CyberRes

Article

Fortify's Latest and Greatest

New Features of Fortify 21.1 Release

Fortify 21.1: Build Secure Software Fast

General Availability—Fortify 21.1.0 Release

We are excited to announce the general availability of our Micro Focus Fortify 21.1.0 release! With enhanced offerings to increase speed, accuracy, scalability, and ease of use, this marks an important chapter in Fortify's elevation of application security. This release contains updates to Fortify Static Code Analyzer, Fortify WebInspect, Fortify Software Security Center, and Fortify Software Composition Analysis.

Fortify SAST

SAST Speed Dial

Have better control of the speed and accuracy of your static testing by tuning the depth of the scan based on application need. Increase scan speeds **by 50%** by utilizing commit and CI dial settings, saving deep SAST scans for when you need them. The following features have been added to SAST Speed Dial:

- Added level 3 and 4 support.
- Improved intermediate development scan speeds by up to 50% (with a reduction in reported issues).
- Reduced scan time for typed languages such as Java and C/C++.
- Level 4 support provides a full scan.

ScanCentral SAST

ScanCentral enables scaling with a static analysis farm that can meet the changing demands of the CI/CD pipeline. The following features have been added to ScanCentral SAST:

- ScanCentral SAST Support in Secure Code Plugins
  - ScanCentral SAST support added to Eclipse Complete Plugin, IntelliJ Analysis Plugin, and Visual Studio Extension.
  - You can now submit ScanCentral SAST scan requests from the plugin.
  - Added support for both local translation and remote translation

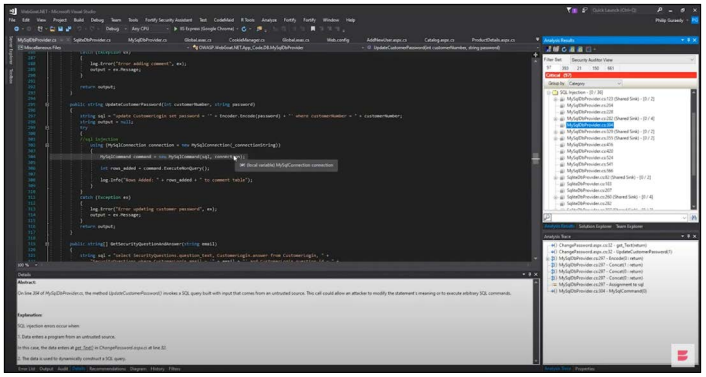

Figure 1. ScanCentral SAST in the IDE

- Improved Job Processing Messages
- New -debug Option
- Improved Sensor Cleanup
- Maven Remote Translation
- New Email Properties

Syntax Highlighting for Additional Languages in Audit Workbench

- Adds syntax highlighting for the following languages: ABAP, Apex, ASP, C# and ASP.NET, COBOL, Cold Fusion, Go configuration files, Kotlin, Objective C, PHP, Python, Ruby, Scala, Swift, VB.NET and Visual Basic 6.0.

New Versions of Reports

- DISA STIG 5.1
- NIST 800-53 Revision 5
- CWE Top 25 2020

These can be generated from Fortify Audit Workbench, the secure code plugins, and the BIRTReportGenerator command-line interface.

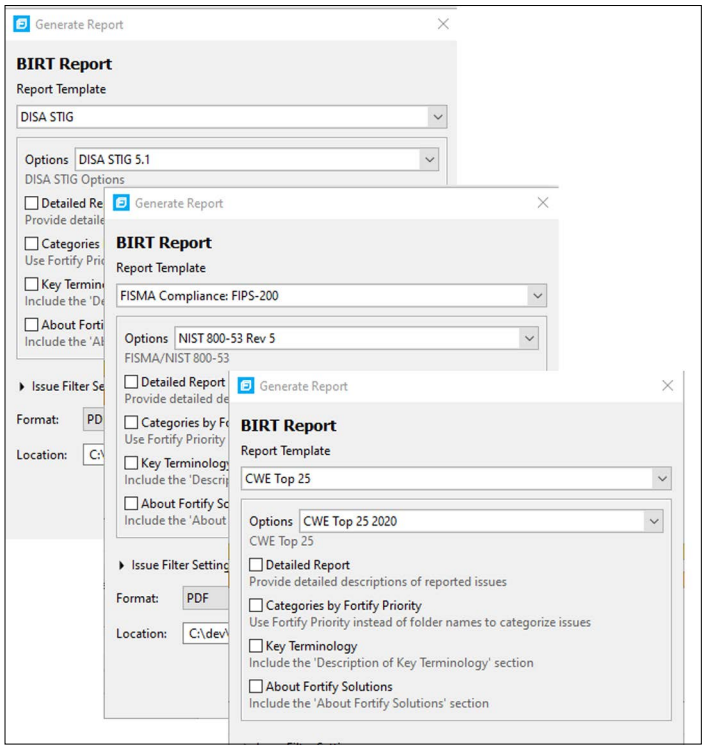

Figure 2. New reports in 21.1

Updated IDE Support

- Added support for Eclipse versions 2020-x and 2021-x in Micro Focus Fortify Plugins for Eclipse.
- Added support for Eclipse version 2021-x in Micro Focus Fortify Security Assistant Plugin for Eclipse.
- Added support for versions 4.x of Android Studio in Micro Focus Fortify Plugins for JetBrains IDEs and Android Studio.

