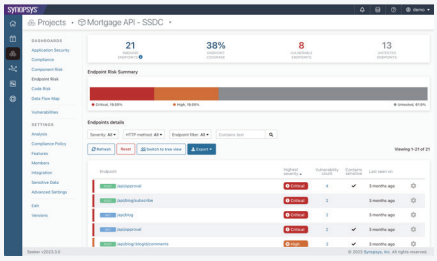
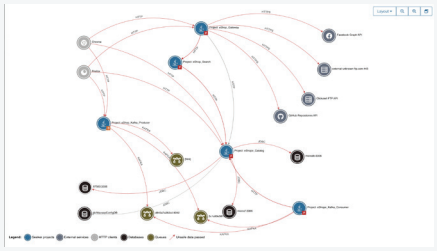
# Seeker
## 交互式应用安全测试

### 易于使用的企业级IAST，可准确识别并验证漏洞



全面的仪表板视图，展示了从应用程序到所涉组件和API的主要安全漏洞。



以图表形式即时提供详细的测试覆盖和数据流跟踪信息，并显示被测系统的架构，包括从各种来源流入应用程序的数据，不同系统组件之间的数据流，以及对第三方API和web服务的外部调用。

## 概述

Seeker® Interactive Analysis是我们的交互式应用安全测试(IAST)解决方案。通过Seeker，您可以一目了然地查看Web应用的安全状况，并且发现违反合规标准（如OWASP Top 10、PCI DSS、GDPR、CAPEC 和CWE/SANS Top 25）相关的漏洞趋势。Seeker使安全团队能够找出并跟踪敏感数据，确保它们得到安全处理，而不会存储在未加密或弱加密的日志文件或数据库中。Seeker还能无缝集成到DevOps CI/CD工作流中，以实现持续的应用安全测试和验证。

与其他只能发现安全漏洞的IAST解决方案不同，Seeker能够判断安全漏洞（如XSS或SQL注入）是否可以被利用，从而为开发者提供一个按风险优先级排序的已验证漏洞列表，以便他们可以立即在代码中修复漏洞。使用专利方法，Seeker能够快速处理数十万个HTTP(S)请求，发现漏洞，并将误报率降至近乎为零。这使得安全团队能够优先关注真正已得到验证的安全漏洞，极大地提高工作效率并降低业务风险，就像有一个自动渗透测试团队全天候检测Web应用一样。

Seeker可以在运行中的应用内部使用代码插桩技术（代理），并且可以通过扩展来满足大型企业的安全需求。它提供开箱即用的准确结果，无需复杂、冗长的配置。Seeker提供详细的漏洞描述、可行的修复建议和堆栈跟踪信息，还能识别出易受攻击的代码行，因此不要求开发者具备深入的安全知识。

Seeker能够持续监控任何类型的Web应用测试，并与自动化的CI构建服务器和测试工具无缝集成。Seeker可基于这些测试（例如登录页面的手动QA或自动功能测试）自动生成多个安全测试。

Seeker还包含了我们的软件组成分析(SCA)解决方案“Black Duck Binary Analysis”，用于识别第三方和开源组件、已知漏洞、许可证类型和其他潜在的风险问题。Seeker和Black Duck的分析结果以统一视图呈现，并且可以自动发送到开发者选择的缺陷跟踪和协作系统，以便开发者作为正常工作流的一部分对其进行分级处理。

Seeker可将单个应用的多个微服务绑定在一起进行评估，因此非常适合基于微服务的应用开发。

Seeker可以分析微服务之间的数据流，从而对整个系统进行分析，而不是只关注不相关的单个应用。Seeker通过HTTP(S)、gRPC和共享数据库等途径跟踪数据流。

