Security Beyond the Desktop

A briefing on zero trust, cloud and the remote workforce

zscaler™ aws govloop

Introduction

The events of 2020 and the resulting adoption of widespread telework forced federal, state and local agencies to implement unexpected changes to their security structure. But even before the sudden shift of circumstance, security experts had foreseen the eventual need for distributed, remotely applied security.

In this booklet, you'll learn how agencies are moving beyond old security models to safely and efficiently support distributed workforces.

Government and industry experts shared their insights on this topic during GovLoop's virtual Briefing Center, "Transforming Government Security for a Cloud-Smart World," a two-hour collection of online trainings. They discussed the need for agencies to securely connect entities, such as users and machines, to applications and services when their locations may be anywhere.

So how exactly can agencies embrace this new path forward, and what does that look like in practice today? Read on to learn more and hear from agencies on this journey.

Watch the recorded sessions:

Transforming Government Security for a Cloud-Smart World Part 1

Transforming Government Security for a Cloud-Smart World Part 2

Experts

Bill Zielinski, Chief Information Officer (CIO), city of Dallas

Chi Kang, Deputy Director for Operations, Cyber Security Division, National Oceanic and Atmospheric Administration (NOAA)

Dovarius Peoples, CIO, U.S. Army Corps of Engineers

Michael Watson, Chief Information Security Officer (CISO), Commonwealth of Virginia, Virginia Information Technologies Agency

Ian Milligan-Pate, Regional Director, State & Local Government, Zscaler

John MacKinnon, Global Telecommunications Partner Development Manager, Worldwide Public Sector, AWS

Jose Padin, Director of Sales Engineering, U.S. Public Sector, Zscaler

Tony Ferguson, Director, Transformation Strategy, Zscaler

A New Normal Means New Security Trends

Before the pandemic, various trends and policies had already presaged a rethinking of security philosophy. Instead of considering security as the protection of one central site or system, the tone has moved in favor of protecting every piece of data and individual application.

More than putting titanium bolt locks on all the doors, agencies are locking every single cabinet and drawer in the house, in a sense. That's the basic idea behind a zero trust approach to security.

"This pandemic hasn't really changed the plan, but it has accelerated the plan," said Bill Zielinski, Chief CIO of the city of Dallas.

The Different Layers of Data Protection

"Data's the foundational element for everything we do," said Dovarius Peoples, CIO of the Army Corps of Engineers. "Once you get the data figured out, everything else will plug and play."

Peoples expounded that the Corps has very closely examined user access to applications and data. The agency operates off a "deny all and allow by exception" methodology, a core tenet of zero-trust cybersecurity strategies, Peoples said. Under this approach, users are given access to only the applications and data they need, and staff verify their identities frequently.

