WHITE PAPER

Zero Trust at Work

A New Baseline for Modern AppSec in Government Agencies

Invicti

Executive summary

Cyber threats remain constant, but the response has changed. Federal organizations have a model to follow for modern cybersecurity needs and guidance to act upon: Zero Trust Architecture.

This white paper will explain the importance of a zero-trust mindset with an emphasis on understanding your full attack surface, including the numerous web applications that exist and are being developed for increasingly digital operations. We'll cover secure government standards and access control guidance critical to zero trust. In addition, we'll outline five near-term tactics that can energize your cybersecurity efforts and accelerate the progress of any organization at any stage of zero-trust implementation.

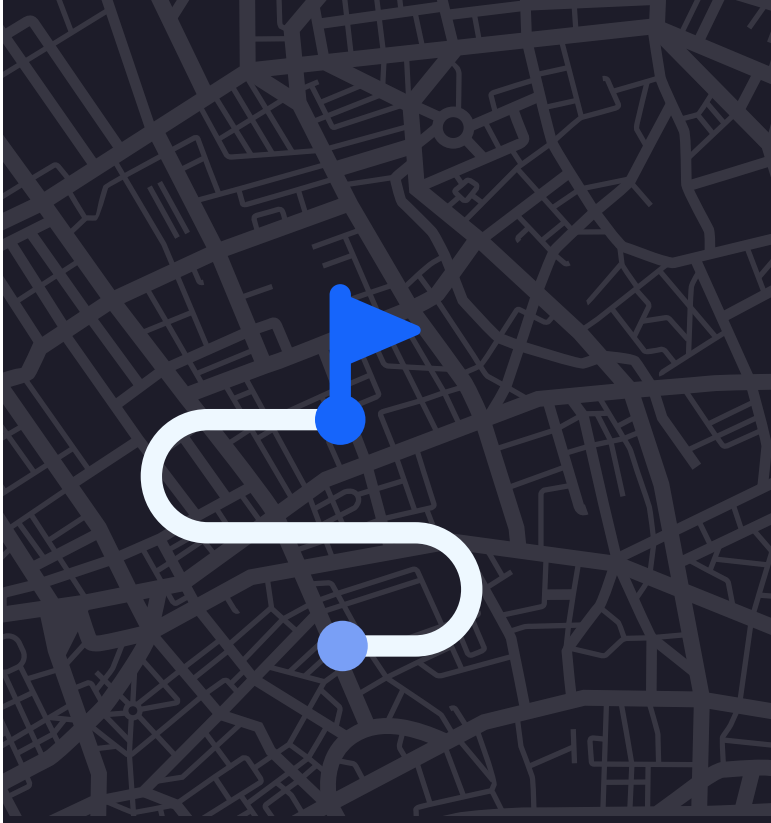
A new strategy for federal cybersecurity

The news is the same, but the response has changed. Daily, we are told of increasingly sophisticated cyberattacks against federal agencies, highlighting the urgent need to enhance federal cybersecurity. But what exactly is the right response? And how can agencies protect themselves in increasingly modernized IT environments while continuously maturing security protocols to keep pace with evolving threats? Security must be ingrained into every phase of the software development process with best practices and modern, automated tooling at practitioners' fingertips.

The wheels are already in motion.
Last year, President Biden issued Executive Order (EO) 14028, Improving the Nation's Cybersecurity, initiating a sweeping government-wide effort to ensure that baseline security practices are in place and the Federal Government is migrating to a zero-trust architecture.

> ***"Incremental improvements will not give us the security we need; instead, the Federal Government needs to make bold changes and significant investments in order to defend the vital institutions that underpin the American way of life."***
>
> *EO-14028*

These sweeping changes are long overdue, so federal agencies can't tread water. To provide guidance, the Cybersecurity & Infrastructure Security Agency (CISA) published the Zero Trust Maturity Model. Now, the race is on as agencies implement Zero Trust Architecture (ZTA) to bring their security up to speed and, when fully implemented, surpass the commercial cybersecurity standards. CISA's Zero Trust Maturity Model and other guidance for federal agencies outline a starting point strategy as well as long-term security architecture migration plans with a crawl-walk-run approach. Let's review the zero-trust mindset agencies will need to navigate the future.



Is zero trust the right roadmap for your agency?

ZTA requires all users to be authenticated, authorized, and continuously validated before being given access to applications and data. However, zero trust is also a framework for digital transformation that addresses many of the challenges facing federal agencies, from securing remote workers to implementing hybrid cloud environments and reducing ransomware risks.

