Securing Digital Government and Citizen Trust

Why zero trust is vital to mission success

VERACODE

FedRAMP

VERACODE

Veracode is proud to announce that the General Services Administration (GSA) has granted us a Federal Risk and Authorization Management Program (FedRAMP) authorization. With FedRAMP authorization we can now support agencies across the federal government with a cloud-based application layer security platform. FedRAMP certification validates that we meet the government's rigorous security and risk assessment standards — and broadens opportunities for government agencies to find and adopt cloud services that are compliant.

Most of the findings in this eBook and quotations cited are sourced from the 'Build Trust Summit' which was produced on April 21, 2022, by the Government Executive Media Group and co-sponsored by Veracode, AWS, and Optiv. Additional findings from Veracode's State of Software Security report are included within the document and cited as they appear. If you would like to view an on-demand version of the event, click here.

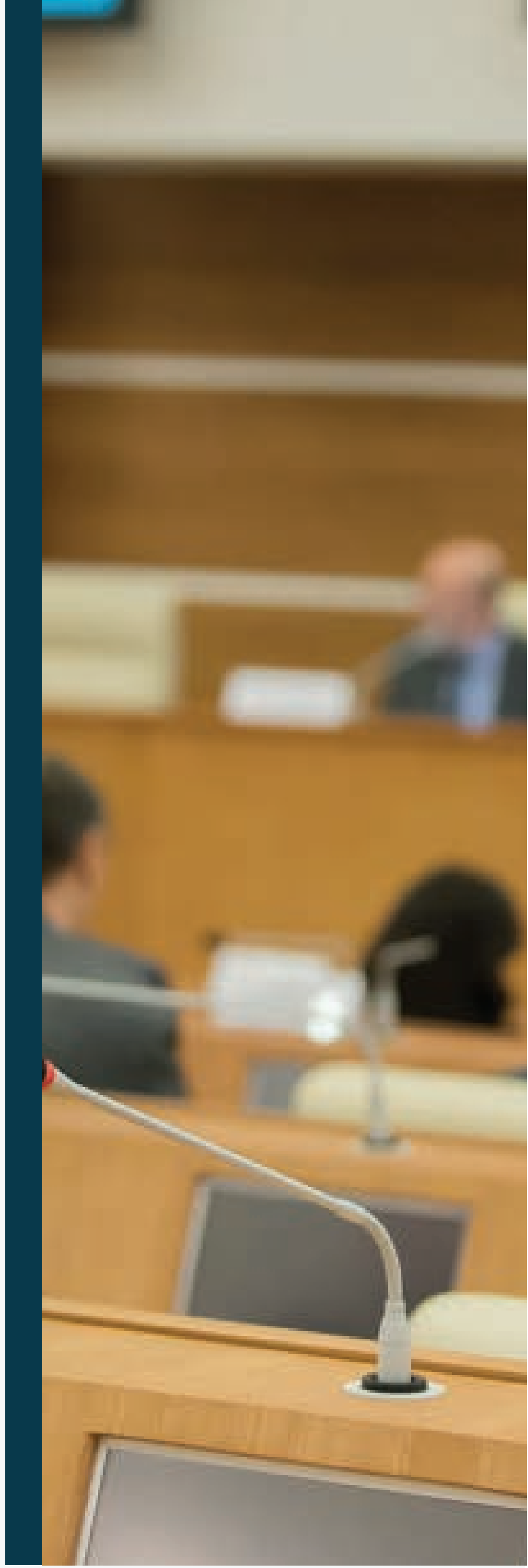


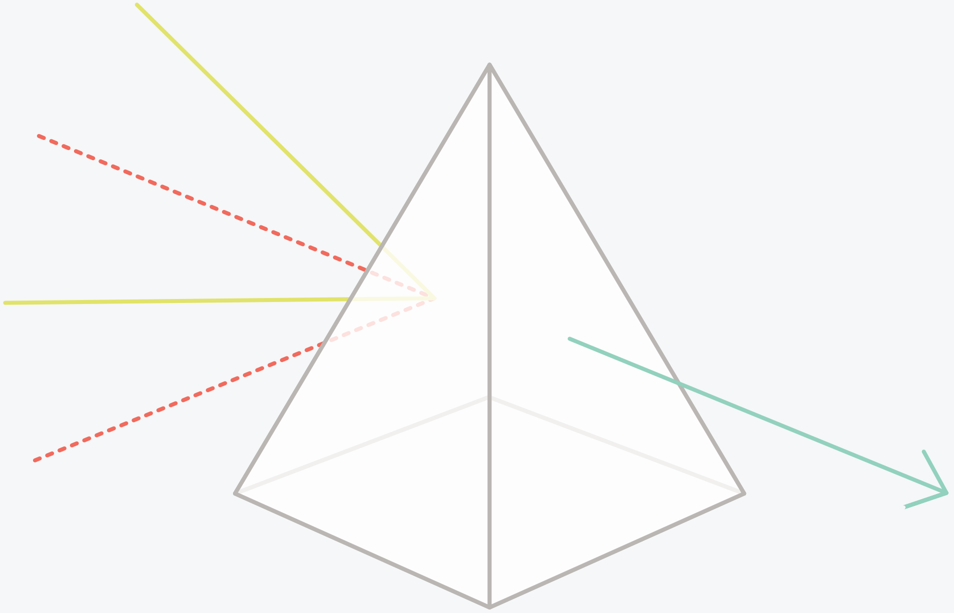
Table of Contents

The growth of digital government, in line with that of the private sector, has advanced since the onset of the COVID-19 pandemic. Remote operations meant organizations had to accelerate their digital transformation efforts in order to remain viable in the market. Digital operations meant customers expected faster frictionless software experiences. For public sector agencies, it's been an ongoing challenge. They have to balance speed to market, IT security, and federal policy in order to rival high-performing private-sector companies. Their success could determine confidence in digital government for years to come.

To start on this mission, government agencies at both federal and state/local levels have been reimagining IT security and turning to zero trust security strategies. Zero trust security strategies enable organizations to continuously validate users before granting them access to data or applications.

> Zero trust is a security model that assumes all network activity is a security threat. As such, it allows organizations to restrict access controls to networks, applications, and environments.

