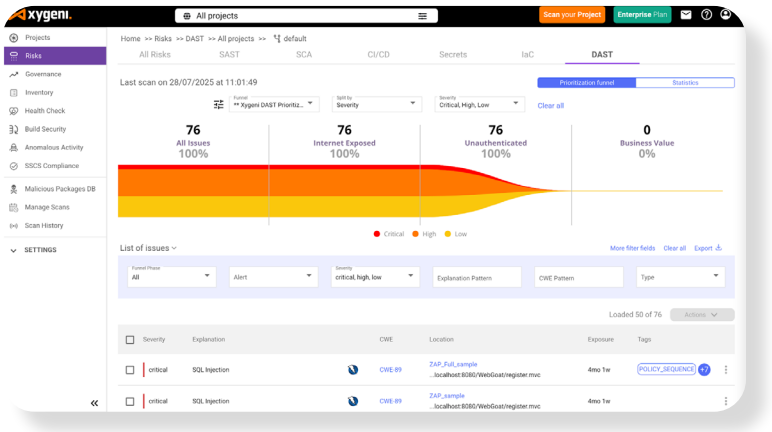
DAST

Solution Brief

xygeni.

Runtime Security That Starts Where Attacks Begin

Stop real-world vulnerabilities. Expose exploitable risk. Fix faster.



Dynamic Application Security Testing (DAST) analyzes running web applications and APIs to identify real-world vulnerabilities from an attacker's perspective. By simulating live attacks against deployed services, Xygeni DAST uncovers exploitable flaws such as SQL injection, cross-site scripting (XSS), authentication weaknesses, and runtime misconfigurations that static analysis alone cannot detect.

With actionable insights and risk-based prioritization, security and development teams can focus on fixing the vulnerabilities that truly impact production environments.

About Xygeni

Xygeni specializes in enhancing software development security and efficiency with our Application Security Posture Management (ASPM) platform. We offer complete control over application risks, a unified security view from code to cloud, and eliminate noise to prioritize risks effectively. Our advanced malware detection and early warning system makes Xygeni a leader in protecting applications from emerging threats, ensuring rapid and secure software delivery.

Dynamic Application Security Testing (DAST) plays a critical role in modern application security by identifying vulnerabilities in running applications before attackers can exploit them. Unlike static analysis, DAST evaluates applications from the outside, simulating real attack techniques against live web services and APIs. This allows security teams to detect runtime vulnerabilities such as SQL injection, cross-site scripting (XSS), authentication flaws, and misconfigurations that may only appear once an application is deployed.

The importance of runtime testing continues to grow as organizations adopt cloud-native architectures and API-driven applications. The global DAST market is projected to reach between **$3 and $4 billion by 2025**, growing at an annual rate of **15–20%**, and expected to exceed **$7 billion by 2030**. At the same time, security risks are increasing: **57% of organizations experienced an API-related breach in the last two years**, highlighting the need to validate runtime exposure before vulnerabilities reach production.

These trends reinforce the importance of integrating runtime security testing into modern DevSecOps pipelines.

57%
of organizations experienced an API-related breach in the last two years.

DAST

Solution Brief

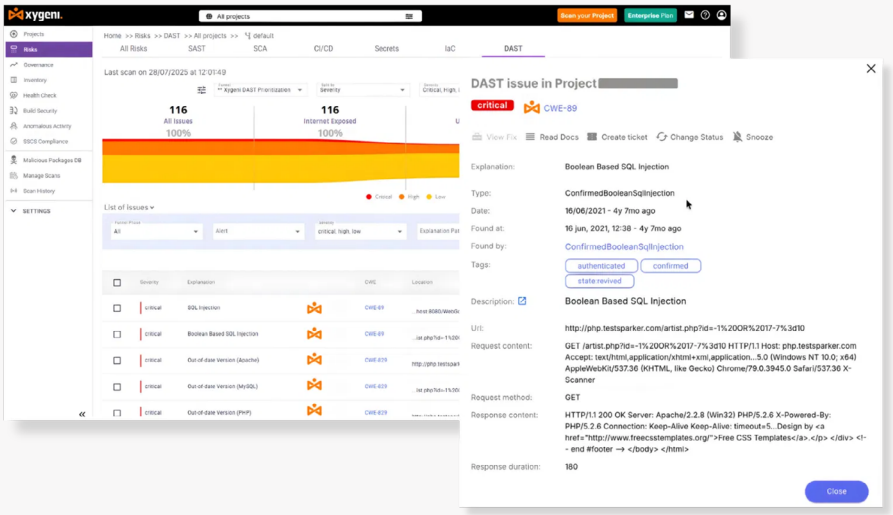
Runtime testing that reveals exploitable vulnerabilities

Xygeni DAST analyzes running web applications and APIs to detect security vulnerabilities that can be exploited in real runtime conditions. By simulating real attack techniques against deployed services, the platform identifies weaknesses such as SQL injection, cross-site scripting (XSS), authentication flaws, and configuration issues that may remain invisible during static analysis.

Integrated within the Xygeni ASPM platform, DAST findings are automatically correlated with code analysis, open-source vulnerabilities, asset exposure, and business context. This unified approach allows teams to focus on vulnerabilities that represent real risk in production environments.

How Xygeni DAST Works

Xygeni DAST continuously tests running applications and APIs by simulating real-world attack techniques. The platform combines automated scanning, contextual risk analysis, and ASPM correlation to identify exploitable vulnerabilities and prioritize remediation.



1. Discover and Scan

The xy-dast scanner analyzes running web applications and APIs, automatically crawling endpoints and launching dynamic security tests against exposed functionality.