The Rapid Shift to Telework and Digital Services

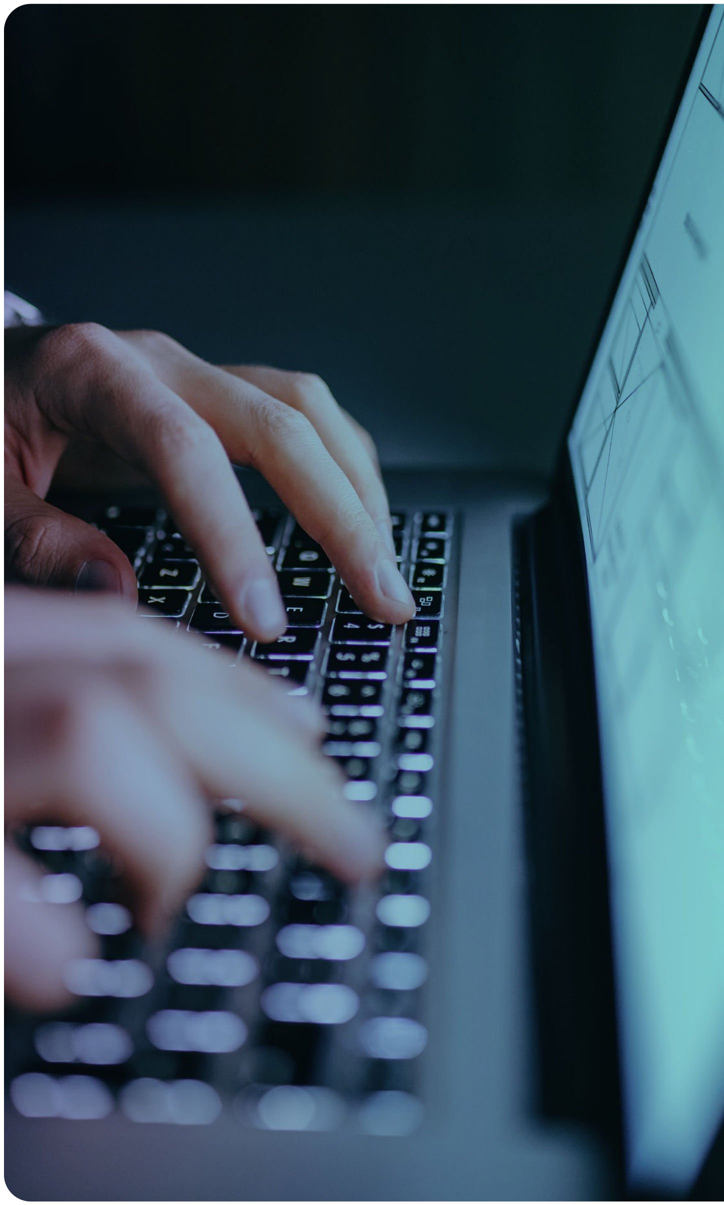
One fundamental truth about security hasn't changed. Security departments' goal is still to enable agencies' mission, just making sure it continues safely.

This was put to the test during the pandemic, when the sudden rush of teleworkers and online customers forced security teams to make compromises on their usual standards.

"We have to be comfortable being uncomfortable," said Virginia's CISO Michael Watson.

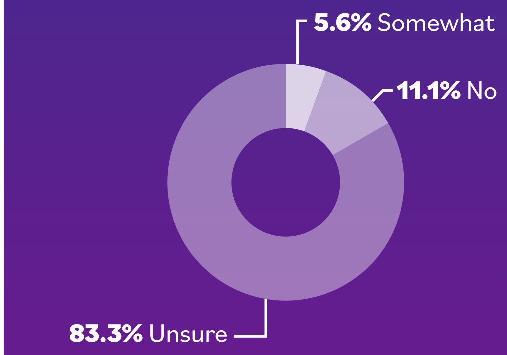
Watson said his team had to accommodate a rapid deployment with a lesser degree of review than would have normally been the case. That's not to say agency databases are left open, but that security teams had to sacrifice some of their standard checks in order to get the workforce up and running remotely. After all, Watson said, sidelining employees for weeks as they set up at home was in no way a possibility.

Zielinski said digital services have met a similar challenge as well. Some services went from 20% online to 100% online overnight. In a city, essential services — such as first response branches — can't afford to go down for even a minute.



Are organizations utilizing TIC 3.0?

During GovLoop's Briefing Center, we surveyed attendees about their agency's use of TIC 3.0. Most were unsure, which underscores Padin's point that everyday employees don't need to know and likely will not know the inner workings of IT networks. The ultimate goal for users is that, hopefully, they'll notice that connecting to networks has gotten easier. Also, TIC 3.0 and its subsequent updates are still fairly new. This year the federal government released telework and other related TIC 3.0 guidance.



The Evolution of Policy and Compliance

TIC 3.0, the latest update to the federal government's most prominent network connection program, is a broader indication of the move to security on an individual level. Though TIC began as a means for agencies to account for and reduce connections to their networks, it has since developed into a use-case-driven manual for securing traditional, cloud and distributed environments. TIC Program Director Sean Connelly told GovLoop in prior interviews that the TIC office is looking at zero-trust use cases.

