zscaler™

U.S. Government Solutions

Carnegie Mellon SEI Industry Day

The 2022 Federal Zero Trust Strategy with Zscaler

Jose Padin-Sr. Director Public Sector Engineering
Jeremy James - Director of Strategic Initiatives
Bob Smith - Federal Systems Engineering Manager

August 30th 2022

Agenda

- Problem Statement
- Federal Zero Trust Strategy
  - Overview and purpose
  - Overall Vision
  - Federal Zero Trust Strategy Goals
- Required Actions for Federal Agencies
  - Identity
  - Devices
  - Networks
  - Applications and Workloads
  - Data
- Appendix A-Financial Breakdown
- Appendix B- Zscaler Resources

> The most difficult part of requirements gathering is not the act of recording what the user wants, it is the exploratory development activity of helping users figure out what they want.
>
> ~ *Steve McConnell*

Problem Statement Review

Filtering Signal from Noise

Nested Federal Requirements

A large U.S. federal agency provides services used by global users. The agency currently is operating a hybrid, multi-cloud enterprise that supports about 45,000 federal employees and 15,000 contractors . The enterprise's networks break down into Information Technology (IT) (75%), Operational Technology (OT) (15%), and Supervisory Control and Data Acquisition (SCADA) (10%). The OT and SCADA networks support the agency's smart buildings' controls/operations and distribution centers.

Identity & Logging

Currently, the agency has identified three high-value assets (HVAs): two legacy systems and one database containing Protected Personal Information (PPI). The agency is currently using four different identity and access management (IAM) systems (Okta Identity Cloud, Cirrus Identity, Azure AD, and Google Cloud Identity) and lacks a centralized security operations center (SOC).

The agency is currently unable to integrate logging information due to the continued use of legacy systems: an organizational structure where SOC operations are broken across different teams and a hybrid, multi-cloud implementation where services provide different formats for the information. The agency must implement two-factor authentication but also must provide multi-factor authentication (MFA) for some parts of the enterprise.

Ecosystem Interoperability

The agency has a budget of $3 million and a one-year timeline during which it must start to address M-22-09. Given this last constraint, each proposal should address its compatibility with the agency's existing hardware and software infrastructure.

> *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:

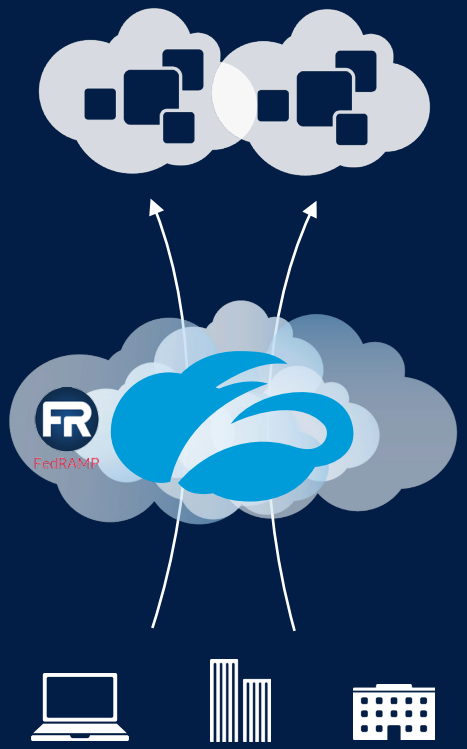
- *No longer depend on conventional perimeter-based defenses to protect critical systems and data.*
- *Provide secure access applications over the public Internet, without relying on a virtual private network (VPN).*
- *Encrypting DNS and HTTP traffic using TLS 1.3 for all internal and external connections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

The memo includes deadlines for implementation plans, inventories, policy changes, and more.

Zscaler Federal Security Cloud

Securely transform IT for a cloud world

Governance policies connect users to apps from anywhere, over any network based on TIC 3.0 Framework



FAST. SECURE. RELIABLE.