2. Detect Runtime Vulnerabilities

The scanner identifies exploitable vulnerabilities such as SQL injection, cross-site scripting (XSS), authentication weaknesses, server-side issues, and security misconfigurations.

3. Correlate Risk in ASPM

The scanner identifies exploitable vulnerabilities such as SQL injection, cross-site scripting (XSS), authentication weaknesses, server-side issues, and security misconfigurations.

4. Prioritize What Matters

Findings are filtered through the Xygeni Prioritization Funnel, highlighting vulnerabilities that are externally exposed, unauthenticated, and relevant to business-critical systems.

5. Fix Faster in DevSecOps

Security findings are integrated into CI/CD workflows, enabling teams to remediate vulnerabilities earlier in the development lifecycle.

DAST

Solution Brief

xygeni.

Enterprise-Ready Dynamic Scanning with xy-dast

Xygeni DAST is powered by xy-dast, an enterprise-grade dynamic security scanner designed for automated runtime testing, CI/CD integration, and detailed vulnerability reporting. Built with a CLI-first architecture, xy-dast enables security teams to automate dynamic scans across development, testing, and staging environments.

Scans can be launched with a single command: `xy-dast scan -u <target_`

This approach allows organizations to continuously validate the security posture of running applications and APIs throughout the SDLC.

- **CLI-driven automation:** Trigger dynamic scans easily from scripts, pipelines, or testing environments using a single command.
- **Flexible scan profiles:** Built-in profiles support traditional web applications, single-page applications (React, Angular, Vue), REST APIs defined with OpenAPI or Swagger, quick smoke scans, and deep maximum-coverage scans.
- **Authenticated application testing:** Scan applications behind login using form authentication, bearer tokens, custom headers, JSON bodies, or script-based authentication workflows.
- **CI/CD pipeline integration:** Integrate seamlessly with DevSecOps pipelines using CLI execution, Docker images, and quality gates that fail builds when vulnerabilities exceed defined thresholds.
- **Detailed vulnerability reporting:** Each finding includes severity, CWE classification, attack payload, affected endpoint, HTTP request/response evidence, and remediation guidance.
- **Exportable security results:** Reports can be exported in structured formats such as JSON or PDF for automation, audit, and SIEM integration.

Xygeni DAST Prioritization Funnel

The Xygeni DAST Prioritization Funnel progressively reduces the number of vulnerabilities by applying contextual filters that identify the most critical risks. This approach removes noise and helps security teams focus on vulnerabilities that are externally reachable, exploitable without authentication, and relevant to business operations.

- **All Issues:** Complete set of vulnerabilities detected by DAST scanners.
- **Internet Exposed:** Filters vulnerabilities affecting assets that are publicly reachable from the Internet.
- **Unauthenticated:** Highlights vulnerabilities that can be exploited without valid credentials.
- **Business Value:** Prioritizes issues affecting critical applications, services, or business workflows.

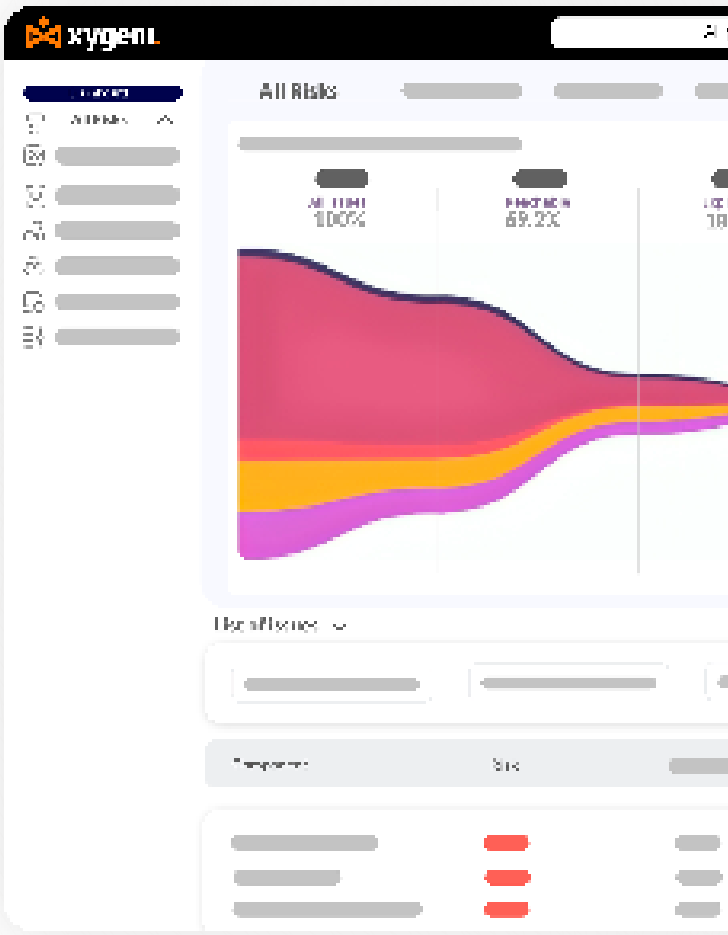
By progressively filtering findings through these stages, security teams can quickly identify the vulnerabilities that pose the greatest risk to production systems.

xygeni.

Secure Your Applications with Xygeni-DAST

Detect exploitable runtime vulnerabilities, simulate real attacks, and protect your applications, all in one powerful platform.

- **No credit card needed**
- **Quick setup, instant results**



Start your free trial

Get in touch today!

www.xygeni.io
https://www.linkedin.com/company/xygeni
https://twitter.com/xygeni