



Veracode Product Descriptions

Effective February 07, 2023

SAAS PRODUCTS

Current Offerings

STATIC-APP-STANDARD	• Static analysis assessments for one (1) application profile during the subscription term. • Access to pipeline scan assessments during the subscription term. • Access to IDE scan assessments during the subscription term. Usage limitations: • This license does not permit analyzing multiple applications in a single application profile • IDE scans are to be used on code in applications intended to be scanned with pipeline, policy, or sandbox scans • Pipeline scans are to be used on applications intended to be scanned with policy or sandbox scans • Excludes scanning of COBOL and RPG programming languages
STATIC-APP-SMALL	• Static analysis assessments for one application profile during the subscription term, for an application with an analysis size below 5MB. • Access to pipeline scan assessments during the subscription term. • Access to IDE scan assessments during the subscription term. Usage limitations: • This license does not permit analyzing multiple applications in a single application profile. • IDE scans are to be used on code in applications intended to be scanned with pipeline, policy, or sandbox scans. • Pipeline scans are to be used on applications intended to be scanned with policy or sandbox scans. • Excludes scanning of COBOL and RPG programming languages
STATIC-COMPONENT	• Static analysis assessments for one (1) application component profile during the subscription term. • Access to pipeline scan assessments during the subscription term. • Access to IDE scan assessments during the subscription term. Usage limitations: • This license does not permit analyzing multiple applications in a single application profile • IDE scans are to be used on code in applications intended to be scanned with pipeline, policy, or sandbox scans • Pipeline scans are to be used on applications intended to be scanned with policy or sandbox scans • This license is intended for use to perform static analysis assessments for application profiles that are components of the application profiles contained within the STATIC-APP-STANDARD and STATIC-APP-SMALL licenses. • Veracode reserves the right to (i) monitor the usage of licenses and (ii) delete all scan results for profiles that are not contained within the application licenses. • Excludes scanning of COBOL and RPG programming languages
STATIC-APP-STANDARD-COBOL/RPG	• Static analysis assessments for one (1) COBOL or RPG application during the subscription term. • Access to pipeline scan assessments during the subscription term. • Access to IDE scan assessments during the subscription term.

	Usage limitations: • This license does not permit analyzing multiple applications in a single application profile • IDE scans are to be used on code in applications intended to be scanned with pipeline, policy, or sandbox scans • Pipeline scans are to be used on applications intended to be scanned with policy or sandbox scans
STATIC-SCAN	• Single static analysis Assessment for one (1) application during the subscription term. • Remediation assessments require separate licenses. • Excludes scanning of COBOL and RPG programming languages
STATIC-SCAN-COBOL/RPG	• Single static analysis Assessment for one (1) COBOL or RPG application during the subscription term. • Remediation assessments require separate licenses.
3RD-APP	• Static analysis and software composition analysis (if included in program scope) assessments for one (1) third-party application profile until such time as compliance with customer's security policy is achieved; no further assessments are permitted once compliance achieved. • The application must be submitted by the third-party that licenses or owns the application. Usage limitations: • This license does not permit analyzing multiple applications in a single application profile. • Applications larger than 5GB cannot be analyzed. • Any usage beyond licensed quantities or amounts will be subject to additional fees and/or may result in reduced access and/or termination of access.
SCA-ADDON-STANDARD	• SCA assessments for up to one (1) application profile and one (1) project during the subscription term. • For more than one license, the total number of licenses is determined by the number of application profiles or projects, whichever is greater.
SCA-ADDON-SMALL	• SCA assessments for up to one (1) application profile and one (1) project during the subscription term. • For more than one license, the total number of licenses is determined by the number of application profiles or projects, whichever is greater.
SCA-ADDON-COMPONENT	• SCA assessments for up to one (1) application profile and one (1) project during the subscription term. • For more than one license, the total number of licenses is determined by the number of application profiles or projects, whichever is greater.
SCA-ADDON-STANDARD-COBOL/RPG	• SCA assessments for up to one (1) application profile and one (1) project during the subscription term. • For more than one license, the total number of licenses is determined by the number of application profiles or projects, whichever is greater.
SCA-DEV	• Unlimited SCA assessments for all application profiles and projects during the subscription term. • One (1) license entitles one (1) Contributing Developer to a given application profile or a project. • Periodically, both parties will report on usage.
SCA-SCAN	• Single assessment SCA assessments for up to one (1) application profile and one (1) project during the subscription term. Usage limitations:

