The 2022 Federal Zero Trust Strategy with Zscaler

Jose Padin
Sr. Director of Sales Engineering, US Public Sector

October 4, 2022

Table of Contents

The Federal Government can no longer depend on conventional perimeter-based defenses to protect critical systems and data.

-President Biden

Federal Zero Trust Strategy

Overview and purpose

On January 26, 2022, the Office of Management and Budget (OMB) released the Federal Zero Trust Strategy in support of Executive Order 14028, "Improving the Nation's Cybersecurity", to adapt civilian agencies' enterprise security architecture to be based on zero trust principles.

The strategy is published as *OMB Memorandum M-22-09, "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles"* . The goal of the strategy is to accelerate agencies toward a **shared baseline of early zero trust maturity.**

OMB memo M-22-09 provides guidance on how to achieve the Zero Trust mandates of the Executive Order. It further codifies the importance of moving off of legacy security structures into a Zero Trust architecture to include:

- *No longer depend on conventional perimeter-based defenses to protect critical systems and data.*
- *Provide secure access applications over the public Internet, without relying on a virtual private network (VPN).*
- *Encrypting DNS and HTTP traffic using TLS 1.3 for all internal and external connections to include APIs.*

The memo includes deadlines for implementation plans, inventories, policy changes, and more. ***Each agency's acceptable implementation plan is due by March 2022.***

Federal Zero Trust Strategy

The strategy envisions a Federal Government where:

Overall Vision

- ❏ Federal staff have enterprise-managed accounts, allowing them to access everything they need to do their job while remaining reliably protected from even targeted, sophisticated phishing attacks.
- ❏ The devices that Federal staff use to do their jobs are consistently tracked and monitored, and the security posture of those devices is taken into account when granting access to internal resources.
- ❏ Agency systems are isolated from each other, and the network traffic flowing between and within them is reliably encrypted.
- ❏ Enterprise applications are tested internally and externally, and can be made available to staff securely over the internet.
- ❏ Federal security teams and data teams work together to develop data categories and security rules to automatically detect and ultimately block unauthorized access to sensitive information.

Federal Zero Trust Strategy Goals

The memorandum requires that agencies must achieve the below goals by the end of FY24.
The goals are organized using CISA's zero trust maturity model and align with CISA's five pillars:

01	IDENTITY	Agency staff use enterprise-managed identities to access the applications they use in their work. Phishing-resistant MFA protects those personnel from sophisticated online attacks.
02	DEVICES	The Federal Government has a complete inventory of every device it operates and authorizes for Government use, and can prevent, detect, and respond to incidents on those devices.
03	NETWORKS	Agencies encrypt all DNS requests and HTTP traffic within their environment, and begin executing a plan to break down their perimeters into isolated environments.
04	APPLICATIONS AND WORKLOADS	Agencies treat all applications as internet-connected, routinely subject their applications to rigorous empirical testing, and welcome external vulnerability reports.
05	DATA	Agencies are on a clear, shared path to deploy protections that make use of thorough data categorization. Agencies are taking advantage of cloud security services to monitor access to their sensitive data, and have implemented enterprise-wide logging and information sharing.

Actions Required to Meet Goals of the Federal Zero Trust Strategy

Vision for "Identity":

Agency staff use enterprise-manage identities to access the applications they use in their work.

Phishing-resistant MFA protects those personnel from sophisticated online attacks.

Required Actions For Pillar #1: Identity

In alignment with CISA's zero trust maturity model

Action #1: Enterprise-wide identity systems

- Agencies must employ centralized identity management systems for agency users that can be integrated into applications and common platforms.

