



Seeker[®]
Agile Software Security

Every build,
Every release,
Every application,
Secured

| SEEKER[®]

Quotium's **Seeker software** enables organizations to produce secure software efficiently.

It provides very high accuracy in vulnerability detection during the software building and testing process. Seeker conducts a unique approach, analyzing code and data flows in runtime to better understand vulnerability context. This approach makes it possible to confirm or disprove the exploitability of detected vulnerabilities with no need for human intervention.

Seeker ties vulnerable code to business impact and exploitation, providing a clear explanation of risks.

Seeker completely eliminates false positives.

Seeker gives a clear view of the security state of applications according to compliance criteria and provides everything needed to secure code and improve security awareness.

The highly accurate results and straightforward UI make it easy to embed into any software development process



| AGILE SOFTWARE SECURITY

Using agile methodologies for web application development is becoming the standard in new projects. There is evidence that Agile delivers higher quality and greater efficiency with reduced “build and change” costs. Essentially Agile delivers value, adaptability, progress visibility and fit against requirements.

The agile software development approach makes building secure software challenging while security is often neglected because of the short time-to-market. Existing approaches for extending agile development processes fall short of providing a method for efficiently ensuring the security of software increments produced at the end of each iteration. As a result, agile software products may lack security protection.

Most security methodologies are built around traditional development methods, which are qualitatively and quantitatively different from agile development. Traditional security methodologies such as code review are sequential while agile is iterative. Integrating heavy weight activities with agile processes may lead to a situation that cannot be Agile and be unacceptable for project teamwork.

Quotium’s Seeker software security solution has been designed to be fully integrated in the agile process. Seeker addresses the three main requirements to comply with agile development processes:

→ Accuracy

Seeker completely eliminates false positives. Seeker conducts runtime analysis of both code and data, to better understand vulnerability context and impact. **Seeker automatically verifies findings by exploiting them** in order to classify their risks. The result is the identification of critical and complex vulnerabilities and logical flaws not detectable with any other technology.

→ Time-to-market

Developers stay on course by focusing their time on fixing vulnerabilities which pose a real threat to the business. Stakeholders know exactly what are the risks of each build and release and can take appropriate decisions.

→ Automation

Seeker test cycles are short and can be included as part of the Agile «build and test» process. Seeker integrates with automatic testing frameworks like Selenium to automatically build an attack scenario. Seeker can be launched from the build server alongside automated functional testing. Results are delivered in formats already used for bug reporting such as ticketing systems. By integrating with the complete Agile & DevOps tool chain, **Seeker provides a strong security automation process.**

“SEEKER HAS BEEN DESIGNED TO BE FULLY INTEGRATED IN AGILE PROJECTS, ALLOWING ALL STAKEHOLDERS TO WORK TOGETHER TOWARDS THE COMMON GOAL OF SECURE SOFTWARE”

BRIDGING THE GAP BETWEEN INFORMATION SECURITY AND SOFTWARE DEVELOPMENT

Software development is concerned with creating software according to customer requirements in the minimum amount of time. Information security is concerned with finding and removing security vulnerabilities and releasing secured software. In order to build secure applications it is important to align application development and security practices.

The separation between security and development working in two different silos has produced software development efforts that lack a thorough contemporary understanding of technical security risks.

These two communities of highly skilled technology experts exist in isolation, yet their knowledge and experience bases are largely complementary. Eliminating silo functionality is difficult and collaboration is essential.

"WHEN CHOOSING SEEKER WE WANTED TO FIND A SOLUTION THAT DEVELOPERS DON'T RESENT"



Seeker addresses three main requirements to help security experts and developers to communicate:

→ **Simplicity**

Seeker does not require any security expertise to operate or to understand its results. Seeker brings simplicity into the SDLC: it adapts itself to the existing process rather than requiring the process to adapt to it.

→ **Clarity**

Seeker speaks the developer's language and provides clear and actionable results to correct the code. Seeker gives the accuracy the security team needs to manage risks across the enterprise.

→ **Awareness**

Seeker helps developers understand the consequences of their insecure coding. By explaining risk and remediation, Seeker is an integral part of security awareness and training programs across teams in the organization.

"SEEKER IS THE
PERFECT TOOL TO
HELP US IMPROVE OUR
SECURITY PRACTICE
TO BUILD EXCELLENT
SOFTWARE"



| COMPLIANCE

PROTECTING YOUR DATA

Compliance requires that you ensure all Web-facing applications are protected against known attacks. If you must store credit card data & sensitive data and are interested in strengthening your current security practices, you have to focus attention on your Web application's security and data handling.

Quotium's Seeker software is a solution that understands how sensitive data is handled by the application - including when stored, transmitted, and when in memory. It tracks data throughout its lifespan across application tiers & components.

Seeker automatically identifies sensitive data, monitors where it flows, and determines whether it is encrypted or not, regardless whether the data is at rest or in motion. Seeker alerts to the lack of SSL controls and cookies, but it also alerts specifically to payment card information being transmitted insecurely. Applications sometimes inadvertently leak confidential information through error messages. These leakages may include security configurations, internal workings, or payment card data.

Seeker's unique technology allows the monitoring of web-service, database and file system calls in the path of sensitive data in order to detect any insecure storage or manipulation.

Seeker monitors where sensitive data is stored and whether data retention and disposal policies are violated. This makes Seeker a strong solution to answer critical compliance requirements such as the PCI-DSS standard.





Seeker addresses three main requirements to help organizations achieve security compliance and governance:

➔ **A continuous security process in the SDLC**

Seeker provides a continuous vulnerability assessment & remediation process across all development projects. It ensures that information security is designed and implemented within the development lifecycle of information systems in accordance with security policies and standards.

➔ **Data risk management**

Seeker looks at vulnerabilities in the context of user data in the application. Seeker explains in simple terms the concrete risks, allowing stakeholders to easily prioritize actions and build a vulnerability management plan.

➔ **Cross-organizational security dashboards**

Seeker gives security managers the ability to monitor and report - at any time - the security risk level and compliance status of all web applications and development projects in the organization

About Quotium

Quotium develops innovative software solutions that guarantee the security and performance of business critical applications throughout their lifecycle. Quotium pioneered Interactive Application Security Testing (IAST) with its security testing software Seeker.

NEW YORK

575 Madison Avenue, 25th fl. New-York, NY 10022, USA
Tel: 212-935-9760 - Fax: 212-755-6385

LONDON

4 Park Place London SW1A 1LP
Tel: +44 (0) 203 178 3681 - Fax: +44 (0) 207 898 9101

PARIS

84/88 bd de la Mission Marchand 92411 Courbevoie Cedex
Tel: +33 (0)1 49 04 70 00 - Fax: +33 (0)1 49 04 71 66

Contact : sales@quotium.com

Follow us on Twitter [@quotium](https://twitter.com/quotium)

www.quotium.com

Quotium