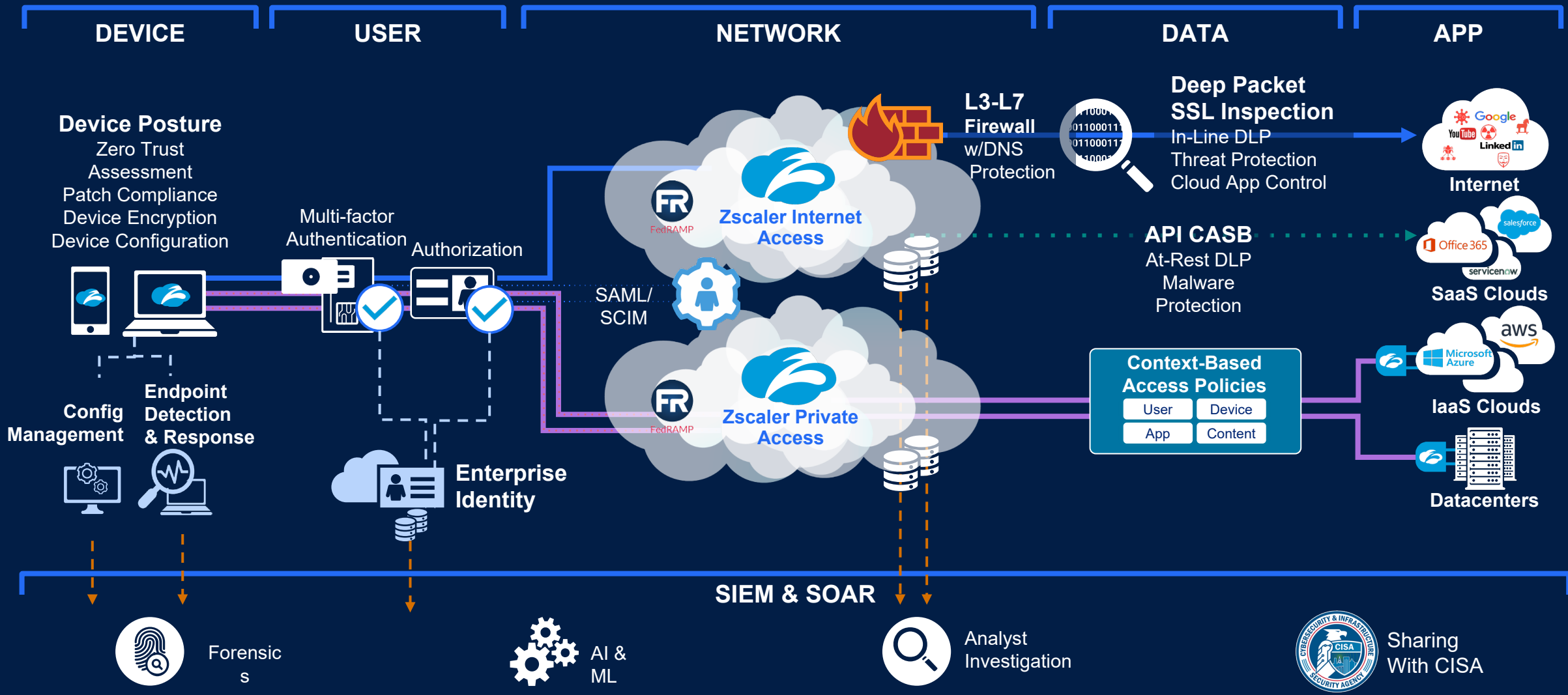
Market Leader **500** of the **Forbes Global 2000**
Nasdaq: ZS

Proven Scale **220 B+** **transactions** processed daily

FedRAMP High + Moderate + DOD Impact Level 5 **5** **data centers** across the U.S.

Zscaler Zero Trust Architecture

Capability Mapping Diagram



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: Identity (Pillar #1)

Aligned 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.

Zero Trust Best Practices: Identity Provider

- **Set up and External IPD-** External Identity Providers are a must- Azure AD, Okta, etc - Benefit provides faster easier integration across multiple Platforms .
- **Must be SAML 2.0 Compliant**
- **Must leverage SCIM**
- Use a Service that is ubiquitous and Easy to manage and maintain

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: Device (Pillar #2)

Aligned 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.

