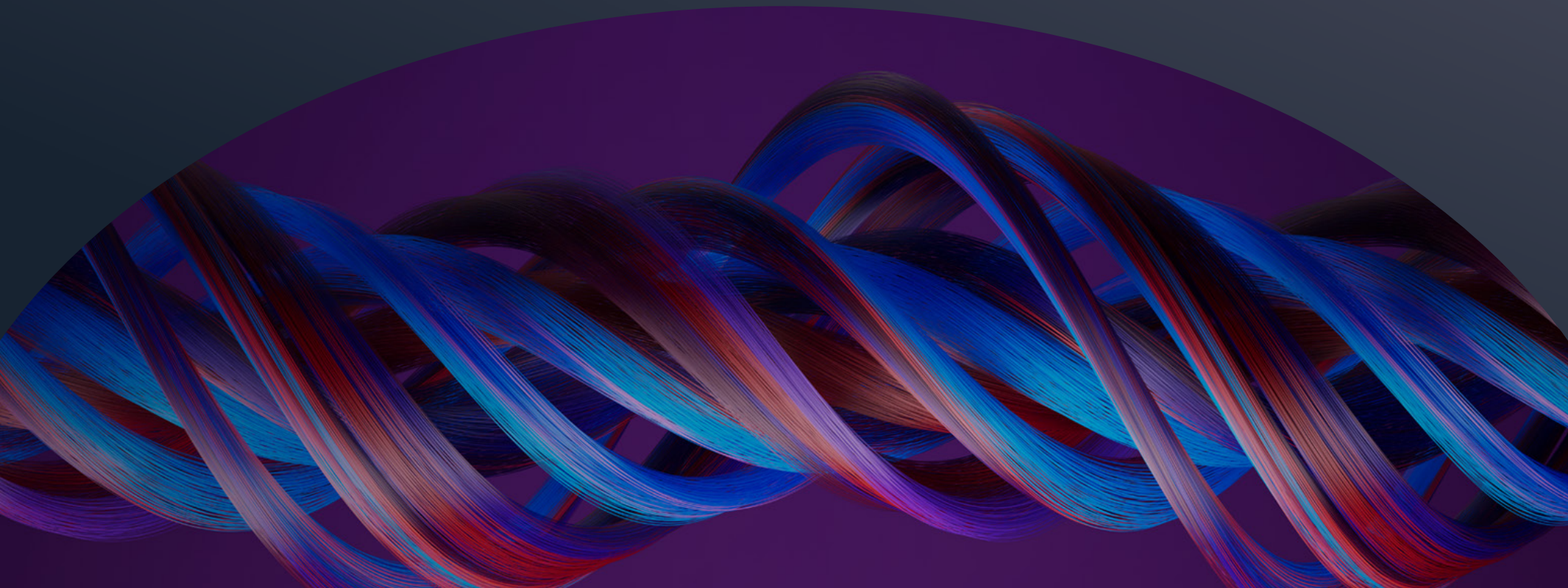
invicti
AppSec with Zero Noise

The Invicti AppSec Indicator

Fall 2022 Edition:

Tuning Out AppSec Noise **is All About DAST**



What's inside:

If we want to quiet the noise in application security (AppSec), modern solutions **must take center stage.**

Ever noticed how noisy AppSec can be?

From buzzword-laden jargon to intense cybersecurity regulations, false positives in scans, and overpromises from subpar tools, **AppSec without clear direction *is loud*.**

Unfortunately, too much noise and not enough automation can seriously stifle your security team's ability to prove their investment in modern 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 that impede innovation and ultimately lead 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] – that's a 13% jump in two years.

But there's good news on the horizon: automated security solutions, specifically 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. When leaders focus on investing in and utilizing the right tools, ROI-validated success will follow, and so will a more secure asset landscape.

$4.35M

the average **cost of a data breach in 2022**

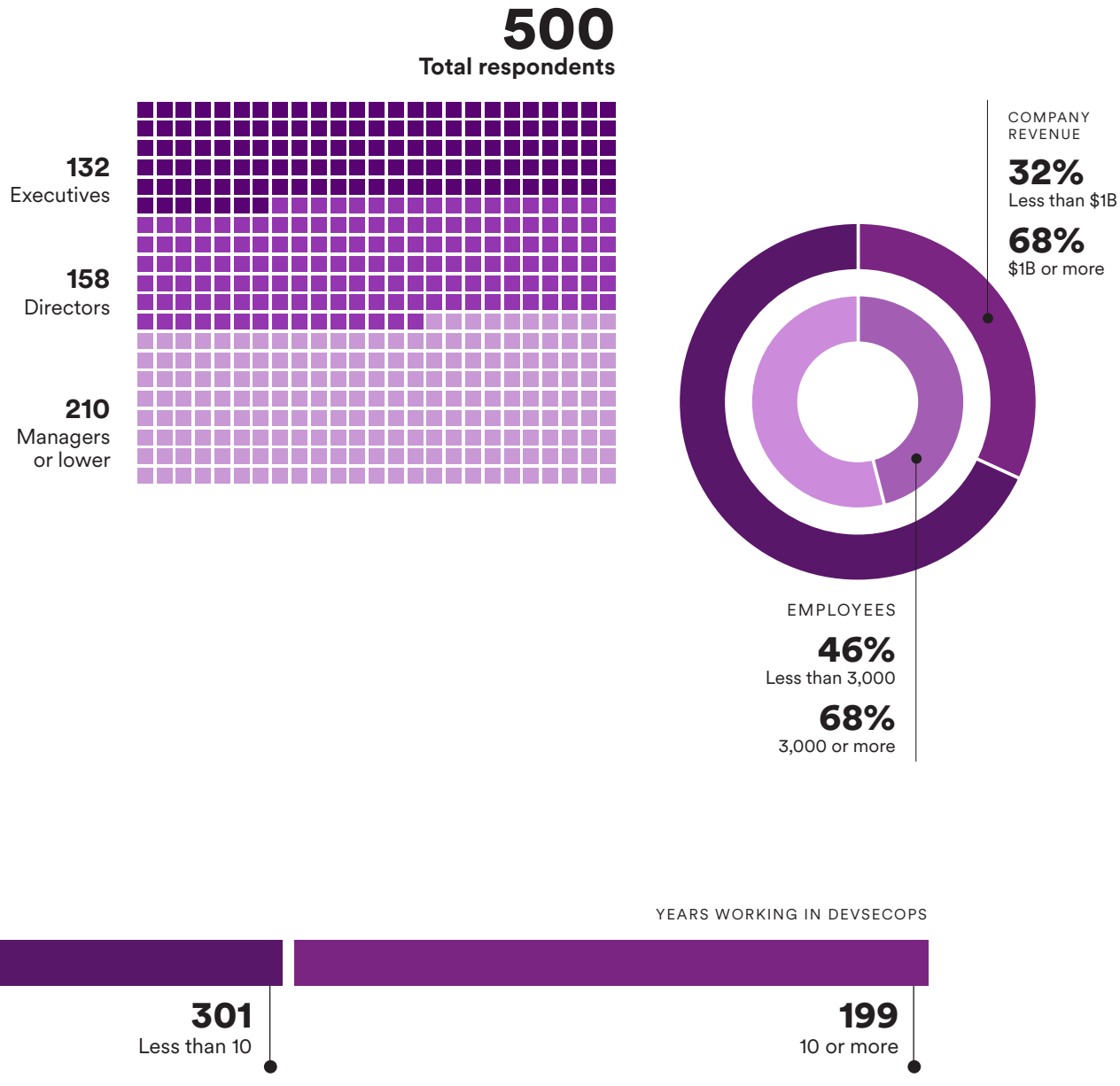
13%

Jump in two years

1 Verizon 2022 Data Breach Investigations Report
2 IBM 2022 Cost of a Data Breach Report

To get into the nitty-gritty of where organizations are truly investing and why, we surveyed the people who live and breathe AppSec **every day**.