	- License does not permit analyzing multiple applications in a single application profile or project. - Any usage beyond licensed quantities or amounts will be subject to additional fees and/or may result in reduced access and/or termination of access.
DYN-URL	- Unlimited dynamic scanning with vulnerability verification for one (1) URL during the Subscription Term. - Dynamic analysis scans include login script, crawl script assistance, and false positive removal service.
DYN-ADDON-STANDARD	- Unlimited dynamic scanning with vulnerability verification for one (1) application during the subscription term. - Dynamic analysis scans include login script, crawl script assistance and false positive removal service.
DYN-ADDON-SMALL	- Unlimited dynamic scanning with vulnerability verification for one (1) application during the subscription term. - Dynamic analysis scans include login script, crawl script assistance and false positive removal service.
DYN-ADDON-COMPONENT	- Unlimited dynamic scanning with vulnerability verification for one (1) application during the subscription term. - Dynamic analysis scans include login script, crawl script assistance and false positive removal service.
DYN-ADDON-STANDARD-COBOL/RPG	- Unlimited dynamic scanning with vulnerability verification for one (1) application during the subscription term. - Dynamic analysis scans include login script, crawl script assistance and false positive removal service.
DYN-URL-CT	- Unlimited dynamic scanning with vulnerability verification for one (1) application during the subscription term. - Dynamic analysis scans include login script, crawl script assistance and false positive removal service. - Ideal for simple log-in workflows. Usage limitations: - Cannot be run behind a corporate firewall. The application must be exposed to public internet.
DYN-SCANS	- Single dynamic scan assessment that can be used to scan one (1) application once at any time during the subscription term. - Dynamic analysis scans include login script, crawl script assistance, and false-positive removal service. Usage limitations: - Concurrent scanning of multiple applications require a separate scan license for each application that will run concurrently. - Any usage beyond licensed quantities or amounts will be subject to additional fees and/or may result in reduced access and/or termination of access.
DISCO	Veracode Discovery analyses an organization's application perimeter to identify and uniquely fingerprint all deployed web applications. Based on the Discovery type noted in the order form: - Single Scan = A single Discovery assessment throughout the subscription term as defined on the order form. - Unlimited Scans = Unlimited Discovery assessments, with one (1) concurrent scan at any time throughout the subscription term as defined on the order form. No Discovery assessment shall include more than 150,000 input IP addresses and hosts and shall be capped at a processing time not to exceed five (5) days. In the

