Hewlett Packard Enterprise

HPE Security Fortify Software

What's New

What's New in HPE Security Fortify Software 16.20

December 2016

Note: The 16.20 release of the HPE Security Fortify Software products was released in two stages. Some of the products in this document were released in September of 2016. This document covers all programs and components that make up the 16.20 release of HPE Fortify Software.

This release of HPE Security Fortify Software includes the following new functions and features.

HPE Security Fortify Software Security Center

The following features have been added to HPE Security Fortify Software Security Center.

Issue-Level Search

Now you can use standard Fortify search syntax to query your documents for information. This function is available from the Audit tab (Issues page) when working at the application version level.

CloudScan Sensor Pools

If your Fortify Software Security Center server is integrated with Fortify CloudScan and you are an Administrator, Manager, or Security Lead, you can create groups of CloudScan sensors, or Sensor Pools. Sensor Pools can be based on any criteria, which you can then target for scan requests.

If a scan request is associated with an application version, the CloudScan Controller queries for available Sensor Pools. Alternatively, CloudScan clients can request a specific Sensor Pool for a

scan request. Sensor Pools give you more control over what sensors are used for scan requests. Here are a couple of examples of how you might use Sensor Pools:

Create pools based on sensor computing power (size of physical memory) and assign scan requests that require a lot of memory to those pools.

Create pools based on teams or business units in your organization. When your resources are distributed, no group can consume resources earmarked for other teams or business units.

Audit Assistant

Audit Assistant provides access to HPE Security Fortify Scan Analytics, allowing you to use historical scan data and artificial intelligence to automatically identify which issues are "True Issues" that require remediation, and which issues are "Not an Issue" and don't require attention.

You can use Fortify Community Intelligence data (pooled, anonymized data from Fortify users), data that your security team has completed, or data from both sources. This data provision is referred to as training. Audit Assistant's assessments regarding the actual threats that issues represent become more accurate as it receives more training data.

New Custom Tags

New custom tags provide greater specificity and flexibility in auditing issues.

- Date
- Decimal
- Text

Issue Stats Dashboard

The Issue Stats dashboard page shows issue status summary information, such as the number of days it takes to review and fix them.

Performance Improvements

Performance has been improved in the following areas:

- Handling user concurrency
- Loading of events into the event log

Batch Auditing

You can now save time by selecting multiple issues with the Shift key, allowing you to audit them at the same time.

RESTful API

Updated to include GET endpoints in Swagger.

Cascading FPR Approval

In previous releases, if you approved one of multiple FPRs, the others were automatically approved. In this release, you can disable that functionality so that multiple FPRs are not automatically approved if one is approved.

HotKeys

Hotkeys can now be disabled from the user profile settings.

JIRA 7

Added support version 7 of the JIRA software development tool.

Permissions Handling

Resolved permissions access issue in the Application Wizard and other areas of the program.

Conflict Resolution Strategies

New configurable strategy option added to Fortify Software Security Center administration to control how audit conflicts are resolved.

New BIRT Reports

Added support for PCI 3.2 and DISA STIG 3.10.

Velocity Templates

Each supported bug tracking system has an associated Apache Velocity template that maps issue information to description and summary fields in the bug tracking application. When you submit a bug for one or more issues, the fields for the bug description and summary are automatically populated in the bug tracking application, and the description field contains a link to the issue or issues in Fortify Software Security Center.

You can edit these templates to include mappings of additional text and text area fields. You can also create your own Velocity templates for bug submission.

HPE Security Fortify Static Code Analyzer

The following features have been added to HPE Security Fortify Static Code Analyzer.

Swift Improvements

Fortify Static Code Analyzer now allows you to scan source code written in Swift 2.2. The features supported in this release include:

- Data flow scan
- Semantic scan
- Control flow scan
- Better object interoperability
- Higher order analysis

.NET

- .NET source code analysis is faster and more robust
- You can now scan Windows Azure applications
- Eliminated the need for the pre-compile step required in previous versions

Gradle Support

Fortify Static Code Analyzer has made it easier to scan code through Gradle via an integrated plugin.

The workflow is similar to that with Ant, Make, or Maven.

Incremental Analysis

Fortify Static Code Analyzer now supports incremental scanning. After performing a baseline scan of the entire code, you can run incremental scans, reducing the amount of time required to run successive scans.

