Security by Design

Meet your mission by transforming your approach to web application security

Invicti
Executive summary

Public sector organizations find themselves at an interesting point in their journey to modernize. Security mandates forecast the future while commercial lessons learned provide avenues to get there. For those grappling with the obvious challenges to change daily, there’s hope. With the right insights, you can modernize and meet compliance milestones comfortably and authentically for your leadership, your people, and your mission.

We’ll look at why architecting your applications with security in mind is important for full coverage, and explore the security features that help optimize workflows, drive efficiency, help with employee retention, and save budget dollars.
Looking for direction? Follow the leader.

We’re in a new era in government IT that’s moving toward modernization and security. The opportunities are endless and exciting, but the reality is less clear.

Read the headlines and you’ll believe that a radical approach is necessary. Buzz words abound. Talent is scarce. Budgets are limited. Legacy processes strain to deliver immediate needs. Bad actors add to the pressure looking for any weakness.

We’re not convinced. Incremental efforts help organizations drive security while transforming at their own pace. As your agency looks at ways to check the box for security, speed, and agility while also addressing needs in development, look to industry best practices and use cases to guide you without scrapping the foundation you have.

Consider the truths that have already emerged from the DevSecOps movement — and what they could mean for the public sector.

- **Developers are busier than ever; automation is the answer**
  We’re looking at a massive shortage of IT talent across all sectors. Technology took off but the workforce hasn’t shifted to meet the need. This puts pressure on the team you do have. Their time is precious. Tools that lighten the burden by fully automating a tedious step or process are welcome additions to development and security testing.

- **Speed AND success are possible**
  Commercial teams have learned that faster deployments don’t necessarily mean DevSecOps success. If you’re building DevSecOps capabilities in your agency, the right tools will help with faster remediation and better prioritization so security within the cycle doesn’t slow the process. And those same tools can help accelerate development to a comfortable cadence with a security-first mindset from leadership that breaks down the silos between developers and security. Once a strong, repeatable process is established, speed will come.

- **Secure the entire attack surface**
  You can’t secure what you don’t know you have. Organizations are challenged by the expanding number of web applications they have in use, including long-forgotten landing pages, online forms, and contact applications. Few have a comprehensive list or repository, making it important to select a security solution that can look for the “unknowns.”

- **“Set and forget” is convenient but dangerous**
  Commercial-off-the-shelf (COTS) solutions make life easier. However, without alerts and user-friendly dashboards, it’s too easy to set and forget, letting risks fall off the radar and developers’ to-do list. Solutions with at-a-glance status updates and connections to ticket-tracking systems get the job fully done.
Shift left and look right
Implementing security earlier in the development process is a better way to build. When developers incorporate security into the very architecture of their application at the start of a project, they have more opportunities to reduce risk and prevent dangerous vulnerabilities. And with modern security tools, legacy solutions, third-party apps, and apps in production are protected continuously instead of once per year through a pen test audit.

There are hundreds of use cases indicating that the best approach to modern security is one that features continuously automated scanning across all web application assets. Marketing pitches make it seem like what goes into the shift to DevSecOps is easy. The truth is that it requires a cultural change that can be challenging for government organizations founded on a specific mission and long-held values. We’re proposing adopting a different mindset — one that places the value on improving business functions and workflow enhancements within your agency for measurable efficiency and cost savings. Across the government, that shift is already starting to happen. Lean on best practices and lessons learned to help your agency modernize security.

The real deal on securing web applications
Web applications are the foundation of how we live our lives and do business. Nearly everything we interact with online is based on a web application — making web applications security-critical.

The stats tell a compelling story
As the number of applications used by both the public and private sectors has exploded, web applications have become a prime target for attackers. In the past two years, while we were focused on the pandemic and workforce adjustments, bad actors stole twice the number of records than they did in 2020. (Risk-Based Security, 2021).

Last year, the average cost of a data breach reached a 17-year high of $4.24 million. If cyberattacks and their consequences aren’t taking a break, how is your agency planning to stay resilient against threats without losing steam? And how will you modernize and move towards DevSecOps to keep pace with innovation?

Securing web applications and APIs is such an imperative that federal initiatives are making sure it happens this year. The latest guidance, including NIST 800.53 SA-11, OMB Memo M-12-30, OMB Memo M-22-09, and CISA’s Zero Trust Maturity Model, have become your marching orders, and even provide a roadmap. Let’s look at how you can comply and drive business benefits.

