Invicti vs Portswigger Comparison

Guidance to Evaluate Burp Suite Enterprise:

- **Explore and validate capabilities:** basic/limited functionality vs effective capability
- **Clarify inclusions, exclusions, and scope:** services, support, infrastructure
- **Clarify product capability vs operator responsibility:** such as verifying vulnerability instances
- **Verify claims of scale — AppSec teams must be able to:**
  - Schedule scans for operator-defined periods
  - Complete scans quickly (and within defined periods)
  - Issue verified vulns for remediation with clarity for dev to fix, not research
  - Obtain accurate results, fostering collaboration and trust across dev and security
- **Clarify total cost to AppSec program:**
  - Licensing
  - Infrastructure
  - Staffing

Consider Total Program Cost Impact:

	Invicti Enterprise	Burp Suite Enterprise
Licensing	• Included in contract	• Included in contract
Infrastructure	• Included in contract	• Not included in contract
Staffing	• Minimal from Proof-based Scanning & Guided Success	• Additional labor: Significant ongoing manual effort to validate un-verified findings

Comparison of Key Capabilities:

Key Capability	Invicti Advantage	Burp Suite Enterprise Gaps
Accuracy & Coverage	• 7,000+ security checks, updated weekly by a dedicated security research team • Covers CWEs and CVEs • ~99.9% accuracy on vulnerabilities, (1 in 5000 FP rate) • SCA: covers open source risk • IAST: identifies vulnerable code location • Website Discovery	• Does not find CVEs (only CWEs) • No stats published on accuracy • Releases new checks, but also relies heavily on community contributions ○ *"Please note that extensions are written by third-party users of Burp, and PortSwigger Web Security makes no warranty about their quality or usefulness for any particular purpose."* • No IAST or SCA capabilities • No Discovery capabilities
Speed	• Shorter scan times and faster remediation times • Continuous R&D investment in speed • Proof-based scanning verifies 94% of high severity vulns removes need to manually check results • Faster remediation with IAST • WAF integrations allows for automated virtual patching	• Slower scan times, often >twice as long as Invicti scans (based on internal tests and customer feedback) • Slower time-to-remediation as results have to be manually checked for false positives • No WAF integrations
Automation	Integrations: • CI/CD pipelines: Jenkins, TeamCity, Azure Pipelines, Circle CI, Bamboo, GitHub Actions, GitLab CI/CD • Ticketing: Jira, Gitlab, Trello, Service Now, Azure Boards, Defect Dojo • Communication: Slack, MS Teams • WAF: AWS, F5, Imperva • Vuln Mgmt: ServiceNow Vuln Manager, Kenna More at: https://www.invicti.com/integrations • Schedule scans and set scan windows	Integrations: • CI/CD pipelines: Jenkins, TeamCity • Ticketing: Jira, Gitlab, Trello • Communication: Slack • No scan windows • No incremental scanning (only full scans)
Services	• Support: standard global support 24/5 and premium 24/7 support • Guided Success: dedicated AppSec experts (white glove service)	• Email support only, limited to UK business hours