Zero Trust in Government

GOVLOOP
E-BOOK
2019

Executive Summary

Cybersecurity is a constant struggle, with governments at every level under siege from persistent, evolving threats. The public's data hangs in the balance, with agencies that fail to protect this sensitive information losing the public's trust.

Despite such high stakes, traditional cyberdefenses aren't keeping agencies safe. Typically, agencies have protected their networks by guarding their perimeters from attack. Unfortunately, this approach doesn't shield data from internal threats or external ones that breach agencies' perimeter defenses. Once inside agencies' perimeters, bad actors can cause irrevocable damage.

To address these challenges, many agencies are segmenting their networks and authenticating the devices and users accessing them. Although these methods provide some safety, they unfortunately don't provide agencies with real-time insights about their network's processes. For example, authentication can't prevent malicious software from running on a network after bypassing an agency's defenses.

Fortunately, a zero trust approach to cybersecurity offers agencies a strategy for detecting and mitigating cyberthreats from both inside and outside their networks. **A zero trust approach to cybersecurity combines specific people, processes and technology to make security pervasive networkwide using two techniques. The first is continuous monitoring of all activities across the network. The second applies least privilege access principles, managing which devices and users are authorized to join specific resources when, where, and how they connect.**

This GovLoop e-book explains how to enforce a zero trust approach to cybersecurity and the philosophy's evolution. The following pages also contain interviews with federal, state and local leaders about a zero trust approach to cybersecurity. Finally, we'll interview experts who are successfully defending government networks with a zero trust approach to cybersecurity.

Ultimately, a zero trust approach to cybersecurity requires more than fancy firewalls, multifactor authentication and network access control; it's a mindset that must govern an agency's people, processes and tools to endlessly shelter citizen data.

The History of Zero Trust

These facts and figures shed light on how the term “zero trust” evolved and what the current state of cybersecurity looks like in federal, state and local government.

2010

“Zero trust” enters the cybersecurity lexicon when Forrester Research, a technology market research company, coins the term that November.

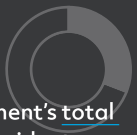
2014

Google starts enforcing a zero trust approach to cybersecurity with the technology giant’s BeyondCorp approach to cyberdefenses.

2017

Gartner, a global advisory and research firm, expands its zero trust approach to cybersecurity to include continuous adaptive risk and trust assessment (CARTA) capabilities. CARTA capabilities work toward constantly adapting agencies’ security postures for new challenges.

31%

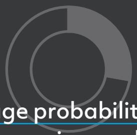


of the federal government’s total information security incidents reported in Fiscal Year 2017 were listed as “other,” or featured an attack method that did not fit into any other type or were unidentified, down from **38%** in 2016.

59%

of federal agencies in 2018 reported having processes in place to communicate cyber risks across their enterprises.

28%



is the estimated average probability in 2017 that global companies would suffer a major, material data breach within two years.

35%

of local government chief information officers (CIOs) in 2016 said lack of end user accountability is either a severe or somewhat severe barrier to achieving their agencies’ highest possible level of cybersecurity.

33%

of local government CIOs in 2016 said their agencies had developed a formal, written cybersecurity risk management plan.

48%

of state chief information security officers (CISOs) in 2018 said their agencies did not have a separate line item for cybersecurity in their overall IT budgets.

35,277

total information security incidents were reported across the federal government in FY 2017.

$17.4B

was the amount in budget authority included in the FY 2020 President’s Budget for cybersecurity-related activities, a **$790 million** (5%) increase above the FY 2019 estimate.

The 'Why' and 'How' of Zero Trust

Unfortunately, reaching a zero trust approach to cybersecurity isn't as simple as buying a new technology and flipping a switch. Rather, it requires a combination of people, processes and technology for greater network safety.

The federal government's lack of official guidelines on a zero trust approach to cybersecurity has left agencies across the U.S. uncertain about the phrase's meaning. Despite this, private sector organizations have long discussed and practiced a zero trust approach to cybersecurity. The examples these companies provide offer valuable guidance to federal, state and local imitators.

For starters, Forrester coined the phrase "a zero trust approach to cybersecurity" in 2010 and then outlined three essential traits for the practice:

- **Eliminating network trust** by assuming that traffic is a threat regardless of its location until it has been inspected, authorized and secured.
- **Segmenting network access** by adopting a least privilege strategy that strictly limits the access that devices and users have on networks by limiting them to the fewest necessary resources for their actions.
- **Gaining network analytics and visibility** by continuous monitoring to constantly examine and log all traffic for external and internal threats.

