zscaler™

EBook

The Power of Zero Trust

Insights from the Public Sector Summit 2023

Contents

Introduction

Public sector organizations at every level of government are deploying Zero Trust architecture to accelerate digital transformation and defend valuable assets. Yet even as they work toward goals and deadlines set by the Office of Management and Budget (OMB), the National Institute for Standards and Technology (NIST), and the Executive Order on Cybersecurity, misconceptions around Zero Trust persist.

To separate Zero Trust fact from fiction, government leaders and industry partners convened at the inaugural Zscaler Public Sector Summit. This eBook collects the best insights from the event, including the challenges agencies may be facing, some of our best practices for developing a robust Zero Trust architecture, and a use case demonstrating how Zero Trust can integrate into every part of your agency's operations.

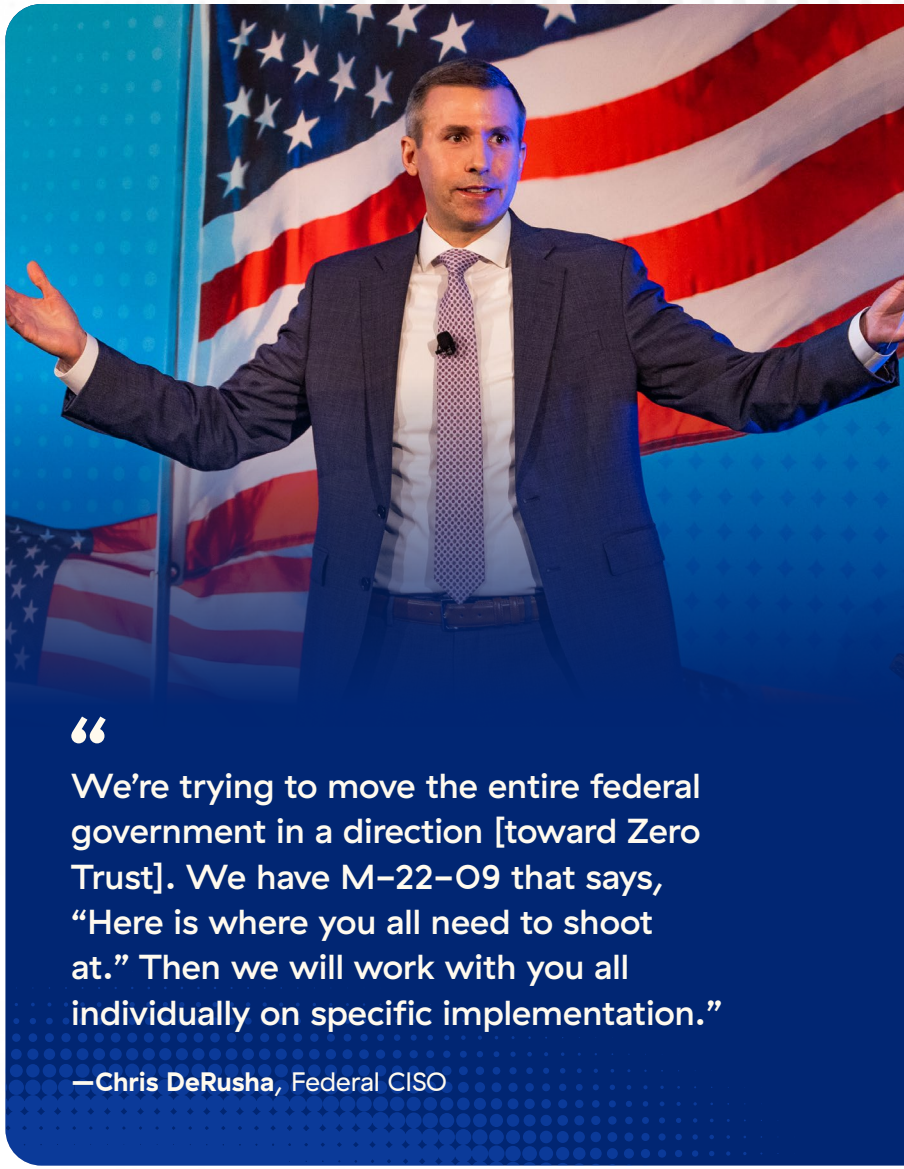
zscaler™ | Public Sector

History of Zero Trust

Zero Trust isn't a new concept. Even before the term was coined in 2010, a working group of technology leaders known as the Jericho Forum championed principles of "de-perimeterization" and created best practices for governing networks without a security perimeter. However, it took time—around 15 years—to develop technology capable of delivering on those best practices. Technologies and practices such as multi-factor authentication that are now part of Zero Trust became more advanced in the intervening years, it wasn't until 2020 that a Zero Trust approach to cybersecurity moved from concept to reality.

