The Zscaler™ Zero Trust Playbook for Federal Agencies

zscaler™

We live in a mobile, cloud-hosted, telework world that has changed when, where, and how the government works. It has also changed how malicious actors commit cybercrimes, which means that the federal government must likewise change how it manages cybersecurity.

In May 2021, the Biden Administration released an Executive Order (EO) on Federal Cybersecurity that underscores the government's growing recognition of cyber-vulnerabilities and IT's vital role in every federal program and mission. The EO outlines a number of actions, including a significant directive for the Department of Homeland Security to develop a federal cloud security strategy that moves the federal government closer to a truly centralized enterprise model. The guidelines set forth in the EO are founded on the principles of zero trust: a framework built on context-aware, least-privileged access, and based on a default-deny threat posture.

The transition from a fixed security architecture designed around a perimeter to one that can address the adaptive IT landscape unique to every organization—while controlling security policy inline to the service—is changing the principles of design and practice.

What is zero trust?

There is a lot of information available about zero trust, but, unfortunately, it's rarely consistent and often unreliable. Talk to three vendors and you'll get three different answers as to just exactly what zero trust is and how to adopt it within your agency. What you need to know is this:

- It is NOT a thing you can buy, set up, and leave alone.
- Your implementation path will depend on your organization's tools and infrastructure.
- You do NOT have to replace all of your legacy systems to start protecting your data right now.

Zero trust IS an ecosystem. Its use is a continuous process and there are practical ways to approach it to meet your agency's security goals. We created this playbook to help our customers wrap their arms around the concept and provide a practical approach to implementing zero trust.

Think of zero trust like thanksgiving dinner

How can we explain a concept that has so many permutations as zero trust? We'll start with an analogy from American life: The Thanksgiving Feast.

No two Thanksgiving feasts are exactly the same—the table looks different in every home depending on family traditions and a range of other factors. But it's likely that the feast includes some common components, such as turkey, stuffing, mashed potatoes, sweet potato pie, green bean casserole, and apple pie.

Among those basics, there may be other family favorites: ham, tofurkey, cornbread, mac-and-cheese, green salad, steamed broccoli. And among the range of dishes, there are multiple ways to prepare each—roasted or deep-fried turkey; cranberry sauce in a can or homemade; apple pie, apple cobbler, apple crumble.

With so many choices, how do you decide how you will approach the feast?

If you want to try everything (without ending up in a food coma), you need a strategy for how you will fill your plate. Your choices and portions will be dictated by your preferences and your health priorities.

If you're a vegetarian, you know to skip the turkey and sausage stuffing. If you're avoiding carbs, you go for the turkey and salad. If you're counting calories, perhaps you avoid the pies entirely.

Regardless, you are going to enjoy your feast one bite at a time. If you didn't get to try everything you wanted, there's always tomorrow.

Approaching your zero trust strategy is like approaching the thanksgiving dinner table. Not all zero trust "feasts" are exactly the same. They will look different depending on each agency's specific environments and requirements. There are dozens of selections that may meet your needs and desires. And there are many more that play a part in the big picture, but they're independent solutions and won't accomplish a complete zero trust posture on day one.

Yet, if your long-term goal is a healthy and secure network, you should plan for a complete, integrated implementation. So, you prioritize the offerings that are right for you.

The zero trust playbook

Knowing that you can approach the zero trust buffet from different angles, how do you extract the most value with the least impact to the environment, while meeting all of your growing compliance requirements?

Zscaler's philosophy is that users should be connected directly to the applications and data they need through a cloud-native proxy—without having to connect to (and expose) a network. This direct connection is based on identity, policy, and dynamic risk scoring. It is not only much safer but also far simpler to administer in comparison to traditional network segmentation.

The NIST guidance provides the baseline for federal zero trust recommendations, and provides the foundation for the Zscaler pillars.

1. All data sources and computing services need to be considered resources.
2. All communication needs to be secured regardless of network location.
3. Access to individual enterprise resources is granted on a per-session basis.
4. Access to resources is determined by dynamic policy—including the observable state of client identity, application, and the requesting asset—and may include other behavioral attributes.
5. The enterprise ensures that all owned and associated devices are in the most secure state possible, and monitors assets to ensure that they remain in the most secure state possible.
6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed.

Pillars for implementing zero trust

Based on the NIST guidelines and others, we developed a set of pillars to use as a five-part playbook for making the decisions that will support your agency's goals:

1 Assess alternatives to legacy network models with a cloud-native zero trust architecture

- Connect users and applications to resources, not the corporate network, to prevent lateral movement of threats, thus reducing security and business risk.
- Make applications invisible to the internet. Applications protected behind the Zscaler Zero Trust Exchange™ are not visible and cannot be discovered, thus eliminating the attack surface.
- Use a proxy architecture, not a passthrough firewall, for content inspection and security. The only way to ensure effective cyberthreat prevention and data protection is by requiring content inspection, including content in encrypted traffic, and policy enforcement before it reaches its intended destination.

We also recommend using a software-defined wide-area network (SD-WAN) solution because it enables a direct-to-internet connectivity model. Conceptually, SD-WAN separates network control from hardware, effectively virtualizing WAN management. When utilizing SD-WAN:

- Use local internet breakouts instead of backhauling traffic from branch offices to headquarters over multiprotocol label switching (MPLS) circuits.
- Make sure you have consistent security available everywhere.