"TIC 3.0 is an enlightened evolution of what the network is and where security needs to be today," said Jose Padin, Director of Sales Engineering for the U.S. Public Sector division of Zscaler.

When it first began in 2007, TIC was prescriptive. For agencies, though TIC tightened up their security standing, it was another policy to comply with. Now, it's more than that.

TIC 3.0 permits agencies to define their own trust zones and offers them multiple ways to establish secure user connections to the network – either going through the cloud, branch offices or traditional access points. Padin said everyday employees don't need to know all of this; just hopefully, they'll be able to tell connecting to networks has gotten easier.

The TIC program office published draft use cases far in advance, allowing agencies to pivot to the new model, said Chi Kang, Deputy Director of Operations for the National Oceanic and Atmospheric Administration (NOAA) Cyber Security Division. That preparation time was crucial for NOAA, which serves as a TIC access provider for other agencies.

The latest edition of TIC also marks the convergence of several key programs, Kang said, including the Continuous Diagnostics and Mitigation (CDM) program that tracks activity and identity on agency networks and across the federal enterprise.

"There's a huge paradigm shift here where everything is converging," Kang said.

Kang seemed to welcome many of the notable changes, including the interpretation of trust zones. In more traditional perimeter security models, the only two trust zones were those untrusted and trusted. Now, agencies can define their own levels of trust for cloud, mobile and remote environments.

NOAA has been looking hard at its cybersecurity capabilities to see which might overlap or which might fill in gaps between the policies, Kang said. One best practice he touted is exchanging notes with industry and agency partners to creatively develop use cases and meet compliance requirements.

Zero-Trust Allows You to Apply the Right Level of Protection

When you assemble a peanut butter sandwich, it doesn't matter whether you're a crunchy or smooth person, you want to spread the condiment evenly across your bread of choice. The consistent symmetrical coverage of the carb is key to an enjoyable sandwich experience.

However, when it comes to cybersecurity, agencies do not want to take a peanut butter perspective, where all systems, applications and data are secured evenly.

"Our culture is used to the peanut butter approach, where we try to protect everything equally," said Gerald Caron, Director of Enterprise Network Management at the State Department. This approach results in some systems being overprotected and overall network functionality being constrained. As the historic Prussian king Frederick the Great once said, he who defends everything defends nothing.

"With zero trust, we protect things most significant to us," Caron said. "The crown jewels, not the baloney sandwich."

But this is just one piece of what zero trust encompasses. Zero trust has become something of a buzzword in recent years, so it's important to understand what it actually is to implement this kind of security architecture. Its core principles can generally be broken into two: Trust no one and tier protections.

Asking the Right Questions About Your Data

At the end of the day, agencies are ultimately trying to protect data through a zero-trust model, Caron said. Identity management controls and solutions are significant, but in the event that identity gets compromised, the first questions security teams ask are around data: What does the hacker have access to? Is there exfil or data extraction?

A key part to understanding your data risk is understanding which data is important and which is not so important. For example, plans for holiday celebrations are not as sensitive and mission-critical as personally identifiable information (PII) on passport applications.

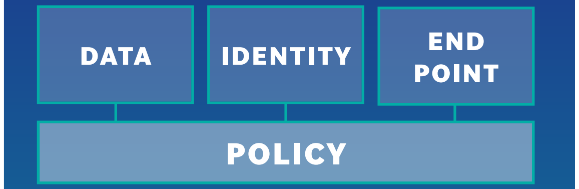
"Zero trust recognizes these differences and categorizes data based on its sensitivity and mission criticality," Caron said.

Again, it goes back to protecting your crown jewels over baloney sandwiches. "I'll remake my baloney sandwich," Caron said. You can't remake the crown jewels.

As agencies put their data in the cloud, it's all the more imperative to understand their data risk. Security certifications on cloud services, such as FedRAMP, mean little if agencies don't take active ownership over their data protection.

Caron's advice: "Do your homework, because at the end of the day, it's still your data."