In 2020, the National Institute for Standards and Technology introduced NIST 800-207, a new cybersecurity paradigm focused on resource protection and the idea that access should never be granted implicitly. Gone are the days of "trust but verify;" this new standard brought about a shift to constant evaluation of users and devices. Less than two years later, the Executive Order on Improving the Nation's Cybersecurity (M-22-09) and a subsequent directive from the Office of Management and Budget, both mandated the adoption of Zero Trust principles for all federal agencies.

Now, agencies are facing a deadline of September 30th, 2024—the last day of the current fiscal year—to meet OMB's initial requirements for implementing Zero Trust architecture. Each organization is in a different place in their Zero Trust journey, but knowledge and best practices from IT leaders will help keep them moving in the right direction.



> "We're trying to move the entire federal government in a direction [toward Zero Trust]. We have M-22-09 that says, "Here is where you all need to shoot at." Then we will work with you all individually on specific implementation."
>
> —**Chris DeRusha**, Federal CISO

Barriers to Zero Trust Adoption

Understanding Zero Trust

Despite existing as a term for more than 15 years, there is still significant confusion surrounding what Zero Trust actually is. It's possible to fall into the trap of viewing Zero Trust as a mere buzzword or something to be handled by agency IT. In reality, Zero Trust architecture takes cooperation from the entire organization to support the secure delivery of the agency's mission. Education surrounding Zero Trust for both the workforce and agency leaders is essential to understanding what it is and how to work toward compliance—as well as how to talk about it.

The saturation of jargon, acronyms, and initialisms surrounding Zero Trust act as another barrier to widespread adoption of more secure network architecture. Terms like "micro- segmentation" and "cloud access service broker (CASB)" can quickly become overwhelming, making it difficult to discern what needs to be done and where to start. For users and experts alike, clarity around the various buzzwords can help increase confidence in Zero Trust by explaining why the changes are occurring and what benefits a Zero Trust architecture can provide.

> "From the CISA side, we've already started to help with some of the training to understand what zero trust means — both to the executive leadership at the agencies down to the practitioner....we're coming out with a zero trust program office, agencies want guidebooks, playbooks... more understanding of what agencies are doing so other ones can build off of that."
>
> —**Sean Connelly,** TIC Program Manager, CISA

Legacy IT

Firewalls entered the technology landscape in the late 1980s, ushering in decades of castle- and-moat network security thinking. In the years between presenting Zero Trust as an idea and developing the technology to deliver on those promises, those perimeter-based security strategies became even more deeply ingrained in agency practices. Even for technology leaders who understand the importance of Zero Trust, the idea of replacing decades' worth of security investments can be off-putting.

Another major obstacle is the fact that agency networks can't simply be turned off to perform an upgrade. Even the smallest interruption to any agency operations and security could have dire consequences for both the delivery of essential services and the maintenance of national security, particularly in today's volatile environment. Therefore, any upgrades have to be made while the network is in use, which takes time and planning.

> "Using a legacy VPN, once you're inside [the network], you can run around amok and … reach all these other applications you shouldn't even have access to. Zero Trust says you don't use the network as a security blanket anymore. Even if you're compromised, the 'blast radius' is only that one application, and not the 8,000 applications that you might be running."
>
> —**Hansang Bae**, VP of Public Sector Strategy and CTO at Zscaler

Solutions and Best Practices

Data

The federal government is taking steps toward becoming more data driven, and agencies are producing and using more data than ever before. As one of the five pillars of CISA's Zero Trust Maturity Model, data plays a key role in Zero Trust strategy not only as a valuable asset to protect, but also as a basis for decision making and policy formation. Knowing what data is stored in your environment is one of the basic tenets of cybersecurity. Mapping data to develop an understanding of what you have, where it is, and which users need access is valuable for identifying the "normal" state of your agency's data. With baseline knowledge in hand, detecting and responding to behavior that falls outside of that scope becomes easier.

Securing the data in your possession is only one piece of the puzzle. Agencies have vast repositories of data at rest to contend with, but they also need to protect data in motion, particularly data stored and accessed via endpoint devices, including those in BYOD programs. Protecting data in each of these states may require multiple interoperable tools, such as inline or endpoint data loss prevention (DLP), browser isolation, or a cloud access security broker (CASB), all of which integrate to form a comprehensive data security architecture.

