netskope

WHITE PAPER

# Netskope for Zero Trust

## The cloud-smart, data-centric approach to Zero Trust for federal agencies

## Why federal agencies need Zero Trust now

Most security architectures in place across federal agencies today were engineered for a technology ecosystem that has significantly changed over the last two decades. And while the pandemic served as a forcing function, causing many federal organizations to come to terms with the shortcomings of their tooling, practices, and approach to security, one could argue that the limitations of legacy (i.e., vulnerable) technology solutions were just as debilitating over the last 20+ years as the pandemic was disruptive over the last 18+ months.

We as a nation are under attack—and the problem is only getting worse. The U.S. felt the impact of the cyberattack on the Colonial pipeline, with the lasting effects of digital destabilization rapidly rippling across the country. These types of attacks aren't necessarily new—but the exponential increase in data combined with data ubiquity, the massive increase in Software as a Service (SaaS) applications, and the shift to remote work have collectively expanded our attack surface, while also shifting the network load to the perimeterless internet.

It's critical that we as a nation alter our course to limit opportunities for further attack and prevent additional damage. The current administration has realized the need for bold changes, significant investments, and swift action, and on May 12, 2021, President Biden signed Executive Order 14028 to improve the nation's cybersecurity and protect federal government networks. While the robust order includes various provisions spanning nine core sections, the term "Zero Trust" appears throughout the order a total of 11 times. Specifically, it requires agencies to "... develop a plan to implement Zero Trust Architecture ..." within 60 days of the date of the order. The aggressive deadlines set forth by the order show the clear intent of the White House to improve both the security posture and practices of the federal government; however, the successful adoption and implementation of a Zero Trust approach will require both short- and long-term planning by each individual agency.

*The exponential increase in data combined with data ubiquity, the massive increase in Software as a Service (SaaS) applications, and the shift to remote work have collectively expanded our attack surface, while also shifting the network load to the perimeterless internet.*

## WHAT IS ZERO TRUST—AND WHAT IS IT NOT?

Zero Trust (ZT) is an architectural principle with two main purposes:

- Replacing implicit trust with explicit trust, continually assessed and adapted as necessary by evaluating not just identity but all of the context surrounding an interaction to determine what level of access is appropriate
- Concealing resources from the public internet so that they remain undiscoverable (not just inaccessible) to anyone not specifically granted approval

While the term itself has become wildly popular in both the public and private sectors, ZT departs so severely from traditional approaches to enterprise security, and requires both the abandonment of legacy (i.e., vulnerable) tooling and the adoption of a cloud-smart, data-centric approach, that thus far the effective agency implementation of a Zero Trust strategy has been little more than dilatory in many federal organizations. The call for action in the recent EO will hopefully speed adoption and spawn the funds needed for successful implementation.

Arguably just as important as defining ZT is understanding what it is not.

1. ZT is not a singular product. Security products should enable ZT for your federal organization, but any purchase of a self-proclaimed ZT product is destined to disappoint.
2. ZT is not solely based on identity. Though an important component of an overall strategy, there are four critical concepts or pillars to an effective approach to Zero Trust: identity, context, resources, and control. While other frameworks like HSPD-12 focus primarily on identification for access, modernization and the shift to a remote workforce and a perimeterless environment require a ZT approach that verifies more than just identity. An effective ZT approach gives careful consideration to other contributing factors such as user activity, location, and time for a more complete view of overall behavior and intent as well as application instance awareness that may require identity revalidation.
3. ZT is not a short-term solution that can be deployed in minutes. While machine learning and automation can be leveraged for certain aspects of a ZT strategy, like policy deployment or simplified granular controls, the journey to a more mature and more secure state via ZT is ongoing and requires both short- and long-term strategic planning and investment.

## NETSKOPE'S APPROACH TO ZERO TRUST

Better security is rooted in the ability to make better business and mission decisions for your federal organization—and the ability to make better decisions relies on understanding the risk facing your organization, in real time with telemetry-rich, data-driven context. Netskope's approach to ZT empowers federal agencies with the ability to not just secure and protect agency data, but to confidently and continuously control access to and interaction with agency data as well.

Netskope implements its ZTA in a layered approach divided into three functional groups; Identity and Access Method, Resource, and Control. This design provides a functional grouping of activity and helps align integrations with technology partners and functions as a reference to understand the flow of a request.

