How Invicti’s Proof-Based Scanning can cut through the AppSec noise and save you $488K per year

invicti

All scanners find vulnerabilities, but drastically reducing false positives can save your application security program thousands of hours.

PROOF-BASED SCANNING | **Confirms 94% of direct-impact vulnerabilities with 99.98% accuracy**

Let’s take a typical enterprise scenario based on what we’ve seen in hundreds of large organizations:

500

Imagine you need to scan 500 websites and applications

(When you add web services and APIs, even 500 scan targets is a conservative estimate.)

20

Your scanner reports 20 vulnerabilities per year per site or application

(Average based on Invicti data.)

10,000

You are responsible for 10,000 vulnerabilities per year

(Ouch.)

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. The average time to manually check a vulnerability, based on an Invicti survey of security professionals
- Your security team needs to manually verify **10,000** vulnerabilities per year
- The average hourly rate for a US-based security engineer is **$50**[1]
- 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

- 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
- Proof-Based Scanning has a confirmation accuracy of over **99.98%** – only 0.02% of confirmed vulnerabilities could be false positives
- Out of 10,000 vulnerabilities per year, Invicti identifies the 4,000 direct-impact issues and automatically confirms **3,760** of them – and these can go directly to the developers to fix
- Your security team now has only **240** exploitable vulnerabilities to check manually, taking 240 hours a year instead of 10,000
- 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.

Organizations no longer need to choose between tedious manual verification or flooding developers with trust-eroding false positives.

And that’s just the beginning – **other benefits include**:

- **Lower risk of costly outages and breaches** through improved security
- **Thousands of developer hours saved** through faster and more effective vulnerability fixes
- Shorter release cycles for **faster business growth**
- **Improved collaboration** between security and development teams

Focus on real, exploitable vulnerabilities

Proof-Based Scanning works by safely and automatically exploiting web vulnerabilities. It incorporates more than a decade of security research, so if it can find and exploit a vulnerability, you know that cybercriminals could, too.

Stop wasting money, start improving security

Proof-Based Scanning cuts through the noise so you can spend your time and money on truly improving application security.