Invicti

Implementing Zero Trust

for State and Local Government Agencies

State and local governments provide essential services, maintain critical infrastructure, and store highly sensitive personal information, making them attractive targets for cyber attackers who want to steal data or extort money. Unfortunately, agencies do not always have the resources to prevent determined attackers from breaching their web application environments. In a recent survey sponsored by Invicti and Meritalk, government cybersecurity leaders cited budget constraints as the No. 1 barrier to modernization of their cybersecurity practices.

Limited resources can have unfortunate consequences. Many government agencies are not aware of their entire attack surface and conduct penetration testing only one or two times a year. Agencies may also primarily focus on protecting mission-critical systems and data, but a single outdated form or forgotten web application can be a backdoor into the network. Continuous testing and validation both help agencies better understand the full scope of their attack surface and identify vulnerabilities.

Recognizing the threat of inadequate government cybersecurity, the Biden administration issued Executive Order (EO) 14028, Improving the Nation's Cybersecurity, which requires federal agencies to implement zero trust architecture, a security framework that requires everyone and everything to be continuously validated in order to access applications and data. In other words, agencies must trust nothing and test everything.

Zero trust is a framework for digital transformation that addresses many challenges facing state and local governments, including implementing hybrid cloud environments, reducing ransomware risks, and securing remote workers. Although the EO addresses federal agencies, zero trust tools and policies developed for federal agencies can also help state and local agencies map out needed security improvements.

Many CISOs at the county and state level have discussed how recent federal directives can be a catalyst for improvements in their own home states.

Virginia CISO Michael Watson noted the imperative to fix "the underlying problem of some sort of actual dedicated budget to cybersecurity at our local levels" but said that the focus on zero trust will help "get us in a really great spot in the future."

> ***"Whenever the federal government does something, we obviously want to pay attention and we want to be in lockstep... It's additional fodder for me to go back to my management and say this is something we need to pursue."***
>
> ***Lester Godsey, CISO of Maricopa County, Ariz.***

As states and localities prepare for that future, examining the new zero trust framework and how it applies to their networks is critical, particularly as state and local agencies that interface with the federal government will need to operate a zero trust environment.

The five pillars of the Zero Trust Maturity Model

The Cybersecurity and Infrastructure Security Agency's (CISA) Zero Trust Maturity Model provides a good starting point for state and local agencies that are implementing zero trust. Defining architecture in terms of traditional, advanced, and optimal levels, CISA's model meets all agencies where they are and advocates an incremental approach that allows agencies to use existing technology.

Although implementing optimal zero trust may take a while, agencies can realize significant benefits by taking steps toward improving security under each of the model's five pillars:

1. **Identity:** Password management and multifactor authentication establish trust and protect against unauthorized access, including account takeover attempts.

2. **Devices:** Every device – whether agency-owned or bring-your-own – is identified and secured so that agencies can protect, detect, and respond to incidents on those devices.

3. **Networks:** Agencies move away from a perimeter protection mindset to a more holistic one; they transition to isolated environments and encrypt all DNS requests and vHTTP traffic.

4. **Applications and Workloads:** All applications are treated as internet-facing and continuously subjected to rigorous testing throughout development and deployment.

5. **Data:** Protections are deployed that use thorough data categorization and take advantage of cloud security services to monitor access to sensitive data and implement enterprise-wide logging and information sharing.

Zero trust resources

Office of Management and Budget M-22-09:
This memorandum sets forth a federal zero trust architecture strategy to reinforce defenses against increasingly sophisticated threats.

National Institute of Standards and Technology Special Publication 800-207:
This document defines zero trust architecture and outlines general deployment models and use cases where zero trust could improve an enterprise's overall security posture.

Zero Trust Maturity Model:
This model helps agencies develop their zero trust implementation plans and explains how CISA services can support zero trust solutions across agencies.

Invicti

Implementing zero trust

Zero trust can help state and local agencies shift from a perimeter-based security model to a more data-centric approach that incorporates fine-grained security controls and provides visibility among users, systems, data, and assets that change over time.

Below are some steps to get started on a zero trust journey:

1. **Map the full attack surface:** Agencies need to know what is in their system, who needs to access it, and where vulnerabilities may exist. Large organizations must build a central inventory of all websites and applications for a holistic view.

2. **Test and maintain cybersecurity incident response plans:** Cybersecurity strategies need top-down adoption of policies and tools, active staff engagement, and regular testing. An effective incident response and recovery plan ensures cyber resiliency across a variety of anticipated incidents.

3. **Add security to every role:** Most cybersecurity incidents are related to malware and ransomware that activate when a user clicks on a phishing link. Cybersecurity awareness and education must be part of an agency's culture for every employee.

4. **Integrate security testing into development and operations:** Every agency becomes a software company once it develops and maintains its own websites and applications. Organizations should adopt a DevSecOps approach that integrates and automates security testing in the application development process.

5. **Accelerate with outside expertise:** Security professionals are often stretched thin; agencies should seek out market-leading products and vendors, looking for security solutions and providers that meet specific needs (instead of generic features with add-ons) and display a long track record with proven results.

Agencies face challenges with zero trust implementation such as outdated, legacy infrastructure, siloed systems, and vendor-specific cybersecurity solutions. Fully adopting a zero trust mindset requires a change in every agency's cybersecurity culture that will take commitment and focused effort at all levels – and solid partnerships to implement proven security solutions across the enterprise.

The case for application security

Zero trust is especially important for web applications, as they are typically the most exposed parts of information systems and may provide an entry point for data breaches and internal network infiltration. As state and local organizations operate a multitude of web-based digital services, they are particularly impacted by web app vulnerabilities.

Overcoming these challenges requires integrating threat protections into application workflows. With security embedded into the very architecture of applications, it is easier to make testing a core aspect of the development and deployment process – including regular automated scans for applications in production. This approach also includes continuous and dynamic application health and security monitoring, along with granular testing policies and reporting.

Invicti's dynamic application security testing (DAST) helps developers and security professionals find and fix runtime web application vulnerabilities. In fact, 80% of respondents in our survey said an automated, iterative approach like DAST would allow their agency to secure the majority of their software development lifecycle, with many who've started already seeing "significant security improvement."

In Invicti's recent study alongside MeriTalk, **86%** of government respondents said they'd experienced a breach originating in a web application in the past year. Some **62%** saw delays in project deployment due to application security concerns, **45%** had experienced data loss, and **51%** had experienced downtime due to a web application vulnerability.

Adding interactive application security testing (IAST) into the core DAST scan can also provide deeper insights into issues and helps identify and test local assets that crawlers cannot see, while dynamic software composition analysis lets agencies efficiently vet open-source components before deploying new apps.

By using a single-platform solution for all these critical scans, agencies can identify and fix more vulnerabilities than with DAST alone to gain the confidence that every application has been fully mapped out and tested.

Invicti

Schedule a demo and discuss how Invicti Security can help customize application security to your unique mission. Hundreds of government agencies already have – and they chose Invicti Security.