In partnership with Wakefield Research, Invicti polled 500 DevSecOps professionals in the United States with a minimum of five years of experience at companies that have at least 2,000 employees. To gain deeper insight into how these trends impact varying industries and where the greatest changes are taking place, we included respondents from the Government, Healthcare, Financial, and Education sectors.



The results show an **upswing in security budgets** for 2023 with a focus on modern solutions and transparent ROI.

73%

of organizations anticipate that they'll increase their investment in AppSec in 2023.

Investing more in modern cybersecurity – specifically DAST – remains a top priority as the economy ebbs and flows.

97%

of respondents ignore a real vulnerability at least once a month assuming it's a false positive.

Cutting through the noise is possible with innovative cybersecurity tools built on automation and accuracy.

100%

of DevSecOps professionals track ROI for their AppSec tools, many under great pressure.

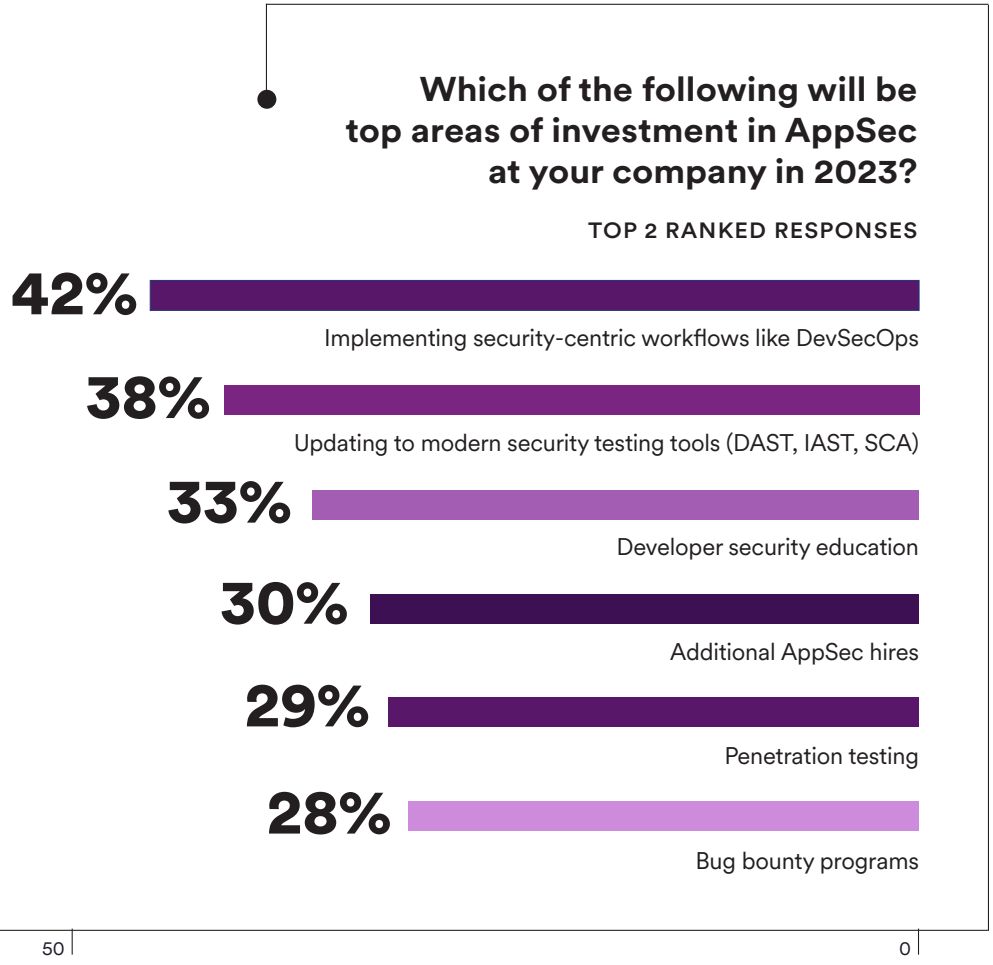
Demonstrating success to leadership requires security solutions that provide concise analytics and remediation guidance.

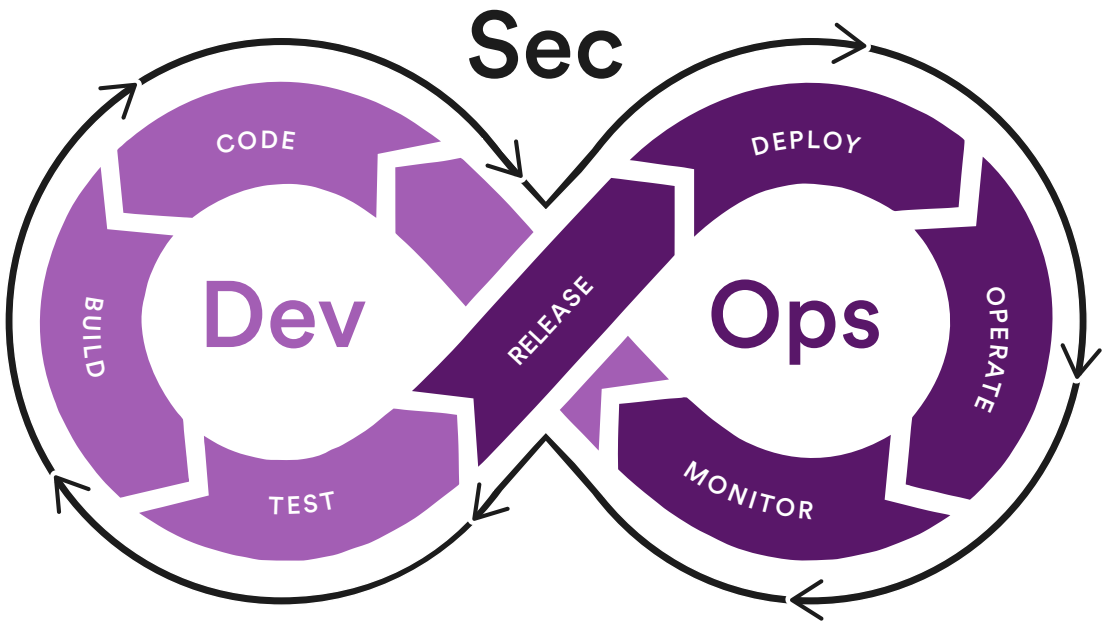
Can’t cut this:

Prioritizing security budgets

Organizations are **investing more than ever** into their AppSec programs as effective DevSecOps shines.