Zero Trust Core Principles



Trust no one

1. **Know your people and your devices**
   Validate identity at every step.
2. **Design systems assuming they are all compromised**
   Distrust everything, so when a breach happens you are as protected as can be.
3. **Use Dynamic Access Controls**
   Access to services must be authenticated, authorized and encrypted at all times and able to be revoked during a session.
4. **Constantly evaluate risk**
   - Include context in risk decisions
   - Monitor and log in every location possible
   - Aggregate log, system, and user data

Right size protections

5. **Invest in defenses based on the classification of data**
   Spend more money defending the systems at greater risk.

Why Agencies Are Talking About Security at the Edge

Security needs to go where users, data and applications go.

That's the simple premise behind a new security model called Secure Access Service Edge (SASE). SASE is gaining interest across government because it provides a way to improve both the performance and security of IT services as more and more users, data and applications reside outside the traditional network perimeter.

That shift, largely driven by the adoption of cloud- and mobile-based solutions, is expected to be accelerated by the large-scale move to remote work, in which nearly everyone has been working outside the perimeter.

In remote work, "users and data are not inside the castle anymore, so why is the focus on protecting the physical network?" Zscaler's Padin said.

Padin and John MacKinnon, Global Telecommunications Partner Development Manager, Worldwide Public Sector at AWS, broke down the value of SASE and what this framework means for government.

The SASE-Zero Trust Connection

SASE reflects a larger trend toward focusing on security at the data and application levels. The traditional castle-and-moat model assumes that anyone within the castle is trustworthy and should have access to resources within the castle.

But that has proven to be a faulty assumption: Malicious actors have become proficient at stealing end users' network credentials, making it possible to get inside a perimeter and moving from one system to another without being detected.

With SASE, no one is given blanket access to resources within the perimeter. If a malicious actor manages to steal someone's credentials, "the only things that they are going to get access to are the one or two apps [the user has] access to, not the entire network," MacKinnon said.

To accelerate positive change, while improving security posture, agencies can adopt a zero trust architecture that incorporates SASE.

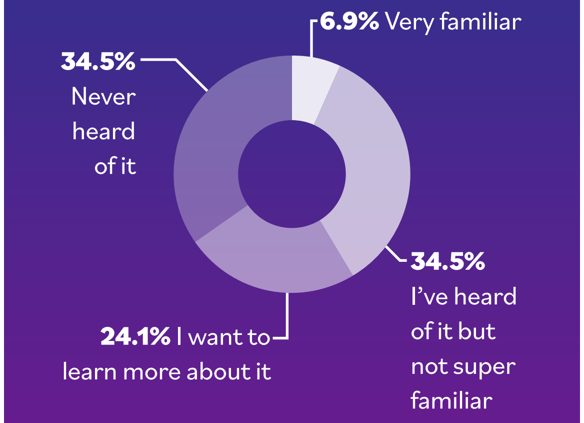
The Future of SASE

At this point, many people in government are still on a learning curve with SASE. A poll taken during the session found that just under 7% of respondents said they were "very familiar" with SASE. Another 34.5% had heard of it but were not super familiar and 24.1% said they wanted to learn more. Nearly 35% said they had never heard of it.

But Padin expects SASE to continue to gain traction for the simple reason that it addresses a pressing need. "We want people to understand that SASE isn't just a marketing term – it is more of a term to define what is already happening," he said. "Secure access is happening at the edge, so we need services at the edge."

How familiar are you with SASE?

Briefing Center attendees were asked how familiar they were with the new security model SASE.



How Zscaler and AWS Help

Zscaler and AWS share a common goal: helping organizations move securely to the cloud while delivering a better user experience.

More than 5,000 government agencies already depend on AWS commercial-level clouds, selecting from either AWS GovCloud (US) or more tailored offerings. Now, TIC 3.0 allows many more agencies to continue moving to the cloud securely and efficiently. After going to the AWS Cloud, agencies receive access to machine learning, mobility and citizen-facing services.

