



# Dynamic Application Security Testing (DAST)

## Validated results. Enterprise scale.

DAST is an “outside-in” or “black box” analysis of a running web application by simulating interactions as an attacker, or that of a malicious logged in user, to discover vulnerabilities and weaknesses. Traditionally, security teams leverage scanning tools to perform DAST across their web application footprint. Automated DAST tools are being branded as *automated* or *continuous* penetration testing solutions, but the reality is, if it is completely automated then it is simply DAST. As any application security expert will tell you, the output of DAST scanning is notoriously *noisy*, full of false positive results, which leaves someone to triage the report.

Edgescan DAST leverages proprietary scanning technology managed and configured by our team of penetration testers, hackers, and security experts, with all outputs automatically validated using the Edgescan Platform’s vast data lake of vulnerabilities or manually by the same team of experts. The Edgescan Platform has its own network vulnerability scanning technology — Edgescan Network Vulnerability Management (NVM) — the service simultaneously runs vulnerability assessments against the application’s hosting infrastructure, achieving full stack visibility, as part of Edgescan DAST. In short, Edgescan DAST provides validated, actionable, and risk-based prioritization of vulnerabilities across all applications and their underlying hosting infrastructure under a “single pane”, scaling your application security program at the speed of the enterprise.

Edgescan *Dynamic Application Security Testing (DAST)* is a software as a service, sold as an annual subscription. For more information on how Edgescan can help secure your business, contact: [sales@edgescan.com](mailto:sales@edgescan.com)

### Key Features and Benefits

**API Discovery:** Continuous detection of APIs across your external footprint.

**Unlimited DAST Assessments:** Automation and analytics, coupled with our certified experts, deliver unparalleled accuracy of vulnerability data across your environment.

**Full Stack:** Includes Edgescan Network Vulnerability Management (NVM) for underlying hosting infrastructure.

**Certified Experts:** Edgescan is a CREST certified organization, combining years of experience with top industry accreditations to deliver industry-recognized foremost service.

**100% Validated Results:** False-positive free vulnerability intelligence prevents wasted cycles between teams.

**Integrated Threat Feeds:** CISA KEV Catalog and EPSS quickly identify vulnerabilities that have been exploited or are likely to be exploited in the wild.

**Risk-Based Scoring:** Traditional vulnerability risk scoring frameworks coupled with Edgescan’s Validated Security Score (EVSS) and Edgescan eXposure Factor (EXF) allows users to quickly contextualize and prioritize which vulnerabilities to fix first.

**Retesting On Demand:** Confirm vulnerability remediation was successful.

**Customized Reporting:** Provide appropriate levels of detail to your stakeholders, on-demand or on a schedule.

**Flexible Integrations:** Route vulnerability data, alerts, and notifications to your existing third-party systems out of the box or via Edgescan’s API.

**Premium Support:** Dedicated support from a certified pen testing team. AI Insights provides real-time tactical advice to assist in immediate security posture improvement.