A request for a resource is a linear progression through the operational model where the identity and access method is first understood and then policy enforcement takes place at one or more levels as the user/entity is gaining access to the resources. The resources are defined as three types: Resource, Application, and Data, with each having an associated policy enforcement point (PEP) to allow the appropriate level of access to the resource. Allowing the user/entity access to a resource is first completed by challenging the user/entity to authentication and understanding the method of the access request and posture of the device for access. Netskope then looks to understand the user/entity level of authorization, which is based on both static policy application as well as dynamic understanding of behavior. Control of policy, learning, reporting, and integrations through the Control Plan are set up to allow for a dynamic feedback loop that is adaptable and modifies controls as needed based on behavior or outside input.

Full or limited access to the resource is controlled through the PEP.  PEPs are capable of doing more than a simple allow/deny. Based on their functional level and understanding of the resource they are securing, they can function up to the Application layer and beyond with cloud-based applications and data.

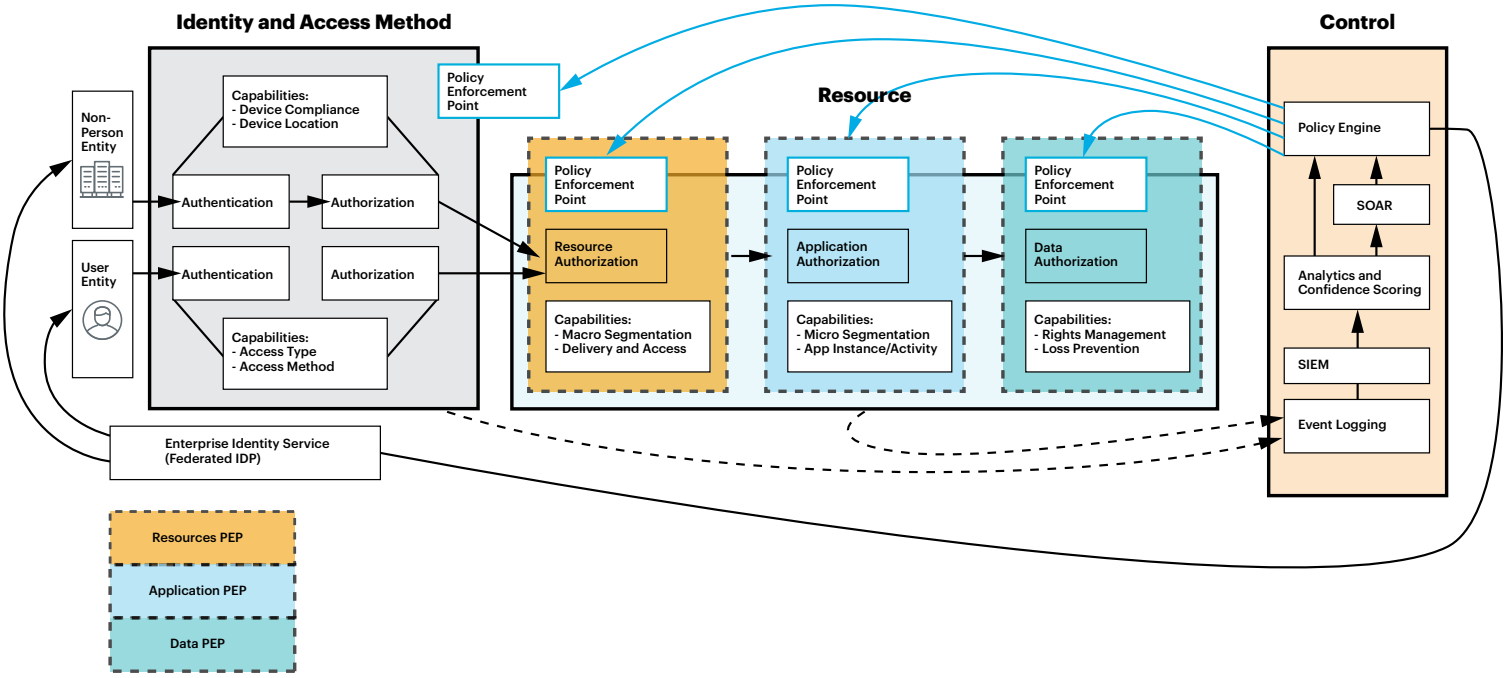
It's important to note that the approach described above isn't just how we think about Zero Trust conceptually—it's an approach that's native to our Cloud Security Platform and can be leveraged by federal agencies for ubiquitous policy control from a single user interface today. Many vendors claim to check the boxes called CASB, SWG, and ZTNA. However, true differentiation—differentiation that actually enables the journey to SASE and a robust, data-driven approach to ZT—manifests as an understanding of context. Legacy technology simply cannot provide the detailed context that federal agencies require in today's modern, perimeterless environment. Netskope's platform is uniquely positioned to provide federal agencies with the context they need for an effective implementation of ZT. The diagram on the following page illustrates the data flow and policy enforcement points of the architecture, and how agencies can leverage the full power of the Netskope platform.