By leveraging a zero trust model, government agencies can further secure the software supply chain, shortening software development and deployment cycles and improving customer experiences.



The software supply chain refers to all components directly involved in developing an application. The components, such as open-source scripts and packaged software, may or may not be developed or manufactured in-house.

Secure software is no longer a recommendation, it’s a requirement.

And that goes for every part of critical infrastructure.

Securing the software supply chain and maintaining the integrity of software written for and used by public-sector agencies will be even more important as both digital services and threats to them grow.

For federal agencies, that means complying with security requirements laid out by recent executive orders, memoranda, and mandates.

Adopting zero trust — and improving cybersecurity generally — will require agencies to develop public-private partnerships committed to collaboration, information sharing, and the security of the software supply chain. Equally important, agencies must continue to find ways to deliver digital services at the speed and quality expected by citizens without compromising security.

Cybersecurity Threats Overview

Modern application development methodologies, including use of microservices and open-source libraries, and increased migration to the cloud, have increased the threat landscape in both sophistication and number. Traditional security methods no longer suffice. **Government agencies — and all software vendors — need to scan their applications for vulnerabilities frequently and throughout the entire software development lifecycle.** Scanning third-party code is also a must.

Microservices are small reusable blocks of logic that can be stitched together into multiple business processes or workflows.

Recent high-profile hacks, like SolarWinds or Log4j, were the direct result of vulnerabilities in open-source libraries. **These attacks, among others, elevate concerns about vulnerabilities within the nation's software supply chain.** Veracode's 12th annual State of Software Security report indicates that 82% of applications used in the public sector have at least one security flaw, a rate that is higher than the average across all private sector industries. (At 76%, however, the private-sector track record isn't much better.)