	program management Discovery package, customer and the Veracode program management team will jointly drive improvements to the customer's Discovery program security posture and maturity in three stages: • During define activities, the Veracode program management team will partner with the customer to launch the program, share best practices on maximizing discovery, and help identify program objectives and goals. Specific activities may include, but are not limited to: a kickoff meeting, milestone and goal planning, and assignment of roles and responsibilities. • During execute activities, the Veracode program management team will help facilitate the implementation of a successful Discovery program. Specific activities may include, but are not limited to: monitoring scans and ensuring they are running in appropriate scan windows, assisting customer to remove unowned web applications from the input list, removing duplicate web applications, providing report of net new web applications found, providing a report of web applications to decommission. • During optimize activities, the Veracode program management team will monitor the program process and hold quarterly business reviews to gauge the progress of the program. Specific activities may include, but are not limited to: business reviews, revisiting program goals, improving input lists for successful future discovery scans. Veracode program management team resources will combine senior and associate professionals who will perform the activities detailed above for up to an average of two (2) hours per week.
CONTAINER-DEV	• Unlimited container security assessments for one (1) Contributing Developer during the subscription term. Usage Limitations: • Licenses may not be shared. Each Contributing Developer requires a unique license.
SECLABS-DEV	• Veracode Security Labs is an online training platform whereby users get realistic secure coding training using live applications. Lesson content demonstrates best practices in application security and secure coding, covering common software risk categories and related topics. Usage Limitations: • Veracode Security Labs is provided on per user subscription basis and Customer may re-assign (i) any assigned, but unused SECLABS-DEV license to a new User, or (ii) any assigned SECLABS-DEV license previously used by a User no longer employed with Customer.
ELEARN-APPSEC	• Full Course Catalog - Designed for software developers, testers, and other technologists, this track provides learners with an introduction to application security and then proceeds to more in-depth coverage of security best practices and common security threats. • With this training, developers can build security into their applications and also meet compliance regulations, such as the Payment Card Industry Data Security Standard, which require that developers be provided with secure development training. • Designed for use through the Veracode platform/learning management system.
ELEARN-SECAWARE	• 1 Course, Security Awareness Course (1 hour of training material) - Designed for employees across all functions of an organization to educate and guide behaviors to improve security posture. • The purpose of security awareness training is to help computer users make smart decisions regarding the security choices that they face every day at work.

	This self-paced, e-Learning course provides an understanding of the basics of security awareness for all employees and contractors, not just technical staff. This course teaches computer users about common security threats to an organization, how to make informed security decisions, and ways in which staff and contractors can become an organization's first line of defense against external and internal security breaches.
ELEARN-IEL	- Full Course Catalog -Designed for software developers, testers, and other technologists. This track provides learners with an introduction to application security and then proceeds to more in-depth coverage of security best practices and common security threats. - With this training, developers can build security into their applications and also meet compliance regulations, such as the Payment Card Industry Data Security Standard which require that developers be provided with secure development training. - All courses included in full course catalog are delivered to channel partners as SCORM files which is designed for use on Customer's learning management system.

FedRAMP Offerings

STATIC-APP-STANDARD-FR	- Static analysis assessments for one (1) application profile during the subscription term. - Access to pipeline scan assessments during the subscription term. Usage limitations: - This license does not permit analyzing multiple applications in a single application profile - Pipeline scans are to be used on applications intended to be scanned with policy or sandbox scans - Excludes scanning of COBOL and RPG programming languages
STATIC-APP-SMALL-FR	- Static analysis assessments for one application profile during the subscription term, for an application with an analysis size below 5MB. - Access to pipeline scan assessments during the subscription term. Usage limitations: - This license does not permit analyzing multiple applications in a single application profile. - Pipeline scans are to be used on applications intended to be scanned with policy or sandbox scans. - Excludes scanning of COBOL and RPG programming languages
STATIC-COMPONENT-FR	- Static analysis assessments for one (1) application component profile during the subscription term. - Access to pipeline scan assessments during the subscription term. Usage limitations: - This license does not permit analyzing multiple applications in a single application profile - Pipeline scans are to be used on applications intended to be scanned with policy or sandbox scans - This license is intended for use to perform static analysis assessments for application profiles that are components of the application profiles contained within the STATIC-APP-STANDARD-FR and STATIC-APP-SMALL-FR licenses. - Veracode reserves the right to (i) monitor the usage of licenses and (ii) delete all