## 持续、快速、实时地提供可操作的结果

全面的分析结果中包含了修复漏洞所需的全部信息：

- 对风险的清晰解释
- 运行时内存值和上下文
- 技术描述
- 易受攻击的代码行
- 基于上下文的相关修补说明

分析结果通过多个详细的窗格显示数据流和恶意插入参数的影响(如动态SQL拼接)，还会显示检测到的漏洞是否已被自动验证为可以利用，或者排除为误报。

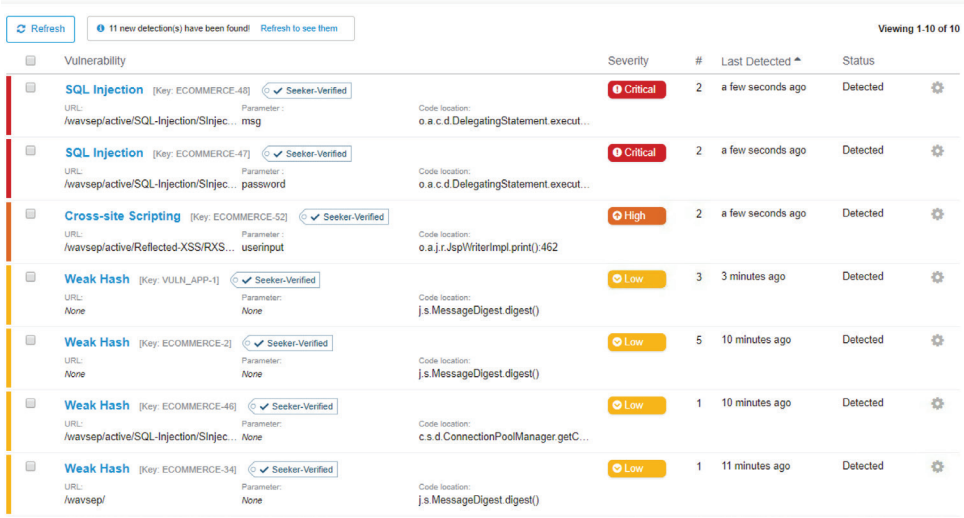
Seeker还集成了Black Duck Binary Analysis和SCA，因此能够将应用的二进制文件发送到组成分析系统，并将结果上传到Seeker的仪表板。

# 具有主动验证功能的唯一企业级IAST解决方案

Seeker独特的主动验证功能使其能够处理数十万个HTTP(S)请求，并快速排除检测到的漏洞中的误报，确保误报接近于零。为了提高测试覆盖率，Seeker的参数识别功能可以检测出未使用的参数，并使用恶意值重新测试它们，从而探索更多潜在的应用攻击面、隐藏参数和后门。

好处:

- 极大地提高安全和开发团队的生产力。
- 降低动态应用安全测试(DAST)或手动渗透测试的总体成本/所需资源。




# 易于部署和使用

Seeker使用仪表化技术和运行时分析技术来持续监控、识别和验证Web应用中的安全漏洞，通常是在集成测试与QA阶段之间、甚至一直到软件开发生命周期(SDLC)的生产部署阶段。无论应用是部署在本地、基于微服务、无服务器函数还是云端，Seeker都能够支持现代应用开发方法和技术。只需在应用程序运行代码的每个层或节点(如Docker容器、虚拟机和云实例等)安装代理，它们就能跟踪应用的运行情况，并实时提供分析结果，无需进行任何额外的扫描。

Seeker不仅能够逐行分析代码，并实时关联数据流和运行时代码的执行情况，而且还能检查代码与敏感数据微服务的交互，以及跨应用层和组件的API调用。该技术能够识别出对关键数据构成真正威胁的漏洞，包括其他技术无法检测到的某些复杂漏洞和逻辑缺陷。

Seeker还与eLearning和Secure Code Warrior集成，为开发者和DevOps团队提供上下文相关的帮助和培训，以便他们深入了解漏洞，并实时轻松地修复漏洞。

## 立即开始使用Seeker

- 无缝融入CI/CD工作流。本机集成和Web API使得Seeker能够与您的现有工具无缝集成，协同支持本地、云端、基于微服务和基于容器的应用开发。
- 快速轻松地部署。Seeker提供开箱即用的实时分析功能，误报几乎为零。
  - 开箱即用的准确性，无需复杂的配置或调整
  - 无需网站登录凭证或特殊扫描
  - 主动验证。可以结合输入验证库和自定义功能来清理输入内容（如SQL注入漏洞）
  - 可在大型企业环境中扩展
- 支持几乎任何类型的测试方法。Seeker的非侵入式被动监控选项使其能够与现有的测试自动化、手动或功能测试以及自动网络爬虫等测试方法配合使用。

# 详细的测试覆盖，包括应用程序和微服务的API发现、跟踪和数据流图

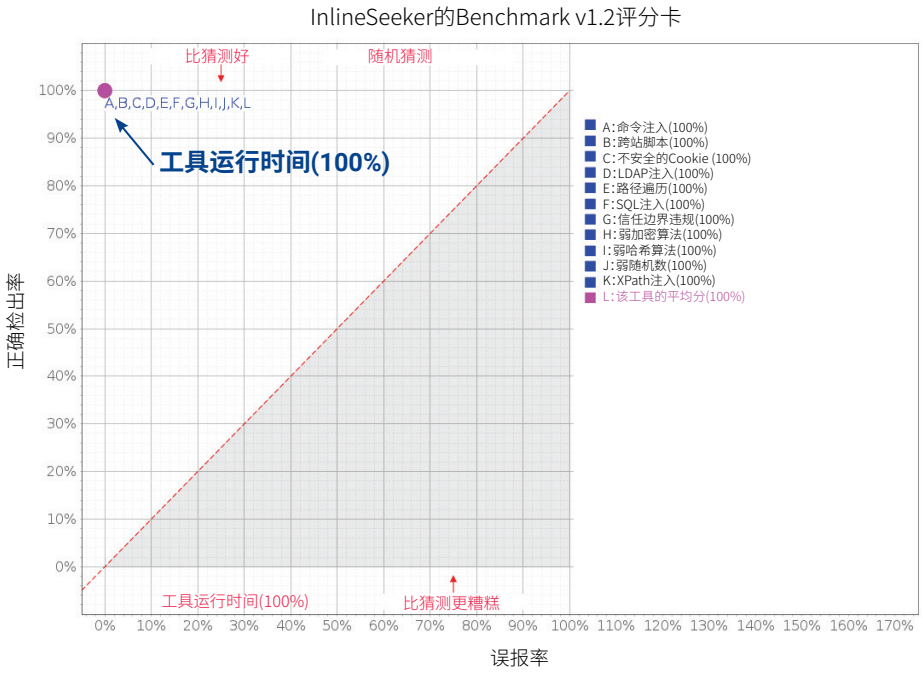
借助自动URL映射、API发现和端点跟踪，可以全面了解Web应用测试的覆盖情况。Seeker以图形方式显示已测试和未测试的内容，同时以图表方式显示数据流映射，以帮助您进行有效的污点分析。您可以轻松比较同一应用不同版本之间的覆盖差异。