Zscaler provides zero-trust, secure remote access to internal applications running on AWS. And the SASE framework is expected to further reduce costs, complexities and risk.

The Zscaler SASE architecture helps accelerate cloud adoption by removing network and security friction through a consolidation and simplification of IT services. Without the need for device management and separate services, Zscaler offers a frictionless and transparent experience for users and standardization across locations for the IT team.

Learn more at www.zscaler.com/government and aws.amazon.com/government-education/government

Security Considerations and Future Implications

So what's next? Security is likely to gain steam as a business enabler of digital services, remote work and modern technologies, experts suggest.

"The pandemic's put security in an interesting spot, because security's never been more important to the business," said Ian Milligan-Pate, Regional Director in State and Local Government for Zscaler.

Specifically, this would follow two models, said Tony Ferguson, Director of Transformation Strategy at Zscaler. Notably, neither includes virtual private networks (VPNs), a common form of connecting into the network and agency resources.

First, Ferguson said, agencies might look to take parts of the internal enterprise offline. As opposed to employees accessing their systems, such as virtual desktops, through online portals and firewalls, agencies could construct a software-defined network that is not physically based within agency offices. Software-defined networks allow for faster, broader access and more granular control — ideal for cloud computing environments.

Then, agencies would implement zero trust within the network, creating stricter access permissions and verifying identity regularly.

These two steps would be crucial for moving to a security-enabled distributed environment of the future, Ferguson said.

That's the goal for Peoples, the Army Corps of Engineers CIO, and his department. As the pandemic set long-term plans into motion, the jolt could spur agency security into a place where office setups are soon in the past.

"Completely untethering the end user from their desktop. We're a very distributed enterprise working in a lot of important areas and disaster relief," Peoples said.

9 Nuggets to Take Away From the Briefing Center

1. Security needs to go where users, data and applications go.

2. The traditional castle-and-moat model is broken. It assumes anyone within the castle is trustworthy and should have access to resources within the castle.

3. Zero trust flips that model by elevating two core principles: Trust no one by default, and tier protections.

4. With zero trust, agencies protect things most significant to them, particularly critical data and applications.

5. A key part to understanding your data risk is understanding which data is important and which is not so important.

6. Zero trust recognizes these differences and categorizes data based on its sensitivity and mission criticality.

7. Now, agencies can define their own levels of trust for cloud, mobile and remote environments.

8. Coupled with zero trust, Secure Access Service Edge (SASE) is also gaining interest across government.

9. SASE provides a way to improve both the performance and security of IT services, as more users, data and applications reside outside the traditional network perimeter.

About Zscaler

Zscaler is built to help you move to the cloud securely while delivering a better user experience. With Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA), agencies can safely connect their users and customers no matter the device, application or location. Unlike traditional approaches based on hardware appliances, Zscaler cloud-based solutions are fully scalable.

ZIA was the first TIC 3.0-approved secure internet and web gateway solution. By helping agencies go directly to the cloud and securely move mission-critical traffic, it removes latency from the process that regularly slows when using a traditional TIC solution or MTIPS. ZPA provides seamless and secure zero trust access to internal applications for authorized users. Traffic does not traverse the open internet, bypassing the need to go through the TIC. Zscaler is ready for agencies' transitions to the cloud under the new use case, leaving latency and static perimeters in the past.

Learn more at www.zscaler.com/government.

About AWS

AWS is designed to meet the needs of government agencies on their cloud journeys. Authorized as FedRAMP-High, the AWS Cloud can service a variety of government missions securely on an affordable and service-based plan.

More than 5,000 government agencies already depend on AWS, selecting either AWS GovCloud (U.S.) or more tailored offerings. Now, TIC 3.0 allows many more agencies to continue moving to the cloud securely and efficiently. After going to the AWS Cloud, agencies receive access to machine learning, mobility and citizen-facing services.

Learn more at aws.amazon.com/government-education/government

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.

www.govloop.com | @GovLoop