	- scan results for profiles that are not contained within the application licenses. - Excludes scanning of COBOL and RPG programming languages
STATIC-APP-STANDARD-COBOL/RPG-FR	- Static analysis assessments for one (1) COBOL or RPG application during the subscription term. Usage limitations: - This license does not permit analyzing multiple applications in a single application profile
STATIC-SCAN-COBOL/RPG-FR	- Single static analysis Assessment for one (1) COBOL or RPG application during the subscription term. - Remediation assessments require separate licenses.
SCA-ADDON-STANDARD-FR	- SCA assessments for up to one (1) application profile and one (1) project during the subscription term. - For more than one license, the total number of licenses is determined by the number of application profiles or projects, whichever is greater.
SCA-ADDON-SMALL-FR	- SCA assessments for up to one (1) application profile and one (1) project during the subscription term. - For more than one license, the total number of licenses is determined by the number of application profiles or projects, whichever is greater.
SCA-ADDON-COMPONENT-FR	- SCA assessments for up to one (1) application profile and one (1) project during the subscription term. - For more than one license, the total number of licenses is determined by the number of application profiles or projects, whichever is greater.
SCA-ADDON-STANDARD-COBOL/RPG-FR	- SCA assessments for up to one (1) application profile and one (1) project during the subscription term. - For more than one license, the total number of licenses is determined by the number of application profiles or projects, whichever is greater
SCA-ADDON-STATIC-FR	- SCA assessments for up to one (1) application profile and one (1) project during the subscription term. - For more than one license, the total number of licenses is determined by the number of application profiles or projects, whichever is greater.
SCA-DEV-FR	- Unlimited SCA assessments for all application profiles and projects during the subscription term. - One (1) license entitles one (1) Contributing Developer to a given application profile or a project. - Periodically, both parties will report on usage.
DYN-URL-FR	- Unlimited dynamic scanning with vulnerability verification for one (1) URL during the Subscription Term. - Dynamic analysis scans include login script, crawl script assistance, and false positive removal service.
DYN-ADDON-STANDARD-FR	- Unlimited dynamic scanning with vulnerability verification for one (1) application during the subscription term. - Dynamic analysis scans include login script, crawl script assistance and false positive removal service.
DYN-ADDON-SMALL-FR	- Unlimited dynamic scanning with vulnerability verification for one (1) application during the subscription term. - Dynamic analysis scans include login script, crawl script assistance and false positive removal service.
DYN-ADDON-COMPONENT-FR	- Unlimited dynamic scanning with vulnerability verification for one (1) application during the subscription term. - Dynamic analysis scans include login script, crawl script assistance and false positive removal service.

DYN-ADDON-STANDARD-COBOL/RPG-FR	- Unlimited dynamic scanning with vulnerability verification for one (1) application during the subscription term. - Dynamic analysis scans include login script, crawl script assistance and false positive removal service.
DYN-ADDON-STATIC-FR	- Unlimited dynamic scanning with vulnerability verification for one (1) application during the subscription term. - Dynamic analysis scans include login script, crawl script assistance and false positive removal service.
CONTAINER-DEV-FR	- Unlimited container security assessments for one (1) Contributing Developer during the subscription term. Usage Limitations: - Licenses may not be shared. Each Contributing Developer requires a unique license.
ELEARN-APPSEC-FR	- Full Course Catalog - Designed for software developers, testers, and other technologists, this track provides learners with an introduction to application security and then proceeds to more in-depth coverage of security best practices and common security threats. - With this training, developers can build security into their applications and also meet compliance regulations, such as the Payment Card Industry Data Security Standard, which require that developers be provided with secure development training. - Designed for use through the Veracode platform/learning management system.
ELEARN-SECAWARE-FR	1 Course, Security Awareness Course (1 hour of training material) - Designed for employees across all functions of an organization to educate and guide behaviors to improve security posture. - The purpose of security awareness training is to help computer users make smart decisions regarding the security choices that they face every day at work. - This self-paced, e-Learning course provides an understanding of the basics of security awareness for all employees and contractors, not just technical staff. This course teaches computer users about common security threats to an organization, how to make informed security decisions, and ways in which staff and contractors can become an organization's first line of defense against external and internal security breaches.