Action #2: Multi-factor authentication

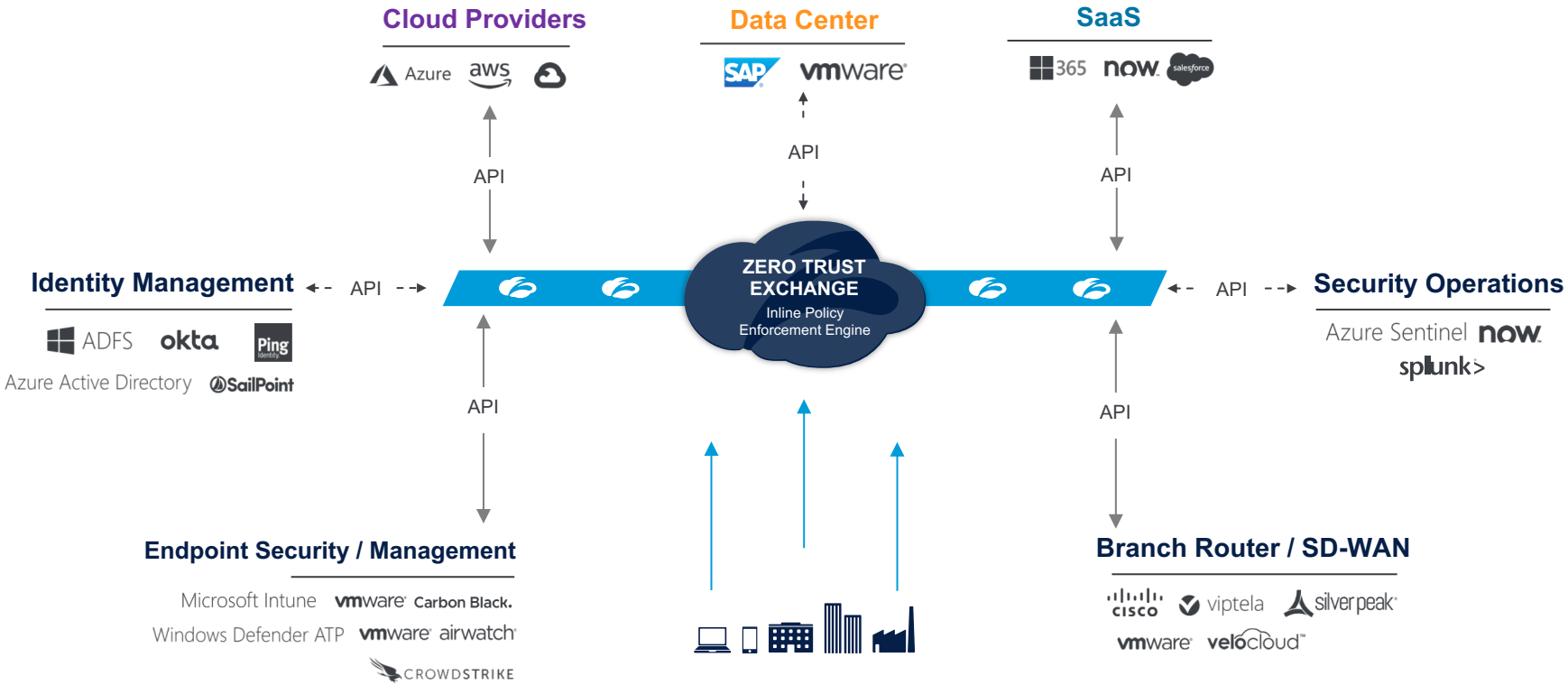
- Agencies must use strong MFA throughout their enterprise.

Action #3: User Authorization

- When authorizing users to access resources, agencies must consider at least one device-level signal alongside identity information about the authenticated user.

Ecosystem of best-of-breed platforms

Platforms eliminate point solutions and allow for vendor consolidation



Zscaler reduces cost and operational complexity

Vision for "Devices":

Agencies maintain a complete inventory of every device authorized and operated for official business and can prevent, detect, and respond to incidents on those devices.