A zero-trust mindset is ideal for driving the kind and scope of security changes that are so urgently needed in many federal agencies. Because CISA's Zero Trust Maturity Model defines the architecture and processes in terms of traditional, advanced, and optimal levels, it meets all agencies where they are now and advocates an achievable, incremental approach.

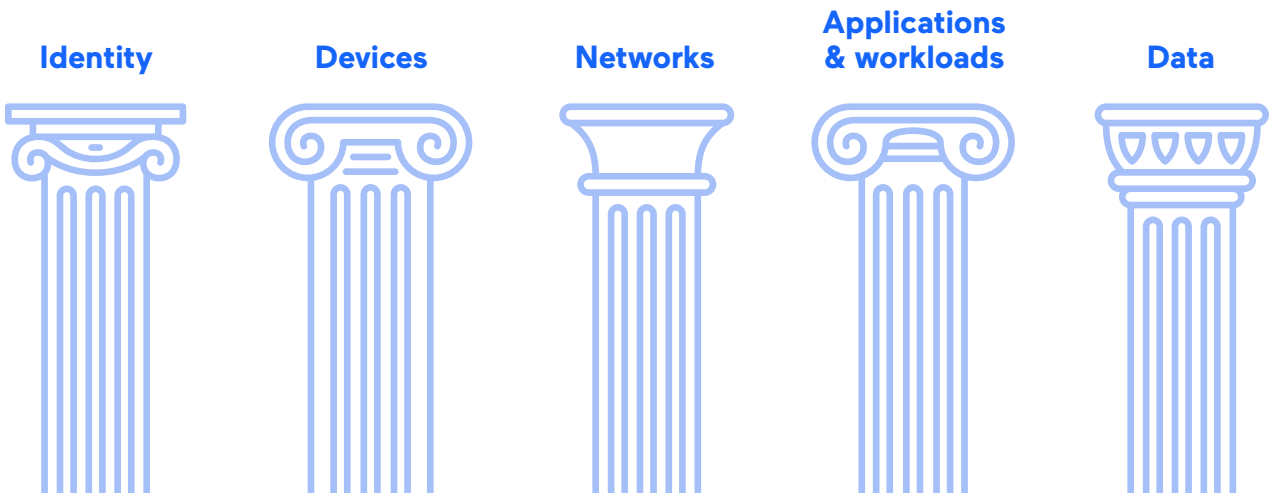
The five pillars of the zero trust maturity model

Federal organizations can be vastly different, with diverse missions and their own unique internal structures and culture. Trying to set standards or policies that adequately cover all federal organizations is tricky. However, the government has succeeded by focusing on ZTA.

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-207 provides the following operative definition of zero trust and ZTA:

> Zero trust provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised.
>
> ZTA is an enterprise's cybersecurity plan that uses zero trust concepts and encompasses component relationships, workflow planning, and access policies.
>
> Therefore, a zero-trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a ZTA plan.

It's important to note:
Zero trust aims to prevent unauthorized access to data and services within all computer systems, networks, and applications. This 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. At the same time, zero trust aims to make access control enforcement as granular as possible.



Invicti

The Zero Trust Maturity Model identifies five pillars, or areas, where advancements can be made. We've added commentary to describe the zero-trust vision for each:

1. **Identity:** Your staff use enterprise-managed identities to access the applications they use for work. Password management and multi-factor authentication establish trust and protect against unauthorized access, including account takeover attempts.

2. **Devices:** Identify and secure every device, whether agency-owned or BYOD (bring-your-own-device), to protect, detect, and respond to incidents on those devices.

3. **Networks:** As your agency moves away from a perimeter-protection mindset to a more holistic one, you'll transition to isolated environments and encrypt all DNS requests and HTTP traffic within an environment.

4. **Applications and Workloads:** Web applications are critical gateways for consumers and internal workers alike, but they're also where malicious threats try to sneak in. The end goal is for your agency to treat all applications as Internet-facing and continuously subject applications to rigorous testing throughout development and deployment while welcoming external vulnerability reports.

5. **Data:** Your agency will deploy protections that use thorough data categorization. You'll take advantage of cloud security services to monitor access to your sensitive data and implement enterprise-wide logging and information sharing.

Although government agencies are beginning this journey now, the U.S. Office of Management and Budget (OMB) has given them until the end of 2024 to implement specific ZTA security standards. Agencies just starting their journey can maintain a slow-and-steady approach to achieve their security goals and will start seeing the benefits of zero trust sooner.