DevSecOps does indeed pay off. In many cases, leadership realizes that the investment means the difference between a headline-making data breach and building a secure business that customers rely on. The proof is in the security pudding: 62% of professionals surveyed say that increasing their budget results in strong security improvements, and, unsurprisingly, **73% of respondents said they anticipate that they'll increase their AppSec budgets in 2023**, including 85% of Government respondents.





Building security right into the software development lifecycle (SDLC), baked into existing workflows, is how you blend security and development harmoniously. DevSecOps is all about adopting a security-first mindset with automated verification right in DevOps pipelines for that smooth validation stream. It integrates security scanning continuously throughout existing workflows, allowing for more agile development without sacrificing safety. By incorporating a complete web application security solution that integrates directly with issue trackers, vulnerability management systems, and CI/CD platforms, you can fully embed web AppSec into your SDLC for more impactful DevSecOps. **Learn more ▶**

From securing the cloud to buttoning up the supply chain, organizations will need to **invest more** if they want to cover their bases (known or otherwise).

The need to cover more ground is ever-increasing as the number of web applications rises daily. After all, you can't defend what you don't know you have – and organizations are producing a lot of web assets today. There are over 1.1 billion websites in the world, with approximately 175 new sites created every minute.[3] As businesses generate apps and microsites quickly to keep up with the competition, it becomes more important to map their entire attack surface. Covering all corners of the threat landscape better prepares DevSecOps teams for new discoveries like the dreaded Log4j vulnerabilities; they're able to respond faster and much more effectively when they know exactly what they're dealing with.

THERE ARE OVER

1.1B

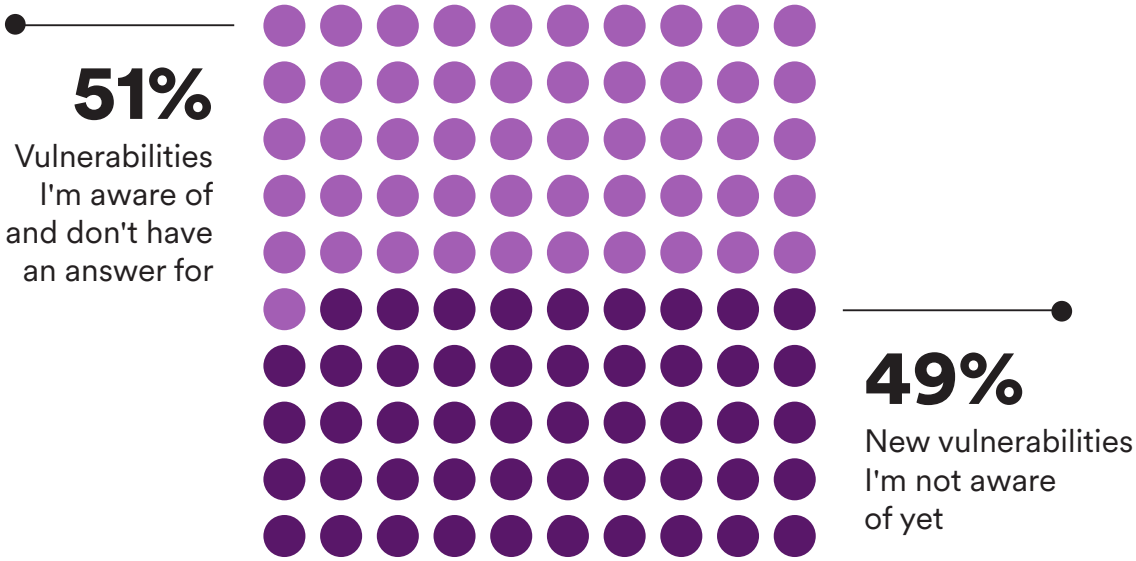
websites
in the world

175 NEW SITES CREATED **EVERY MINUTE**

If you want to secure your entire threat landscape, you need a discovery tool that can find everything quickly and help you maintain a complete web inventory. A strong discovery engine makes this a breeze, scanning for lost, hidden, and unknown web-facing assets with automatic results in seconds to cut out manual guesswork. ***Learn more*** ▸

3 How Many Websites Are There in the World

Which of the following are you more worried about?



Invicti Insights

Looking ahead, how will investments in critical security budgets change, for better or worse?

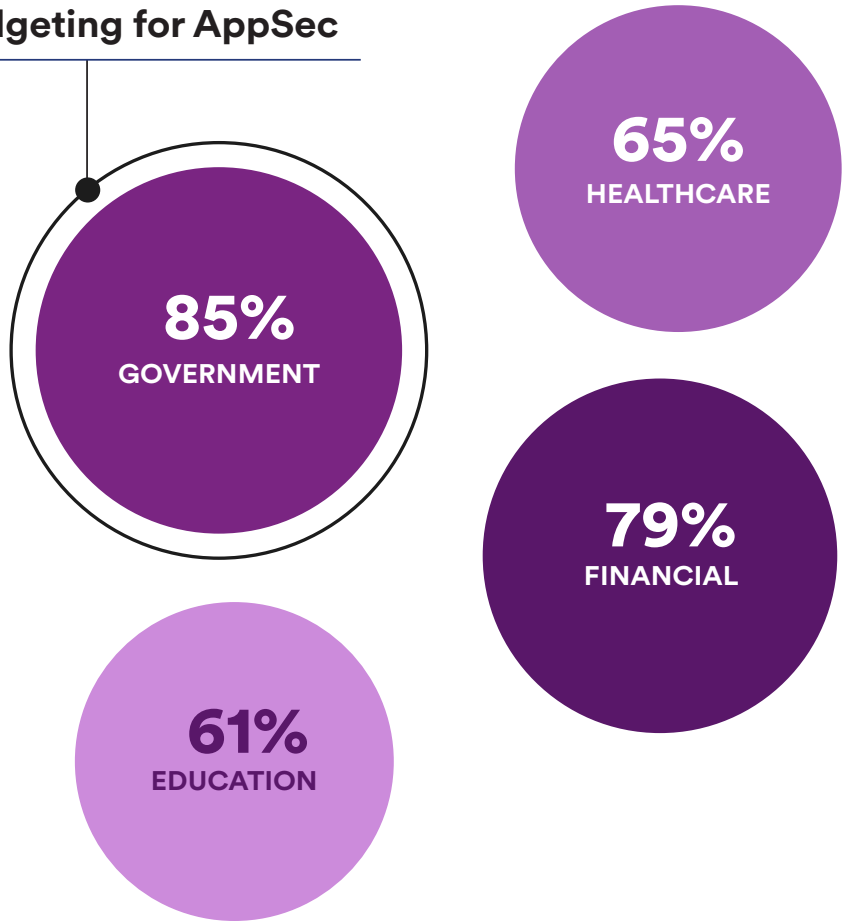
> AppSec budgets will continue to increase for a variety of reasons. Log4j being a major driver for this year, but more than that, it is about essentially anything new being developed, is being written as an app or an API in some shape or form. I predict more spending for cloud-native-friendly security products, APIs, and SCA. SBOMs and software supply chain will take priority, as will containers and orchestration.

