

INVICTI

AppSec ROI Calculator

Executive Explainer — Channel Enablement Tool

Prepared by Noel Slane, VP Global Channels & Alliances | July 2026

Executive Summary

The Invicti AppSec ROI Calculator is a channel enablement tool built to give our partner sellers and CAMs a credible, data-driven way to quantify the business value of Invicti in a prospect conversation. It translates Invicti's core platform capabilities — proof-based DAST, correlation engine, risk prioritisation, SAST/SCA contextualisation, and API discovery — into hard operational savings and a separately explained breach risk reduction figure.

The tool is fully interactive, built in HTML with no external dependencies, and available in two versions: a standalone branded file for direct sharing and a portal embed version for the Invicti partner portal. Every number in the output reconciles transparently to the inputs the prospect provides — there are no hidden assumptions or black-box calculations.

Why we built this

Channel partners and AE's selling Invicti consistently face the same objection at mid and late stage: "How do we justify the investment?" The tools available to address this have typically been generic ROI frameworks that don't reflect Invicti's specific differentiators — particularly the false positive reduction enabled by proof-based DAST, which is the single largest driver of operational waste in an AppSec programme.

The calculator was built to solve three specific problems:

- Seller / Partners lack a quantified value story tied to Invicti's actual capabilities rather than generic AppSec claims.
- Prospects underestimate the cost of false positives — the industry average is 71–88% of scanner findings, representing thousands of developer hours wasted on alerts that go nowhere.
- MTTR (Mean Time to Remediate) is widely cited but rarely connected to the specific levers Invicti improves — FP noise, proof-based context, and risk prioritisation. This tool makes that connection explicit and defensible.

What the tool does

The calculator takes six primary inputs from the prospect and produces a five-section ROI report, all calculated in real time in the browser.

Primary inputs

Number of developers	Total engineering headcount — drives vulnerability volume and FP waste cost
AppSec engineers	Security team size — drives triage tax and MTTR via the dev:AppSec strain model
Applications / APIs	Portfolio size — drives total scanner finding volume at 17.5 new vulns/app/month (Contrast Security 2025)
Developer hourly rate	Fully loaded cost — applied to all remediation and FP waste calculations
Current MTTR	Set by the organisation from their own data — Invicti improvement is derived from this, never assumed
Baseline FP rate	Defaults to 71% (Black Duck 2025 industry avg) — adjustable if prospect knows their own rate

The five output sections

- Section 1 — Operational metrics: MTTR improvement, false tickets eliminated, triage hours freed, dev:AppSec ratio with strain indicator
- Section 2 — Cost breakdown: Two columns (A: baseline, B: with Invicti), fully itemised with working shown for every line
- Section 3 — Operational savings (A - B): A single green banner showing the exact subtraction. This is the primary commercial figure.
- Section 4 — Breach risk reduction: Fully separate, in its own yellow-bordered section with the working shown. Guidance is included on when to present this (CISOs, risk officers) and when to exclude it (engineering, finance).
- Section 5 — Capability contribution: Maps the savings back to DAST validation, correlation engine, SAST/SCA, and API discovery — connecting the commercial output to the Invicti platform story.

How the model works

The calculator uses three independently validated models that interact:

1. Vulnerability volume model

Total scanner findings = applications × 17.5 new vulns/month × 12 months (Contrast Security Software Under Siege 2025). Real vulnerabilities are treated as a property of the organisation's codebase — Invicti does not change how many real vulnerabilities exist, it changes how many false tickets are raised to developers. With a 71% baseline FP rate, approximately 71% of all scanner alerts are false positives. Invicti

reduces this to 6% through proof-based DAST validation (Snyk 2024). This is the largest single driver of operational savings.

2. Dynamic MTTR model

The organisation sets their current MTTR. Invicti's improved MTTR is then calculated from three compound drivers:

FP noise reduction	Scales with the baseline FP rate. Higher FP rates mean more queue noise — removing it contributes up to 40% MTTR improvement at the industry maximum of 91% FP.
Proof-based context & fix guidance	A constant 25% per-ticket improvement from validated findings with exploit proof and remediation steps, reducing per-ticket research time (Contrast Security case study data).
Risk prioritisation	Scales with the dev:AppSec engineer ratio. At 20:1 (well staffed) this contributes 10%. At 100:1+ (high strain) it contributes 20%. A strain badge is displayed so the prospect can see their specific position.

The three drivers are combined using a compound formula $(1-(1-a)(1-b)(1-c))$ to avoid linear overcount. A floor of 14 days is applied — Invicti cannot overcome physical constraints like sprint cycles and deployment pipelines.

Fix time reductions per severity are derived from the combined MTTR improvement: criticals receive 90% of the gain (most complex, most research overhead), high 70%, medium 50%.

3. Breach risk model (Section 4 — separate)

Breach risk is calculated from the exploitation window — the gap between a critical vulnerability being disclosed and being fixed. Industry data shows attackers exploit critical vulnerabilities within approximately 5 days of disclosure (CISA KEV analysis). The baseline exploitation window is therefore the organisation's MTTR minus 5 days. The Invicti window is the derived Invicti MTTR minus 5 days. The risk reduction is the proportional shrinkage of that window, capped at 35% (conservative maximum). This is applied to an average breach cost from IBM's Cost of a Data Breach 2024 report, scaled to organisation size, multiplied by an annual breach probability from Ponemon Institute 2024 data.