1. www.statista.com/chart/19058/number-of-websites-online
2. Edgescan’s 2021 Vulnerability Statistics Report
3. Verizon DBIR
4. Microsoft Survey
Is zero trust the right roadmap?

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

"The zero trust mindset is ideal for driving the kind and scope of security changes that are so urgently needed in many federal agencies."

CISA’s Zero Trust Maturity Model defines the architecture and processes in terms of traditional, advanced, and optimal levels, meeting agencies where they are now with a very doable incremental approach.

By now, you’ve already started the process by submitting plans to explain how you will automate and integrate security testing into your development pipeline. That’s foundational to DevSecOps. The results of faster identification of risks and faster remediation are a game-changer in the public sector. However, the impact on your agency goes further.

Zero trust requires deploying modern dynamic application security testing (DAST) + interactive application security testing (IAST) tools that can identify all web assets, quickly and accurately scan for issues, prioritize the issues based on risk, and enable automated workflows.

Let’s pick that apart to look at the measurable business impacts.
Modern security attributes, more efficiency gains

What’s the bottom line on modern security transformation? Federal and commercial sectors don’t seem to place the same value on agility, but they do share the need to reduce development costs and deliver applications faster. On the agency side, automation is a critical part of the equation, helping to reduce the burden on the federal workforce and hone processes for efficiency gains.

A quick review of the situation is illuminating. The traditional approach to application security testing can take time to discover vulnerability issues, including a high number of false positives that developers need to investigate. The results are so cumbersome that issues are often not resolved before deployment. This routinely requires applications to be re-developed or even pulled down for remediation, with add-on costs, frustration, and delays. That’s if they aren’t attacked on day one.

By contrast, the modern security approach enables agencies to scan automatically and continuously, across all web applications and services, for more secure applications at deployment and increased awareness of vulnerabilities across the attack surface.

Comprehensive scanning helps focus agency efforts on timely remediation — the whole point of having an application security program in the first place. Ideally, your automated security scans will be paired with an automated workflow. That way when a vulnerability is found, the workflow opens a trouble ticket and assigns it to the appropriate developer to fix, prioritized by the risk factor. Ideally, that ticket includes details about where the vulnerability is as well as how to fix it. Closing the ticket triggers another automated scan to confirm that the vulnerability is fixed.

Many agencies have development and security teams embedded in multiple areas or sub-agencies of the organization so automating security scans and remediation processes can help to unify efforts and manage workloads. This is significant as security challenges have grown faster than many federal teams. The seamless approach to assigning tickets for remediation helps individual team members get ahead of their to-do list, leaving time for more advanced transformational efforts like implementing more innovative features.
**Security by design**

The push to “shift left” by integrating security with software development has gotten lots of attention, and we think it’s warranted. It’s a significantly better and more secure way to develop applications by shortening the feedback loops within the development process. It’s also an opportunity for many agencies to reevaluate teams, structures, and processes to better address modern development needs — and their evolving mission.

While agencies aren’t mandated to adopt DevSecOps into their processes, there’s no downside to transitioning to the model. The change, however, requires a culture shift as well as process shifts – a challenge for any large organization but especially thorny for government organizations. For those on the front lines of app development, DevSecOps can be a sanity saver that increases speed and agility while deploying fundamentally more secure applications.

- When security moves left, baked into the very architecture of applications as they’re designed, teams are able to build more secure software from the start.
- Security and development teams become collaborators instead of wrestling with each other over timing.
- In agencies producing large numbers of apps, shifting left also reduces re-development, saving money and lowering risk, with fewer vulnerabilities making it into production.

![Diagram: Security + (Speed + Agility) = Increased Reliability + Lower Costs and Risks](image)

A large agency was spending thousands per month on outsourced manual testing. The results were delivered in a PDF that agency developers had to then investigate. The process took hours per test to process and resulted in few remediations. Many of the issues turned out to be false positives.

Deploying a web application security solution significantly shifted security testing for the agency. With scan results delivered right to their development team, with proof of the vulnerability, they could be much more efficient. They were also able to reduce the spend and reliance on outsourced test engineers. The shift gave agency leadership newfound confidence that critical security issues could be identified and fixed with internal resources.
Shift left but don’t forget the right
While it’s absolutely true that agencies need to shift security left and consider the risks while in architecture and design phases, you certainly can’t forget about securing the assets and components to the right. Dedicated DevSecOps tools place a heavy focus on scanning in the development stages, giving agencies a false sense of security if that’s all they focus on. With so many legacy and third-party apps, they require continuous scanning of both production and deployed assets to protect the entire attack surface.