Frank Catucci, Chief Technology Officer and Head of Research at Invicti

When we break down **future budgets by industry**, the Government is leading the pack.

The data shows the Government is stepping up more than other industries when it comes to increasing their cybersecurity budget. On the tail of President Biden's Executive Order on Cybersecurity, it's no surprise that the public sector is making moves. And not a moment too soon, considering that in the Invicti AppSec Indicator: Spring 2022 Edition, we discovered, likely due to legacy web technology and processes, as many as 32% of Government organizations experienced at least one SQL injection (SQLi) occurrence in 2021.[4]

How key industries are budgeting for AppSec



4 Invicti AppSec Indicator: Spring 2022 Edition

Vulnerability stress is (still) real

Last year, we found that vulnerabilities were causing **unnecessary stress** for development and security teams.

Both discovered and undiscovered vulnerabilities remain a time-consuming and stress-inducing problem. And things just aren't getting better: data from the Invicti AppSec Indicator: Fall 2021 edition underscored serious gaps in security due to time constraints, bandwidth issues, and inadequate tooling or processes.[5]

FALL 2021 APPSEC INDICATOR

80%

of respondents said security processes delay their delivery timelines somewhat or significantly.

45%

frequently complete projects without carrying out all security steps because of the pressures at their organization.

1 in 3

issues under remediation makes it to production without being caught in testing or development stages.

READ MORE

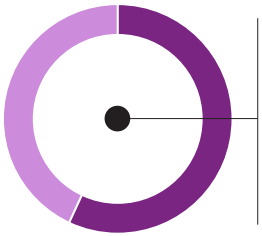
Compare this year's report with previous trends by reading the Fall 2021 edition of the Invicti AppSec Indicator

Learn more ▸

5 The Invicti AppSec Indicator: Fall 2021 Edition

This year, similar trends point to the **lingering impacts** of inadequate AppSec.

Why's it such a big deal?
The pace of web development and application releases is always full-throttle, but teams simply can't keep up with the demand and especially struggle to include critical security considerations at every step. In 2023, the biggest security challenge organizations expect to face is building and maintaining more secure applications – and that requires more effective DevSecOps.

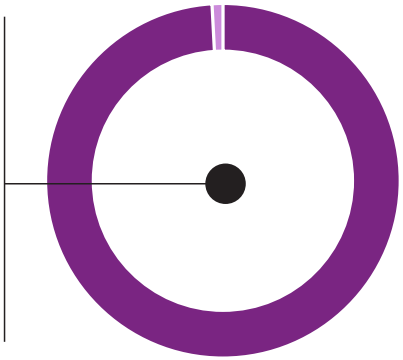


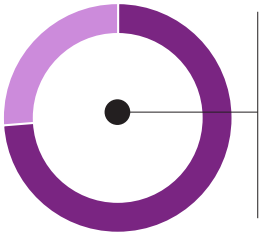
57%

of DevSecOps professionals say that building secure applications and preventing or mitigating attacks are the biggest security challenges for their organization.

99%

struggle to address vulnerabilities for a multitude of reasons, including the need to ensure fixes are effective and a lack of necessary security skills or modern tools.





74%

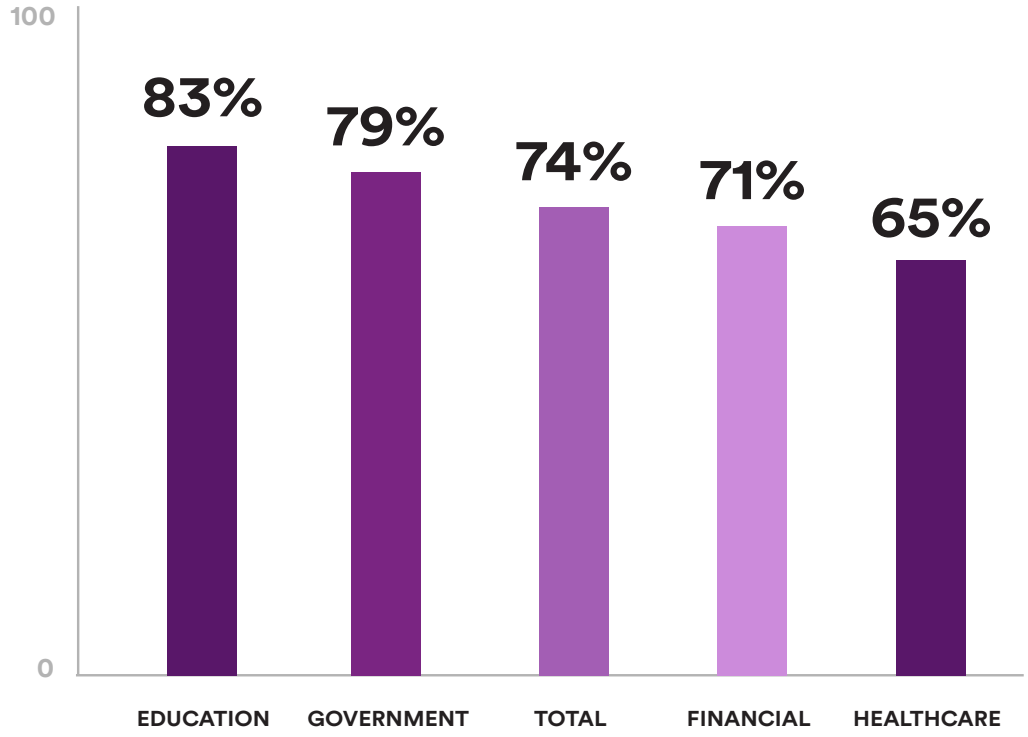
release vulnerable applications "often" or "always" as they face challenges integrating security into the software development lifecycle (SDLC).

Vulnerable apps are still being released across industries, **constantly**.

A sizable 74% of organizations release software with unaddressed vulnerabilities regularly. Education and Government lead the pack as they often struggle with antiquated systems and security processes, all of which compete with the need for rapid software release and critical user access.

RISK IN RELEASE

Those who admit to regularly releasing software with unaddressed vulnerabilities



“Release fast or die.”

That’s the mentality developers often live by, which ultimately leads to skipped or missed security steps as they race to meet deadlines. When they don’t have the skills or tools necessary to cover security as they rush to meet those deadlines, they can inadvertently let severe vulnerabilities slip through the cracks and compound existing risk.