Zero trust can help with the shift from a location-centric model to a more data-centric approach for fine-grained security controls between users, systems, data, and assets that change over time – all while gaining critical visibility. In turn, fully adopting a zero-trust mindset will require a change in every agency's culture around cybersecurity that will take commitment and focused effort at all levels.

Links to federal resources for zero trust

National Institute of Standards and Technology Special Publication 800-207

Department of Defense Zero Trust Reference Architecture

National Security Agency Embracing Zero Trust Security Model

Federal Zero Trust Resource Hub

A deeper dive into application workloads

The federal government faces a number of challenges in transitioning to ZTA, most obviously that legacy systems rely on implicit trust. This conflicts with the concept of adaptive trust that is core to ZTA. As more data and processes move to the cloud, securing and testing everything – including a growing number of web-enabled applications – is paramount. Traditional or legacy approaches that focus on the network layer are no longer sufficient to address cyberthreats.

The Zero Trust Maturity Model's fourth pillar specifically outlines traditional, advanced, and optimal approaches to functions such as threat protection, application security, and governance capability.

The traditional approach is where many agencies are now. Your threat protection and application security may not be fully integrated into application development workflows, which can lead to disjointed security efforts. In this approach, application security testing is done prior to deployment, primarily through static and manual testing methods. It can not only cause hiccups or delays in deployment but also leaves unseen holes in your security coverage.

In an optimal approach, your agency has deeply integrated threat protections into application workflows. With security embedded as part of the very architecture of your applications, it's 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.

The key components for ZTA web application security are:

Automation **Coverage** **Accuracy**

DAST + IAST + SCA

At Invicti, dynamic application security testing (DAST) helps developers and security professionals find and fix runtime web application vulnerabilities. Adding interactive application security testing (IAST) capabilities to the core DAST scan provides deeper insights into issues and helps identify and test local assets that crawlers can't see.

With an IAST sensor deployed locally, the DAST scanner has access to the full website structure, including unlinked and hidden files, so it can crawl and test all pages, not just the ones that are currently accessible to crawlers. And having dynamic software composition analysis (SCA) in the mix means you can vet your open-source components more efficiently before deploying new apps.

Using a single-platform solution that takes care of these critical scans, your agency can identify and fix more vulnerabilities than with DAST alone to gain the confidence that every application has been fully mapped out and tested.

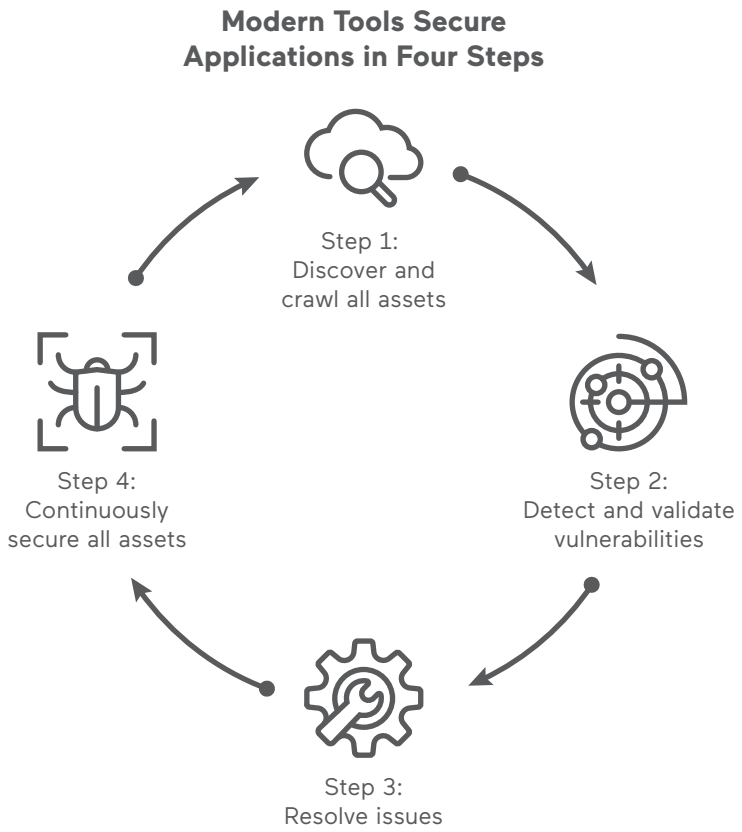
VIP: the very important place for web application security

Zero trust isn't just about cybersecurity; it's also about digital transformation. The entire ZTA initiative will usher in a new era of operations for many agencies, including big changes in how agencies create and maintain applications. The push for the optimal approach to securing application workloads is a clear call for the level of orchestration, automation, and governance that only modern web application security testing solutions can provide.