Required Actions For Pillar #2: Devices

In alignment with CISA's zero trust maturity model

Action #1: Inventorying Assets

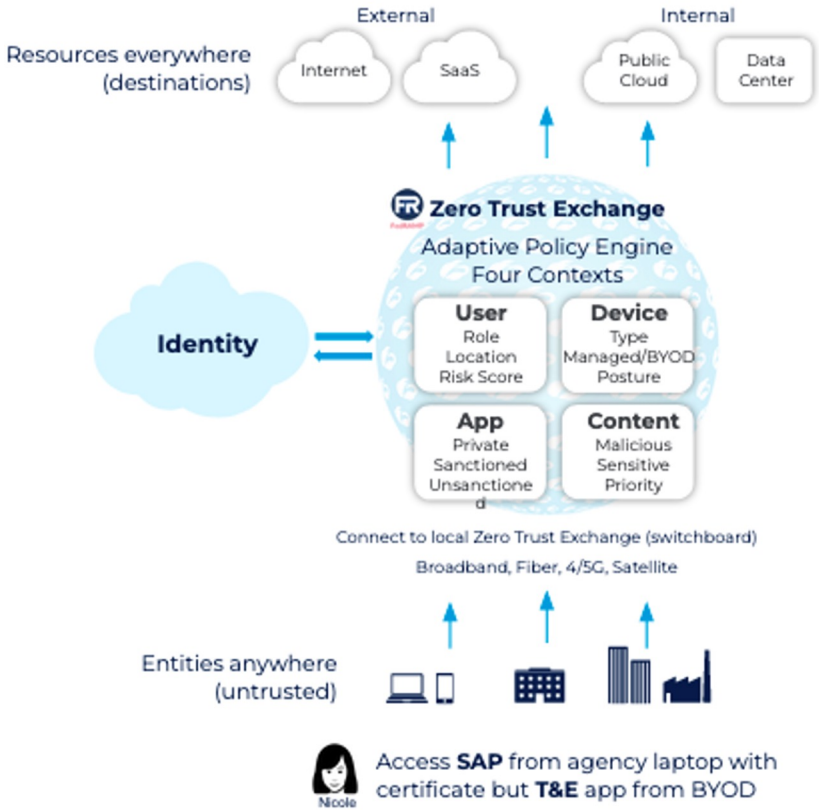
- *Agencies must create reliable asset inventories through participation in CISA's Continuous Diagnostics and Mitigation (CDM) program.*

Action #2: Government-wide endpoint detection and response

- *Agencies must ensure their Endpoint Detection and Response (EDR) tools meet CISA's technical requirements and are deployed widely.*
  - *Agencies must work with CISA to identify implementation gaps, coordinate the deployment of EDR tools, and establish information-sharing capabilities.*

How Zscaler Assures Device Security

Posture



- Endpoint Posture assurance
- Dynamic Access based on Identity & Device Profile
- BOD-22-01
  - Ensure Endpoints are patched for known vulnerabilities before application or data access.
    - Validate Windows 10 Build Version
    - Query EDR status

Vision for "Networks":

Agencies encrypt all DNS requests and HTTP traffic within their environment and begin executing a plan to break down their perimeters into isolated environments.

Required Actions For Pillar #3: Networks

In alignment with CISA's zero trust maturity model

Action #1: Encrypt DNS traffic

- Agencies must resolve DNS queries using encrypted DNS wherever it is technically supported.

Action #2-3: Encrypt HTTP and email traffic

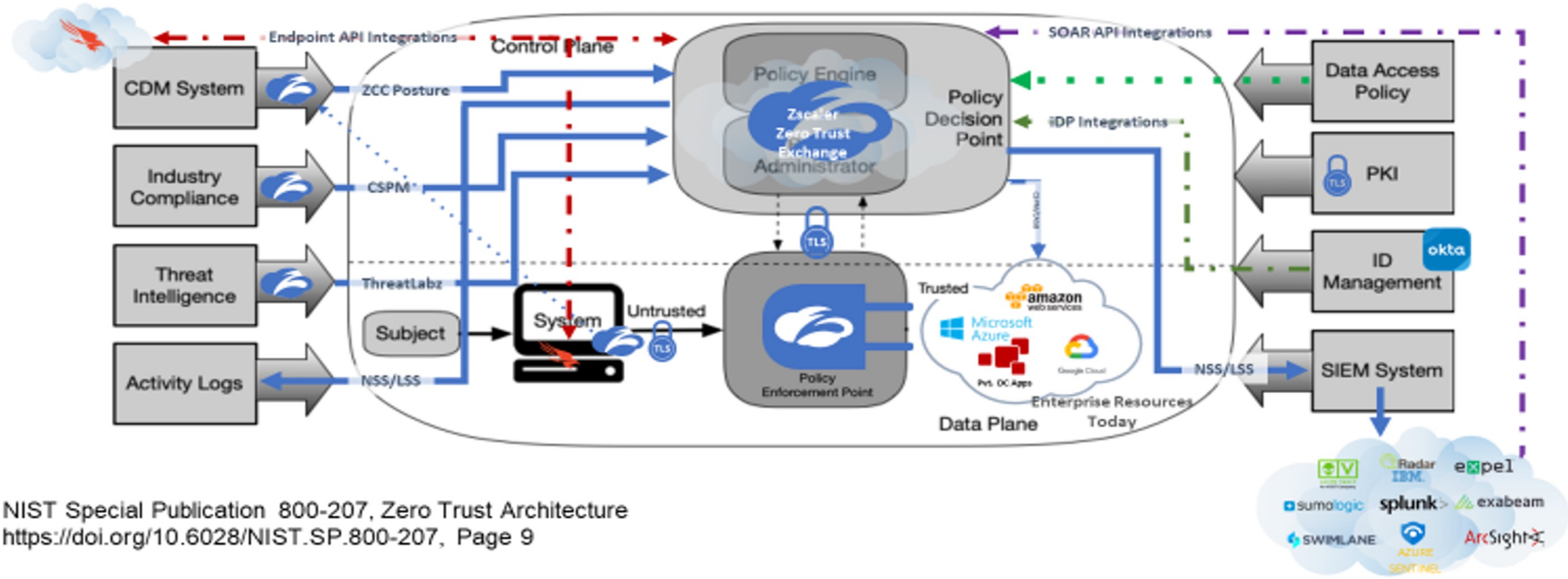
- Agencies must enforce HTTPS for all web and application program interface (API) traffic in their environment.
- CISA will work with FedRAMP to evaluate viable Government-wide solutions for encrypted email in transit and to make resulting recommendations to OMB.