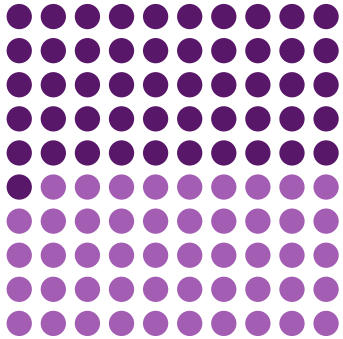
By embedding security farther left in the software development process to cover design and architecture and integrating security on the right to cover later stages of production, fewer flaws slide through under the radar. Shifting automated security left and right in the software development lifecycle makes security adoption easier and closes development blindspots.

Learn more about how organizations shift left and right with Invicti ▸

Why are nearly three-quarters of DevSecOps professionals often or always **releasing vulnerable apps**?

Teams are still having a hard time finding and addressing vulnerabilities before release, mostly due to subpar tools and inadequate know-how around security best practices. Most often, it's a combination of reasons that makes security seem too much of a hassle – and it's a serious problem that puts organizations at operational and financial risk.

When we asked whether DevSecOps professionals were more concerned about known or unknown vulnerabilities, 51% said they're most worried about known vulnerabilities that they don't have an answer for. Factor in that many attackers use a low-and-slow approach, and it's easy to see how this can cause significant damage, even stemming from a minor vulnerability.



51%

said they're most worried about known vulnerabilities that they don't have an answer for

Invicti Insights

If a team relies on APIs, are minor vulnerabilities really a problem?

> "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 risk."

Dan Murphy, Distinguished Architect, Invicti

We see in the data that addressing vulnerabilities isn't always happening quickly. If vulnerabilities aren't properly prioritized, they introduce more risk by the day, but good tools can help DevSecOps teams better understand where they should focus their time, effort, and energy to reduce that risk. For other concerns, automation is critical: if you can't keep up with the release schedule, building automated security into the SDLC helps you cover the entire testing pyramid. From static scans (SAST) to software composition analysis (SCA) running on every check-in, and dynamic testing (DAST) on each deployment of a micro service's REST API to the development stack – each of these plays a healthy role in robust application security.

If lack of skill set is a glaring issue, understand that it takes time to build up the best practices and know-how necessary to prevent dangerous exploits. Managed security tools, like Invicti, offer more value by encapsulating expertise right in the software to provide proper guidance and clarity and help cut through the noise. At the end of the day, as cybersecurity roles remain unfilled (more to come on that) and team members are absorbing unnecessary manual tasks, this level of insight truly matters.

Why is software released with unaddressed vulnerabilities?

ASKED AMONG THOSE WHOSE COMPANY RELEASES SOFTWARE WITH UNADDRESSED VULNERABILITIES

45%
Addressing vulnerabilities isn't a priority

41%
Vulnerabilities are too difficult to identify before releasing

38%
Don't have the right tools to identify them

37%
Can't keep up with the release schedule

31%
We don't have the right talent or skill sets

Tuning out noisy AppSec

Can you hear me now?

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

One of the many reasons stress compounds within DevSecOps workflows is all of the unnecessary noise. From acronym-filled jargon to false positives and confusing analytics, it's no surprise that security and development have trouble communicating effectively if they don't have the right tools and processes in place.

Whether teams are stretched too thin to deal with a vulnerability when it is discovered, or they simply don't know how to handle it, the most common tactic is to ignore the noise. Without tools built on accuracy integrated into the SDLC, vulnerabilities pile up and can easily slip through the cracks. This is especially true for false positives that erode team confidence in reporting and turn up the volume on noisy distractions.

97%

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

False positives remain a pesky problem, but **accurate automation** is the cure.

Many application scanners are prone to false positives that can send teams chasing a problem that doesn't even exist. These cacophonous little false alarms make automation impossible, as security professionals must manually find, verify, and assign or discard vulnerabilities in tedious additional steps.

In the buffet of security features that help to reduce noise, accuracy and automation take the cake. Automating three manual steps – find, verify, and assign – can save large companies hundreds of hours every month and cut down on the noise of false positives. With automated proof of vulnerability in hand, DevSecOps teams are operating on confidence: if the scanner found it and can exploit it, a hacker can too.

Proof-Based Scanning by Invicti cuts through the noise – and the uncertainty – of scan results. Not only does it show you which vulnerabilities are real, but also it fortifies DAST results by uncovering exploitable flaws so that you can prioritize more effectively. Proof-Based Scanning automatically confirms over 94% of direct-impact vulnerabilities with 99.98% accuracy, giving developers and security professionals the conclusive evidence and confidence they need. ***Learn more***

Covering your AST with DAST

The **right toolset** goes a long way in AppSec.

There's no dancing around it: today's web application security landscape is peppered with challenges. But the good news is many organizations understand the importance of effective AppSec tools, and they're already investing where it matters most by embedding DevSecOps and DAST solutions into development.

38% of DevSecOps professionals say investing in DAST, IAST, and SCA is a priority in 2023

94% already use DAST tools to scan production applications

39% scan extensively with DAST

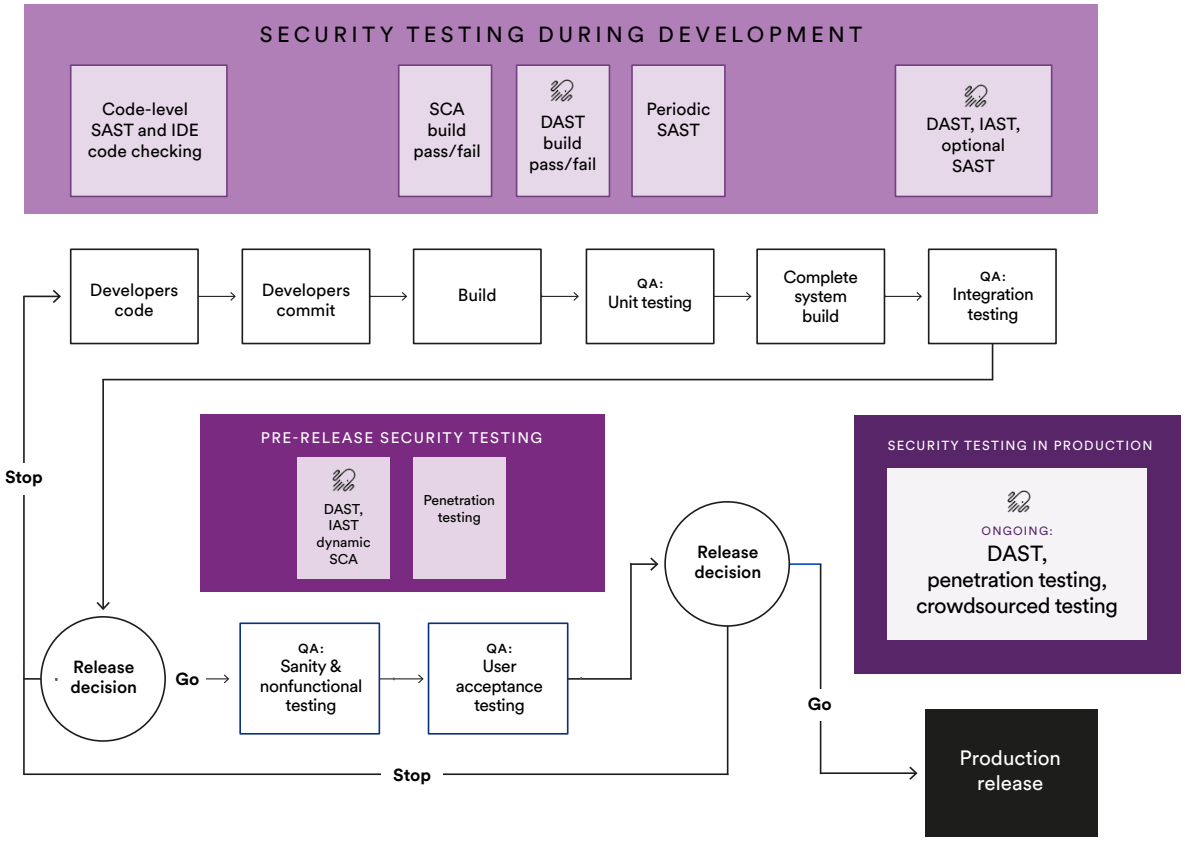
What's so special about DAST, anyway?