Forrester's model, however, lacked remedies for when threats gain access to trusted systems. In 2017, Gartner proposed an updated framework for a zero trust approach to cybersecurity containing three more attributes:

- **Zero trust of people** by continuously authenticating and monitoring people rather than authenticating them once for future access.
- **Zero trust of workloads** by enforcing controls across an entire stack of applications, especially the connections between cloud-based containers and hypervisors. Containers are packages of software, while hypervisors are software for creating and running virtual machines (VMs) that emulate computer systems.
- **Zero trust of data** by securing, managing, categorizing, and developing classification frameworks for data. This information must also be encrypted in transit and at rest.

Let's look closer at the evolution of a zero trust and how it impacts government people, processes and technology today.

The Evolution of Zero Trust

Early government cybersecurity focused on defending network perimeters with tools such as firewalls to block external threats. Like castle walls around a city, however, this approach can't stop threats that come from within or breach physical boundaries.

Next, agencies added continuous monitoring and least privilege access control to their cybersecurity strategies. Continuous monitoring gives agencies visibility into all activities across their networks; least privilege access control allows them to control what devices and users gained access to their networks. Although valuable, neither of these approaches results in pervasive network security for agencies.

In 2010, the phrase "a zero trust approach to cybersecurity" emerged to describe continuous monitoring and least privilege access control working together. Three steps also became synonymous with improving this pairing: eliminating network trust, segmenting network access and gaining network analytics and visibility.

Eliminating network trust assumes that all traffic, regardless of location, is threatening until it has been authorized, inspected and secured for verification. For example, traffic from friendly agencies is considered dangerous until undergoing the verification process.

Segmenting network access, meanwhile, involves adopting least privilege access control. Agencies strictly enforce cybersecurity by allowing access to only the resources that devices and users need for their roles. This segmentation keeps the entire network from being affected if one part is compromised.

Gaining network analytics and visibility, finally, requires continuous monitoring. All internal traffic is constantly examined and logged, as is the perimeter for external threats. This vigilance is then paired with real-time protection capabilities for stronger cybersecurity.

The 2010 model isn't perfect, however, and shortcomings soon emerged. For instance, agencies weren't prepared for their trusted systems being compromised. Once compromised, invaders such as malicious software could hide undetected on agencies' networks. These hazards could also damage previously healthy network segments. Agencies needed a stronger battle plan.

Zero Trust Today and Moving Forward

Seven years after the zero trust approach to cybersecurity's emergence, Gartner expanded the phrase's definition. In 2017, Gartner proposed three new capabilities for securing data and workloads beyond agencies' networks.

The first capability that was advanced was zero trust in people. Zero trust in people requires authenticating users before continuously monitoring and governing their access and privileges. Unlike older strategies, this style doesn't authenticate users once before trusting them with future network access. Zero trust in people also differs from previous methods by securing users once they interact with the internet.

After this, the second capability that was urged was zero trust in workloads. Zero trust in workloads enforces security controls across agencies' entire app stacks. These stacks include connections between cloud-based containers and hypervisors; zero-trust in workloads subsequently covers both agencies' legacy and modernized IT workloads.

The final capability that was called for was zero trust in data. Zero trust in data features securing and managing data; other tactics include classifying this information into frameworks called schemas and encrypting data both at rest and in transit.

Ultimately, all three processes were collected under the continuous adaptive risk and trust assessment (CARTA) umbrella. Essentially, CARTA centers on agencies assuming a constantly adapting security posture. CARTA moves agencies away from static, predefined cybersecurity rules to dynamic, flexible defenses.

Agencies practicing CARTA assume their digital risks are continuously shifting, and they place their trust in digital entities accordingly. Governments also rate and score the risk presented to them by all digital agencies and how to consequently parcel out their trust.

CARTA moves agencies away from deciding once if digital entities are good or bad before moving on. This approach measures how agencies' data is accessed, used and protected regardless of location. Data can reside anywhere for modern agencies, so the aim is helping them make faster, more accurate and adaptive security decisions. Agencies that adhere to CARTA allow users to get their jobs done in a risk-appropriate manner.

DHS CISO: ‘I See Zero Trust as Our Future’

Chief Information Security Officer (CISO) Paul Beckman says that the Homeland Security Department (DHS) is well on its way to a zero trust approach to cybersecurity. DHS’s Continuous Diagnostics and Mitigation (CDM) program will serve as the basis for a healthy zero trust approach to cybersecurity at his agency, Beckman said.