Action #4: Develop enterprise-wide architecture and isolation strategy

- Agencies must develop a zero trust architecture plan that describes the agency's approach to environmental isolation in consultation with CISA and submit it to OMB as part of their zero trust implementation plan.

The NIST Zero Trust Framework

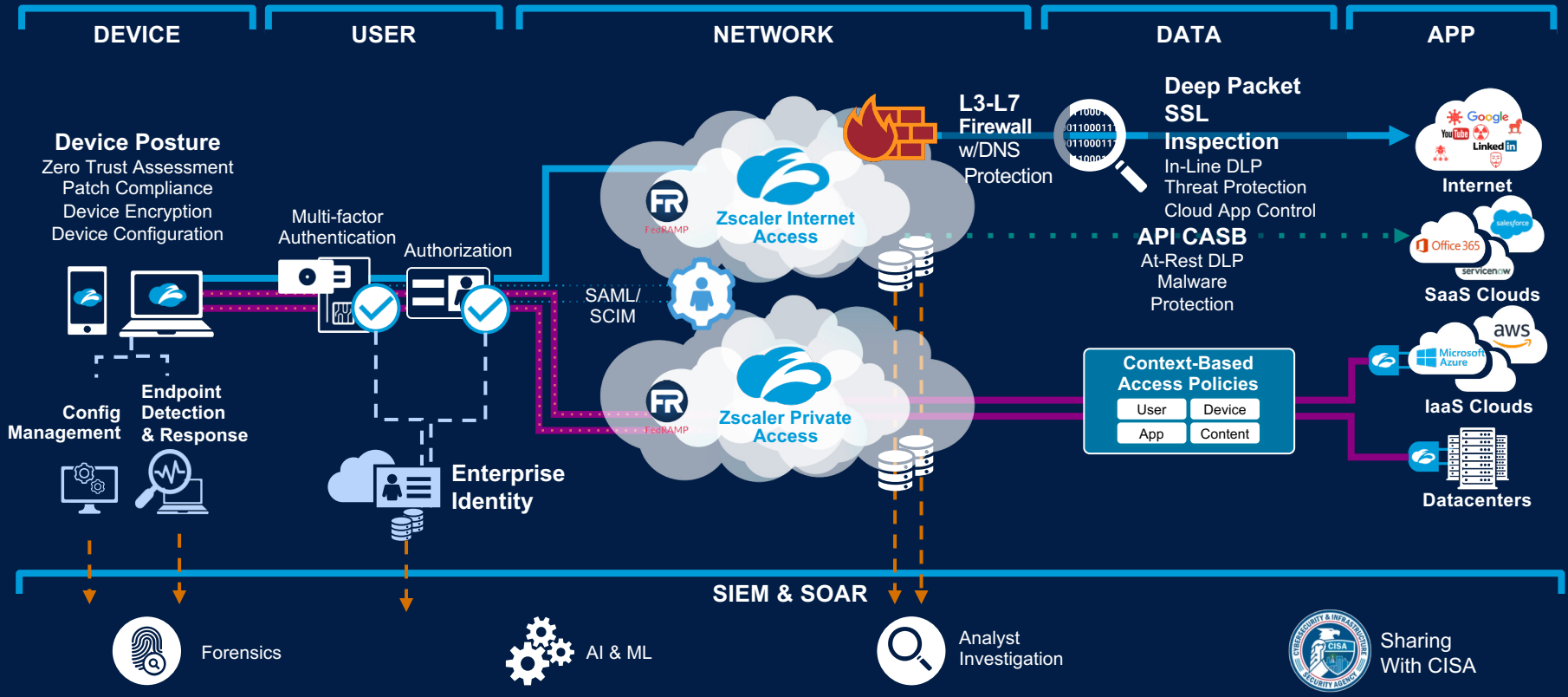
Where does Zscaler fit in?



