A **CENTER FOR DIGITAL GOVERNMENT** ISSUE BRIEF | ZSCALER

Why Transportation Agencies Need Zero-Trust Security

Using a cloud-native security platform to protect smart and connected infrastructure

Across roads, rails, airports and water, transit authorities are deploying sensors, cameras and other systems to enhance user experience, improve safety and promote efficiency. The latest IoT Analytics report shows the number of Internet of Things (IoT) connections grew by 18% in 2022 to 14.3 billion active IoT endpoints, and a significant portion are from the transportation industry. Yet there are security challenges associated with infrastructure that increasingly relies on IoT and collects vast amounts of data.

Securing operational technology (OT) such as industrial controls or traffic management systems used to be straightforward: Transportation agencies segregated OT devices and applications from the public internet, making online attacks extremely difficult. But that model is breaking down as agencies modernize traffic management and implement intelligent infrastructure programs that rely on the scale and flexibility of the cloud.

Cloud tools require cloud security. One prudent way to get there is to implement an online platform that secures users and workloads on any internet-connected device in any location. This helps transportation agencies modernize OT and expand smart-infrastructure applications while addressing a broad spectrum of security challenges.

The Importance of a Cloud-Native Security Platform for IoT/OT

Transportation agencies need flexible and modern tools to reduce cyber risks and protect critical infrastructure. That's been clear since the Colonial Pipeline ransomware attack, which interrupted fuel supplies for days across the Eastern U.S. in the spring of 2021.

"We're seeing foreign actors looking to disrupt the normal lives of people," says Karen Mayerik of Zscaler, maker of a cloud-native platform that provides a modern, Zero-Trust approach to security. Zero Trust helps agencies confront security issues that arise during the modernization of traffic management systems and deployment of IoT devices. The biggest challenges:

- **Legacy/proprietary technologies.** Older devices are not secured for modern risks. "They were built with the security mindset of 20 years ago, not the advanced threat vectors we see today," says Mayerik, U.S. sales engineering director for state and local government and education with Zscaler. Moreover, a mix of nonstandard device and software protocols can make protection cumbersome and inefficient.

- **System complexity.** Interconnected devices and software create dependencies where a single problem can disrupt downstream services. Huge varieties of firmware and software must be patched and secured. In many organizations, third-party vendors add further complexity.

- **Large attack surface.** The proliferation of IoT devices has increased the entry points and vulnerabilities that attackers can exploit to gain access to networks and data. "We like to say if it's reachable, it's breachable," says Mayerik.

- **Visibility.** IoT systems administrators need advanced monitoring and real-time protection against threats to prevent data exfiltration and compromise.

Many legacy applications lack controls around identity and were not built with security in mind. "This is where we can help agencies," Mayerik says. "We can help identify where to start and how to incrementally eliminate legacy architectures."

A cloud-native platform with a Zero-Trust security architecture can reduce the attack surface and increase visibility. These platforms can also use artificial intelligence and machine learning (AI/ML) algorithms to identify and defeat adversaries.

Creating a Zero-Trust Security Culture Starts at the Top

A Zero-Trust network uses software to assess the risks of interactions between people, devices and workloads. Identities are always verified. Device and application behaviors are tracked to detect anomalies that signal malicious activity. This can be unfamiliar terrain for rank-and-file employees, who may resist defenses like multifactor authentication and tight navigational controls within a network.

"People in the organization don't always understand the broader value that they're getting when moving to a Zero-Trust architecture," Mayerik says. The never-ending stream of news articles about ransomware and data breaches can leave people feeling overwhelmed. This, too, can lead to paralysis that slows the adoption of Zero-Trust security.

But agencies need to shift their security culture toward "who needs access to what" rather than granting broad access to network users in a dynamic environment, Mayerik says. "The conversation needs to start at the executive level."

Leaders should reinforce to staff that their time and effort to embrace Zero Trust is a priority because they're reducing the risk of damaging breaches. "That really drives quick adoption," she says.

Best Practices for Implementation

Cloud-based security platforms are simpler to deploy and manage than their on-premises counterparts because the platform vendor keeps the software safe and current. There's no hardware for your agency to buy, install and support.

Even so, transportation agencies should follow some basic best practices to ensure a smooth transition to a cloud platform for IoT security.

Address your biggest risks. Agencies need to identify their most valuable assets — data, documents, applications, hardware and so on. These assets require the tightest access controls.

Identify your riskiest users. Remote workers whose devices are attractive to thieves may merit extra scrutiny. Vendors can pose a threat, too. "A contractor can access everything in your environment," Mayerik says. Securely automating vendor onboarding adds another layer of protection against supply-chain and third-party attacks.

Modernize your security incrementally. Moving your entire organization at once to a new security philosophy and platform tends to be overwhelming. "You're not going to change something overnight that has been built over 30 years," Mayerik says.

Instead, think of it as a journey with many segments. Begin with one application to get users accustomed to the new approach. Once they're comfortable, you can scale the approach throughout your IT environment.

Adopt standard security frameworks. Following security guidelines and models from agencies like the federal Cybersecurity and Infrastructure Security Agency (CISA) provides the flexibility you'll need when adapting to future threats.

Don't waste time and energy replicating every feature of your current environment. "Orient around outcomes," Mayerik says. Focus on the areas where new Zero-Trust principles have the biggest impact.

Securing the Future of Transportation

Cloud technologies are pivotal to developing smarter highways and transit systems. Cloud-native platforms that securely verify devices, applications and users will be crucial to these initiatives. The best results will come from savvy selection of technology and thoughtful implementation with an eye toward building a more secure transportation culture.

Mayerik advises nurturing the natural curiosity of your staff. "How do we stay in front of these attackers? With people and their ingenuity."

Remote workers and vendors may be some of your riskiest users.

This piece was written and produced by the Center for Digital Government Content Studio, with information and input from Zscaler.

Produced by:

CENTER FOR DIGITAL GOVERNMENT

The Center for Digital Government, a division of e.Republic, is a national research and advisory institute on information technology policies and best practices in state and local government. Through its diverse and dynamic programs and services, the Center provides public and private sector leaders with decision support, knowledge and opportunities to help them effectively incorporate new technologies in the 21st century.

www.centerdigitalgov.com

Sponsored by:

zscaler™

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile and secure. The Zscaler Zero Trust Exchange, a SASE-based platform, is the world's largest inline cloud security platform, protecting thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications over any network.

www.zscaler.com

ADOBESTOCK.COM