Built on Netskope’s NewEdge network, our modern, cloud-smart, data-centric platform brings together our Next Generation Secure Web Gateway (NG SWG) with URL filtering and advanced web protection with our Cloud Access Security Broker (CASB) that allows federal organizations to govern access to thousands of cloud applications, and cloud-native data loss protection (DLP) for a unified, cloud-native platform solution that keeps each of the services as close to the user as possible, allowing the control point to follow the user—and the data—wherever they are.

Netskope’s approach provides federal agencies with a concept of operations that allows agencies the ability to create tailored structures based on unique agency needs.

## Netskope Zero Trust Capabilities Mapping

Native to Netskope's Cloud Security Platform providing ubiquitous policy control from a single UI




## CORE TENETS

In addition, Netskope's approach to ZT aligns to the guidelines from NIST 800-207, the DoD Zero Trust Reference Architecture, and CISA's Zero Trust Maturity Model. The core tenets include:

1. Trust no one: Know your people and your devices
2. Validate identity at every step: Design systems under the assumption of compromise
3. Distrust everything: When a breach happens you are as protected as you can be
4. Use Dynamic Access Controls: Access to services must be authenticated, authorized, encrypted at all times, and can be revoked during a session
5. Constantly evaluate risk: Include context in risk decisions, monitor and log in every location possible, and aggregate log, system, and user data
6. Right size protections: Invest in defenses based on the classification of data and the systems at higher risk

## FUNDING

It's important to note that while the executive order (EO) is a mandate for the executive branch, it's not a law. Only Congress can legislate and enact laws; however, the president can order policy for executive branch agencies. Appropriated funding, on the other hand, must come from Congress. Agencies, however, can only meet the requirements of this EO with the necessary funding, and as the order suggests, significant funding will be needed.

With that said, there's already been an infusion of funding available to agencies. Earlier this year, the $1.9 trillion American Rescue Plan added $1 billion to the Technology Modernization Fund (TMF), a revolving fund that awards five-year loans to agencies for IT modernization projects that demonstrate a strong return on investment. The Biden administration asked for an additional $500 million of TMF funding in its recent FY2022 budget request, and representatives are hoping additional funding will be forthcoming.

Additionally, federal agencies can leverage the Zero Trust Architecture Buyer's Guide provided by General Services Administration. The guide provides information that can help agencies identify a broad range of products and services to help develop, implement, and mature agency Zero Trust implementation plans.

## ADDITIONAL GUIDANCE AND BEST PRACTICES

There are a number of resources available to federal agencies, including:

1. The NSA's "Embracing a Zero Trust Security Model" Guidance Document
2. NIST Special Publication 800-207, Zero Trust Architecture
3. CISA's TIC 3.0 Core Guidance Documents
4. DoD Zero Trust Reference Architecture
5. Gartner's Market Guide for Zero Trust Network Access
6. Gartner's What Are Practical Projects for Implementing Zero Trust?

## CONCLUSION

The idea of Zero Trust has created a lot of noise in recent years, but what we're seeing most recently with EO 14028 is the much-needed planning, coordination, and preliminary action that's needed to make long-term critical improvements to federal security. As evidenced by both the recent OMB Memo on Protecting Critical Software Through Enhanced Security Measures and the Security Measures for "EO-Critical Software" Use Under Executive Order (EO) 14028 released by NIST, what we're seeing is a genuine effort to reset the baseline of security in the federal government.

It's important to remember the scale of this challenge holistically—redefining security across an organization with more than 4.2 million FTEs, not to mention contractors and support personnel, massively complex networks, and countless tools in use across each individual agency both for mission sustainment and security—there is no easy button or one-size-fits-all solution. So, while initial efforts and support documentation may not be comprehensive, and the adherence to the guidance may not eliminate the need to implement additional security measures, it does give agencies the freedom to pursue the most innovative technologies and modern security solutions on the market.

We expect additional guidance from the White House, as well as appropriations and funding to support the changes required across the federal government. The agencies that will prove most successful in improving their security posture are those that start planning for Zero Trust adoption now and put together a long-term strategy for continuous modernization.

Netskope, the SASE leader, safely and quickly connects users directly to the internet, any application, and their infrastructure from any device, on or off the network. With CASB, SWG, and ZTNA built natively in a single platform, Netskope is fast everywhere, data centric, and cloud smart, all while enabling good digital citizenship and providing a lower total-cost-of-ownership.

To learn more, visit, https://www.netskope.com.