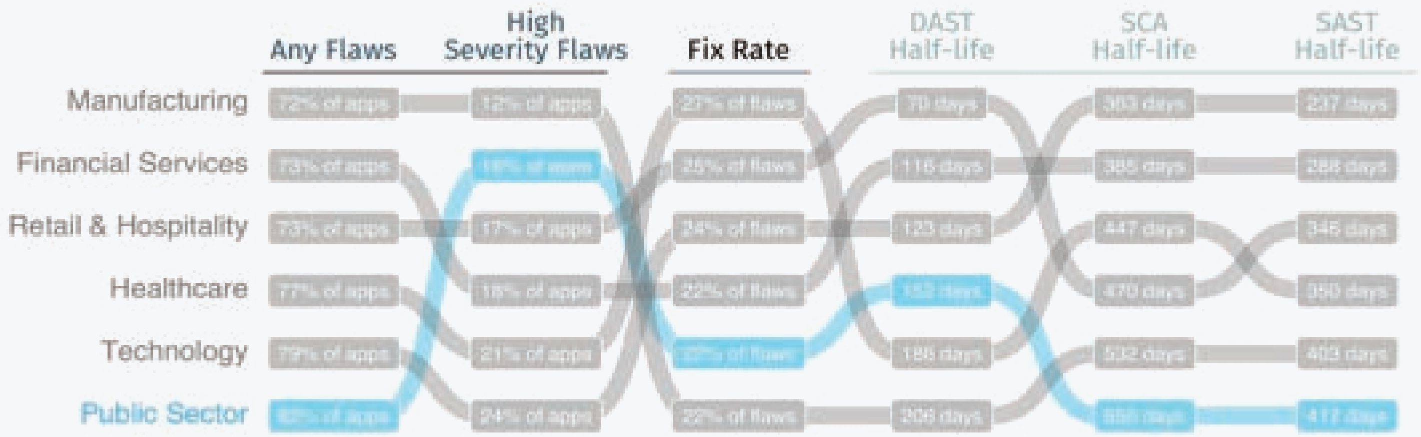


Figure 1: Values and rankings for key software security metrics by industry.

A software bill of materials (SBOM) is the full inventory of an application (components, libraries, modules, etc.) SBOMs provide critical visibility into software components and supply chains to ensure safety of all its components.

The news isn't all bad. The public sector has made a stronger effort as of late to prioritize high-severity security flaws. Research found that throughout 2020-2021, **the public sector reduced the number of high-severity security flaws found in applications by 30%,** according to Veracode's most recent State of Software Security report.

More than ever, cybersecurity risks are interconnected or systemic. In the public sector, exploitation of those risks results in loss of public trust or disruption of public services.

Government agencies need to adopt frameworks like CISA's Zero Trust Maturity Model, which outlines steps for advancing your cyber security program. Acknowledging that application security is a major component of overall IT network security — and a pillar of CISA's approach — compels agencies to ensure software security earlier in the process of developing software. Developers call it **"shifting left."**

CISA's Zero Trust Maturity Model outlines steps that organizations can follow on their path to building a zero trust architecture. It includes five pillars with traditional, advanced and optimal benchmarks to aim for as you mature on your journey.

Policy

The President's Executive Order on Improving the Nation's Cybersecurity **focused attention on systems underpinning the nation's critical infrastructure and government networks – and the threat posed to them by malicious actors seeking to exploit known software vulnerabilities.** The SolarWinds breach and the Log4j vulnerability underscore the point.

> “The impact of a cyber event can unhinge the very services that people rely on. When one thing has a problem, unfortunately, multiple things tend to have a problem.”
>
> **Geoff Brown**
> Vice President of Global Intelligence Platforms, Recorded Future

Significant guidance and mandates shaping the cybersecurity landscape include:

- **The President's Executive Order (EO) on "Improving the Nation's Cybersecurity (14028),"** issued on May 12, 2021. It charges multiple agencies — including NIST — with enhancing cybersecurity through a variety of initiatives related to the security and integrity of the software supply chain.
- **Executive Order 14058 – Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government**
- **OMB Memo M-22-09** requires agencies to implement zero trust architecture strategies by the end of fiscal year 2024.
- **CISA's Zero Trust Maturity Model** – threads Application Security into their Zero Trust Guidance

In the year since the rollout of the Cybersecurity Executive Order to improve the security of government data and networks, policymakers and government officials have taken greater notice of security issues within software supply chains and begun to take steps to bolster IT security across government.

