address all the pillars of a zero trust solution.




**ThreatLabz** – ThreatLabZ is the embedded research team at Zscaler. This global team includes security experts, researchers, and network engineers responsible for analyzing and eliminating threats across the Zscaler security cloud and investigating the global threat landscape. The team shares its research and cloud data with the industry at large to help promote a safer internet. With insight into a global cloud that processes more than 40 billion transactions per day, our researchers have unique insight into threat trends related to countries of origin, target destinations, and volumes, as well as threat categories and specific family names. ThreatLabz offers a number of free public tools to assess and monitor your risk.

## Next steps

You've done the hard work to transform from an on-premise based workforce and service delivery model to one that better reflects the remote and digital nature of our post-COVID world. Continue your transformation by shifting from legacy network infrastructure to a zero trust model that will improve your security posture and user experience. Continue the shift to a Whole of State strategy with technology that enables a collaborative ecosystem while empowering government at all levels to shape their cyber policies based on independent requirements. With the collaboration of Zscaler, our partners and our state and local governments, we are a stronger force together against cyber threats.

zscaler™ | Experience your world, secured.™

**About Zscaler**
Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.



+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com