2 Implement consistent, user- and application-centric security controls.

Moving to a cloud model does not mean sacrificing security and performance for user experience. You can have the best of both worlds if you:

- Move security as close as possible to the service leveraging a cloud-based security tool with local points of presence. Recognize and account for scalability costs as user traffic increases using a FedRAMP accredited cloud-based security tool.
- Invest in tools that allow fast, secure, policy-based access between users and the applications they connect to, regardless of the network. Security is essential, but it is the first thing users discard or bypass when they're having a bad or slow experience, which makes a poor user experience the greatest security risk of all.
- Monitor dynamically. Using identity alone is not sufficient. Policy should be based on context using dynamic attributes, such as a user's device, location, threat posture, behavioral anomalies, etc. Aim for a default-deny policy with comprehensive oversight of data in transit, and use microsegmented connections leveraging Transport Layer Security (TLS) to encrypt each session individually.

3 Invest in a federated identity and access management (IAM) platform.

A federated identity and access management system allows you to link a person's electronic identity and attributes across apps and platforms. When investing in a platform, it's key to:

- Start with the legacy directories you have today, but plan for migration to a modern IAM that supports single sign-on (SSO) and leverages protocols, such as security assertion markup language (SAML), to integrate with your cloud ecosystem.
- Simplify partner access. Giving partners access to a particular application should not mean giving them full access to your network. If an employee at your partner's organization leaves, you should not have to worry about whether that employee still has access to your application.
- Provide multiple identity providers (IDPs) with tight integration with the other zero trust principles. This must be foundational to an organization's IAM strategy.

4 Revisit your endpoint management system.

As workers move to the cloud, your agency must reevaluate endpoint management. Two practices to consider incorporating for endpoint management in a cloud environment are:

- Integrate endpoint management into security operations center (SOC) workflows. Infected machines and devices must be controlled and isolated.
- Establish policy-based orchestration. Updates (such as for configuration or patches) should be controlled, and policy should be able to be set at a granular level, e.g., "Push this setting out to all Macs running version X tonight." The orchestration of connectivity is tied back into the Zero Trust Exchange, and access is never permitted until the endpoint management has passed its checks.

5 Consolidate logs in a SIEM system.

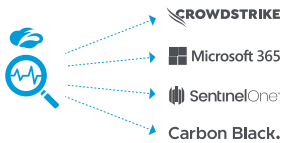
Event management, like most traditional hub-and-spoke network functions, has to evolve to function properly (read: securely) in a cloud environment. The cybersecurity executive order mandates log sharing and detection enhancements, so ensuring that security logging is robust and centralized is a must. IT leaders moving to the cloud need to ensure SIEM can handle the impacts of the transition. When doing so:

- Ensure the "new SIEM" can handle the explosion of data from multiple cloud services and have the smarts to correlate events and glean actionable insights.
- Avoid sampling. Sampling logs can lead to missed security events and issues with compliance and regulatory requirements when you have audits.
- Integrate SIEM with SOC workflows. As with endpoint management, IT leaders must ensure SIEM and SOC workflows are integrated and automated as much as possible.

Executive order on improving the nation's cybersecurity

1 Implement Cloud-Native Zero Trust Architecture

2 Improve Endpoint Detection & Response Capabilities



Executive Order On Improving the Nation's Cybersecurity

3 Improve Collection of Logging and Telemetry

4 Implement Multifactor Identity & Access Management

5 Facilitate Direct Log Sharing with DHS CISA

President Biden's Executive Order to address the "persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector" outlined eight areas to address, which build upon the above pillars:

1. Removing Barriers to Information Sharing
2. Modernizing Federal Government Cybersecurity
3. Enhancing Software Security Supply Chain
4. Establishing a Cyber Safety Review Board
5. Standardizing the Cybersecurity Playbook for Responding to Cybersecurity
6. Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Networks
7. Improving the Federal Government's Investigative and Remediation Capabilities
8. Improving National Security Systems

It is critical for federal agencies to embrace the EO and important cloud security frameworks—including TIC 3.0, CMMC, and NIST SF-800-53, to name a few—as they will shepherd agencies into this new Cloud Secure era.

Zscaler enables security modernization per the executive order in a variety of ways:

- We can help the federal government modernize to a cybersecurity cloud platform, in accordance with Section 3(b) of the EO. We have a FedRAMP High platform that meets federal government authorization needs.
- We can help the federal government adopt a zero trust architecture, as outlined in Section 3(b)(ii). The Zscaler Zero Trust Exchange architecture can help the government reduce its attack surface and connect users to applications and data, not networks, as outlined in NIST's Zero Trust Architecture.
- When a federal government agency leverages Zscaler, it gains visibility into user behavior wherever the user works.
- Zscaler facilitates log sharing directly with CISA. This logging information can expedite threat hunting, detection, protection, and response from a cybersecurity event.

Zero trust is an ecosystem

Remember, zero trust is an ecosystem, not a product. It is not a one-size-fits-all approach, just like that Thanksgiving feast. It will evolve over time and is, therefore, something that should be consistently revisited and adapted.

If you follow the pillars outlined in the simple five-step playbook, you will not only comply with guidance, you will be able to start with bite-size solutions. This approach will give you the freedom to pivot and evolve your network as needed.

Zero trust is about intent. Whatever you implement, and wherever you start, the goal is to protect users wherever they are and gain proper context before providing access.

Don't wait. You can follow the playbook and begin benefiting from zero trust today, regardless of what tomorrow may look like.

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 SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com