World Wide Technology | Forcepoint

LET'S TALK ABOUT TRUST

Why the Future of Government Security Depends on a Zero Trust Framework

IN A RECENT GOVEXEC WEBCAST, GOVERNMENT AND INDUSTRY LEADERS WEIGHED IN ON HOW AGENCIES CAN ADOPT A ZERO TRUST ARCHITECTURE. HERE ARE THE TOP TAKEAWAYS FROM THE EVENT.

When it comes to cybersecurity, government agencies can never be too careful. That's especially true today: As more employees telework, security has become an even greater concern. With fewer users working from the same location, cyberthreats have skyrocketed because of hostile public networks and unstable Wi-Fi. Not only are these threats costly — they can also make it difficult for an agency to effectively fulfill its mission.

To tackle these complex yet common security challenges, many public sector organizations are embracing a Zero Trust architecture. This framework, which has gained prominence in the public and private sectors over the last decade, calls for a proactive, risk-based approach to cybersecurity, requiring systems verify users inside or outside its perimeter before granting them access. Zero Trust takes into consideration a number of factors before granting access, including the nature of the request and the user's location, access patterns and system configuration.

At "Strategies for Implementing and Operating a Zero Trust Architecture," a recent GovExec webcast sponsored by World Wide Technology and Forcepoint, government and industry leaders came together to share best practices around how agencies can drive adoption of Zero Trust across the public sector. Here are a few key takeaways from the event.

1. Know the 4 Pillars of Zero Trust

Before an agency can effectively adopt a Zero Trust architecture, it's important to understand the guiding principles behind this framework.

- **Data Discovery and Inventory:** How to gain visibility into all the endpoints on your network
- **Data Classification:** How to build a system that systematically tracks, monitors, protects and accesses your most critical information
- **Data Protection:** How to monitor and protect data based on its risk and value
- **User Identity and Privilege Access:** How to provide the right access to the right people at the right time

Once organizations understand these principles of Zero Trust, they can begin implementing it successfully. That's according to John Evans, chief technology advisor for state and local government and education at World Wide Technology and the moderator of the webcast.

"Zero Trust offers a holistic strategy and framework that's not tied to a single technology," he explained at the event. "It enables agency leaders to promote and support enterprisewide shifts in where and how access is provided to data and/or systems and applications."

The pillars, Evans continued, offer agencies actionable steps to take as they look to improve their security posture.

75% OF GOVERNMENT EMPLOYEES IDENTIFIED ZERO TRUST AS A VITAL COMPONENT OF THEIR AGENCY'S CYBERSECURITY POSTURE.

- Source: "Trust In Zero Trust?", Government Business Council, June 2020

2. There's No One-Size-Fits-All Approach to Security

According to a June 2020 Government Business Council survey, underwritten by Forcepoint, three out of four government employees identified Zero Trust as a vital component of their agency's cybersecurity posture. But what Zero Trust means to one agency might vastly differ from what it means to another.

The Cybersecurity and Infrastructure Security Agency and the National Institute of Standards and Technology have each released general guidance on Zero Trust to help equip agencies with the tools they need to successfully adopt this model. But according to Brian Campo, deputy chief technology officer at the Department of Homeland Security, agencies must also develop specific guidelines tailored to their own unique security needs.

"It's still up to each agency to understand their risk posture, to understand the threat vectors that are most important to them and develop their own [guidance]," he said at the event.

3. Start by Looking at the Data

While data discovery and inventory is the first pillar of Zero Trust, Forcepoint Senior Solutions Engineering Manager Victor Martinez says agencies must treat it not as a single step, but rather as a continuous process.

"It's something you start and you iterate," he said at the event. "I don't think you're ever going to finish your data discovery because data transforms. People create new data. Data is shared. Data is deleted."

Martinez recommends conducting data discovery and inventory in tandem with other steps in the Zero Trust journey.

Equally important? Gaining visibility into that data.

"You need to start looking at the data through a lens where you're asking yourself questions like: What sensitive data do I have? Where is it, and who needs access?" Kevin Finch, global security strategist at WWT, said at the event.

Still, organizing and managing this data can prove challenging — especially for large government organizations.

> "ZERO TRUST OFFERS A HOLISTIC STRATEGY AND FRAMEWORK THAT'S NOT TIED TO A SINGLE TECHNOLOGY. IT ENABLES AGENCY LEADERS TO PROMOTE AND SUPPORT ENTERPRISEWIDE SHIFTS IN WHERE AND HOW ACCESS IS PROVIDED TO DATA AND/OR SYSTEMS AND APPLICATIONS."
>
> *- John Evans, chief technology advisor for state and local government and education, World Wide Technology*

Campo understands this perhaps better than anyone. DHS, after all, is the fourth largest federal agency and the second largest federal civilian agency in the U.S.

"[At DHS], we've got such a broad range of what we do that our data needs are astronomical," he explained. "We do disaster recovery, we do border management, we do import-export, we do cybersecurity."

DHS was producing so much data for each of these various missions that it became impossible to keep track of it all.

"We're seeing our data ballooning every time we're doing an inventory," Campo said. "So trying to get data under control has been a challenge."

DHS began looking at data through a more segmented lens. Instead of just assessing DHS' data, the department investigated how these insights were produced and leveraged across portfolios within the larger organization. This new approach has enabled Campo and his team to create more consistent data standards and reduce redundancies across the agency.

Automated solutions can also play a role in helping solve this data management challenge. AI-driven tools can sift through data faster than humans, empowering employees to make informed decisions on how to analyze this information. According to Finch, this combination of human and artificial intelligence can help agencies manage data more effectively by removing data that's no longer useful to them.

4. Rethink Your Data Protection Strategy

Once an organization has taken steps to classify its data, agency leaders can begin to understand how to protect it. For years, organizations relied on a static set of data loss prevention policies to keep this information safe, but Martinez says these rules aren't always as effective as we'd like them to be.

"There hasn't been a whole lot of enforcement," he said.

The key, Martinez explained, is to implement a data loss prevention solution strategy that combines an understanding of human behavior with technology designed to track and mitigate risks. As a result, people, not walls, become the perimeter.

Moreover, these types of capabilities are more prevalent today than ever.

"Before, we could say that a person was only ever going to work inside a building, or in a controlled access point," Campo said.

But today, more government employees are working from coffee shops and from home, "sharing a network, sharing a Wi-Fi connection, using a personal router that may have been compromised," Campo explained.

"Zero Trust becomes absolutely vital," he said. "It's effectively one of the most important frameworks for security we've seen in current times."