Service Integrations

- Added support for Azure DevOps Server 2020.

Fortify SAST Language Support

Fortify SAST provides accurate support for **27**+ major languages and their frameworks, with agile updates backed by the industry-leading Software Security Research (SSR) team. We're adding many new supported languages versions, and in a few cases have fundamentally improved and simplified how we work.

The following language updates have been added to Fortify Static Code Analyzer:

.NET

Added support for the following languages and frameworks:

- .NET 5.0
- C# 9
- ASP.NET Blazor

To improve MSBuild integration, the custom msbuild executable and its assemblies were replaced by a Fortify-specific .targets file and task assemblies. These changes favorably impact translations under MSBuild Integration performed by the system's MSBuild tool.

MSBuild Support Update

Added support for version 16.8 and 16.9.

Go

- Added support for Go versions 1.15 and 1.16
- Added support for the GOPROXY environment variable

Java

- Updated JSP translation produces fewer false positives
- Improved bytecode analysis

JavaScript

Added support for the following languages and frameworks:

- TypeScript 4.1
- Angular 10 and 11

Kotlin

Added support for Kotlin 1.4.20

PHP

Added support for PHP 7.2, 7.3, 7.4, and 8.0

Python

Added support for the following languages and frameworks:

- Python 3.9
- Django 3.1

Swift/Obj-C

Added support for Xcode 12.4

Operating Systems (Linux)
Added support for the following Linux servers:

- SUSE Linux Enterprise Server 15
- Red Hat Enterprise Linux 8.2
- CentOS Linux 7.6-1810 and 8.2-2004
- Ubuntu 20.04.1 LTS

Micro Focus Visual COBOL (Technology Preview)
Added support for Micro Focus Visual COBOL 6.0.

C/C++ (Technology Preview)
Improved support for constructs in C++11 using new Clang-based translation.

Fortify ScanCentral DAST

With our next generation dynamic application security testing capabilities, you can enable, scale and automate DAST in your CI/CD process using ScanCentral with the existing Fortify Jenkins and Fortify Azure plugins, creating a more holistic AppSec approach. The following features have been added to ScanCentral DAST:

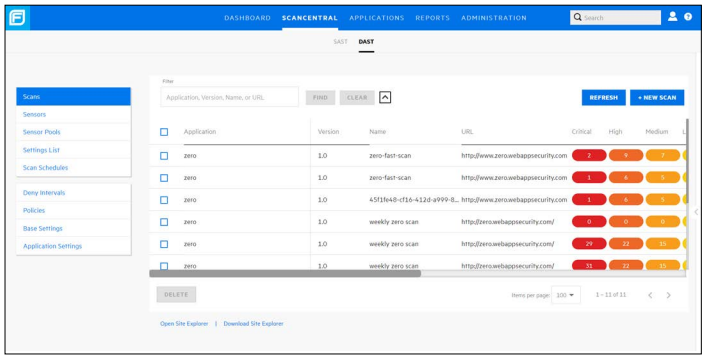

Figure 3. ScanCentral dashboard in SSC

Functional Application Security Testing (FAST)
FAST provides a CI/CD-friendly way to capture traffic from functional tests and send it to ScanCentral DAST for targeted DAST scanning. Unlike IAST, FAST is not limited by what the person creating the test thought of. FAST scans against your app but then keeps crawling to find everything your functional test didn't expose.

API Scanning with Postman
In 21.1.0, ScanCentral DAST continues to simplify API scanning with its Postman integration. A new workflow in the WebInspect sensor automatically detects the authentication requests and excludes them from attack by default. There are also improvements to Oauth2.0 support.

Hacker Level Insights
Hacker Level Insights is a new framework that exposes those insights about an application that are interesting from a security perspective, but not necessarily a vulnerability. Detection of JavaScript client-side frameworks is included in 21.1.0.

Data Retention Policies
Configuring data retention policies at the application or scan level allows automatic purging of stale data to support ScanCentral DAST database maintenance and system performance in high usage environments.

Deny Intervals
ScanCentral DAST supports application and scan-level deny intervals when currently running scans are paused or forced to complete, and new scans do not start.

Base Settings
Base Settings provide ScanCentral DAST administrators the ability to apply scan setting templates across all applications or specific applications. Admin can pre-configure a scan template and provide that to users to scan their apps—no security knowledge required.