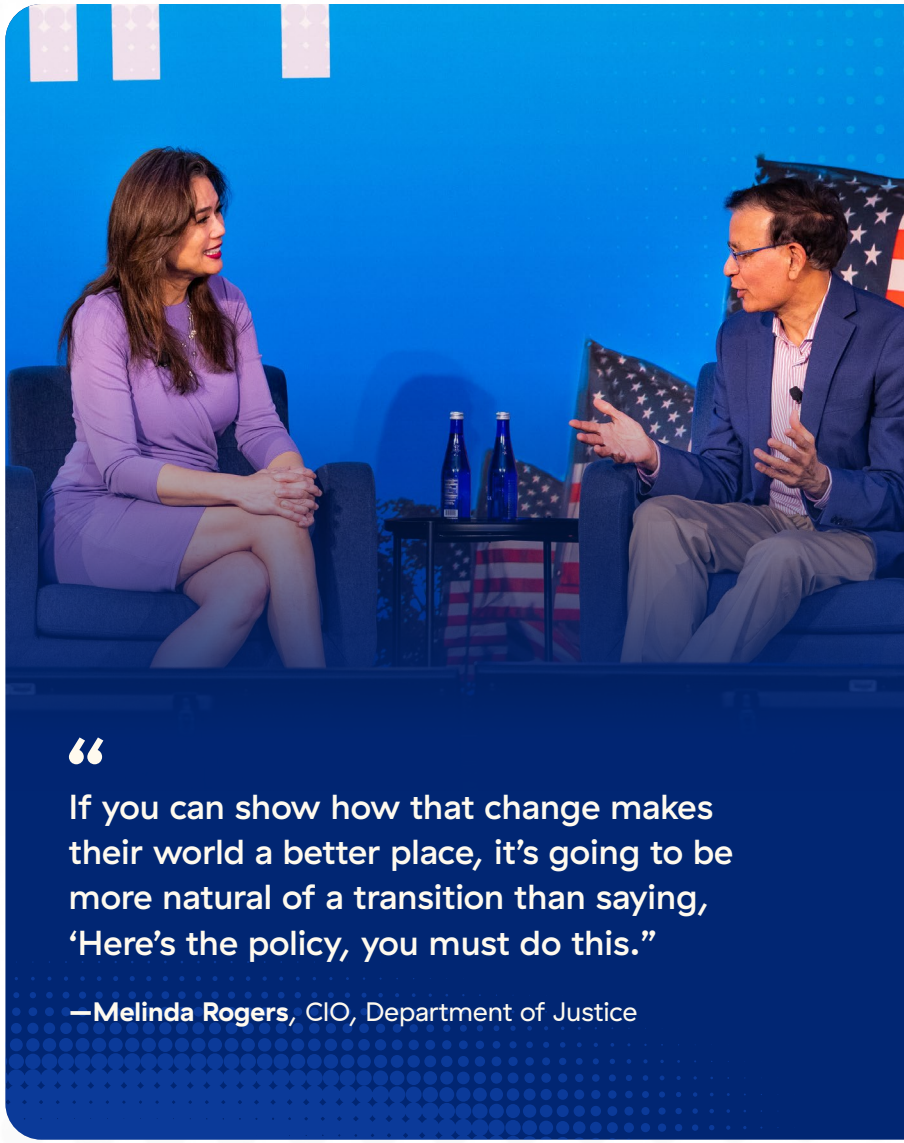
> "Understanding what you have and what you can do is very important in understanding where your gaps are and how to fill those gaps. Understand what your risk thresholds are and where you're going to draw those lines. Understand what normal looks like, so you can take the appropriate actions when needed."
>
> —**Gerry Caron**, CIO, International Trade Administration

User Experience

One of the largest obstacles facing agency technology leaders when implementing Zero Trust is how the changes will be received, and that reception is impacted by the manner in which Zero Trust policies are developed. In many organizations, the task of creating Zero Trust architecture and policies is given to the IT department, which then pushes the new procedures out to the rest of the organization. Without clear communication of any changes or a focus on delivering a seamless user experience, Zero Trust can create some challenges for both agency employees and civilian customers.

It's important to consider how users' normal site or system interactions will be redefined by implementing Zero Trust architecture and communicate not only any changes, but the reasoning behind them. Simply adding a new feature, such as multi-factor authentication, with no context or explanation creates tension between decision makers and users, especially if that feature adds extra steps to their workflows.

