

4 Ways Zero Trust Can Protect Government

Zero Trust Security has a Bright & Necessary Future in Government

The old method of putting up firewalls and then allowing authorized users inside the network to access government resources is no longer a viable security strategy. Government assets are increasingly distributed right out to the network edge, as are the authorized users who need to access them. And attacks don't just come from the outside anymore. You have to assume that sophisticated attackers may already be inside government networks, and figure out how you can still detect and stop them.

Enter the zero trust framework, which could be the answer in government. Zero trust is both a mindset and a methodology that maintains that no user should ever be trusted. At a minimum, they should be heavily verified, and even then only given temporary access and just enough permissions to accomplish the task at hand.

Three experts recently joined a [FedInsider virtual panel](#) to discuss the current threat landscape, and ways that zero trust can make a difference in government.

1. Understand Why Zero Trust is Necessary in Government

A recent report titled The National Counterintelligence Strategy of the United States predicted more attacks as well as more complex attacks from hostile actors. The old methods of trying to protect government using a perimeter security mindset have long since been circumvented by skilled attackers.

"I wish I could say no, but the reality is that cybercriminals are getting smarter," said Chief Information Officer of the Air University at the United States Air Force Jeff Lush. "And although IT is doing a wonderful job trying to keep up with this overwhelming tide of challenges, when it comes to cyber, it's difficult."

Lush said that it is helpful to teach government employees how to maintain self-awareness by telling them not to do things like clicking on links or attachments where the source cannot be verified. But ultimately, someone is going to make a mistake, and unless you have something like a zero trust framework in place, there is a very good

Featuring:

■ Jeff Lush

Chief Information Officer, U.S. Air Force Air University



■ Mahreen Huque

Cybersecurity Technology Consultant, Ernst & Young



■ Susie Adams

Chief Technology Officer, Microsoft Federal



■ Frank Briguglio

Global Public Sector Strategist, SailPoint



chance that attackers will find a way to slip through your defenses.

2. Reduce Exposure & Improve Access Management on the Path to Zero Trust

As evidenced by the SolarWinds breach, insufficient security can act as an open invitation for hostile actors, and government is no exception. However, the situation could have been avoided or mitigated if agencies had reduced their exposure or had better access management and zero trust elements in place. The attack would have still probably happened, but its effects would have been minimal.

"The thing that the government is pretty focused on these days as far as cybersecurity is threat detection," said Cybersecurity Technology Consultant with Ernst and Young Mahreen Huque. That is good, but there needs to be more of a focus on post-breach response. "The recent attack on the software supply chain of the federal government showed the huge amount of exposure an attack can have" if it gets past that initial detection-based protection, she said.

Another element of zero trust that Huque recommends for government is eliminating static access levels, especially for highly credentialed users. Granting unlimited access to critical systems after a simple password or identity check should never be done anymore. SolarWinds and other companies caught in recent supply chain attacks clearly demonstrate the need to limit exposure and maintain a strong zero trust framework, even with established vendors like Microsoft.

3. Don't Rely on Measures Such as PIV Cards & Other Basic Authentication

While many agencies have grown accustomed to access measures involving things like PIV and CAC

cards to ensure authorization, there is growing concern that those methods might no longer be enough. As cyberattacks continue to evolve, the static authentication procedure offered by a PIV card probably won't be enough to stop a skilled attacker.

"Government can't rely just on a strong credential like a PIV card or active directory any longer," said Global Public Sector Strategist for SailPoint Frank Briguglio. "We have to implement suitability policies and interrogations at the device level, and for whatever resource is being accessed and whatever action is being performed."

By enforcing stronger authentication methods that force the system and users to communicate and constantly verify themselves, it prevents a hostile actor from simply mimicking PIV access and then having free reign within an agency's system.

4. Zero Trust Provides the Best Methods to Handle Evolving Threats

All three experts agreed that in the face of the overwhelming threats arrayed against government, zero trust is the most viable option for keeping agencies safe. It works

even after a breach occurs to mitigate damage and restrict what an attacker can actually do even if they initially gain access.

"You have to think of zero trust as several layers," said Huque. "We have the users, the application, the data and the network. It's about authenticating users to data applications and systems in an adaptive way based on risk context and user attributes."

Briguglio added that the hardest part of implementing zero trust in government is getting "systems and organizations to work together." It has to be a team effort where management, the IT teams and rank and file employees all understand the need for zero trust and support its implementation to protect their agency. Zero trust might be difficult to implement, but it's the best path forward to protecting government against the increasingly brutal threat landscape. 

FEDInsider

Hosky Communications Inc.

3811 Massachusetts Avenue, NW
Washington, DC 20016

- ☎ (202) 237-0300
- ✉ Info@FedInsider.com
- 🌐 FedInsider.com
- 📱 [@FedInsiderNews](https://www.facebook.com/FedInsiderNews)
- 🌐 [Linkedin.com/company/FedInsider](https://www.linkedin.com/company/FedInsider)
- 📱 [@FedInsider](https://www.instagram.com/FedInsider)

carahsoft

Carahsoft

1493 Sunset Hills Road
Reston, VA 20190

Contact: Maggie Manfredi

- ☎ (703) 230-7488
- ✉ Maggie.Manfredi@Carahsoft.com
- 🌐 [Carahsoft.com/vendors/SailPoint](https://www.carahsoft.com/vendors/sailpoint)
- 📱 [Facebook.com/Carahsoft](https://www.facebook.com/Carahsoft)
- 🌐 [Linkedin.com/company/Carahsoft](https://www.linkedin.com/company/Carahsoft)
- 📱 [@Carahsoft](https://www.instagram.com/Carahsoft)

SailPoint

SailPoint

11120 Four Points Drive
Austin, TX 78726

Contact: Cathy Cromley

- ☎ (703) 517-4419
- ✉ Cathy.Cromley@SailPoint.com
- 🌐 [Sailpoint.com/identity-for/government](https://www.sailpoint.com/identity-for/government)
- 📱 [Facebook.com/SailPoint](https://www.facebook.com/SailPoint)
- 🌐 [Linkedin.com/company/SailPoint-Technologies](https://www.linkedin.com/company/SailPoint-Technologies)
- 📱 [@SailPoint](https://www.instagram.com/SailPoint)

© 2021 Hosky Communications, Inc. All rights reserved. FedInsider and the FedInsider logo, are trademarks or registered trademarks of Hosky Communications or its subsidiaries or affiliated companies in the United States and other countries. All other marks are the property of their respective owners.

carahsoft

SailPoint

MISSION BRIEF | [FEDINSIDER.COM](https://www.fedinsider.com)