Objective-C for Xcode 8.0, 8.1

Fortify Static Code Analyzer now supports scanning Xcode projects in Objective-C for Xcode 8.0 and 8.1.

HPE Security Fortify Static Code Analyzer Tools

The following features have been added to HPE Security Fortify Static Code Analyzer Tools.

New Plugin for Visual Studio 2015

New Visual Studio plugin based on Microsoft's new VSIX platform for Visual Studio extensions.

- Works with the latest version of the Visual Studio IDE
- Admin privileges are not required to install the extension
- Can be installed on machines without HPE Security Fortify Static Code Analyzer
- Scans Azure and Modeling projects

Team Foundation Server Support

- File bugs to Team Foundation Server from within HPE Security Fortify Audit Workbench and the HPE Security Fortify plugins for Eclipse

JIRA 7 Support

- File bugs to JIRA 7 from within HPE Security Fortify Audit Workbench and HPE Security Fortify Plugins for Eclipse

New Custom Tags

New custom tags provide greater specificity and flexibility in auditing issues.

- Date
- Decimal
- Text

Scanning in Fortify Plugin for Eclipse

With Advanced Scan, you can now analyze other languages in addition to Java from the plugin; JavaScript projects, PHP projects, C/C++ projects, and any other project type supported by HPE Security Fortify Static Code Analyzer.

New BIRT Reports

Added support for PCI 3.1, PCI 3.2, DISA STIG 3.10, and DISA STIG 4.1.

HPE Security Fortify WebInspect

Silent Installation

- Unattended installation of Fortify WebInspect from the command line or a script
- No user interaction is required when installing; the installation is not blocked by UI popups

WIConfig Program

- Allows you to override default configuration settings after installation
- Configuration settings such as DB settings can be configured automatically
- Can be invoked using a script
- Enables configuration changes during silent install

Support for PKI/CAC - Common Access Card Readers

- Now supports client authentication through certificates generated from a common access card (CAC) reader connected to your computer
- Available for Guided Scans, Basic Scans, and when creating a new proxy file in the Traffic Viewer tool
- Enables customers using CAC-based authentication for login to conduct WI scans

Reuse Scan Settings

- Scan Reuse command-line parameter and configurable options enable you to create a settings file that uses the same settings as a source scan
- Options include using crawl sessions from the source scan and modifying the policy
- Reusing settings helps to optimize scans and improve scan speed

WISwag Tool

- A command line tool that parses a REST API definition and converts it into a macro or settings file that Fortify WebInspect uses for auditing
- Use the Swagger REST API definition to automate the scanning of API
- Enhanced audit capability to scan REST API services

OData Protocol Support

- Ability to fuzz the individual parameters in an OData filter
- Improves vulnerability detection and ability to audit

Multipart/Mixed Format Support

- Parameter manipulation engines now support stepping into multipart/mixed format
- Enhanced Audit capability

REST API

- Swagger support for the REST APIs provides a visual representation of the API and includes detailed schema, parameter and example code information to enable you to more tightly integrate with Fortify products
- API documented in Swagger definition format
- Added new endpoints

DOM Explorer

- Improved memory management and depth of discovery in single page applications (SPAs)
- Improved DOM state crawling
- Reduced memory usage and improved accuracy
- User experience improvement

Site Explorer Findings Tab

- New Findings tab provides the ability to review vulnerabilities discovered during a scan and verify evidence
- User experience improvement; part of overall strategy for evolution of WebInspect UI

Site Explorer and Traffic Viewer Parameters Detail View

- Both Site Explorer and Traffic Viewer now include a Parameters detail view that displays the Type, Name, and Value of parameters embedded in an individual traffic session
- The Parameters detail view displays a grid with one record for each cookie or query string used in the traffic session
- You can view every traffic record in which the same parameter is used

Hewlett Packard Enterprise

Platform and Dependency Support

Platform support has been broadened to include:

- Windows 10
- SQL Express 2014
- .NET Framework 4.6.1

HPE Security Fortify WebInspect Enterprise

REST API

- Swagger support for the REST APIs provides a visual representation of the API and includes detailed schema, parameter and example code information to enable you to more tightly integrate with Fortify products
- API documented in Swagger definition format
- Enhanced the REST API for WebInspect Enterprise with new endpoints

Contacting HPE Security Fortify Support

If you have questions or comments about using this product, contact HPE Security Fortify Technical Support using one of the following options.

