# Fortify Audit Assistant

**Triaging and validating raw static analysis results is the most time intensive process within application security testing. Fortify Audit Assistant leverages past audit decisions to power machine learning-assisted auditing—validating results immediately and dramatically reducing auditing effort.**

## Product Highlights

### Current Challenges with Securing Applications

As the world becomes more connected than before, businesses rely heavily on applications to succeed. To meet business expectations, developers face tight deadlines and ambitious feature, functionality requirements. Software vulnerabilities are a serious problem introduced by mistake, through poor software security practices, or intentionally by internal threat actors. One of the best methods to avoid negative impact is to develop code with quality and security in mind from the early phases of development.

### Static Application Security Testing

Static application security testing (SAST) is a great method to ensure that code is being developed without security issues and these issues (if any) are fixed early in the development process. SAST provides the enterprise with the intelligence necessary to identify, monitor, and reduce the business risk from an application's source code and provides recommendations to remediate issues. It has been widely recognized as a necessary component of securing the digital enterprise for nearly two decades.

### Auditing SAST Results

SAST takes application source code or binaries and returns raw scan results (set of potential issues) which are then audited by human auditors. Auditors validate and prioritize true positives, eliminate false positives (or "uninteresting findings" depending on context) and add additional insight to findings. Developers then receive the audited and validated list of issues to work on fixes.

Auditing raw static scan results is the most time consuming and effort intensive aspect of SAST and requires a skill set that's often difficult to find and keep. The scan results from a scan that takes minutes to run can take days or weeks for human auditors to review and validate. With traditional methods, auditing of raw scan results continues to be one of the significant bottlenecks for application security and makes it harder for security teams to deliver the speed requirements of developers. Combined with the skills shortage in application security, auditing raw scan results can become a challenge for organizations, especially for organizations running application security programs at scale. Human auditors are typically a resource that is very difficult to scale, and Fortify Audit Assistant is ready for the challenge.

### Leveraging Machine Learning for Auditing

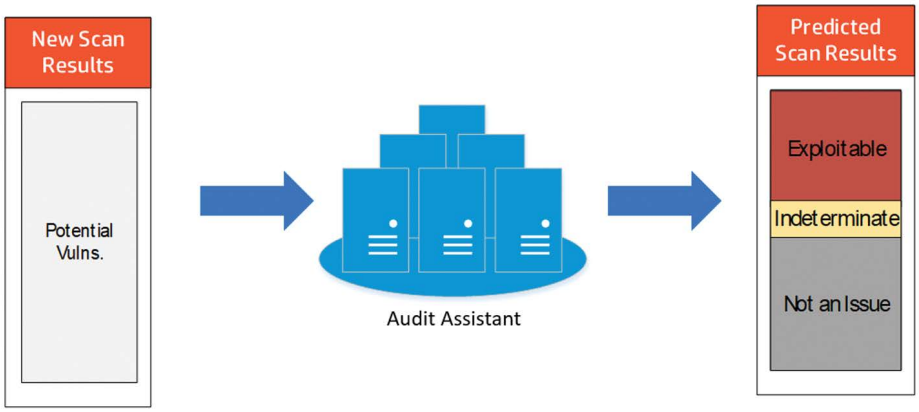
Fortify has been the industry leader in static application security testing for over a decade and is no stranger to the problems above. In addition to continuous customer feedback, we operate our very own application security as a service offering (Fortify on Demand), running thousands of static, dynamic and mobile scans per week, scanning billions of lines of code. Static application security testing service of Fortify on Demand takes customer application source code or binaries and runs scans, then passes these raw scan results to the team of expert auditors who are subject matter experts. Auditors point out and prioritize the noteworthy findings while removing the noise from the results. Consequently, Fortify on Demand customers receive actionable results and can primarily focus on fixing these issues.

Over the years, Fortify developed machine learning algorithms which feed off of the hundreds of millions of anonymized audit decisions from Fortify on Demand experts. These decision models have been tested and verified to provide up to 98% accuracy in addition to being actively used and developed for Fortify on Demand. These expert decisions can now be automatically applied to Fortify Static Code Analyzer results by using Audit Assistant.

### How Does Audit Assistant Work?

Audit Assistant leverages the knowledge and experience of these previous audit decisions and applies them for scan results with similar patterns. The audit decision model offers immediate value using these models, can be customized for organizational preferences and context. Customers can also opt to create their own audit decision models and leverage their previous audit decisions to do so.

Machine learning assisted identification of relevant scan results




Audit Assistant integrates with Software Security Center (SSC) and customers can opt to auto-apply analysis tags or review these automated audit decisions before applying in their environments. It is available as a cloud hosted service offering or as an on-premise installation.

Audit Assistant validates raw static scan results immediately and reduces manual audit effort.

## Key Benefits

- Get immediate and actionable results to developers,
- Reduce manual audit time and effort by up to 30%,
- Identify and prioritize high impact issues (with up to 98% accuracy),
- Remove up to 90% of false positives.

## Key Features

- Start getting audit results in minutes by using Fortify on Demand's dataset comprised of subject matter experts audit decisions
- Start with as a service in minutes—with no local installation, configure SSC and get audit results,
- Deploy on-premise for isolated networks,
- Create and train your own classifiers & policies for your organization's unique context with regards to auditing
- Benefit from up to 98% audit decision accuracy from the start, continuously improve the accuracy through feedback.

Learn more at
**www.microfocus.com/appsecurity**

Whitepaper: Increase Efficiency with Automated Auditing of Static Scans with Fortify

Contact us at **CyberRes.com**
Like what you read? Share it.

760-000029-001 | M | 04/21 | © 2021 Micro Focus or one of its affiliates. Micro Focus and the Micro Focus logo, among others, are trademarks or registered trademarks of Micro Focus or its subsidiaries or affiliated companies in the United Kingdom, United States and other countries. All other marks are the property of their respective owners.

CyberRes
A Micro Focus Line of Business