Using modern security tools to create optimal zero-trust workflows allow you to integrate security into development (i.e., shift left) by building reliable security scans directly into the software development lifecycle (SDLC) and scanning as early as possible. This approach will minimize risks and eliminate delays for new features and releases.

> ***"Continuous integration and continuous deployment models that integrate security testing and verification into each step of the process can help provide assurances about deployed applications."***
>
> *CISA Zero Trust Maturity Model*

Your agency doesn't have to stop there. The same tools and methodologies can be applied to the entire application life cycle to keep an eye on production and deployed assets (on the "right") by continually monitoring and mitigating vulnerabilities.



At face value, web application security is just the tip of the iceberg in ZTA guidance. Still, it has a disproportionate impact on your agency's ability to deliver compliant applications at scale. With more than 1.9B web apps in use today, serious vulnerabilities put government agencies at risk. As agencies move to a cloud-first environment where data and functionality are accessible from anywhere in the world, they must focus on this zero-trust pillar and implement modern security solutions to provide visibility into every website and application. There is simply no such thing as an unimportant application; without the right security measures in place, any app is an open door to danger.

A more secure government by design

The zero-trust approach conceptualizes a secure government that has:

- Enterprise-managed accounts for federal staff that provide access to everything needed to complete tasks while also staying secure
- Devices that are tracked and monitored constantly while also taking into consideration how secure they are before granting access to internal resources
- Isolated agency systems with encryption for all network traffic moving between those systems
- Internal and external testing for enterprise applications that are securely accessible to staff via the internet
- Federal security teams and data teams working together to develop data categories and security rules that automatically detect – and ultimately block – unauthorized access to sensitive information
- Collaboration between federal data teams and security teams to build data categories and rules to detect and block unauthorized access

Following zero-trust guidelines where no asset is considered 100 percent trusted, these efforts fold nicely into cybersecurity strategies that aim to encrypt and authenticate all traffic. However, to stay ahead of threats, secure data flows will need to be one part of a more extensive application security program. The program needs to cover all bases, from tooling to processes, enablement, third-party component checks, and even vulnerability disclosure. We'll get there one step (or one "pillar") at a time.

A more secure government can't be built in a day. Even so, your agency can help move the needle for the federal sector as you better manage workloads, increase the efficiency of individuals and teams, streamline operational processes, and lower costs and risks – all as side benefits of a more robust modern approach to security.

The timing of your zero-trust response is imperative. The SolarWinds case reminds us that supply chain security is vital. The war on Ukraine underscores how cyberattacks can be used to disrupt government operations. And the Log4Shell incident highlights how important an effective, rapid incident response can be. Identifying your path to an improved security posture isn't just about protection today — it has the potential to impact agencies for decades to come.

73%
of federal cybersecurity decision-makers say their agencies are aggressively adopting zero-trust security principles

9/10
believe that federal policy directives for zero trust adoption are useful for the shift

Source: MeriTalk and Merlin Cyber

Strategy meets tactics

Using zero trust as an evolution strategy, we've developed near-term tactical recommendations that your agency can use to energize its transformation efforts and accelerate zero-trust progress, no matter what stage you're at now.

Tactic 1: Map your full attack surface

Cybercrime has become an everyday companion to government agencies, and cybersecurity risk should be a major consideration for operational resilience. With more of your data and infrastructure residing in the cloud and incorporating open-source components, the crucial first step is knowing what you have in your arsenal, who needs to access it, and where vulnerabilities may exist.

- Because it is so easy to spin up new applications and add web-accessible resources, accounts, services, and all kinds of devices (including notoriously insecure IoT systems), it's important to map out your entire online presence to understand your attack surface. This is where an SBOM, or a software bill of materials, can come in handy, as it helps you outline everything that went into building a particular piece of software. Should a single component need updating down the road, your developers and security professionals have easy access to the information and know exactly what to check.
- Large organizations need to build a central inventory of all websites and applications for a holistic view as well. One way to get started is with a web asset discovery service such as Invicti's built-in discovery capabilities. Maintaining an asset inventory helps quickly find web-facing applications and web technologies associated with your agency and provides a starting point for assessing vulnerabilities.
- With so many data breaches caused by cloud storage misconfigurations, keeping track of data online and enforcing cloud security policies is critical to maintaining data privacy and protecting your intellectual property.