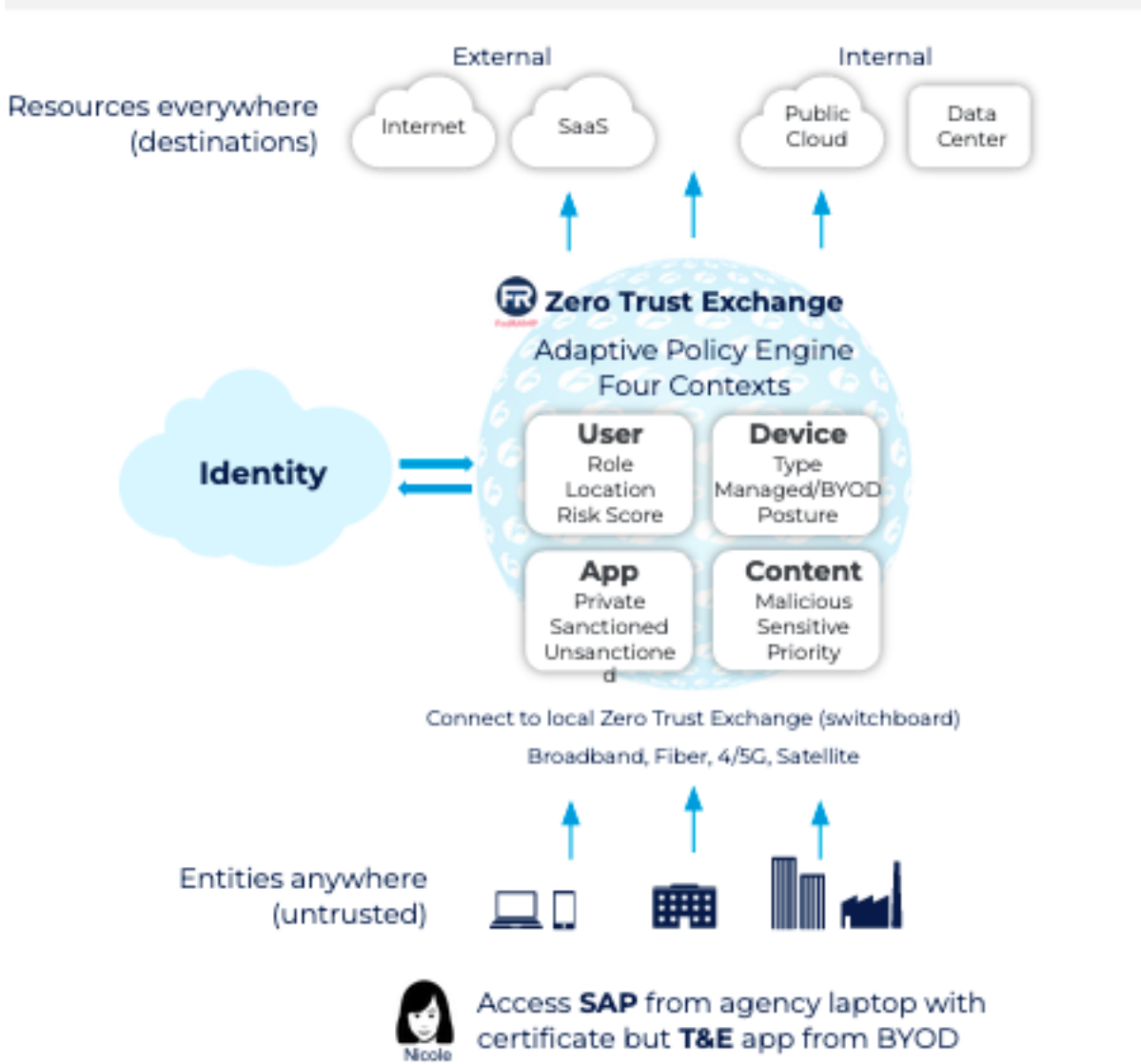
Action #2: Government-wide endpoint detection and response

- ❑ 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 Checking

- 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



Best Practices for Endpoint Device Posture Assessment

- What is the bare minimum “risk score” we as an organization are willing to tolerate?
- Will this solution integrate well with other vendors and Platforms- what level of API integrations are available.
- Does the EDR solution work well in the cloud?
- Can it integrate with deception technologies?