Important: the breach risk figure is intentionally separated from the operational savings. It is presented in its own section with full working shown and guidance on when to include or exclude it. It is never added to the Section 3 operational saving.

Data sources and benchmark basis

Every assumption in the model is sourced from published 2024–2025 industry research. The key benchmarks are:

MTTR (critical vulns)	Edgescan 2025 (74.3 days critical avg); Veracode State of Software Security 2025 (252 days overall avg); Contrast Security (84 days with coordination overhead)
False positive rate	Black Duck DevSecOps Report 2025 (71–88% industry average); proof-based DAST FP rate 5–8% (Snyk State of Security 2024)
Triage burden	Pixee State of AppSec 2026 (80% of AppSec engineer time on triage; ~\$134K/engineer/yr wasted)
Fix cost per critical	IBM/Veracode/Snyk (25 hours labour per critical CVE at fully loaded developer rate; \$5K–\$12K per critical)
Vulnerability volume	Contrast Security Software Under Siege 2025 (17.5 new vulns/app/month)
Breach cost	IBM Cost of a Data Breach 2024 (\$4.88M enterprise global avg; scaled to \$2.5M mid-market, \$1.2M SMB)
Breach probability	Ponemon Institute 2024 (scaled to critical vuln exposure: 6% at low exposure, 12% moderate, 20% high)
Context & fix guidance gain	Contrast Security case study data (25% per-ticket improvement from validated findings with remediation guidance)

What has been delivered

Two production-ready HTML files have been built, tested, and are available for immediate deployment:

invicti-roi-calculator.html — Standalone version

- Full Invicti branding: dark hero header, purple accent scheme, Invicti logo, partner-facing footer
- Five clearly labelled sections as described above
- Four primary input sliders (developers, AppSec engineers, applications, developer cost) with MTTR prominently positioned as an organisation-set input
- Advanced inputs panel for AppSec engineer cost and baseline FP rate
- Three org-size presets: Enterprise (500 devs / 14 AppSec / 80 apps), Mid-Market (150/5/30), SMB (40/2/10)
- Self-contained — no server, no dependencies, no tracking. Opens in any browser.
- Suitable for: direct attachment in Slack or email to partners, hosting on a landing page, inclusion in partner enablement packs

invicti-roi-calculator-embed.html — Portal embed version

- Compact layout without site header/footer — designed to sit inside an iframe
- All the same logic and sections as the standalone version
- Drop-in ready for the Invicti partner portal using a standard iframe tag
- Recommended embed height: 1800px (auto-resize script available on request)

How partners use this in a sales conversation

The tool is designed to be used live with a prospect, not sent as a static document. The recommended flow:

- Open the tool at the start of discovery or during a technical evaluation conversation.
- Ask the prospect: "Do you know your current MTTR for critical vulnerabilities?" — set the slider to their number. If they don't know, the 84-day default is the Contrast Security benchmark and is a credible starting point.
- Ask: "How many developers do you have? How many AppSec engineers?" — these two inputs drive the dev:AppSec ratio and the strain-based MTTR model, making the output specific to their organisation.
- Walk through Section 2 line by line — the working is shown for every figure so the prospect can interrogate and adjust any assumption they disagree with.
- Present Section 3 (operational savings) as the primary commercial figure. This is a hard number derived from their inputs, not a vendor claim.
- Introduce Section 4 (breach risk) only if the audience is a CISO or risk officer. Frame it as: "This is a separate figure — an expected value model based on how much faster we close your exploitation window. Your CFO may prefer to leave this out of the business case and rely on the operational saving alone."

The tool is designed to be interrogated. If a prospect challenges an assumption, adjust the slider. The numbers move in real time and always reconcile. Transparency is the point.

Recommended next steps

Partner portal deployment	Embed invicti-roi-calculator-embed.html in the partner portal as a live tool. Requires web team to add a single iframe tag to the relevant portal page.
CAM enablement	Distribute invicti-roi-calculator.html to all CAMs via Slack with a brief talk track covering the five sections and when to use/exclude Section 4.
Prospect-facing version	Consider hosting the standalone version on a dedicated landing page (e.g. invicti.com/roi) that partners can link to directly in prospect emails.
Localisation	Developer cost defaults to \$96/hr USD. For EMEA/APAC conversations, the slider can be adjusted. A localised default could be set by region if needed.
Validation	The model benchmarks should be reviewed by the Invicti product marketing team annually as new industry reports are published (Contrast Security, Veracode, Black Duck, IBM CODB).

Integration	A future enhancement could connect to Salesforce opportunity data to pre-populate org size and auto-generate a PDF leave-behind for specific deals.
-------------	---

This document was prepared by Noel Slane, VP Global Channels & Alliances, Invicti Security. July 2026. All benchmark data sourced from publicly available 2024–2025 industry reports. Calculator figures are indicative and should be adjusted to reflect the specific prospect environment.