Dynamic application security testing, or DAST, is a powerful approach to AppSec. Modern DAST tools can scan all web assets regardless of origin and permit teams to run security tests already during development to find and fix issues sooner. By checking production deployments for vulnerabilities, DevSecOps professionals can more quickly and efficiently gauge just how secure their live environments are through reliable, accurate results. Before selecting a DAST product to integrate into the SDLC, make sure that your solution of choice is:

- ☑ Trustworthy and accurate to reduce the amount of false positive results
- ☑ Comprehensive for maximum test coverage and swift vulnerability detection
- ☑ Flexible enough to work with multiple web technologies and languages
- ☑ Ready to integrate with existing development workflows and collaboration tools

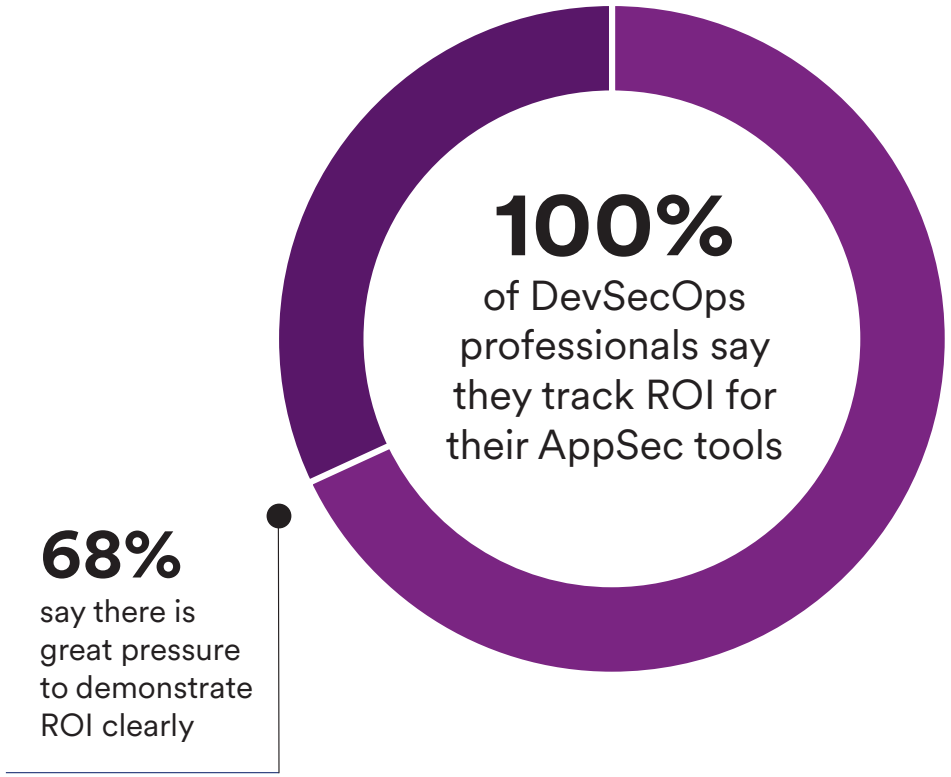
Invicti DAST plugs right in to help your teams **work smarter**, not harder.

When paired with other tools that integrate into the SDLC, dynamic testing is versatile and powerful. Invicti DAST was designed with scalability and automation at the top of mind, incorporating Proof-Based Scanning so that our customers experience true accuracy and confidence in the results.
Learn more ▶



The **pressure to prove ROI is real**. Automated DAST helps relieve it.

Results speak for themselves, and in AppSec, those results carry a lot of weight. 100% of DevSecOps professionals say they track ROI for their AppSec tools, which means it remains a top priority. The tough news? For 68% of them, there is great pressure to demonstrate ROI clearly. Fortunately, modern AppSec tools like DAST have accuracy and automation baked in as fundamental features to h p teams take their reporting to the next level. Opt for tools with detailed reports that clearly outline remediation statistics you can tie back to a reduction in manual labor.



Proving ROI with Invicti is **seriously easy**.

Invicti customers know that threats aren't going away and that proving ROI in AppSec starts with automated, accurate tools. In a co-sponsored report with the Enterprise Strategy Group (ESG), we highlighted how two of our customers save critical time and money by integrating Invicti tools directly into their development workflows. These security processes help close critical coverage gaps and are more accurate than previous solutions, ultimately cutting back on manual work and freeing up valuable innovation time.

$180,000

"By using Invicti products, we probably saved ourselves, in the first year alone, $180,000."

CISO

LEADING TELEVISION NETWORK COMPANY

"Once it's set up, it can free up 10-15 hours of time for each person, with automated scans and reports instead of taking time with manual tasks testing an application."