Gotcha’s for EDR solutions

- Is the EDR solution dependent on being able to scan the network?? M-22-09 removed end users from the network?
- What options are available for client to server communication?
- Log format compatibilities and support

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: Networks (Pillar #3)

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.

Best Practices: DNS Security

- **Ensure DNS logs all activities** Look for signs of Cache poisoning and redirects .
- **Lock DNS Cache**
- **Enable DNS filtering -** Provides administrators the ability to block users from going to malicious sites.
- **Use DNSSEC to validate integrity-** ensures that DNS responses have a valid digital signature.
- **Ensure accurate configuration of access control lists**
- **Separate authoritative from recursive name servers**
- **Use Anycast to enable forwarding routers to redirect DNS queries**
- **Hide the primary DNS server**

Required Actions: Applications & Workloads (Pillar #4)

Aligned with CISA's Zero Trust Maturity Model

Vision for "Applications & Workloads":

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

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

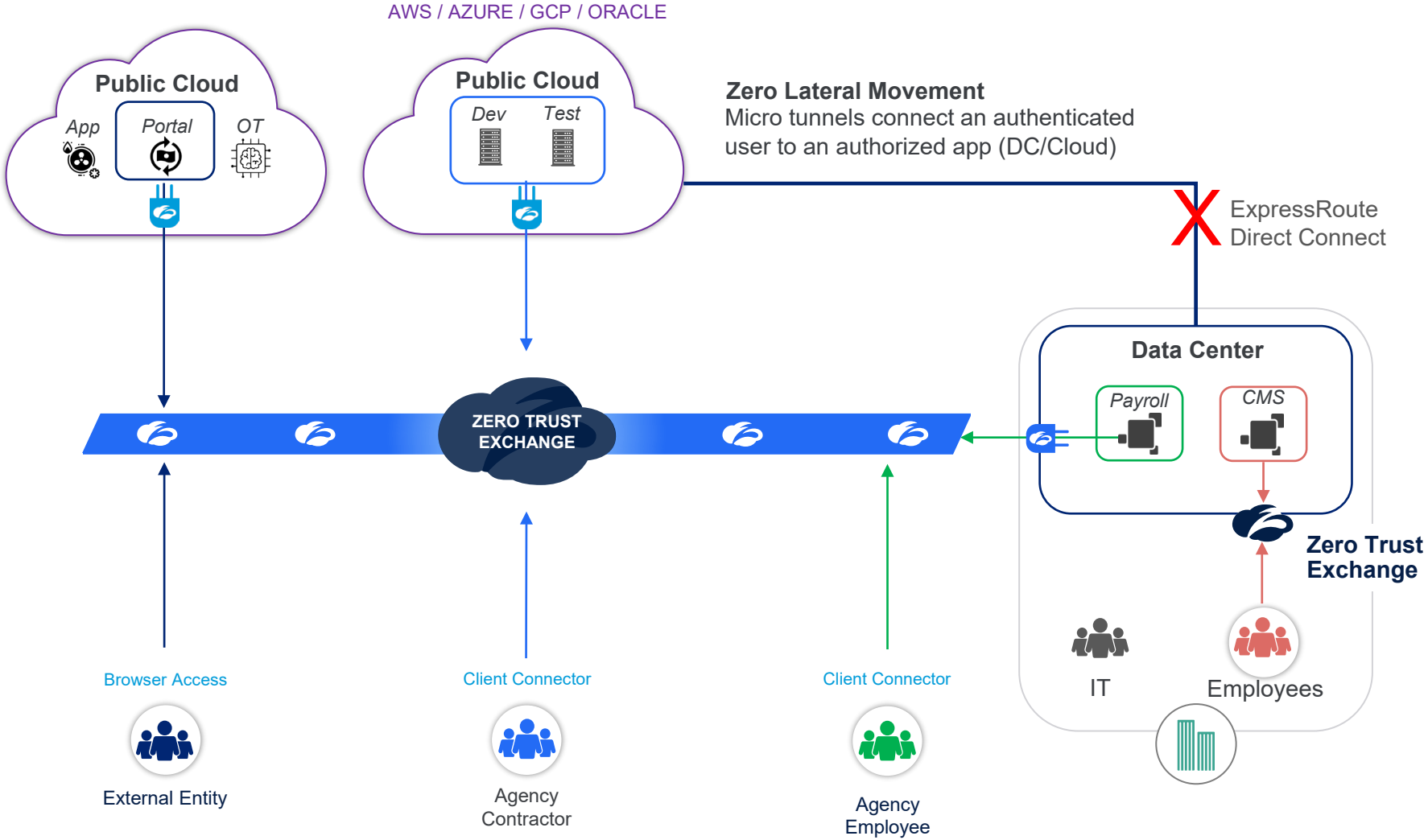
- ❑ Agencies must identify at least one internal-facing FISMA Moderate application and make it fully operational and accessible over the public internet.

