U.S. Government Civilian Agency Secures Apps and AWS GovCloud with the Zscaler™ Zero Trust Exchange

U.S. Federal Government Civilian Agency

Location: Washington, D.C.

Industry: Government Administration

Customer Size: Safeguards hundreds of millions of constituents across the U.S.

Investigators at this U.S. Federal Government Civilian Agency investigate significant travel accidents worldwide, develop factual records and make safety recommendations with one goal: ensuring that such accidents never happen again. For nearly 100 years, investigators have worked to provide timely recommendations that save lives.

Legacy security causes access woes

During the process of modernizing, mobilizing, and expanding the deployment of cloud-based applications, the IT department at this U.S. Government Civilian Agency realized its legacy security infrastructure had become obsolete.

"We faced multiple challenges with accessing both cloud-based applications and those in the data center," explained the CIO for the Washington, D.C. headquartered Agency. "Users experienced latency and connection issues and our legacy solution also had inherent security insufficiencies. We needed a new solution that delivered a seamless and secure path to the cloud."

FedRAMP-authorized ZPA holds the key

Responsible for reducing travel accidents for all U.S. residents, this Agency requires reliable, high-performance, secure connectivity to applications for speeding incident responses across the country and worldwide.

In accordance with the Office of Management and Budget's (OMB's) Cloud Smart strategy, the Agency is rapidly adopting cloud technologies to streamline work processes and serve constituents faster. By evaluating solutions authorized by FedRAMP, the Agency determined that it could begin moving to a Zero Trust security architecture with the adoption of **Zscaler Internet Access (ZIA)** and **Zscaler Private Access (ZPA)**, which are fundamental building blocks of the **Zscaler Zero Trust Exchange platform**.

CHALLENGE

Replace complex legacy network security and frustrating access processes with a FedRAMP-authorized Zero Trust approach

SOLUTION

- Zscaler Internet Access™ (ZIA™)
- Zscaler Private Access™ (ZPA™)
- Advanced Cloud Sandbox
- Zscaler™ Zero Trust Exchange™

OUTCOMES

- Cut the time required to complete a comprehensive accident investigation in half
- Accelerated migration to an AWS GovCloud environment while obtaining flexibility and agility
- Gained the highest level of protection against known and unknown threats, including patient-zero attacks
- Eliminated traditional firewalls and VPNs, reducing IT burdens, security risks, and costs while boosting user experiences
- Enabled utilizing cost-effective broadband and cellular connections, replacing expensive and restrictive MPLS contracts

Old approach drains performance and relies on MPLS

Prior to adopting cloud-native Zscaler, the Agency secured its network using a traditional castle-and-moat model that relied on firewalls and virtual private network (VPN) technology. In that complex environment, all traffic was routed through the data center, either via VPN, for accessing internal applications, or a complex Trusted Internet Connection (TIC), required at many government agencies, for accessing the internet and SaaS-based applications.

In addition, the Agency was dependent on dedicated Multiprotocol Label Switching (MPLS) circuits for transmitting data, regardless whether the VPN or TIC was used. Consequently, application performance was significantly diminished and communications expenses were high.

"Before the Zscaler implementation, it could take our investigators many hours to upload accident artifacts, particularly when accessing internal applications from our most distant offices," said the CIO.

Sometimes the connections were so challenged that the workaround was filing reports using ground delivery services to courier data and documents.

Stripping away complexity while boosting security

As Zero Trust can't be implemented using firewalls and VPNs, which also create back doors that allow threats to enter, the Agency deployed the Zero Trust Exchange platform to strip away complexity and streamline access. By phasing out VPNs and firewalls with Zero Trust, the Agency also boosted security as the platform inspects all traffic, including encrypted traffic, for the effective prevention of threats and data loss.

For internet access, the Agency designed an innovative and secure "TIC-in-the-Cloud" using ZIA. Internal application access transitioned to VPN-free ZPA. Using these two solutions significantly improves security by establishing connections between users and applications, rather than connecting them to the network. This makes users and applications invisibile to external threats.

Another benefit comes from preventing lateral movement of threats within the network. That's because ZPA enables granting users least-privileged access, which means only providing access to the specific applications a user needs to complete their assignments.

Speedy access boosts inter-agency collaboration

With the Zero Trust Exchange, the Agency's investigators can now access mission-critical applications and share pertinent information rapidly, whether they're in a highly-developed urban area or a sparse rural location. This has enhanced productivity, increased job satisfaction, and reduced frustration.