Policy Import
ScanCentral DAST supports using custom policies at both the application level and scan level.

Alerting
A messaging framework displays information about the quality and performance of scans in progress.

SiteExplorer Download
A link is provided in ScanCentral DAST to download SiteExplorer for visualization of a scan.

Horizontal Scaling (Technology Preview)
Horizontal scaling of sensor script engines provides dramatically faster scanning.

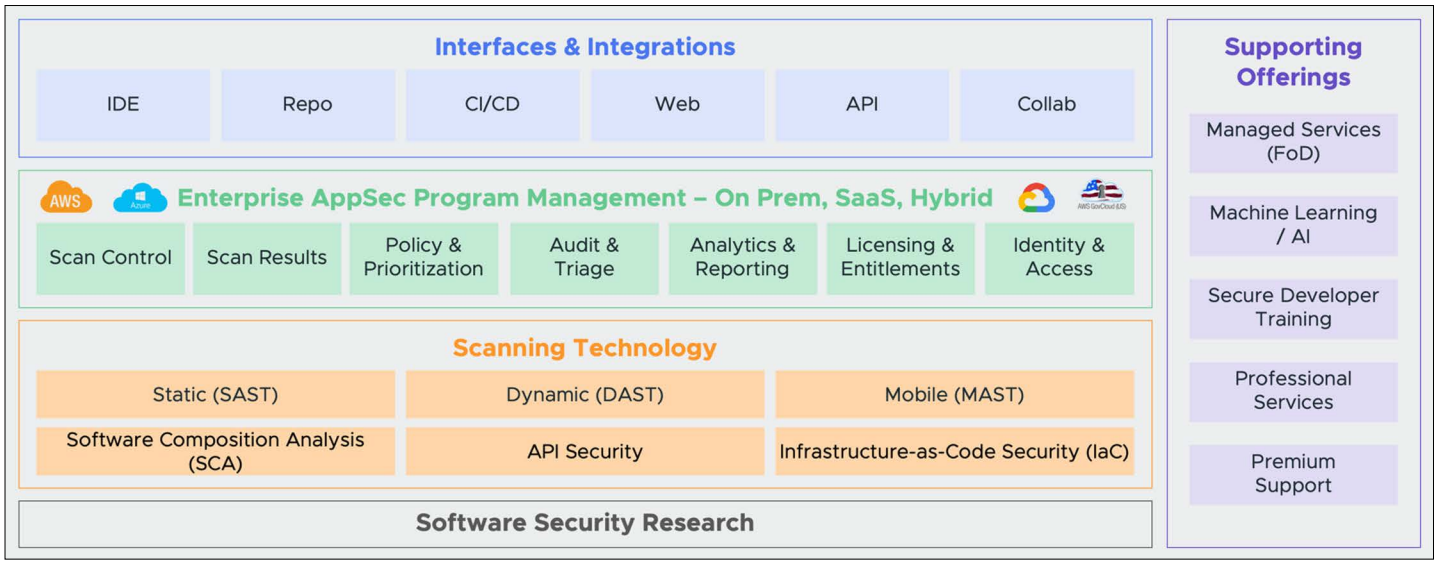

Figure 4.

Fortify DAST

HTTP/2 Support
Modern applications have begun leveraging HTTP/2 to improve the user experience with improved speed and more efficient client/server communication. WebInspect now supports applications that use HTTP/2 technology.

Engine 6.0 Updates
Fortify continues to enhance its engines to improve scan coverage and performance. WebInspect 21.1.0 provides a faster crawl and audit, and better application support from the Web Macro Recorder with Macro Engine 6.0.

Masked Parameters in TruClient
The Web Macro Recorder with Macro Engine 6.0 allows values for parameters such as password to be masked so they are hidden from view.

Watch our on-demand webinar What's New in Fortify 21.1 where Fortify Head of Product Management Dylan Thomas presents our key strategy of Fortify moving forward, as well as outlining the exciting roadmap currently in development for the upcoming year.

Simplified User Agent Selection
Selection of a User Agent in settings during scan configuration is now applied to both TruClient macros and the scan settings.

Alerting
Alert-level scan log messages provide information about the quality and performance of scans in progress.

OpenSSL
The OpenSSL technical preview is now the default SSL/TLS implementation in WebInspect. This integration provides support for TLS 1.3, and provides an option for customers whose system administrators may be restricting the Microsoft SCHANNEL stack.

API Scanning with Postman
WebInspect continues to simplify API scanning with its Postman integration. A new workflow in the sensor automatically detects the authentication requests and excludes them from attack by default. There are also improvements to Oauth2.0 support.

Learn more at
www.microfocus.com/en-us/cyberres/application-security

Contact us at **CyberRes.com**

Like what you read? Share it.

CyberRes
A Micro Focus line of business