To Manage Your Support Cases, Acquire Licenses, and Manage Your Account

https://support.fortify.com

To Email Support

fortifytechsupport@hpe.com

To Call Support

1.844.260.7219

For More Information

For more information about HPE Security software products:
http://www.hpe.com/software/fortify

Hewlett Packard Enterprise

What's New in HPE Security Fortify Software Security Center 16.10

April 2016

This release of HPE Security Fortify Software Security Center includes the following new functions and features.

HPE Security Fortify Software Security Center

- Common Access Card (CAC) support
- Kerberos/SPENGO support
- Updated help when requesting a new account or logging in
- RESTful API v1 documentation
- REST API access with limited action tokens
- New CloudScan Controllers, CloudScan Sensors, and CloudScan Scan Requests interfaces
- Bugtracker support for Team Foundation Server
- Improved job management performance and reliability
- You can now cancel and change job priority (of prepared jobs)
- Improved performance for out of order scan processing
- Improved performance when deleting scan artifacts
- Unlock user accounts (Admin)
- Advanced "Copy From" options are now available when creating a new Application version
- Show more records on the dashboard on user request
- Administratively disable/enable legacy UI
- Change user passwords in the new UI
- Variables and Performance Indicators are now available in the Version level trend chart
- Aggregate/Filter/Group by all custom attributes at the global dashboard level
- Aggregate/Filter/Group by custom tags at the application version level
- User persistence across user sessions (some selections)
- Group by Folder on issue page
- Enable email alerts for logged in user

- Multiple LDAP configuration moved to Administration page and support for multiple LDAP servers added
- Syntax highlighting for Swift
- HPE Security branding

HPE Security Fortify Static Code Analyzer (SCA)

- Support for Objective-C++
- Performance improvement for the Higher Order analyzer
- Initial support for Swift
- Improved @ModelAttributes for SpringMVC
- Improved DOM/selector support for jQuery
- Xcode 7.3 support
- HPE Security branding
- Quality improvements for
  - Java translator
  - Javascript translator
  - Rule processing
  - JSP translator
  - C/C++ translator

HPE Security Fortify Runtime Products: Runtime Application Logging, Runtime Application Protection, and WebInspect Agent

- Support for Syslog-NG connection using UDP, TCP, and TLS connections
- Support for event deep-link in the ESM CEF events
- Improvements to SLQi detection and prevention
- Performance improvements
- Bug fixes and stability improvements

Hewlett Packard
Enterprise

HPE Security Fortify Static Code Analyzer Tools

- New Maven plugin with enhanced Maven support
- BIRT reporting for Visual Studio Plugin
- Improved usability of SCA Analysis and Translation errors for AWB and Eclipse plugin
- Group by FileType added to Audit Workbench
- Custom rules support for Security Assistant
- Xcode 7.x support
- Improved Team Foundation Server bugtracker integration for Visual Studio plugin
- Jenkins plugin now supports 1.652
- HPE Security branding