The Agency's Zero Trust approach is also supporting the interactions with other federal agencies and private industry partners that are critical to speeding accident investigations and disaster responses.

> "With the Zero Trust Exchange platform we're giving users the best experience possible while ensuring IT has the tightest possible security controls."
>
> – **CIO**
> **U.S. Federal Government Civilian Agency**

"Previously, a comprehensive investigation and report typically took about a year to complete," said the CIO. "Now, we can do so within six months, which is half the time, or less, than before."

Eliminating firewalls and VPNs reduces complexities, costs, and risks

Other benefits of adopting Zscaler stem from simplifying IT infrastructure, improving business application performance, and providing visibility for controlling access and troubleshooting.

By reducing infrastructure complexity, the Agency also alleviates IT staff burdens, overhead costs, and security risks. "Leveraging ZIA for the TIC-in-the-Cloud approach significantly reduced the need to manage traditional on-premises firewalls," said the CIO.

"Also, with ZPA, we no longer need VPNs, which are equally difficult to maintain," he added. "In both cases, eliminating appliances reduces the exposure of our applications to the internet. As a result, we've improved security, reduced taxpayer costs, and significantly enhanced user experiences."

In addition, the Agency's modernized security infrastructure is enabling work process transformations. One example is video collaboration, which is now viable due to performance gains as well as visibility around access control and troubleshooting.

"With Zscaler, we've increased our ability to observe and control access to enterprise applications and services," said the CIO. "We can also more effectively pinpoint and address challenges."

AI-powered protection against patient-zero attacks

More recently, the Agency was able to improve its threat protection when **Advanced Cloud Standbox** achieved FedRAMP authorization. This expansion to the Agency's Zero Trust Exchange protects against patient-zero attacks.

Using real-time, AI-powered analysis, Advanced Cloud Sandbox conducts inline inspections of suspicious files and issues an instant verdict, quickly allowing benign traffic to continue. The remaining traffic is quarantined and receives further AI analysis.

Concurrently, this suspicious traffic is blocked for every Zscaler user, preventing any instances of this never-before-seen threat from reaching other customers' networks. As an integrated service in the cloud-native Zscaler platform, protections are updated in real time from billions of transactions per day.

"Advanced Cloud Sandbox gives us another layer of security for safeguarding our data," said the CIO.

> "Now we can complete comprehensive accident investigations within 6 months, which is half the time, or less, than before."
>
> – **CIO**
> **U.S. Federal Government Civilian Agency**

Zero Trust accelerates a secure migration to AWS GovCloud

Today, the Zscaler platform is also helping the Agency secure its migration of on-premises servers and core applications to Amazon Web Services (AWS) GovCloud. This includes agency-specific applications, document management, and a cross-agency web application for accident management. ZPA will also assist with maintaining secure connections to legacy applications and several key systems hosted by other government agencies.

Using Zscaler's tight integration with AWS, the Agency can accelerate its AWS GovCloud adoption, enable dynamic best path routing for workloads across AWS regions, and deliver a better customer experience.

"Zscaler gives us maximum flexibility and agility in terms of how we route traffic to the applications in our AWS GovCloud environment, as well as providing additional visibility into that traffic, and lets us control who is allowed access to what in that environment," said the CIO.

Building out Zero Trust elevates experiences and controls

Moving ahead, the Agency looks forward to further expanding its Zero Trust Exchange platform by adding **Zscaler Digital Experience (ZDX)**, which is in the final phases of achieving FedRAMP authorization. With ZDX, the Agency can gather and analyze granular telemetry and application performance data to improve user experiences. Using ZDX will enable the Agency to quickly locate and resolve the source of an issue, whether it's the user's device, an application, the Agency's network, or an external communications network.

"Insights we acquire from ZDX can enable us to troubleshoot more rapidly and provide the visibility we need for proactively detecting and resolving issues before they impact users," the CIO said.

"Overall, our Zero Trust deployment is enabling us to further advance our security posture while empowering our inspectors to get their jobs done," he added. "This gives users the best experience possible while ensuring IT has the tightest possible security controls."

> "Zscaler gives us maximum flexibility and agility in terms of how we route traffic to the applications in our AWS GovCloud environment."
>
> – **CIO**
> **U.S. Federal Government Civilian Agency**

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com