Associate Director for Security Testing and Assurance,

LEADING GLOBAL TRAVEL AND VACATIONS COMPANY

CASE STUDY

For deeper insight into how organizations save time and money with Invicti, check out this case study with Channel 4. ▸

READ MORE

We recently published a report with ESG, "Automated Application Security Testing for Faster Development"

Learn more ▸

Don't just take their word for it – **here's the math:**

WITHOUT AUTOMATED VERIFICATION

Things get tedious and costly

Every vulnerability report could be a critical issue, but it can also be a false alarm

Developers start ignoring the flood of vulnerability reports

1 hour

The average time to manually check a vulnerability, based on an Invicti survey of security professionals

10,000 hours

Your security team needs to manually verify 10,000 vulnerabilities per year

$50/hour

The average hourly rate for a US-based security engineer is $50[1]

-$500,000

That's 10,000 hours wasted checking uncertain vulnerability scan results, costing $500,000 a year

WITH PROOF-BASED SCANNING

Proof-Based Scanning automates the legwork so you immediately know what to fix

40%

Typically, 40% of scan results are direct-impact vulnerabilities[2]

94%

of direct-impact vulnerabilities are automatically confirmed by Proof-Based Scanning, based on six years of usage data

99.98%

Proof-Based Scanning has a confirmation accuracy of over 99.98% – only 0.02% of confirmed vulnerabilities could be false positives

3,760

Out of 10,000 vulnerabilities per year, Netsparker identifies the 4,000 direct-impact issues and automatically confirms 3,760 of them – and these can go directly to the developers to fix

240

Your security team now has only 240 exploitable vulnerabilities to check manually, taking 240 hours a year instead of 10,000

+$488,000

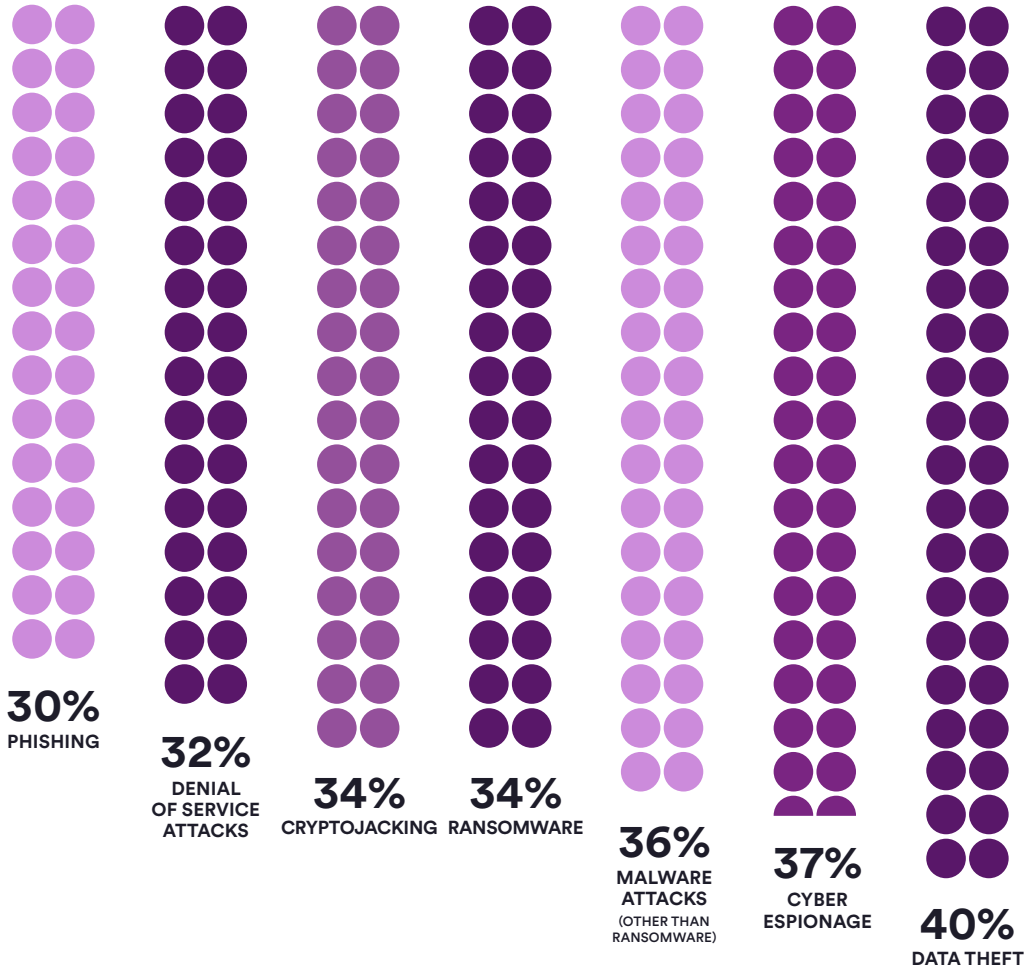
That leaves you with 9,760 hours and $488,000 to spend on high-value security and development projects

1. Glassdoor typical rate as of Aug 2021. Actual rates will vary depending on the position and region, so adjust this for your organization.
2. Based on usage data. Direct-impact vulnerabilities are weaknesses that can be exploited remotely without special prerequisites and have direct consequences for security.

The next year of AppSec – and beyond

Data theft, cyber espionage, and malware, **oh my!**

Pressure is mounting to prove ROI for AppSec tools while vulnerabilities remain a top stressor. As 100% of DevSecOps professionals have cybersecurity concerns heading into the next five years, it's no surprise that we're seeing a continued push for modern DAST and effective DevSecOps. The top concerns are alarming – data theft, cyber espionage, malware, and ransomware – worries undoubtedly compounded by the cybersecurity skills gap, subpar tooling, and a lack of AppSec confidence in general. That's where DAST and automation take center stage.

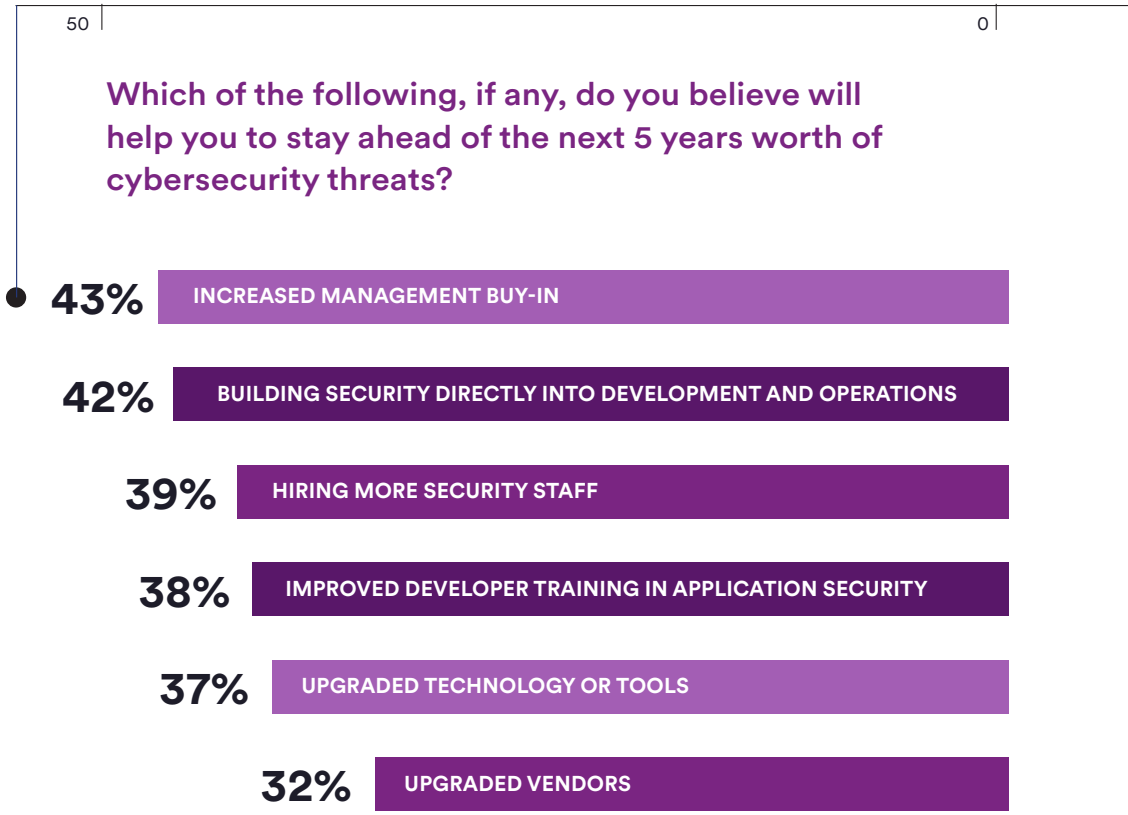


What are your biggest cybersecurity concerns, if any, heading into the next 5 years?