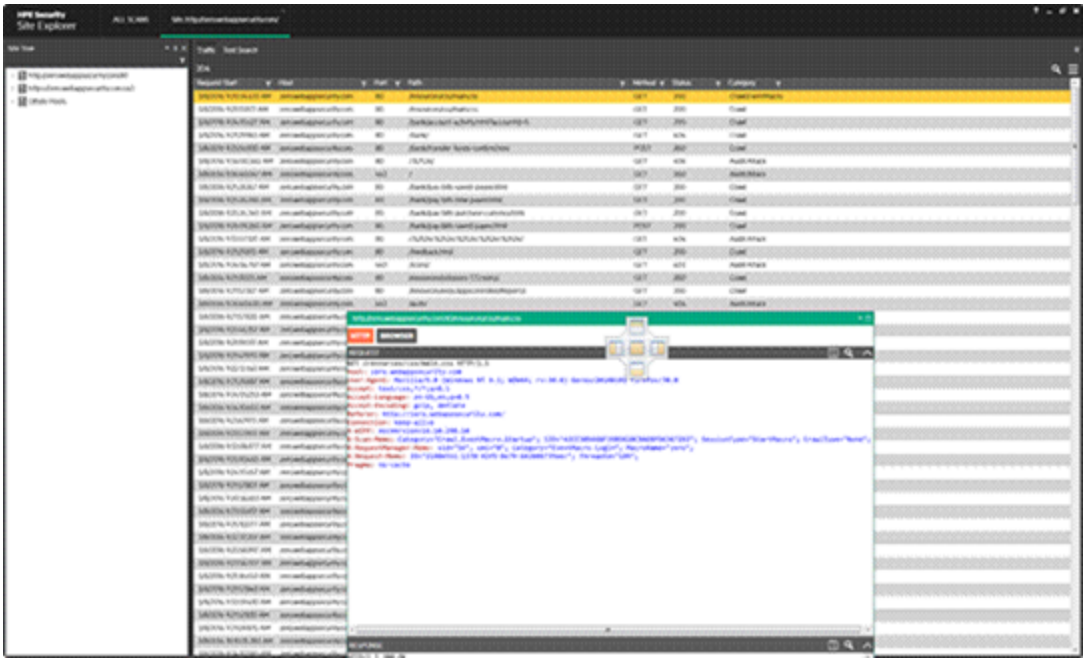
HPE Security WebInspect

- **Site Explorer**

  After working with customer feedback about numerous designs, we have begun to reimagine and restyle the WebInspect user interface (UI). To give our users a first glimpse at the new UI style and allow them to provide feedback, we have released our work as a separate tool that can be accessed from within WebInspect. The tool is called Site Explorer, and is available in this release as a technology preview. Although the work is not complete, users can view their own scan data, previously completed or currently running, inside the new UI. The vulnerability review section, however, has not been implemented and is not available in this version of the tool.

  One of the top priorities for this UI redesign has been performance. Site Explorer runs as a separate process, allowing Windows to better distribute resources between the UI and the scanning engine. We have also created a new file type called the TSF which functions as a virtual database. The structure of this new format allows Site Explorer to load scan files in an incredibly short order, which will save users valuable time in triaging results.

  To better accommodate our users of various skill levels, we have included multi-window capabilities and advanced search functionality throughout Site Explorer. Currently the site tree, traffic grid, and the detail views can be floated and docked to any part of the UI or moved to another screen as seen below. Additionally, the request/response for an open session can be cloned to create a duplicate request/response.



The traffic grid shows all of the traffic data from the scan. Each session can be drilled down into and parent sessions and related traffic are easily accessible. The traffic can be searched with plain text, using special commands such as server, type, or origin ID, or filtered based on the column data.

- **DOM Explorer**

  DOM Explorer is another technology preview tool that customers can use to crawl single-page applications (SPAs) or other "Web 2.0" sites that make heavy use of JavaScript and other client-side technologies. The term DOM stands for Document Object Model and is defined by W3C as "a platform- and language-neutral interface that will allow programs and scripts to dynamically access and update the content, structure and style of documents."

  The modern concepts of SPAs and JavaScript-heavy pages have proven a challenge for the traditional crawling and script engines used in DAST products. In order to overcome these challenges, we returned to the drawing board, creating our own engine which can navigate and understand the frameworks of "Web 2.0" sites. This new engine will provide WebInspect unparalleled control over the state of the DOM, allowing WebInspect to perform advanced testing techniques not currently available on the market.

  The DOM Explorer can be started either as an .exe or from the tools menu in WebInspect. Once started, users can enter a single URL to be scanned or use a login macro to authenticate and crawl the site. Instead of the usual site tree structure, users will see a DOM event tree listing the individual elements and events that are exercisable on the page. If possible, when a specific element is selected in the DOM tree, the affected area of the page will be highlighted in the browser view. The traffic that was captured from the crawl can be explored and saved as a workflow macro. This macro can be used in an audit-only scan in WebInspect to perform attacks against the site.

  It is important to note that the DOM Explorer is a technology preview and is not 100% complete as a feature. We have released it as a technology preview to enable our customers to begin

taking advantage of the new technology and to provide us feedback on its capabilities. As we continue to build out this functionality, it will eventually become a part of the default crawler behavior.

