Zero Trust: A Potent Weapon Against Cyberattacks

HOW TO MODERNIZE OUTDATED SECURITY APPROACHES TO ADDRESS ESCALATING THREATS

Zero trust security has broad implications for state and local governments — giving them a potent weapon against escalating cyber risk.

Cybersecurity has been a top government concern for years, but the COVID-19 pandemic made the problem even bigger. Rapid growth of remote work and digital government services in response to the pandemic expanded the threat surface for cyberattacks. And cybercriminals have shown no mercy for public sector organizations, often targeting state and local government offices and schools with increasingly disruptive exploits.

How does zero trust security help solve this relentless challenge? Proponents of the strategy often point to an analogy of a castle and moat. Traditional security controls like firewalls, intrusion detection and endpoint management secure the castle's perimeter. But sophisticated attackers keep crafting digital drawbridges and getting inside anyway.

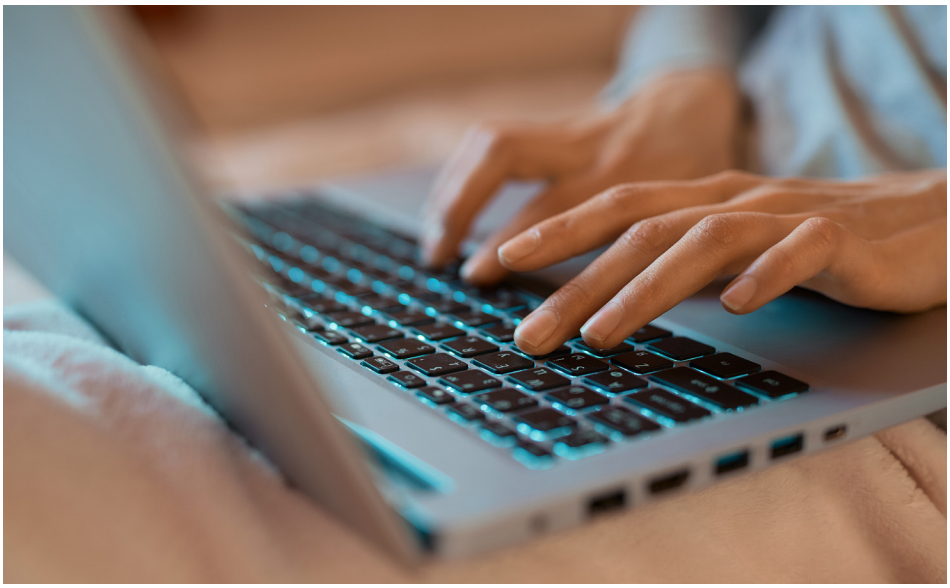
A zero trust approach considers intrusions inevitable. It locks every door inside the castle, requiring every user, device and transaction to be authorized. In the old paradigm, anybody inside the castle was trusted to avoid places where they didn't belong. This ends under zero trust, which controls where users can go and what they can do through specific access privileges. Zero trust limits network users' access only to the data and applications they require to do their work.

This brief is drawn from a recent webinar convened by *Government Technology*, which brought together experts from the Center for Digital Government (CDG), Google Cloud and the New York City Cyber Command. We explore the core challenges zero trust addresses, lay out the benefits of this approach and provide best practices for getting started — especially in cloud environments.

How We Got Here

Before we delve into the advantages of zero trust, it helps to review why this approach came to be.

Historically, network access controls gave people broad authority to navigate through networks once they were logged in. In essence, network administrators trusted people not to misbehave inside their networks. Given that users had strong incentives to keep their jobs, it made sense to trust them — especially when authorizing every user, device and transaction on a network was a daunting prospect.



Relentless cyber intrusions make the trust model untenable. Firewalls, intrusion-detection algorithms and endpoint management software are essential. But a single successful bot attack can still infect an enterprise network. It's impossible to completely prevent employees from accidentally giving away their log-in credentials in a phishing attack, for instance.

Today, it makes more sense to verify every user, transaction and device. Fortunately, advances in automation make this option increasingly viable.

It can't happen soon enough. The evolving threat environment gives state and local governments little choice but to embrace the protections of a zero trust environment to secure sensitive data and critical IT assets.