Legacy Offerings

STATIC-APP	- Unlimited static analysis assessments for one (1) application profile during the subscription term. - This license does not permit analyzing multiple applications in a single application profile. Usage limitations: - Applications larger than 5GB cannot be analyzed. - Any usage beyond licensed quantities or amounts will be subject to additional fees and/or may result in reduced access and/or termination of access. - Excludes scanning of COBOL and RPG programming languages
STATIC-MB	1MB of Static Analysis Assessments. - Each application profile will consume a minimum of 1MB and a maximum of 30MB, based on the analysis size. - The aggregate amount of megabytes is calculated as the sum of the analysis sizes of the largest scan for each application profile used by the customer. - Unlimited static analysis assessments are included for each application profile

	during the subscription term. - This license does not permit analyzing multiple applications in a single application profile. Usage limitations: - Applications larger than 5GB cannot be analyzed. - Any usage beyond licensed quantities or amounts will be subject to additional fees and/or may result in reduced access or termination of access. - Excludes scanning of COBOL and RPG programming languages
SCA-PROJECT	- Unlimited SCA assessments for up to one (1) application profile and one (1) project during the subscription term. - For more than one license, the total number of licenses is determined by the number of application profiles or projects, whichever is greater.
SCA-STANDALONE	- Unlimited SCA assessments for up to one (1) application profile and one (1) project during the subscription term. - For more than one (1) license, the total number of licenses is determined by the number of application profiles or projects, whichever is greater.
SCA-ADDON-STATIC	- SCA assessments for up to one (1) application profile and one (1) project during the subscription term. - For more than one license, the total number of licenses is determined by the number of application profiles or projects, whichever is greater.
SCA-APP	- Unlimited SCA assessments for up to one (1) application profile and one (1) project during the subscription term. - For more than one (1) license, the total number of licenses is determined by the number of application profiles or projects, whichever is greater. - Periodically, both parties will report on usage. Usage limitations: - License does not permit analyzing multiple applications in a single application profile or project. - Any usage beyond licensed quantities or amounts will be subject to additional fees and/or may result in reduced access and/or termination of access.
SCA-MB	- Unlimited SCA Scans for each application profile or project licensed during the subscription term. - Periodically, both parties will report on usage. Usage limitations: - This license only permits scanning applications that are also covered by a Static-MB license. - Any usage beyond licensed quantities or amounts will be subject to additional fees and/or may result in reduced access and/or termination of access.
DYN-ADDON-STATIC	- Unlimited dynamic scanning with vulnerability verification for one (1) application during the subscription term. - Dynamic analysis scans include login script, crawl script assistance and false positive removal service.
DYN-APP	- Unlimited dynamic scanning with vulnerability verification for one (1) application during the subscription term. - Dynamic analysis scans include login script, crawl script assistance, and false positive removal service. Usage limitations: - Concurrent scanning of multiple applications requires a separate license for each

	- application which will run concurrently. - Any usage beyond licensed quantities or amounts will be subject to additional fees and/or may result in reduced access or termination of access.
DYN-SCANNER	- Unlimited dynamic scanning with vulnerability verification for an undefined number of applications, with one (1) concurrent scan throughout the Subscription Term. - The number of applications a customer can scan is only limited by the total time available for scanning during the subscription term. - Dynamic analysis scans include login script, crawl script assistance, and false positive removal service. Usage limitations: - Concurrent scanning of multiple applications requires a separate license for each application which will run concurrently. - Any usage beyond licensed quantities or amounts will be subject to additional fees and/or may result in reduced access and/or termination of access.
GL-DEV	- The Veracode Greenlight solution enables a customer's software developers to quickly detect and fix security related defects in software code while coding in the customer's IDE. - Utilizing Veracode's static analysis engine, Veracode Greenlight allows customers to find issues early, reduce costs, and release code on time at the speed of the customer's development operations process. Usage Limitations: - Veracode Greenlight is provided on per user subscription basis and subscriptions are non-transferable.

SERVICES PACKAGES

VS-STANDARD	Veracode services are offered to help customers get the most out of their Veracode application solutions. All Veracode services offerings are designed to assist you with integrating Veracode's application security testing solutions into your software development lifecycle, and driving your application security program's success. During the subscription term, the Standard Veracode services offering includes up to three (3) sessions of the following activities in any combination: - Program optimization review - Integrations support - Plug-ins support - APIs support - Remediation coaching The Standard Veracode services offering also includes access to the Veracode Community, and a program kick-off during the subscription term. Response times for support cases submitted via email or phone during standard business hours (US Eastern time) is twenty-four (24) hours or less, based upon the severity of the issue.
VS-PREMIER	Veracode services are offered to help customers get the most out of their Veracode application Solutions. All Veracode services offerings are designed to assist customers with integrating Veracode's application security testing Solutions into their software development lifecycle, and driving their application security program's success.

