Invicti
AppSec with Zero Noise

Fall 2022 AppSec Indicator

Government relies on DAST to bolster security

From securing the cloud to buttoning up the supply chain, Government agencies will need to invest more and cut through the security noise if they want to reduce risk and cover all their bases – *known or otherwise*.

Too much noise and not enough automation can seriously stifle your security team's ability to prove their investment in innovative tools and relay ROI up the chain. And when the results don't speak for themselves or get overly complicated, they compound existing stressors between security and development teams, ultimately leading to the introduction of more vulnerabilities down the road.

Preventing new vulnerabilities and taking care of lingering security risks is crucial, especially for web applications.

In 2021, web applications were a top attack vector, accounting for roughly 70% of security incidents.[1] **The average cost of a data breach increased from $3.86 million in 2020 to a hefty price tag of $4.35 million in 2022,[2] – and in 2021, there were 3,244,455 victims in public sector-related cybersecurity breaches alone.[3]**

But there's good news on the horizon: Dynamic application security testing (DAST) tools that enable teams to find vulnerabilities earlier and with greater accuracy remain a top investment priority as organizations face the headwinds of unsteady economies and increasing cyberattacks.

To get into the nitty-gritty of where organizations are truly investing and why, we surveyed 100 public sector developers and security professionals in our most recent AppSec Indicator report. The results show an upswing in security budgets for 2023 with a focus on modern solutions and transparent ROI.

1 Verizon 2022 Data Breach Investigations Report
2 IBM 2022 Cost of a Data Breach Report
3 Identity Theft Resource Center Q3 Data Breach Analysis

INVICTI INSIGHTS FOR 2023

"Businesses are glued together with APIs. Many are internally facing and are often poorly secured, as we have seen from major breaches in 2022. Because they lack a visible user interface and work in the background, they can suffer from being out-of-sight and out-of-mind, creating a dangerous area of risks."

Dan Murphy
DISTINGUISHED ARCHITECT AT INVICTI

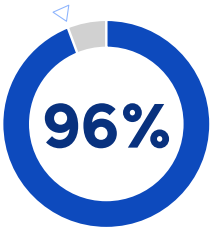
AppSec trends to watch in Government

When we break down future budgets by industry, we see that Government is making moves on budget increases. And Government organizations are seeing actual positive change when they increase cybersecurity budgets – especially with DAST taking center stage.

85%
of respondents plan to increase their cybersecurity budgets in 2023

AND IT SHOULD COME AS NO SURPRISE THAT

70%
of professionals say that budget increases result in strong security improvements



of respondents say they rely on DAST solutions either moderately or a great deal

AND

also consider future DAST technology investments to be a top or high priority

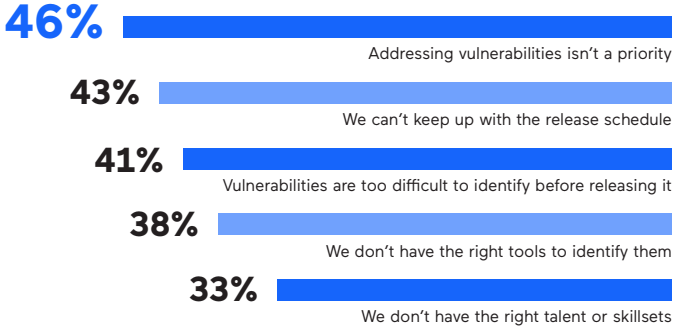
Updating security scanning technology is a mission-critical task that spans industries too, with vulnerabilities slipping through the cracks and subpar tools causing too much noise.

79%
of Government organizations release software with unaddressed vulnerabilities always or often – a problem that's fairly typical across industries

WHY IS SOFTWARE GETTING RELEASED WITH UNADDRESSED VULNERABILITIES?

For nearly half

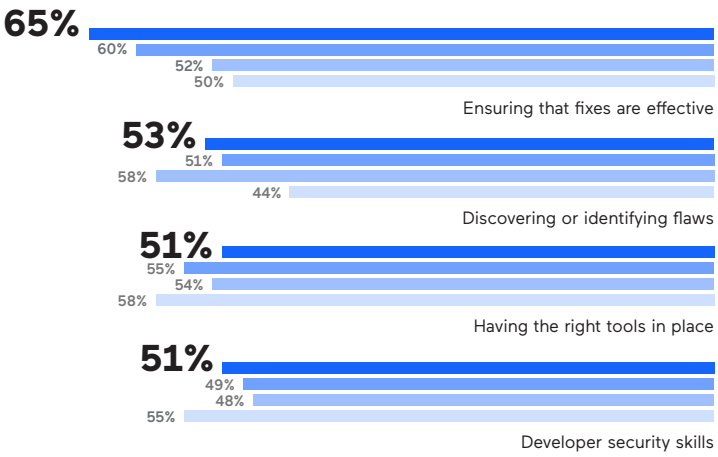
of DevSecOps professionals in the public sector, these flaws either are not a priority or cannot be addressed without breaking the deadline-driven release cycle.



THE STRUGGLE IS REAL FOR THOSE WHO CAN'T KEEP UP

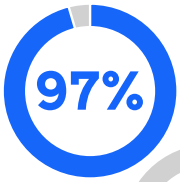
In Government, 65% of respondents have a difficult time ensuring that fixes are effective, while 51% don't have the right tools in place to get the job done

Which of the following, if any, does your company struggle with when addressing web application vulnerabilities?

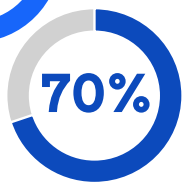


CAN YOU HEAR ME NOW?

When AppSec grows too noisy, vulnerabilities get the silent treatment:

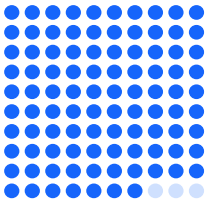


of DevSecOps professionals say that their team ignores a real vulnerability thinking it was a false positive at least once per month



of respondents in the public sector say that false positives are discovered in vulnerability reports all the time or often

The heat is on, but automated DAST tools help lower the temperature: among the public sector professionals surveyed, **97% feel pressure** when it comes to proving their return on investment.



Modern AppSec tools like DAST have accuracy and automation baked in as fundamental features to help teams take their reporting to the next level while also reducing the noise that comes from false positives. As you plan for 2023 strategies, opt for tools with detailed reports and clear remediation statistics that you can tie back to a reduction in manual labor and improved security posture.

Invicti
AppSec with Zero Noise

Download the full report to get all the details about the latest trends in AppSec ▸