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

Zero Attack Surface
All connections are inside-out, no inbound connections allowed



Partner / B2B
Provide access to apps / systems, not network access

Remote Workforce
Fast, direct access to apps
Seamless (No VPN Headaches)

In Office Workforce
Traffic stays local (in region)
Same security/experience as being remote

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 Action: Data (Pillar #5)

Aligned with CISA's Zero Trust Maturity Model

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.

12 Months Active Storage

18 Months Cold Data Storage

~ M-21-31

Required Actions: Logging

Aligned to OMB M-22-09, M-21-31 & CISA's eVRF

Action #1: Assess Event Logging Maturity

- ❑ Perform full compliance with requirements for implementation, log categories, and centralized access. Agencies should also prioritize their compliance activities by focusing first on high-impact systems and high value assets (HVAs).

Action #2: Develop Visibility Coverage Map(s)

- ❑ Use current digital capabilities scope current visibility coverage and gaps

Action #3: Timely Access to Logs

- ❑ Implement comprehensive logging and information sharing capabilities, as described in OMB Memorandum M-21-31.

*Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents

Zero Trust Best Practices: Logging

- **Identify HVAs and Critical Level 0 Logs**
- **Define what needs to be logged and monitored, and why-**
- **Identity which assets and events need to be monitored, and why**
- **Design logging and monitoring systems with security in mind**
  - Automate as much of the monitoring process as possible
  - Tailor alerts and log sources to emerging threats and Incident Response Teams
  - Ensure that log and alerts are generated in a standardized format
- **Establish active monitoring, alerting and incident response plan**
  - Enforce role-based access controls and least privilege
  - Encryption at rest and transit
- **Adopt organization wide logging and monitoring policies**

Logging best practices

- **Separate Signal from the Noise- look for KIOC (Key Indicators of Compromise)**focus on user activity, firewall allow block policies,
- **Implement Structured Logging-** implement structured logging and write logs in a format like JSON or XML that's easier to parse, analyze and query.
- **Build Meaning and Context into Log Messages-** logs should be descriptive and detailed with timestamps, unique identifiers and unique requesters
- **Avoid Logging Non-essential or Sensitive Data-** ensure you are only logging meaningful data and avoid logging sensitive data like HIPAA etc that could violate privacy laws.
- **Index Logs for Querying and Analytics-** optimizes data queries
- **Configure Real-Time Log Monitoring and Alerts-**ensure multiple people and teams are alerted on high severity or anomalous events.
- **Optimize Your Log Retention Policy** institute HSM policies for log data 12 Months Active/ 18 Months of Cold storage

Zscaler Integrations with DHS CISA

Logging and DNS

Industry Differentiators

Certifications:

- Zscaler Private Access (ZPA) has achieved FedRAMP-High JAB Authorization, FedRAMP Moderate, and DOD IL5 P-ATO
- Zscaler Internet Access (ZIA) has achieved FedRAMP-High JAB Authorization, FedRAMP Moderate, and DOD IL5 “In Process”
- The Zscaler Zero Trust Exchange complies with NIST’s guidelines for Zero Trust architectures