主动验证功能可以自动生成一系列请求，以提高基于OpenAPI/Swagger和Graph-QL的应用的测试覆盖率。

# 敏感和机密数据跟踪

Seeker独一无二的敏感和机密数据跟踪能力为业界首创。用户可将数据标记为“敏感”（如信用卡号、令牌和密码），这样，只要这些数据未经加密存储在日志、数据库或文件中，便可以及时对其进行跟踪。跟踪敏感数据可以帮助您满足PCI DSS以及其他行业标准和法规（如GDPR）的数据加密要求。与手动检查相比，这将能够帮助您极大地提高生产力，并节省时间、成本和资源。

# OWASP基准测试最高分



# Seeker | 技术规格

### 支持的语言
- ASP.NET
- C#
- Clojure
- ColdFusion
- Go
- Gosu
- Groovy
- Java
- JavaScript (Node.js)
- Kotlin
- PHP
- Python
- Scala (incl. Lift)
- VB.NET

### 支持的平台
- Java
  - Any Java EE server
  - GlassFish
  - Red Hat JBoss Enterprise Application Platform
  - Red Hat JBoss Web Server
  - Tomcat
  - WebLogic
  - WebSphere
- .NET Framework
  - IIS
  - WCF
  - OWIN
  - SharePoint
- .NET Core
- Node.js
- PHP

### 运行时/框架
- .NET/CLR
  - ASP.NET MVC
  - Enterprise Library
  - Entity Framework
  - NHibernate
  - Ninject
  - NVelocity
  - OWASP ESAPI
  - SharePoint
  - Spring.NET
  - Telerik
  - Unity
- GO
  - Chi
  - Echo
  - Gin
  - Net/http
- Java/JVM
  - Enterprise JavaBeans (EJB)
  - Grails
  - GWT
  - Hibernate
  - Ktor
  - Micronaut
  - OWASP ESAPI
  - Play
  - Ring
  - Seam
  - Spring/Spring Boot
  - Struts
  - Vaadin
  - Velocity
  - Vert.x
- Java Runtime:
  - AdoptOpenJDK
  - Amazon Corretto
  - Eclipse OpenJ9
  - IBM
  - Oracle HotSpot
  - OpenJDK
  - Red Hat OpenJDK
- Node.js
  - Express
  - Fastify
  - Hapi
  - Koa
- PHP
  - Laravel
  - Symfony
- Python
  - Django
  - Flask

### 技术
- 数据库
  - NoSQL DB
    - Cassandra
    - Couchbase
    - DynamoDB
    - HBase
    - MongoDB
- 关系型数据库管理系统/SQL
  - DB2
  - HSQLDB
  - MS SQL
  - MySQL
  - PostgreSQL
  - SQLite
  - Oracle
- 应用程序的类型
  - Ajax
  - JSON
  - 微服务
  - Mobile (over HTTP/S)
  - RESTful
  - 单页应用程序
  - Web (包括HTML5)
  - Web APIs
  - Web服务
- 进程间通信
  - HTTP(S)
  - gRPC
  - Kafka
  - Apache Dubbo
  - RabbitMQ
  - JMS
  - 数据库表

### 云平台
- Azure PaaS/Azure Function
- AWS
- AWS Lambda
- Google Cloud
- Tanzu (PCF)

## Black Duck与众不同

Black Duck® 提供业界最全面、最强大、最值得信赖的应用安全解决方案组合。我们拥有无与伦比的专业知识和经验，来帮助世界各地的组织机构快速保护其软件，在其开发环境中高效集成安全性以及使用新技术进行安全创新。作为软件安全领域公认的领导者、专家和创新者，Black Duck拥有您构建可信软件所需的一切。如预了解更多信息，请访问www.blackduck.com。