- **Updates to Traffic Viewer**

  Several UI features and functionality that were developed for Site Explorer have also been added to the Traffic Viewer tool. For example, you can customize the detail views, drill down in the Traffic grid view to see related traffic, and use breadcrumbs to help you navigate the traffic for a resource in the traffic grid.

- **New Audit Setting to Suppress Off-site Vulnerabilities**

  If your Web application includes links to hosts that are not in your Allowed Hosts list, WebInspect may identify passive vulnerabilities on those hosts. You can use the new Suppress Offsite Vulnerabilities to suppress all vulnerabilities against sessions for off-site hosts that are not in your Allowed Hosts list.

- **New Application Setting to Create Scan Data for Site Explorer**

  During a scan, WebInspect creates a SQL Express database (.mdf) file or adds the scan to an existing SQL Server database (.mdf) file. However, Site Explorer uses a variation of the traffic session file (.tsf) format. You can use the Create Scan Data for Site Explorer setting to have WebInspect create a traffic file that can be displayed in Site Explorer.

HPE Security WebInspect Enterprise

- **WebInspect Enterprise REST API**

  As part of the WebInspect Enterprise installation, a REST API service is installed. You can use the REST API to work with scans, scan settings files, scan schedules, projects, and other functions programmatically. The REST API includes a complete set of online documentation with code samples. For information about accessing the WebInspect Enterprise REST API and its documentation, see the HPE Security WebInspect Enterprise Installation and Implementation Guide.

- **Using SAN or Wildcard Certificates and Non-Standard Ports in IIS**

  The WebInspect Enterprise Initialization Wizard does not overwrite certificate and port bindings that you create in IIS. As a result, you can use SAN or wildcard certificates and non-standard ports when configuring the WebInspect Enterprise Manager Web Service during initialization.

- **New Options for HTTPS Bindings for the Root Web Site in IIS**

  If you have configured HTTPS bindings for the root web site in IIS, only those bindings will be listed in the Available Certificates. You will not be able to create a new binding for a web site in the WebInspect Enterprise Initialization Wizard. You can create a new binding only in IIS. Your options when configuring the WebInspect Enterprise Manager Web Service are now based on your IIS settings.

- **WebInspect Enterprise Manager Web Service Uses IIS Integrated Mode**

  During upgrade, the WebInspect Enterprise Manager Web Service (WIE server) will be set up in IIS using the IIS integrated mode for the application pool. This means that the WebInspect Enterprise web site no longer needs to have ISAPI filters configured or ISAPI and CGI restrictions configured in IIS. Integrated mode does not use either of these elements. The WebInspect Enterprise Initialization Wizard will no longer warn you if these elements are not configured in IIS.

- **WebInspect Enterprise Installation and Implementation Guide**

  The WebInspect Enterprise Installation Guide and the WebInspect Enterprise Implementation Guide have been combined into a single guide. The new HPE Security WebInspect Enterprise Installation and Implementation Guide contains all of the information from the two guides.

Hewlett Packard Enterprise

What's New in HP Fortify Software Security Center 4.40 and HP WebInspect 10.50 Products

November 2015

This release of HP Fortify Software Security Center includes the 10.50 release of WebInspect and WebInspect Enterprise. The WebInspect products were developed in conjunction with the 4.40 components and are an integral part of the HP Fortify Software Security Center 4.40 release.

Software Security Center (SSC)

- SSC now requires a case-sensitive collation for all databases.
- Performance improvements have resulted in decreased time for data purge, FPR processing, and report generation processing.
- SSC has an entirely redesigned user interface (UI) that's simpler and easier to navigate.
- The Dashboard now includes summary charts which, like tooltips, are visible when you move your cursor over findings for a "top risk maker."
- Entities that were termed "projects" in earlier versions are now termed "applications."
- Entities that were termed "project templates" in earlier versions are now termed "issue templates."
- SSA projects and process templates have not yet been migrated to the 4.40 user interface. However, for this release, you can work with SSA projects in the legacy user interface.
- The term "Collaboration Module" is no longer used.
- You have the choice of using the redesigned UI, the legacy UI (v4.30), or both.
- The **Runtime** and **CloudScan** tabs do not exist in the new UI. You can find this functionality in the legacy UI, but in order to use it, you must configure your Runtime and CloudScan connections in the new UI.
- The UI now contains an icon to alert you when application data displayed are not up to date. You can click this icon to refresh the data. The icon disappears when the refresh is complete.
- You cannot change the format for date and time display in the new UI. You must use the legacy Flex interface instead.
- You can now integrate SSC with SAML 2.0 or Oracle Identity Management providers for single sign-on.