97% of DevSecOps professionals say investing in DAST in 2023 is a **high priority**

Whichever way you cut it, modern AppSec can't exist without DAST. As more organizations scan more of their attack surface than ever before and shift from point-in-time scanning to continuous coverage, DAST provides a unique and critical view into their web security posture that other tools just can't give. And 97% of professionals agree that it's no longer a mere nice-to-have but an essential part of their SDLC.

What else are DevSecOps professionals doing to stay ahead of cyberthreats over the next five years? Nearly half (43%) believe that increased management buy-in around security efforts and budget is key. It's refreshing to see that nearly 40% of professionals want to dedicate more time and effort to developer training and upgraded technology, too. That's especially important as 70% of Information Systems Security Association (ISSA) members say that the skills gap in cybersecurity has directly impacted their organization.[8]



8 ESG/ISSA Report - The Life and Times of Cybersecurity Professionals 2020

Predictions from the front lines of Invicti show even more promise for DAST and DevSecOps.

We asked four of our in-house experts what 2023 will look like for the state of DAST in AppSec, and what you **should be thinking about as you prepare for the next few years of cybersecurity.**

"In 2023, the dialogue will change from shifting left and shifting right to continuous application security. Our customers are automating continuous scanning by integrating Invicti DAST into their development, security, and operations tools, testing all of their web applications and APIs. Government and industry regulations and standards, along with the increased focus on security from executive teams and their boards, will continue driving rapid growth of DAST technology."

Sonali Shah
CHIEF PRODUCT OFFICER

"In 2023 and beyond, DAST becomes an effective tool to scan at scale and measure the effectiveness of the various layers of security protection that a company has in place. Using the same techniques that the bad guys use gives an end-to-end view of security debt that is directly actionable."

Dan Murphy
DISTINGUISHED ARCHITECT

"The regular scanning of APIs and API integrations will increase in 2023 due to the sheer volume of services being developed and deployed. DAST is in a great spot to scan those effectively, especially with key integrations, providing much-needed insight and security for headless services."

Frank Catucci
CHIEF TECHNOLOGY OFFICER
AND HEAD OF RESEARCH

"DAST can also scan production environments regularly and continuously whereas the 'shift left' methodology really just focuses on everything pre-production. Additionally, scanning with DAST allows checks of the server configuration in which the web application is hosted and may provide additional vital vulnerability coverage."

John Mandel
SENIOR VICE PRESIDENT, ENGINEERING

Cybersecurity impacts **everyone**.

The entire organization must step up and ensure that they're following the right policies and procedures if we want to achieve well-oiled DevSecOps. Ultimately, building and orchestrating DevSecOps workflows comes down to leadership, budget, and capable tools. With solutions that provide accurate results and consistent support from the top, effective DevSecOps is achievable.

Even though data theft remains a top concern and vulnerability reports are causing excessive noise, it's promising to see that many DevSecOps professionals are optimistic about investing more in security measures. Organizations know they need to pump up the budget now more than ever; when the economy turns rocky, having the right tools in hand is critical both for maintaining adequate security coverage and demonstrating your security ROI.

As we in the AppSec industry collectively move toward ever-advancing tools with growing automation, any noise in results is prone to multiplication and amplification. **Especially with technologies to prove exploitability, modern DAST is uniquely positioned to cut through the noise and help in making the right security decisions:**

- ☑ DAST is performed on running applications and helps shift security left and right as it can be integrated at any stage of the SDLC, unlike most other testing types. Plus, it can run on assets that have already been deployed without needing to modify them. That's important for catching issues in existing or legacy applications.
- ☑ Because it simulates user actions, there are fewer false positives and false negatives when using DAST – especially when paired with Proof-Based Scanning – which helps cut through the noise for faster remediation and clearer ROI
- ☑ Advanced DAST solutions can test APIs, and the language of choice used to create an application doesn't matter with DAST. It has the capability to test any application with a web user interface, whether implemented using traditional server-side rendering of HTML or a modern Single Page Application (SPA) implemented in TypeScript.
- ☑ Modern DAST works in synchronicity with critical features like web asset discovery, vulnerability assessment, and vulnerability management to take security to the next level

Modern AppSec is all about DAST and tuning out the unnecessary noise.
With fewer distractions and more focus, DevSecOps professionals have more freedom to deliver secure, innovative applications that their customers rely on every day.

Schedule a DAST demo

Methodology

The Invicti Survey was conducted by Wakefield Research among 500 US DevSecOps professionals, with a minimum of 5 years experience working in DevSecOps, at companies with a minimum of 2,000 employees and with oversamples of 100 respondents in each of the following industries: Government, Healthcare, Financial, Education, between September 9th and September 20th, 2022, using an email invitation and an online survey. Results of any sample are subject to sampling variation. The magnitude of the variation is measurable and is affected by the number of interviews and the level of the percentages expressing the results. For the interviews conducted in this particular study, the chances are 95 in 100 that a survey result does not vary, plus or minus, by more than 4.4 percentage points in the main sample and 9.8 percentage points in each of the oversamples, from the result that would be obtained if interviews had been conducted with all persons in the universe represented by the sample.

About Invicti Security

Invicti Security is transforming the way web applications are secured. An AppSec leader for more than 15 years, Invicti enables organizations in every industry to continuously scan and secure all of their web applications and APIs at the speed of innovation. Through industry-leading Asset Discovery, Dynamic Application Security Testing (DAST), Interactive Application Security Testing (IAST), and Software Composition Analysis (SCA), Invicti provides a comprehensive view of an organization's entire web application portfolio and scales to cover thousands, or tens of thousands of applications. Invicti's proprietary Proof-Based Scanning technology is the first to deliver automatic verification of vulnerabilities and proof of exploit with 99.98% accuracy, returning time to development teams for critical projects and innovation. Invicti is headquartered in Austin, Texas, and serves more than 3,500 organizations all over the world.

invicti

FIND US

linkedin.com/company/invicti-security
twitter.com/invictisecurity
facebook.com/invicti-security
invicti.com
invicti.com/contact/