	During the subscription term, the Premier Veracode services offering includes up to ten (10) sessions of the following activities in any combination: • Program optimization reviews • End user product enablement • Integrations support • Plug-ins support • APIs support • Remediation Coaching • Secure SDL/DevOps blueprint development • Policy and maturity workshops Also, during the subscription term, Veracode works with customers to determine the appropriate access to the following activities: milestone/goal planning, and program management consulting. The Premier Veracode Services offering also includes access to the Veracode Community, and a program kick-off during the subscription term. Response times for support cases submitted via email or phone during standard business hours (US Eastern time) is sixteen (16) hours or less, based upon the severity of the issue.
VS-PREMIER-PLUS	Veracode services are offered to help customers get the most out of their Veracode Application Solutions. All Veracode services offerings are designed to assist customers with integrating Veracode's application security testing Solutions into their software development lifecycle, and driving their application security program's success. During the subscription term, the Premier Plus Veracode services offering includes up to fifteen (15) sessions of the following activities in any combination: • Mitigation proposal reviews • Secure SDLC/DevOps blueprint development Also, during the subscription term, Veracode will work with you to determine the appropriate access to the following activities: • Milestone and goal planning • Program management consulting • End-User product enablement • Program optimization reviews • Compliance and governance reporting • Integrations support • Plug-ins support • APIs support • Policy and maturity workshops • Remediation coaching (with priority next-day scheduling, based on availability) The Premier Plus level Veracode Services offering also includes access to the Veracode Community, and a Program Kick-off during the subscription term. Response times for support cases submitted via email or phone during standard business hours (US Eastern time) is eight (8) hours or less, based upon the severity of the issue.
VS-PARTNER-NOSERVICES	Partner will perform all services to Customer with the exception of Basic Technical Support Services. For more information on Basic Technical Support Services please

	see: https://www.veracode.com/resources/datasheets/technical-support .
VS-PARTNER-STANDARD	This SKU is limited to Veracode partners, which have a valid Veracode partner agreement that permits their managed service access and use of the Veracode solution only. Veracode program management, security consulting, and advanced support solutions (i) help customers integrate Veracode’s application security testing solutions with their SDLC, (ii) help drive the application security program’s success, and (iii) provide one-on-one remediation coaching sessions with our application security consultants. Program management activities may include initial set-up and guidance on best practices and usage of Veracode products. Security consulting activities may include application upload or result review calls to discuss remediation and mitigation guidance with development teams. Availability of consultation calls will be based on the consultation scheduling calendar in the platform. Advanced Support calls may be used for support on Veracode plug-ins, wrappers, VSA installation, integration and API assistance, and debug build issues. Case initial response time during hours for email and phone cases is two (2) business days. For information on purchasing additional program management or security consulting solution packages, please contact Veracode sales. During the subscription term, Veracode will provide three (3) hours total for such activities from program management or security consulting or advanced support. Each activity will be measured at a minimum of thirty (30) minute increments.
VS-PARTNER-PREMIER	This SKU is limited to Veracode partners, which have a valid Veracode partner agreement that permits their managed service access and use of the Veracode solution only. Veracode program management, security consulting, and advanced support solutions (i) help customers integrate Veracode’s application security testing Solutions with their SDLC, (ii) help drive the application security program’s success, and (iii) provide one-on-one remediation coaching sessions with our application security consultants. Program management activities may include initial set-up and guidance on best practices and usage of Veracode products. Security consulting activities may include application upload or result review calls to discuss remediation and mitigation guidance with development teams. Availability of consultation calls will be based on the consultation scheduling calendar in the platform. Advanced Support calls may be used for support on Veracode plug-ins, wrappers, VSA installation, integration and API assistance, and debug build issues. Case initial response time during hours for email and phone cases is two (2) business days. For information on purchasing additional program