Launched in 2013, CDM helps agencies continuously monitor their IT systems and then prioritize the best order for tackling risks and vulnerabilities. Beckman said that CDM naturally fits a zero trust approach to cybersecurity, as the program’s purpose is continuously monitoring agencies’ networks.

During an interview with GovLoop, Beckman said that many agencies are moving toward a zero trust approach to cybersecurity with efforts such as continuous monitoring. Beckman added, however, that federal, state and local agencies must combine several tools and tactics to reach true zero trust status.

This interview was lightly edited for length and clarity.

GOVLOOP: What are DHS’s biggest cybersecurity concerns, and what cyberdefenses does your agency have for protecting its assets?

BECKMAN: The first challenge isn’t a technical one, but it’s one that’s prevalent across not just DHS, but the industry as well. It’s the workforce. The last survey that I saw had about 53% of the organizations reporting a systemic problem and shortage in fielding cybersecurity talent. I’m feeling that pain here at DHS as well. Cybersecurity talent is in high demand, and there’s very little supply to go around.

One of things that we’re doing about that here is finally implementing cyber retention pay. We can go out and compete salary-wise with private industry. We can compensate these people commensurate with the skill levels that they bring to bear. We can tie performance to certifications and your competencies. We can then pay up to 25% of your base salary accordingly. By combining both performance and competencies and compensating them for that, I believe that'll be a far greater retention plan than what we have today.

Our second challenge is maintaining visibility. Specifically, it's maintaining visibility in what we consider a much more diverse, complex and distributed architecture. Many people are saying the network perimeter is dissolving, but the perimeter is expanding exponentially. It's to the point that zero trust is going to be the only way that you keep up with that ever-expanding pace.

How do you define a zero trust approach to cybersecurity and how does this philosophy influence DHS's approach to cybersecurity?

A zero trust approach to cybersecurity is a buzz term that's starting to get abused. The term means different things to different people. A zero trust approach to cybersecurity is about more than just zero trust in your networks. It's also about the user, the device, the network connection, the applications, and the data. It's also about how you wrap threat determination, access control, and monitoring around each of these things. A lot of people hear "zero trust" and think it's a networking thing, but it's much, much more.

CDM's helping us build the foundations that are truly needed to architect a zero-trust cybersecurity effort. CDM helps you find what's on your network and who's on your network. Back to my point about wrapping everything around users, devices, applications and data, CDM is the thing that's going to help us populate the inventory for all these things as we start.

I don't think anybody's fully there on a zero trust approach to cybersecurity, however. As far as DHS, we're not there either. We're starting to look at the building blocks for that zero-trust architecture.

Many people think that zero trust is something you can go out and buy. You can't do that. Zero trust is more of a journey than a destination. What a lot of people don't realize is that they've already invested in core cyber technologies that are required for that zero-trust foundation. It's tools such as next generation firewalls, network virtualization, identity management, and network access control. These are things most people already have but they simply don't realize they have the foundations of zero trust. It's simply a matter of implementing what you've got. A zero trust approach to cybersecurity gives CISOs significant improvements on visibility and assurances that their trusted data can live externally, even on an untrusted network. There are things that every agency can do right now to build a zero-trust cybersecurity architecture without spending a dime.

How does CDM boost cybersecurity, and why is this program so well-suited to the zero-trust mindset?

Most of CDM's value comes from continuous monitoring and how it seeks to get its arms around who and what's on your network. You can't protect or monitor what you don't know that you have. CDM answers that question. It gives organizations a full inventory of their hardware, their software, the configurations of each and who's using what. That's the foundation that any continuous monitoring effort must be built on top of, and that's what CDM gives us.

What's next for DHS's cybersecurity, and what role will zero trust principles play in your agency's strategy?

I see zero trust as our future. As we move to the cloud and that perimeter is expanding exponentially beyond my control, I don't see any means by which I can do things securely without zero trust. Without question, zero trust is the future we are marching toward.

CISCO

Zero Trust for Government

Take the guess work out of adopting a trust-centric approach

Learn More

Making Networks Enforcers With Zero Trust

An interview with Peter Romness, Cybersecurity Solutions Lead, Public Sector Chief Technology Officer Office; and Joseph Muniz, Security Architect, Americas, Cisco

When it comes to cybersecurity, agencies have a problem with provisioning the right level of access to devices and people. Agencies that trust the wrong devices and users are risking their data; agencies that apply too many controls over access to data can impact their employees' daily workflows, leading to a negative impact in production.