NIST Special Publication 800-207, Zero Trust Architecture
https://doi.org/10.6028/NIST.SP.800-207, Page 9

Zscaler Zero Trust Architecture

Capability Mapping Diagram



Vision for "Applications & Workloads":

Agencies treat all applications as internet-connected, routinely subject their applications to rigorous empirical testing, and welcome external vulnerability reports.

Required Actions For Pillar #4: Applications & Workloads

In alignment with CISA's zero trust maturity model

Action #1 Application security testing

- Agencies must operate dedicated application security testing programs.

Action #2 Easily available third-party testing

- Agencies must utilize high-quality firms specializing in application security for independent third-party evaluation.

Action #3 Welcoming application vulnerability reports

- Agencies must maintain an effective and welcoming public vulnerability disclosure program for their internet-accessible systems.

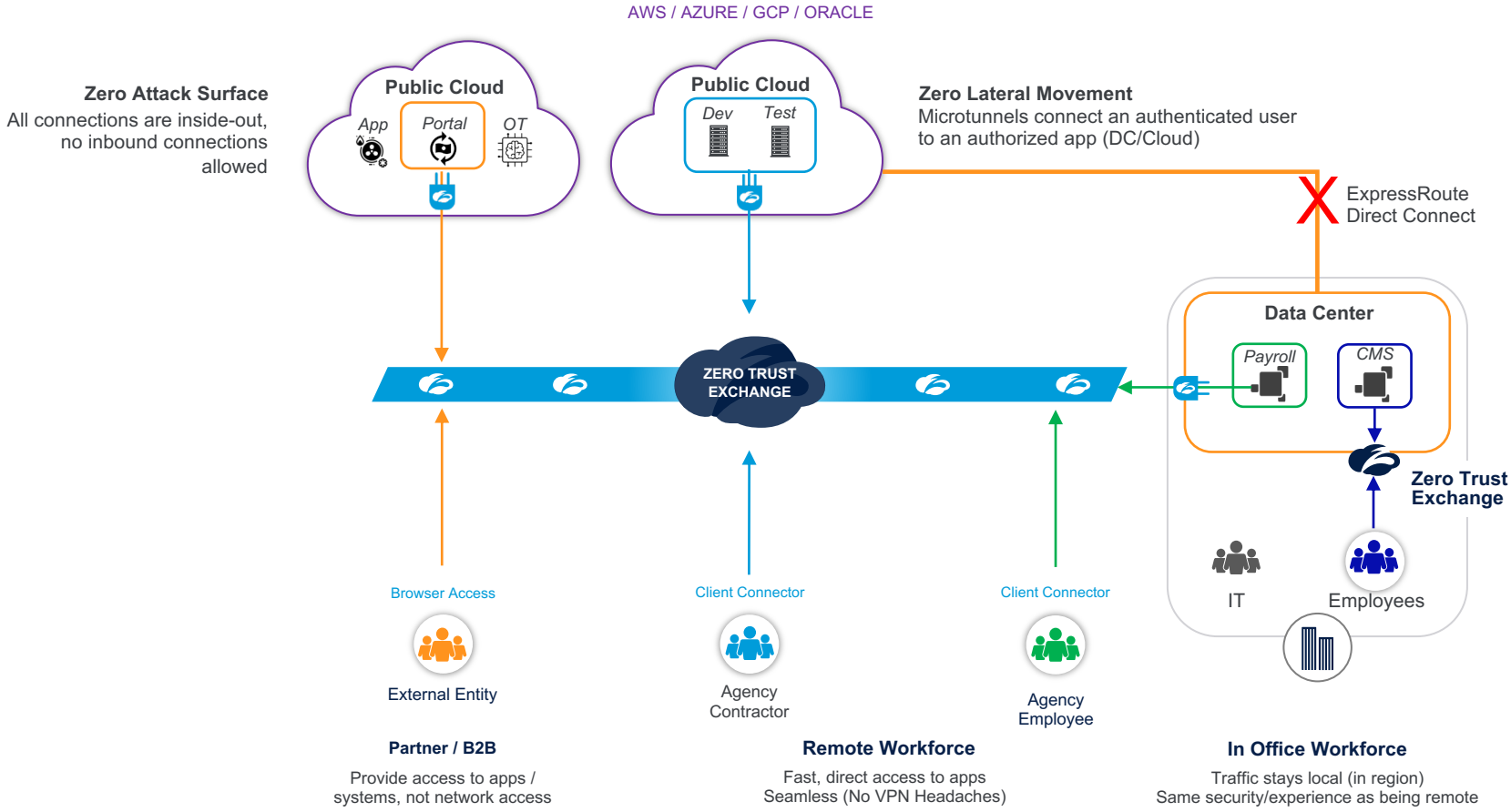
Action #4 Safely making applications internet-accessible