Tactic 2: Test and maintain your cybersecurity incident response plans

Even the most complete cybersecurity strategy is still just a document without top-down adoption of policies and tools, active engagement from your workers, and continuous refinement to keep up with emerging threats.

- To turn policy into action, you also need an effective incident response and recovery plan to ensure cyber resiliency across a variety of anticipated incidents.
- Again, good plans require action and refinement, so procedures must be regularly tested and updated. When (not if) your agency is attacked, everyone knows exactly what to do and whom to contact to get the ball rolling on remediation.
- Preparation often includes running simulated incidents to assess the effectiveness of response and recovery processes and identify any gaps.

Each critical cybersecurity risk identified during mapping should have a response and recovery plan. Of note, the risk of data loss should be addressed by a suitable data backup policy and testing of data restoration to the required level and in the required time.

Tactic 3: Add security to every role

We tend to think of cybercriminals as highly advanced and sophisticated evil hackers. While these certainly do exist and operate (as evidenced by the SolarWinds hack), the everyday truth of cybersecurity is far more mundane. The majority of cybersecurity incidents are related to malware and ransomware infections and are often initiated by someone clicking a phishing link.

This is your defender dilemma: no matter how robust your cybersecurity strategy is on the surface, the bad guys only need one gap in your defenses to get through. In these days of mission-critical web applications, remote work, and single sign-ons, one person's inattention could be enough to compromise your entire agency.

- Cybersecurity awareness and education must be an everyday part of your agency's culture for every employee and contractor.

Tactic 4: Integrate security testing into development and operations

Whether obvious or not, every agency becomes a software company once it develops and maintains its own websites and applications. And if your agency is in the business of software, security cannot be an afterthought – you simply can't afford backlogs that leave applications vulnerable to attack.

- The only systematic solution is to integrate security testing into the application development process itself and automate as much as possible, adopting an integrated DevSecOps approach.
- A modern dynamic application security testing (DAST) + interactive application security testing (IAST) solution like Invicti can deliver accurate scan results and help your agency secure thousands of websites and apps with a small security team.
- Effective tools should also have an option for securing open-source components, such as an SCA solution that plugs right into existing workflows.

Tactic 5: Accelerate with outside expertise

Though nearly all agencies have some internal cybersecurity expertise, federal security professionals are often stretched thin.

- To achieve zero-trust milestones efficiently, seek out renowned products and market-leading vendors from the commercial sector. You'll be choosing not only a security solution but also a partner with expertise and perspective who can help with smooth implementation, integration, and even customization.
- Look for security solutions and providers that:

    1. Meet your specific needs instead of offering generic features with add-ons.
    2. Display a long-term track record (10+ years) with proven results of identifying common vulnerabilities and offering remediation guidance.
    3. Prove a release history of the product (a new release at least every 3 months to keep up with new threats).
    4. Continue to show corporate growth in sources such as Gartner reports, Peer Insights, and G2 Crowd, which provide insights into genuine customer satisfaction.

Zero trust: your cybersecurity agenda

Federal organizations finally have a holistic approach to cybersecurity that covers more of the critical bases. Cyber threats remain a constant, but federal organizations now have a plan for a bold response using the zero-trust mindset. Though implementing optimal zero-trust methods may take a while, agencies can already realize significant benefits from taking incremental steps toward each of the five pillars of the Zero Trust Maturity Model and attaining greater integration of security across operations.

Zero trust is a clear, achievable plan for agencies, but making it a reality will take commitment and focused effort on all levels, not to mention solid partnerships to implement proven security solutions. There's no room for delays or misdirection with growing pressure to be efficient, mounting workforce challenges, and looming cyber threats.

Zero trust has set a new baseline and a new agenda for your agency.

Invicti

About Invicti Security

Invicti Security is a leading provider of DAST, IAST, and SCA web application security solutions for government environments. Through our platform, we provide solutions designed to close web application security gaps. Invicti products automate application vulnerability identification, confirmation, and management to keep public information and critical infrastructure secure.

Call to schedule a demo and discuss how we can help customize our application security to your unique mission. Hundreds of federal agencies and branches already have — and they chose Invicti Security.

Our federal users call it like they see it:

> **Critical.**
> **Massive time saver.**
> **Security feedback earlier in our development cycle.**
> **DevSecOps success.**
> **Global visibility for our CISO.**

The best statistic of our consistent delivery and reliability is our renewal rate – over 90% in 2021!

fedgov@invicti.com

invicti.com/fedgov/

220 Industrial Blvd #102, Austin, TX 78745

facebook.com/invicti-security

linkedin.com/company/invicti-security

twitter.com/invicti-security