Core Challenges

Multiple factors are pushing agencies toward zero trust:

Changing work arrangements. Since the arrival of COVID-19, many more public sector employees are outside the traditional network perimeter. "The rapid adoption of remote work and virtual services dramatically altered and expanded the risk landscape for public organizations," says Deborah Snyder, former chief information security officer (CISO) for the state of New York, who is now a CDG senior fellow. CDG surveys of state and local government officials consistently show that hybrid work schedules — where employees work remotely at least part time — will be permanent for many agencies going forward.

Rising expectations. Residents and staff alike want more from government applications — better interfaces, smoother user experiences, more automation —

without added risk to personal data and IT assets. “Constituents expect a level of service that’s a lot higher than what government agencies have been prepared to deliver,” says Chris Hein, head of customer engineering for public sector at Google Cloud. Although the private sector notion of “move fast and break things” isn’t acceptable for government, agencies still must move faster to launch convenient and secure digital government services.

Expanding threat surface. Device varieties and quantities grow every day with the addition of IoT sensors, smartphones, web-native applications and dedicated mobile tools for jobs like inspections. “You have more things connecting to more things,” says Colin Ahern, deputy chief CISO for security sciences with New York City Cyber Command. “It really does create this attack surface that is much richer and harder to defend.”

Shifting attack tactics. “Threats are increasing in complexity and velocity — basically by any measure,” Ahern says. It’s becoming more difficult to distinguish between cybercriminals and nation-state actors, which complicates diagnosing anomalous activity on a network. “You have nation states conducting activities that are untargeted and look a lot like cybercriminals; you have cybercriminals that are getting much more sophisticated,” looking more like nation states, Ahern says. This means government agencies need every available tool and tactic to secure their networks.

Aging technologies. Governments often use a mishmash of old hardware and new software-as-a-service (SaaS) capabilities. Legacy systems, mainframes and application frameworks that support critical systems are often out of step with current needs. “When these systems were designed, they mostly reflected paradigms that are just not what we’re seeing today,” Ahern says.

Hein adds: “You’re doing this amalgamation of enterprise services, some of which were built for cloud and some of which were built for the 1970s, and you’re still dependent on them. You have to really figure out the right way to do this.”

The advantage of zero trust is that it gives agencies a path toward a more secure future despite all these challenges.

Moving Toward Zero Trust

Zero trust security adds a critical extra layer of protection because it does not presume any user has a right to be on a network. It always asks, always checks.

“What zero trust implies is that I don’t trust you just because you happen to be on my network,” says Hein. In action, zero trust locks valuable services or data behind doors. When a user tries to open the door, algorithms correlate data from multiple sources to determine whether they should be granted a key to get in.

Thus, implementing zero trust controls makes it much more difficult for intruders to do damage or discover valuable data. And it encourages them to pursue softer targets.

When configured correctly, zero trust applications give intruders little room to maneuver. They can wander the castle halls, but they can’t pick the locks on secure doors. “Even if an attacker gets access to one person’s credential, it won’t let them go across the network to everything else that might be there,” Hein says.

Google uses a zero trust approach to protect its own operations, Hein adds,

> **“The rapid adoption of remote work and virtual services dramatically altered and expanded the risk landscape for public organizations.”**
>
> ***Deborah Snyder,** former CISO, State of New York*

> **“You have more things connecting to more things. It really does create this attack surface that’s richer and harder to defend.”**
>
> ***Colin Ahern,** Deputy Chief CISO for Security Sciences, New York City Cyber Command*

and requires every employee to use a hardware-based security token to access critical data and services. “That in and of itself reduced our attack threats by a considerable amount,” he says.

At the New York City Cyber Command, zero trust was implemented before the COVID-19 pandemic hit. With the amount of network devices growing rapidly in the city, the Cyber Command needed a security approach that would enable it to work safely in this evolving environment. Like Google, NYC also shifted to multifactor authentication.

“Our primary purpose as cyber defenders is making sure our incident-response team, which is 24/7/365, is able to continue their work unimpeded,” Ahern says. This requires ingesting, normalizing, processing and storing vast amounts of telemetry and security data about who is accessing what, for what reason, and where. “We built a high-velocity data pipeline in the cloud that helps us accomplish that task,” Ahern adds.