- Agencies must identify at least one internal-facing FISMA Moderate application and make it fully operational and accessible over the public internet.

Action #5 Immutable workloads

- Agencies should work toward employing immutable workloads when deploying services, especially in cloud-based infrastructure.

Secure User to App Access over Any Network



Vision for "Data":

Agencies are on a clear, shared path to deploy protections that make use of thorough data categorization. Agencies take advantage of cloud security services and tools to discover, classify, and protect their sensitive data, and have implemented enterprise-wide logging and information sharing.

Required Actions For Pillar #5: Data

In alignment with CISA's zero trust pillars

Action 1: Federal data security strategy

- Agencies must employ centralized identity management systems for agency users that can be integrated into applications and common platforms.

Action #2: Automating security responses

- Agencies must implement initial automation of data categorization and security responses, focusing on tagging and managing access to sensitive documents.

Action #3: Auditing access to sensitive data in the cloud

- Agencies must audit access to any data encrypted at rest in commercial cloud infrastructure.

Action #4: Timely access to logs

- Agencies must work with CISA to implement comprehensive logging and information-sharing capabilities.

Zscaler Integrations with DHS CISA

Logging and DNS

Zscaler differentiators

Certifications:

- Zscaler Private Access (ZPA™) has achieved FedRAMP-High JAB Authorization and DOD IL5 P-ATO
- Zscaler Internet Access (ZIA™) has achieved FedRAMP “In Process” status at the High Impact level, sponsored by a U.S. Department of Defense (DoD) Command and prioritized for Joint Authorization Board (JAB) authorization currently (authorized at the Moderate Impact Level)
- The Zscaler Zero Trust Exchange complies with NIST’s guidelines for Zero Trust architectures

Threat intelligence sharing:

- Zscaler shares logging information directly with CISA to expedite threat hunting, detection, protection and response to cyber security events
- Our deep integrations with EDR vendors, like Crowdstrike and Microsoft, enhance threat context

Validation:

- Zscaler currently supports 100+ federal agencies and federal integration partners

Zero Trust Maturity

Federal Zero Trust Strategy

Executive Summary

- There are specific definitions that define Zero Trust Architecture.
  - CISA has defined Zero Trust around 5 Pillars
- Federal Government Agencies are encouraged to immediately embrace and leverage Zero Trust Architecture in their agency.
- As a specific action Federal Government Agencies are asked to choose one FISMA Moderate system that is not reachable via the internet and make that system accessible via Zero Trust Architecture in 365 days.
  - The use of a FedRAMP authorized Zero Trust Private Access system to rapidly facilitate that access.