A back of the envelope survey of federal agencies indicates:

- 20% of their web applications are in development
- 80% of web applications that are already deployed

See everything
In our experience, nearly all federal agencies underestimate the number of assets they have, and few have created a catalog with identified “owners” to lead remediation efforts. Modern AppSec solutions offer target discovery capabilities, which help your agency find all the websites and web applications that may have been overlooked until now.

Add IAST depth to DAST coverage
The fundamental job of a dynamic application security testing (DAST) tool is to help developers and security professionals find and fix web application vulnerabilities. Combining interactive application security testing (IAST) capabilities with DAST provides deeper insights into runtime 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. This means your agency can identify and fix more vulnerabilities than with DAST alone, for confidence that every application has been mapped and tested.
Fix issues before they become vulnerabilities

While exploring the application environment, the IAST sensor also identifies and analyzes local configuration files that are inaccessible to the DAST engine and flags insecure configurations that could lead to problems in the future — even if they aren’t causing a vulnerability today.

The left and right approach requires vision and a champion at the top to set the tone. It’s the leaders who help drive a culture that values security and facilitates the relationship between development and security teams by endorsing integrated application security testing tools.

In a recent head-to-head evaluation by a major federal agency, Invicti scored 94% vs. 72% and 76% from the contending on-premises and cloud platforms.

The independent evaluation scored on functionality, performance, reliability, support, and price.

A large federal agency used Invicti to scan production sites across each of its sub-agencies. The scope amounts to tens of thousands of sites yet the process is comfortably managed by just two people. "It’s a force multiplier."
Fix faster

Results are important. Flagging vulnerabilities only does half the job. Addressing them is the other, often tougher, half. Many web application security scanners are prone to false alarms. These false positives are a major problem for agencies as they make security testing slower, less accurate, and more frustrating. Since the goal of modernizing security is to reduce the burden, solutions that automate time-consuming tasks and assist teams in fixing vulnerabilities with accuracy offer far more value.

No matter how many vulnerabilities a scanner reports, your teams can’t start addressing them until they are sure they are real and exploitable issues. The performance benefits of using an automated scanner are greatly reduced when security professionals have to manually weed out false positives.

Confidence in scan results: Invicti offers Proof-Based Scanning to safely exploit vulnerabilities found by the scanner, in effect simulating the actions of a penetration tester. This feature automates the investigative process, enabling agencies to continuously scan all web assets without overwhelming the security team with manual validation tasks.

Pinpoint root causes: Information extracted during vulnerability testing can accelerate remediation — giving developers the details they need to fix the vulnerability faster and easier.

Proof-Based Scanning technology automatically confirms 94% of direct-impact vulnerabilities with a confirmation accuracy of 99.98%
Better together

IT infrastructure modernization was named among the top trends for 2022 by FedTech, “The digital shift comes amid an overall push to upgrade outdated IT infrastructure throughout government agencies. Experts predict that 2022 will see a major focus on these enhancements across the federal government.”

We view that shift as an opportunity: Anything that is changing — be it new software, new processes, or hybrid work environments — needs to have a wide-reaching, transformational impact.

We’re in a new era in government IT moving toward modernization and security. The synergies at work are three-fold.

1) Development and security
More than ever, agencies need all-hands-on-deck for cyber resilience. Security solutions that help organizations shift left, or begin to integrate development and security, are heading in the right direction. Aligned and collaborating, these two interests provide a foundation for better security by design. Astute leaders can build on that progress, leveraging it to break down long-established silos, centralize development resources, and automate processes.

2) Government and industry
The cyberspace battlefield is always evolving and it's more important than ever for the public and private sectors to work together to secure public information and critical infrastructure. Some agencies are partnering with the private sector, but all should be studying it to benefit from lessons learned and best-of-breed technologies that harden security postures.

3) Modernize and optimize
We’re helping to raise federal organizations’ expectations for robust web application security by highlighting the business benefits that can be gained through continuous and comprehensive, automated, and verifiable scanning and reporting. It’s not just security. It’s an incremental step towards modernization and optimization that helps agencies remain mission-ready in an evolving environment.
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.

Schedule a demo to 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!