White Paper

Adopting a Whole of State Zero Trust Approach

Highlights from a July 2022 Roundtable

The Federal Government has M-22-09 guiding its transition to Zero Trust, but no broad-based decree exists at the state and local levels. Each state sets its own path to Zero Trust, some are further along than others. Despite the lack of Federal direction, state and local cybersecurity leaders are moving quickly to modernize their network architectures.

The Advanced Technology Academic Research Center (ATARC) hosted a roundtable in partnership with Zscaler to discuss how state and local government agencies can successfully plan, develop, and execute a Zero Trust strategy, while being restrained by comparatively fewer resources and staffing.

> One third of local governments are unable to tell if they are under attack, and more than half have IT policies and procedures that are not in line with industry best practices.
>
> *Source: University of Maryland, Baltimore*

Panelists included Chief Information Security Officers (CISOs) and experts from state and local governments, who shared many problems and experiences similar to those at our past Federal-centric Zero Trust roundtables. But all panelists agreed that it is just as crucial for state and local entities to ensure their networks are prepared for today's threat landscape.

Same Problems, Fewer Resources

Panelists shared similar stories on their reasons for transitioning to Zero Trust. Like the federal government, state and local institutions also saw massive increase in remote work (WFH) due to the pandemic. They also noted an increase in attacks on non-federal government agencies and organizations, with states having tens if not hundreds of thousands of endpoints to secure. Notably – this is just as many if not more than some federal agencies.

Panelists acknowledged the hesitation in starting on a Zero Trust transition is partly due to the amount of work involved. State and local governments work with far smaller IT budgets, and in some locales, the role of a CISO is filled only part-time, if one exists at all. In some of the smallest municipalities, there may be only a handful of employees regularly accessing network resources.

Panelists agreed, however, that this is not a reason to delay a move to Zero Trust. They noted making use of software that is intended to help make a piecemeal approach simpler and cost-effective. Panelists also emphasized the importance of knowing where you stand: taking an inventory of hardware and software before searching for a Zero Trust solution makes the process much easier and less stressful.

A Larger Attack Surface

The rapid transition to WFH because of COVID lockdowns opened new avenues for cybercriminals to exploit. IT departments often spun up quick solutions to keep agencies running remotely, which created security issues that a planned deployment would not have caused.

Virtual Private Network (VPN) was the most commonly used method among the panelists in attendance, even though it is not as secure as most people think. In some cases, the increase in VPN usage caused IT departments to reprioritize other efforts to ensure eliminating any security vulnerabilities that could put their networks at risk.

However, some panelists said that they had already begun efforts to secure their VPN connections, often focusing on things like Multi-Factor Authentication (MFA) to provide additional security.

Reduce the Threat and the Strain on Your Network

- Check your VPN settings. If VPN traffic overwhelms your network, sometimes outdated or incorrect settings can increase bandwidth needs
- Use cloud-based Zero Trust solutions. This helps eliminate your external attack surface. The more you can push into the cloud securely, the less anyone needs to access your internal network
- Move from a responsive to a proactive model of security. Responding to events after they happen is unnecessary with zero trust. Since every connection is a potential threat, it is challenging for attackers to get past your defenses.

Making Zero Trust a Reality

Panelists had various suggestions on how to best manage Zero Trust transitions at the state and local levels. As clearly established, resources are far more limited for these agencies. Therefore, it is crucial to understand what is needed to make the transition smooth and trouble-free.

Returning to the concept of an inventory, the first step is to catalog any connected apps, services, and devices that access internal network resources. Secondly, this inventory should be divided into three groups: those that can readily be migrated to Zero Trust architecture, those that first require upgrades, and those that cannot migrate. Prioritize transitioning the groups of endpoints from easiest to hardest.

Devices unable to migrate to Zero Trust can be replaced during the transition, especially if they are close to their planned End-of-Life (EOL). It is vital to ensure everything at this stage aligns, before adding any new (Zero Trust-ready) systems.

Flexibility is key to a Zero Trust transition, panelists urged. While apps have made transitioning to Zero Trust easier, the transition is rarely perfect. Expect issues, they added.

Getting Stakeholder Buy-in

The consensus among panelists was that getting buy-in from stakeholders was not difficult, as states and localities are experiencing the same cybersecurity challenges as the federal government. However, all stressed that finding solutions to well-defined problems is a far better approach than introducing a multitude of solutions in search of a problem they could fix.

Panelists recommended demonstrating Zero Trust benefits through the somewhat easier success of tackling "low-hanging fruit" first. This would encourage stakeholders to continue with what will be a challenging transition for all involved.

Getting User Buy-in

Panelists warned that no Zero Trust transition can be meaningful without user buy-in and clear understanding of their role in keeping the organization secure. Panelists also cautioned against punitive measures over poor security practices and urged attendees to make it a collaborative effort.

Education is a crucial part. One panelist shared internal research in their organization that showed a near-perfect correlation (.9) between training and the reduced likelihood of being fooled by phishing e-mails and scams.

Other panelists recommended integrating Zero Trust into pre-existing processes in a seamless manner. If it doesn't interfere with their jobs, that is the solution to choose. Perhaps the easiest is to eliminate passwords and use other seamless forms of end user authentication. One panelist put it simply: wrap the protections around natural human behavior if you can.

Changing Mindsets

Zero Trust requires organizations to completely rethink network security. Panelists underlined that this effort is a journey, not a sprint, and will take some time and effort to complete, especially considering state and local entities' limited resources.

But with attractive modern security solutions that provide a more comprehensive approach to security by connecting the right user to the right application based on the organization's policies, state and local agencies can stay a step ahead of attackers and keep our constituents' data protected.

Getting Buy-In

- Focus on quick wins first: Instead of focusing on broad zero trust concepts, look for ways to use these principles on smaller projects. Passwordless authentication, risk-based access, and real-time monitoring, all critical parts of zero trust, are good places to start.
- Know your environment: A smooth transition helps get buy-in from all sides. Knowing what can and cannot be migrated allows you to minimize any downtime or help desk support calls.
- Make it compelling: User experience is everything. The easier your zero trust solution is to deploy, manage and use, the faster adoption will occur. Many zero trust solutions are available that speed up and secure the authentication process, much better than the password/MFA combination most commonly used today.

Current multi-factor authentication is not enough. One-time passwords and magic links are still hackable if the attacker has access (which is why phishing attacks are so common against enterprise targets). Instead, cryptographic credentials and hardware-based security keys should be preferred. The technology is there to do this today.

One thing is certain: an organization cannot simply educate away potential security risks. A security strategy based solely on reprimanding users for careless clicks or insisting on unique passwords, is bound to fail.

Adopting a Zero Trust strategy assumes no connection is secure from the beginning. Therefore, natural human behavior is not a security risk in a Zero Trust environment.

Where To Find Help

Read about **Zscaler** state and local focused Zero Trust solutions here.

Contact ATARC today to learn more and get involved in ATARC's Cybersecurity Working Group, or attend our many security-themed events.