- If your organization uses SAP NetWeaver Code Vulnerability Analyzer (CVA) to search for vulnerabilities in ABAP source code, you can now use the NetWeaver plugin to map your CVA scans to an SSC application version, and then import the results for investigation from SSC. SSC displays the individual CVA findings, identifies their source code file names and line numbers, assigns each a Fortify priority order, and displays them in the SSC UI for auditing.
- SSC now has robust, category-based search functionality that applies search terms across application versions, issues, reports, comments, and users. Its new search engine returns results almost instantaneously.
- To add an extra measure of security to BIRT reporting, you can create a database user account with read-only access to the SSC database, and then use the account credentials to configure BIRT reporting in SSC. For even greater security, you can also enable a strict mode for running reports in a separate Java process.
- If you are not an administrator and you need to change your own account information, including your password, you must revert to the legacy UI to make these changes. (See "Changing Your Account Information (Legacy UI)" in the documentation.)
- The new UI in this version does not support extensible custom tags, which enabled users to add new custom tag values during audits. The legacy UI still supports extensible custom tags, and allows users to use all the new values while performing an audit.
- The new UI does not support showing issue attachments. You must use the old UI for this functionality.
- If your single sign-on (SSO) server works with Security Assertion Markup Language (SAML), you can now integrate SSC with SAML 2.0.
- The legacy Flex interface does not work when run from WebLogic and accessed through Internet Explorer.

HP Fortify Static Code Analyzer (SCA)

- There are numerous fixes to the type inference engine for Java translation. As a result, many more expressions involving lambdas and type arguments are assessed correctly.
- Support has been added for iOS9 Objective-C applications in Xcode 7.
- Enhancements have been made to Higher Order Analyzer to improve performance and analysis capabilities.
- There is improved support and numerous bug fixes for JavaScript.
- SCAState has been updated with a `-liveprogress` option which displays a text window to provide a regularly updated interface of current scan progress and analyzer information. On Unix-like platforms, this feature uses the current terminal window if you use the `-nogui` option.
- Several Python bugs were fixed resulting in improved accuracy of analysis.
- Support has been added for all ColdFusion 9 and 10 tags and functions, as well as a number of syntax extensions. Future support is still needed for "components" and other ColdFusion 9 and 10 features.

- SSC now has extended support for Java coding and logic flaws.
- SAP ABAP support has been added for “Access Control: Authorization Bypass.”

Static Code Analyzer Tools

- A real-time, in-line Security Assistant Plugin for Eclipse has been added. The Security Assistant Plugin works with HP Fortify security content to provide alerts to potential security issues as you write your Java code.
- Support for Xcode Maven projects has been added to the HP Fortify Maven plugin.
- You can now run HP Fortify SCA scans on projects in the Xcode development environment (IDE) using the HP Fortify Scanning Plugin for Xcode.
- Audit Workbench now verifies all necessary permissions before downloading the FPR for collaborative audits. This feature helps to ensure that you can continue auditing results even if your connection to SSC is temporarily lost. Additionally, Audit Workbench can now recover when collaborative auditing loses connectivity to the server.
- Audit WorkBench and the Eclipse remediation plugin now provide BIRT reports. These are the same reports in content, look, and feel as the reports available in SSC. We will continue to expand the reports available in the other tools in future releases.
- The HP Fortify Maven plugin now supports CloudScan.
- The HP Fortify Jenkins plugin now supports Jenkins version 1.6.
- The Scan Wizard now supports Java bytecode.
- All tools now support Bugzilla 4.x.

WebInspect Version 10.50

- **Privilege Escalation**

  WebInspect can now test whether a lower-privilege user can gain access to pages and capabilities that should be available only to a user with higher-privilege rights. It does so by using two separate login macros to crawl the site for both users and then comparing the results to identify pages that the lower-privilege user does not have a link to but can access by direct navigation. With this capability, customers can now automate even more of their dynamic testing. For more information, see “About Privilege Escalation Scans” in the WebInspect help.