In addition to easing adoption, providing a convenient and reliable user experience enhances the security that Zero Trust can provide. If security is implemented in a way that makes the end user's job more difficult, they will find a way to work around it. Shadow IT—applications, websites, and other systems that haven't been approved by agency IT teams— may improve a single employee's productivity, but the vulnerabilities they introduce into an IT environment far outweigh those benefits. For Zero Trust to eliminate those attack surfaces, the new user experience has to be intuitive as well as secure.



> "If you can show how that change makes their world a better place, it's going to be more natural of a transition than saying, 'Here's the policy, you must do this."
>
> —**Melinda Rogers**, CIO, Department of Justice

Information Sharing

Secure information sharing is one of the primary goals of the federal government's Zero Trust transformation, but it's also part of the foundation of a robust Zero Trust architecture. Every agency has its own unique requirements that everyone involved in Zero Trust implementation needs to understand in order to work toward a unified modernization goal. Through collaboration between agencies and industry partners, Zscaler shows agencies a full picture of their security landscape using best-in-class products that work together seamlessly.

> "When I think about the [Zero Trust] ask, I think about our system or product owners and then their customers. How is their normalcy going to be redefined by implementing this measure that, in the end, benefits us all? Because now I have to tell someone that there's an extra step or two in order to access the application, different than what it was just last week. And at the end of the day, I need them to be okay."
>
> —**Dr. Aaron Drew**, Technical Director for Health Environmental Logistics Management, Department of Veterans Affairs

Zero Trust in Action

New Jersey Judiciary Builds Stronger Security Posture with Zero Trust

The emergence of Zero Trust architecture has created myriad opportunities for public sector agencies to build a stronger and more secure network that can keep pace with evolving workforce, constituent, and mission needs.

Implementing Zero Trust enabled the New Jersey Judiciary (NJJ) to enable its remote workforce and virtual offerings during the COVID-19 pandemic and to continue leveraging these investments to accelerate their ongoing digital transformation journey. A solid foundation of Zero Trust has enabled NJJ to secure employees from anywhere, expand service capabilities, and build a more resilient security posture.

> “Don’t forget your advocacy. Part of our role as leadership of a centralized IT organization is being a leader and explaining the reasons behind why we’re doing what we’re doing. Being able to articulate that not only is this going to make your life easier, but you get this visibility, this control—look at what you get to do.”
>
> —**Roger Gibson**, COO, State of New Jersey

NJJ's Zero Trust journey began in 2019 with a search for a CASB solution to support the court system's cloud migration. State officials, including NJJ Chief Information Officer Jack McCarthy, saw the cyberattacks that impacted courts in Atlanta, Philadelphia, and the state of Texas as a warning about the limits of traditional perimeter-based security. Securing the state's infrastructure to meet these new realities became a top priority. McCarthy's team identified Zero Trust as a viable defense against threats tailored to meet the needs of legacy systems.

Less than a year after its initial investment in Zero Trust, the COVID-19 pandemic exacerbated the state's existing challenges with legacy technology and security. The shift to remote work required NJJ to expand its VPN usage from 2,300 users to nearly 10,000, which dramatically increased security risks. Users also began experiencing difficulty connecting, frequent disconnects, and blurry video conference images, and the NJJ help desk team found itself spending hours trying to diagnose their connectivity issues.

With their knowledge of Zscaler's Zero Trust approach from a pre-pandemic proof of concept, NJJ decided to pivot from VPNs to a Zero Trust architecture to support and secure the newly remote workforce. The new infrastructure enabled NJJ to deploy unified, consistent security policies across their cloud channels, which allowed the state to distribute access to local IT managers in 21 counties. Rather than requiring an in-person consultation or relying on employees to accurately assess and describe their issues, IT managers can now access their devices remotely and diagnose the problems themselves.

NJJ's Zero Trust journey has enabled the court system to continue operations regardless of environmental conditions and expand the accessibility of the courts system for employees and constituents. By using a Zero Trust architecture, the state has developed a high level of security and laid the groundwork for NJJ's on- going digital transformation journey. Implementing Zero Trust, meeting compliance mandates, and navigating cyber risk management doesn't have to be a struggle. With these lessons learned, the public sector can continue to modernize its cyber environment and achieve the promise of Zero Trust.

Don’t miss this year’s insights! **Save your spot** › for the 2024 Zscaler Public Sector Summit.

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 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**.

+1 408.533.0288

Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134

zscaler.com