They understand that the security of the government — across all levels — correlates directly to citizen trust.

Customer Experience and Citizen Trust

Seven months after the White House released the EO, President Biden signed an Executive Order on “Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government.”

With this EO **the Federal Government puts citizens — its customers — first by mandating well-designed technology that focuses on user experience and security, and frictionless customer experiences.**

The EO also signaled the White House’s intention to simultaneously bolster cybersecurity while improving the government’s digital services. It is a departure from the conventional wisdom that puts the pursuit of security at odds with the pace of application development and the quality of customer experience.

The Bureau of Fiscal Service of the US Department of the Treasury uses cloud-native services alongside a shift-left approach to application security that requires earlier testing and continuous testing throughout the software development life cycle. **This approach enables them to focus on customer value and revenue drivers. Adopting zero trust controls and practices directly contributes to building citizen trust.**

Since adopting cloud-native services and a shift-left approach, The Bureau of Fiscal Service has improved its time to market, improved the quality of its services, and discovered more effective ways to enhance customer experiences.

> “From rising geopolitical conflict to the increasing digitization of our economy, cybersecurity is more salient than ever, and it’s critically important that the public and private sectors work closely together to protect our nation’s cyber infrastructure.
>
> **U.S. Representative Jake Auchincloss, 4th Congressional District of Massachusetts**

Public-Private Partnerships and the Software Supply Chain

The Cybersecurity Executive Order and other recent mandates highlight the need for improved collaboration and information-sharing between public and private entities to secure the software supply chain. **For that to happen, business and government must work together.**

Cybersecurity attacks, such as the breach of Colonial Pipeline, and continuing actions by the government to deter future attacks, have created a sense of urgency around cybersecurity. The EO mandating software bills of material (SBOMs) and standardization of NIST documents, for example, is a driver of that evolution.

> “Historically, public sector folks were looked at as somewhat laggards in technology, but software security standards is not one of those areas. I believe the public sector is setting the bar, and people are following. They're looking to us for the standards that they need to follow, which is pretty cool.
>
> **Jim Helou; Worldwide Leader of Business Development, AWS Marketplace Public Sector**

About the Sponsors

aws

Amazon Web Services (AWS) places security at the heart of every offering to help you fully realize the speed and agility of the cloud. AWS integrates comprehensive security controls, superior scaling visibility, and automated security processes into its infrastructure to create a secure foundation on which you can build. The Shared Responsibility Model outlines important distinctions between ‘security of the cloud’ and ‘security in the cloud,’ as the security and compliance responsibilities vary depending on the services used, the integration of those services into your IT environment, and applicable laws and regulations.

OPTIV

A SINGLE PARTNER FOR EVERYTHING YOU NEED

- As the cyber advisory and solutions leader, we deliver strategic and technical expertise to more than 7,000 companies across every major industry, size and scale
- We partner with organizations to advise, deploy and operate complete cybersecurity programs from strategy and managed security services to risk, integration and technology solutions
- With clients at the center of our unmatched ecosystem of people, products, partners and programs, we accelerate business progress like no other company can
- The unique power behind Optiv is that we combine a deep understanding of your business with a 360-degree view of your security program; we can meet you wherever you are in your journey, AND help you forecast for the future

Veracode is a leading AppSec partner for creating secure software, reducing the risk of security breach, and increasing security and development teams' productivity. As a result, companies using Veracode can move their business, and the world, forward. With its combination of process automation, integrations, speed, and responsiveness, Veracode helps companies get accurate and reliable results to focus their efforts on fixing, not just finding, potential vulnerabilities.

Veracode serves thousands of customers worldwide across a wide range of industries. The Veracode solution has assessed more than 53 trillion lines of code and helped companies fix more than 71 million security flaws.

Learn more at www.veracode.com, on the Veracode blog and on Twitter.

VERACODE