- **Traffic Viewer Tool**

  As a first step towards moving to a new style of user interface, the WebInspect team has created the new Traffic Viewer tool. This tool displays the traffic monitor data and will eventually replace the proxy tool. It is available in both WebInspect and WebInspect Enterprise, allowing traffic monitor data to be captured by a WebInspect Enterprise scan for the first time.

Having a separate tool to visualize the data means that customers can split the applications between multiple screens to visualize the scan progress or vulnerabilities while simultaneously parsing the traffic data. For more information, refer to the Traffic Viewer tool online help or the Tools Guide for WebInspect Products.

- **Selenium Support**

  WebInspect 10.20 made it possible for customers to use the WebInspect application program interface (API) to automate the capture of traffic from their Selenium scripts and translate it into a workflow macro. Over the last year, several customers asked us for improved integration with Selenium scripts to make it a more native integration. In this release, we have added native support for Selenium integrated development environment (IDE) scripts for use as both automated login macros and workflow macros. Customers who have other teams in their company using Selenium scripts for automated testing can now reuse those scripts to enhance the coverage of their WebInspect scans. For more information, see “Using Macros” in the WebInspect help.

- **Updates to the WebInspect API**

  As a part of our commitment to creating the most robust and flexible dynamic application security product on the market, we continue to expand our API with each release. In WebInspect 10.50, we have added the ability to modify any input fields in a macro which have been “parameterized” to allow for a change in the value before the scan is initiated. This eliminates the need to bring up the user interface and modify the password as it expires every few months; instead, the new password can simply be supplied as a part of the command line or API call. For more information, see “WebInspect API” in the WebInspect help.

- **Link Sources Settings**

  WebInspect 10.50 includes a new Link Sources crawler settings page that allows users to select Pattern-based or DOM-based link parsing, and to customize which DOM-based link sources are ignored during a crawl. These settings may be useful in preventing potentially large volumes of bad links from cluttering the crawl and resulting in extremely long scan times. For more information, see “Crawl Settings: Link Sources” in the WebInspect help.

- **New Audit Engines**

  WebInspect includes a new Directory Extension audit engine. Directory extension checking involves adding extensions to directories and removing the trailing slash to find archived directories left on the server. WebInspect attempts to locate all directories that have been left on your server that could be used by an attacker.

  WebInspect includes a new File Prefix audit engine. Network administrators and developers often leave backup files and scripts on the web server. These files commonly contain

information that can be used to breach a site's security. Prefix checking involves affixing a value to file names, and then looking for older or backup versions stored on the site.

WebInspect Enterprise Version 10.50

- **Macro Repository**

  Customers working with WebInspect Enterprise 10.50 now have the option of storing their login or workflow macros as an artifact inside a project version. Each macro can be downloaded for modification or use, overwritten by uploading a newer version, or referenced as a part of the scan wizard. As with all items in WebInspect Enterprise, access to these macros can be controlled using the permissions model to prevent unauthorized users from downloading or modifying them.

- **New Project Version Wizard**

  WebInspect Enterprise 10.50 incudes a new wizard for creating new project versions. Customers no longer need to shift to the Software Security Center (SSC) portal just to create a new project version for scanning. The wizard prompts the user to choose which organization and group the project version belongs to in WebInspect Enterprise so an administrator is not needed to move it after creation.

- **Privilege Escalation**

  For a description, see WebInspect Version 10.50. For more information, see “About Privilege Escalation Scans” in the WebInspect Enterprise Thin Client Download help.

- **Traffic Viewer Tool**

  For a description, see WebInspect Version 10.50. For more information, refer to the Traffic Viewer tool online help or the Tools Guide for WebInspect Products.

- **Selenium Support**

  For a description, see WebInspect Version 10.50. For more information, see the following topics in the WebInspect Enterprise Thin Client Download help:

  - Configuring Web Site Scans Using a Predefined Template
  - Configuring Mobile Web Site Scans Using a Mobile Template

- Configuring Native Scans Using a Mobile Template
- Link Sources Settings

For a description, see WebInspect Version 10.50. For more information, see “Crawl Settings: Link Sources” in the WebInspect Enterprise Thin Client Download help.