Fortunately, a zero trust approach to cybersecurity can help agencies strike a balance between carelessness and caution on their networks. But enforcing a zero trust approach to cybersecurity is easier said than done. Truly practicing a zero trust approach to cybersecurity requires the right people, process and technology.

To understand more about a zero trust approach to cybersecurity and how industry can help agencies, GovLoop spoke with Peter Romness, Cybersecurity Solutions Lead, Public Sector Chief Technology Officer (CTO) Office, and Joseph Muniz, Security Architect, Americas at Cisco. Cisco is a networking and telecommunications hardware provider specializing in industry best practices for cybersecurity, including implementing a zero trust strategy.

Traditionally, agencies have practiced reactive rather than proactive cybersecurity. Agencies have also been very perimeter focused for their cyber defenses. But this style fails when threats come from within. "We've seen the realization across government that they need to do a better job," Romness said.

The blind spots facing agencies, meanwhile, include malware and insider threats. Malware is intentionally harmful software, while insider threats are anyone with access to an organization's sensitive, internal assets. A zero trust approach to cybersecurity responds to threats such as these by not trusting workloads, workforces and workplaces. "You're not trusting the people, the network or the process," Muniz said. "You must provide the least amount of required access for people to do their work, limit access to devices with segmentation, and monitor the network and workloads for unusual or malicious activity."

> *"All the who, what, where, when, why, and how are taken into consideration. You can then allow network access based on those things."*
>
> **- Peter Romness, Cisco**

Ultimately, agencies enforce a zero trust approach to cybersecurity by focusing on their people, process and technologies. A zero trust approach to cybersecurity requires authentication, segmentation, least privilege access control, and continuous monitoring. Automating these techniques reduces the burden on employees, letting them devote more energy and time to their agency's mission. "It's network as a sensor and enforcer," Romness said.

After establishing an equal focus on people, process and technologies, tools such as those Cisco provides are the ingredients for a thriving zero trust approach to cybersecurity program. Cisco's Identity Services Engine (ISE), for example, provides least privilege access control for any devices and users everywhere on agencies' networks. The company's Duo Security tool, meanwhile, continuously authenticates users anytime they access agencies' systems. Finally, Cisco's Tetration tool maps out device workloads and can help develop a whitelist approach to security. "Cisco is the company you want to get a holistic cybersecurity solution," Muniz said. "We provide security for the workload, workforce and workspace."

Takeaway: Enforcing a zero trust approach to cybersecurity requires agencies' people, processes and technology to work together on defense.

Jefferson County, Colorado CISO: Do the Basics Before Zero Trust

Jill Fraser strives to focus on the basics of cybersecurity as Jefferson County, Colorado's CISO. Every day, Frazer's office assesses the county's assets, how important these resources are, and the best ways to protect them. This risk management strategy drives Jefferson County's security, including the county's zero trust practices.

During an interview with GovLoop, Fraser said she hopes agencies keep cybersecurity's fundamentals front and center as they encounter strategies such as a zero trust approach to cybersecurity. Fraser argued that governments will struggle with a zero trust approach to cybersecurity if they don't master rudimentary cybersecurity first.

This interview was lightly edited for length and clarity.

GOVLOOP: What are Jefferson County's biggest cybersecurity challenges, and what cyberdefenses does your county have for meeting them?

FRASER: There's no more difficult place to do cybersecurity than local government. That's because we typically have all the same types of data that larger organizations need to protect, but in some cases, we have additional types of sensitive information, such as criminal justice information, healthcare information, personally identifiable information [PII] and payment card industry [PCI] information. We aren't typically blessed with the types of funds or the number of resources – personnel, technical or otherwise – that the larger organizations are fortunate enough to have. Additionally, local governments don't receive the same type of discounts from vendors that nonprofits, education organizations and state and federal agencies receive. When it comes to challenges, that's one of our biggest ones.

To address that, we're bringing together local governments across Colorado. Instead of working as separate, individual entities trying to do the same thing in siloed pockets across our organizations, we're discussing viable options to come together and act as a unified entity to do some amazing work for all our citizens and taxpayers.

How is Jefferson County using authentication and segmentation to protect the county's networks and cybersecurity?

I think what you'll find in many governments is that there are different elected officials that head up different pieces of an organization. For example, in my organization, we don't have a mayor or governor. Instead, we have multiple elected officials over different areas who are responsible for their areas. We don't have centralized IT. I think we've got seven different IT groups. Subsequently, what we've identified is the risk across our organization for cybersecurity incidents to spread laterally.