As a result of adopting zero trust, the Cyber Command was prepared when the pandemic forced city agencies to work from home in March 2020. The organization did not need to make configuration changes. Incident-response experts stayed on the job uninterrupted. “We’re very proud of that,” Ahern says.

Best Practices: Tips for Adopting Zero Trust Security

Zero trust is not a technology purchased from a vendor. It's an approach applied across a technology ecosystem. Zero trust has three core components: vision, cloud strategy and technology selection.

Creating a zero trust vision: Success with zero trust requires a focus on outcomes. Don't dive into it because it's the security topic of the week. "Do it because it is the only provable way to accomplish your goals," Ahern says.

Ahern suggests starting on a specific application or service with well-defined stakeholders who care deeply about it. "You want to find something big enough to be relevant, but small enough to be doable."

Once you've identified a starting point, establish security operations metrics to help document what's working. "Oftentimes, that comes too late in the process," Hein cautions.

It's also crucial to maintain a sharp vision of what you aim to accomplish. Create clear objectives in areas like recovery times and enforce them with service level agreements. And make sure the vision is adaptable, with baked-in agility and scale.

Building a cloud strategy: A zero trust approach requires provisions for cloud-based software, public cloud services and hybrid cloud infrastructures. Hence, a sound cloud strategy is essential.

As-a-service offerings for platforms, infrastructure and identity management often support zero trust principles.

Cloud services also are central to backing up and recovering data and applications if a cyberattack brings systems down. A cloud strategy requires provisions for capacity management, demand forecasting and incident response.

"You want to think very carefully about capacity planning because if something isn't reliable, it can't be considered secure," Ahern says. He warns that no plan survives contact with the public or an adversary, so you need to be prepared to adapt on the fly.

In addition, it's important to test disaster recovery programs to ensure everything works properly. "Unless your plan has been tested, it is not a real plan," Hein says.

Choosing the right technologies: Hein and Ahern share these tips for picking technologies and vendors that support zero trust.

- Build relationships with experienced, trusted vendors.
- Document everything you hope to accomplish.
- Assess total cost of ownership and the opportunity costs of technology choices.
- Invest in identity management upfront. Clarify identity policies and standards — including the life cycle of onboarding, rights, delegations and offboarding.
- Clarify endpoint security. Define a good configuration and how to assess it.
- Establish how to mediate deviations and how to deploy and update security tools. Clarify who manages everything.

> **"[The cyberattack threat] won't just go away on its own. You have to change something."**
>
> ***Chris Hein,** Head of Customer Engineering for Public Sector, Google Cloud*

Trusting the Zero Trust Approach

The cyberattack threat will only get worse. "It won't just go away on its own," Hein cautions. "You have to change something."

For starters, it's time to rethink the castle-and-moat model. After all, today's security perimeter is nothing like a wall — it's more like a mosaic of devices, applications and users.

Zero trust principles give government agencies an opportunity to safeguard this mosaic. With a carefully considered strategy and implementation, zero trust can help agencies improve public services while securing sensitive data and applications.

To learn more about cybersecurity, check out on-demand sessions from the Google Cloud Government and Education Summit.

This piece was developed and written by the Government Technology Content Studio, with information and input from Google Cloud and AMD.

Produced by:

government technology

Government Technology is about solving problems in state and local government through the smart use of technology. Government Technology is a division of e.Republic, the nation's only media and research company focused exclusively on state and local government and education. **www.govtech.com**

For:

AMD

With Secure Encrypted Virtualization (SEV), AMD EPYC™ processors help safeguard privacy and integrity by encrypting each virtual machine with one of up to 509 unique encryption keys known only to the processor. Learn more about how Google's Confidential VMs and Confidential GKE Nodes enable AMD Secure Encrypted Virtualization to help deliver confidential computing for the cloud. **https://cloud.google.com/confidential-computing**

Google Cloud

Google Cloud accelerates organizations' ability to digitally transform their business with the best infrastructure, platform, industry solutions and expertise. We deliver enterprise-grade solutions that leverage Google's cutting-edge technology – all on the cleanest cloud in the industry. Customers in more than 200 countries and territories turn to Google Cloud as their trusted partner to enable growth and solve their most critical business problems. **cloud.google.com**

IMAGES PROVIDED BY SHUTTERSTOCK.COM