Crowd-sourced Threat intelligence:

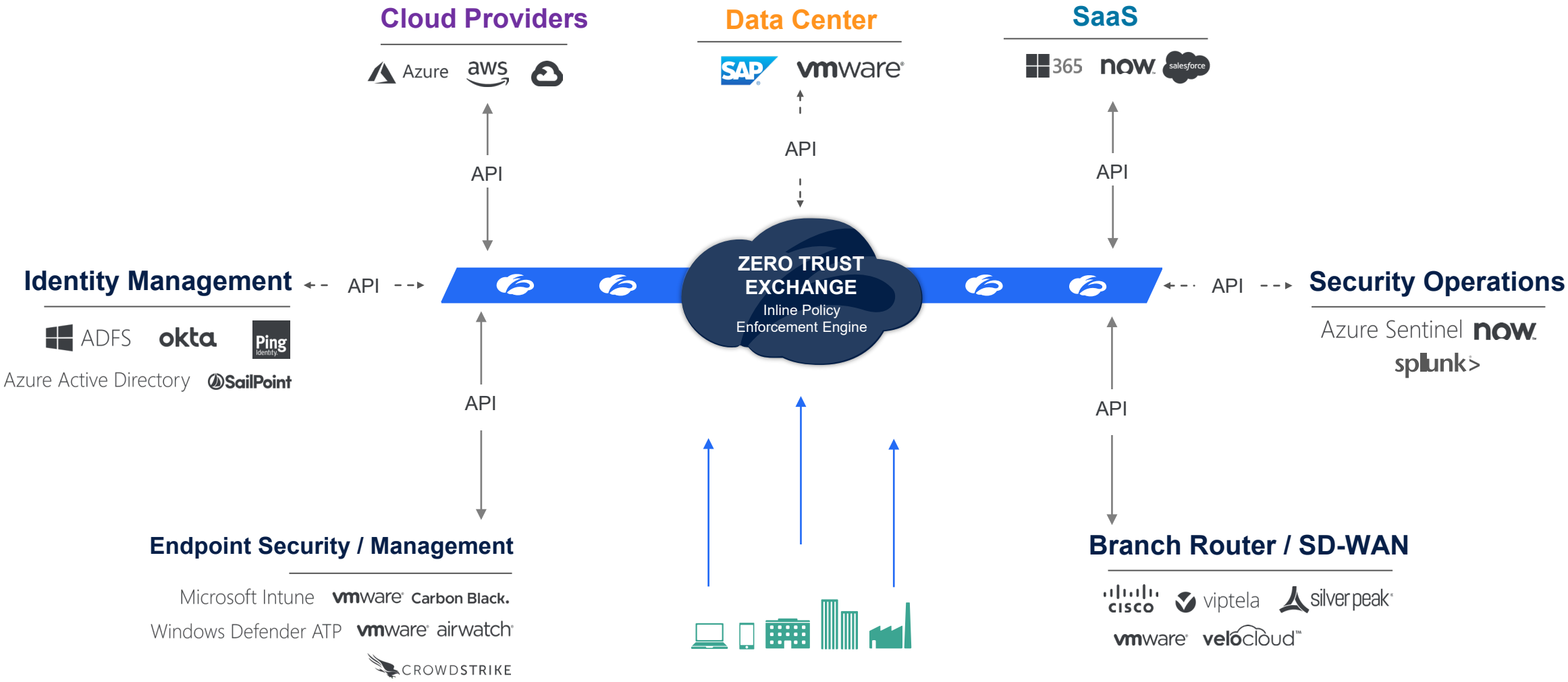
- Zscaler shares logging information directly with CISA to expedite threat hunting, detection, protection and response to cyber security events
- Our deep integrations with EDR vendors, like Crowdstrike and Microsoft, enhance threat context

Validation:

- Zscaler currently supports 150+ federal agencies and federal integration partners

Ecosystem of best-of-breed platforms

Platforms eliminate point solutions and allow for vendor consolidation



Zscaler reduces cost and operational complexity

U.S. Government Solutions

Thank you

Appendix A- Financials breakdown and ROI

How does Zscaler deliver value to Agency XYZ?