We want to have a level of visibility between our separate, segregated areas, so that we can understand where our risk is and where our sensitive information is. In addition to having that knowledge, we now also have knowledge of what's happening on our network, what's expected and what's not expected.

As far as segmentation, we've spent the last few years examining and investing in both technology, policies and procedures, identifying ways to break up our network so that if there were an event, then we'd be able to segment control over it to a smaller portion of our organization. Instead of our entire organization being impacted by an attack, outage or ransomware, we could isolate it. That would mean a faster recovery time and shorter down time. There'd be less impact on our employees and citizens.

We also utilize multifactor authentication for all our remote access, and we're investigating deploying it further for other services. It's deployed for all our administration on Microsoft Office 365. We're looking to deploy it for all our end users and applications that maintain sensitive information. The difficulty that we run into with those layers is the extra effort that it takes for end users.

What is a zero trust approach to cybersecurity, and how is Jefferson County using that philosophy for the county's cyberdefenses?

The general definition that I've heard is never trust, always verify. In practice it means having a better understanding of the impact of lateral movement within an organization.

At the end of the day, a zero trust approach to cybersecurity falls under risk management. It's understanding what you have that you care about and knowing how much you care about it. It's also ensuring that you've taken those things into consideration and then appropriately protected them. Or, you've accepted the risk because you understand what could possibly happen if something affects that information.

If it were just about technology, then we all would have implemented that technology. We would have the magic patching platform or the magic tool that tells our end users, 'Don't click on that.' But it's not that simple. If our end goal is to increase cybersecurity maturity, that we would find a better way to communicate with folks and help support them in that effort. It's to help them understand when they're an organization that's ready for a zero trust approach to cybersecurity. The real goal is to help folks get to a place where they can protect the things that they care about in a manner that's budgetarily responsible.

Conclusion & Next Steps

Agencies enforcing a zero trust approach to cybersecurity must first transform their people, processes and technology. Subsequently, a zero trust approach to cybersecurity doesn't appear overnight; practicing this philosophy is an ongoing journey rather than destination. The following suggestions can help agencies get started.

Decide What Needs Protecting

Agencies store large amounts of citizen data, and they're also responsible for their own mission-critical information. Determining which data is the most sensitive and why helps agencies decide the best methods for defending it.

Trust and Verify on Authentication

Agencies should authenticate the devices and users on their networks. The process shouldn't stop there, however; permanently authenticating entities after one successful log-in can leave them with network access even if they're compromised. Agencies can avoid this risk by authenticating entities every time they need access to their networks.

Segmentation Saves Networks

Segmentation can help agencies by shielding their entire networks from sections that are compromised. Segmented networks are harder to damage from the inside or the outside, offering stronger protection from all threats agencies face.

Leverage Least Privilege Access Control

Assuming a less-is-more approach to network access can keep agencies' data safe. Agencies that restrict network access to precisely the resources that devices and users need make sure they can't reach assets they're not supposed to. Consider government contractors, or private sector employees temporarily working for agencies on a contractual basis. Agencies can keep contractors from accessing their resources outside of business hours, allowing them to keep better tabs on what actions these individuals are taking. Additionally, least privilege access control guards healthy network segments from compromised ones during cybersecurity incidents.

Keep Aware With Continuous Monitoring

As the number of devices and users grows, agencies will have more trouble seeing the entirety of these entities on their networks. Continuous monitoring can keep agencies constantly aware of what's on their networks by making their vigilance ongoing and networkwide. Endless, networkwide visibility can aid agencies with finding, identifying and stopping cyberthreats faster. It's a state that also assists them with understanding what's happening on their networks, when and why.

Don't Hesitate to Automate

Automation can save government employees' energy and time, subsequently reducing costs for their agencies. Cybersecurity is no exception, and automation can alleviate some of the human labor involved with a zero trust approach to cybersecurity. Agencies that use automation for a zero trust approach to cybersecurity lose none of their safety while gaining more momentum for their missions.

Zero Trust Doesn't Run on Technology Alone

Enforcing a zero trust approach to cybersecurity takes more than technology; people and processes must also evolve for this philosophy to work. If people don't change their routines or the processes they have for them, no technology can help agencies practice a zero trust approach to cybersecurity.

Thank you to Cisco for their support of this valuable resource for public sector professionals.

About GovLoop

GovLoop's mission is to inspire public sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to the public sector.

For more information about this report, please reach out to info@govloop.com.

govloop.com | @govloop