Secure connectivity

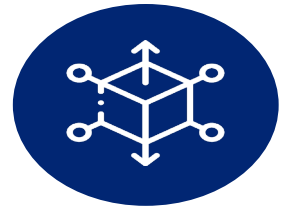
Establish direct and secure access for users and devices (regardless of physical location) without a VPN, reducing the attack surface and adhering to regulatory compliances

Optimized performance

Keep users productive on the task at hand with improved availability and frictionless connections with least privileged access to only authorized applications

Operational Efficiencies

Real-time visibility into performance degradation and outages cloud applications enables quick resolution of user issues



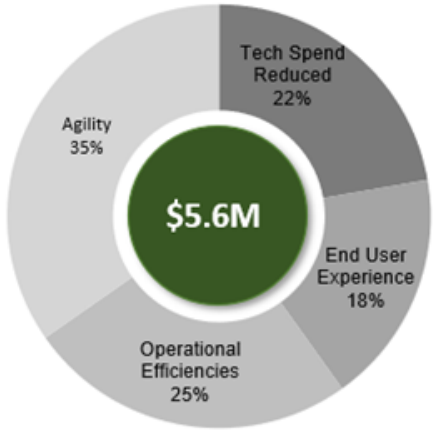
Total Cost of Ownership

Cloud-delivered zero trust network access (ZTNA) simplifies network architecture while providing infinite horizontal scale

Potential Benefits for Software Engineering Institute

Value Drivers	As-Is	To-Be with Zscaler	Annual Benefit (at full maturity)	Business Outcomes
Tech Spend Reduced *Cost of related Comparable Technology*	**$4.05 M**	**$2.13 M**	**$1.92 M / ▼ 48%**	Reduction of legacy infrastructure and appliances by ~ 50%
End User Experience *Lost Productivity Cost*	**$4.77 M**	**$3.22 M**	**$1.54 M / ▼ 32%**	Fast and seamless access to any app from any device/location resulting in decreased latency (~ 30%) that improves productivity
Operational Efficiencies *Applicable Operations Cost*	**$4.25 M**	**$2.08 M**	**$2.18 M / ▼ 51%**	Simplification of operational management needs resulting in an improved efficiency and scalability of Security and Network staff by ~50%
Contractor Onboarding *15k contractors*	**$15.00 M**	**$12.00 M**	**$3.00 M / ▼ 20%**	Enable faster, more efficient resource optimization while also reducing time and cost to integrate (~20%)
Subtotal - Benefits	**$28.07 M**	**$19.43 M**	**$8.64 M / ▼ 31%**	
Zscaler Solution Licensing & Deployment		**$3.00 M**	**$-3.00 M**	Note: The Zscaler licensing & deployment costs represented are for modeling purpose and do not represent final pricing. Final pricing is delivered by our partners.
Total - Net Benefits	**$28.07 M**	**$22.43 M**	**$5.64 M / ▼ 20%**	
Long Term ROI (3 Year)	**188%**	**Pay Back Period**	**Year 1**	

Annual % contribution by Outcome



Appendix B- Technology links and Contacts

Relevant Technical Documentation

Zscaler Public Sector landing page

https://www.zscaler.com/industries/public-sector

Zscaler landing page for M-22-09 mandate

https://www.zscaler.com/industries/government-cisa

Solution Brief for TIC 3.0

https://www.zscaler.com/resources/solution-briefs/sase-based-tic-3.0.pdf

Best Practices for IDP integration

https://help.zscaler.com/zpa/idp-configuration-best-practices

Endpoint Technology Alliances

https://www.zscaler.com/partners/technology/endpoint

Integrating Security Analytics into your logging

https://www.zscaler.com/resources/white-papers/zscaler-security-analytics.pdf

Key Contacts from Today

Jose Padin

Sr Director Public Sector Sales Engineering

JPadin@Zscaler.com

Jeremy James

Director Strategic Initiatives- Public Sector

JJames@zscaler.com

Bob Smith

Federal Systems Engineering Manager

BSmith@zscaler.com