	management or security consulting solution packages, please contact Veracode sales. During the subscription term, Veracode will provide twelve (12) hours total for such activities from program management or security consulting or advanced support. Each activity will be measured at a minimum of thirty (30) minute increments.
CS-SC-SUPPLEMENT	Supplemental security consulting activities include application upload assistance or result review calls to discuss remediation and mitigation guidance with development teams. Activities are tied to further driving the active customer success bundle package purchased. Please see: https://www.veracode.com/products/customer-success-programs. During the subscription term, Veracode will provide up to twelve (12) hours/year of security consulting. For information on purchasing additional program management, security consulting, or advanced support solution packages, please contact Veracode sales.
CS-AS-SUPPLEMENT	Supplemental advanced support activities include help with Veracode plug-ins, wrappers, VSA installation, integration and API assistance, and build issues. Activities are tied to further driving the active Customer Success Bundle Package purchased. Please see: https://www.veracode.com/products/customer-success-programs. During the Subscription Term, Veracode will provide up to twelve (12) hours/year of advanced support. For information on purchasing additional program management, security consulting, or advanced support solution packages, please contact Veracode sales.
CS-PM-SUPPLEMENT	Supplemental Program Management activities can be utilized to help further drive the application security program's success. Activities are tied to further driving the active customer success bundle package purchased. Please see: https://www.veracode.com/products/customer-success-programs. During the subscription term, Veracode will provide various hours/week of Program Management (unused hours do not carry over from month to month). For information on purchasing additional program management, security consulting, or advanced support solution packages, please contact Veracode sales.
CS-MPR-APP	Veracode's Mitigation Proposal Review is a solution that provides customers with a review of proposed mitigation commentary within the Veracode platform to help the customer better understand and manage application risk. Veracode will review proposed mitigations for a single application and provide commentary in the Veracode platform which will describe whether the proposed mitigations conform to risk tolerance guidelines (defined during a service initiation meeting). All work will be provided remotely. For more information on mitigation proposal review, please see: https://www.veracode.com/resources/customers/mprapp
CS-MPR-WK4	For a period of twelve (12) months, Veracode will provide up to an average of four

	(4) hours per week (with no rollover of hours between weeks) for reviewing proposed mitigations in applications, which will describe whether the proposed mitigations conform to risk tolerance guidelines (as defined during a one-time service initiation meeting). All work will be provided remotely. For more information on mitigation proposal review, please see: https://www.veracode.com/resources/customers/wklympr
CS-MPR-SETUP	During the subscription term, Veracode will dedicate up to two hours per business day between 06:00 and 17:00 EST to review any proposed mitigations which have been submitted by Customer prior to the respective daily review period (Rolling Review). The daily review period may be increased or decreased as agreed by customer and Veracode. All hours allocated for the Rolling Review will be deducted from customer's CS-MPR-WK4 packages and customer must purchase at least two (2) CS-MPR-WK4 packages in order to use this service. At the end of the daily review period, Veracode will provide feedback on as many of the submitted proposals as can be processed during the allotted time. If there are more proposals than can be reviewed during the allotted time, additional proposals will, when possible, be resourced and reviewed on an ad-hoc basis the same day or be carried over to the following daily review period, with all such ad-hoc review time also being deducted from customer's CS-MPR-WK4 packages. If an application profile with a large number of mitigations is proposed, Veracode may schedule, on customer's behalf, a review period to perform mitigation reviews for the application outside of the daily rolling review period, with the time devoted to such a review also being deducted from Customer's CS-MPR-WK4 packages.
CS-TAM-DYM	Supplemental Technical Account Management activities can be utilized to help support the application security program's success. Activities are tied to supporting the use of the Veracode Dynamic product. Specifically, these activities relate to pre scan login verification assistance and crawl script creation and verification. Please see: https://info.veracode.com/veracode-services-packages-datasheet.html. During the subscription term, Veracode will provide up to four (4) hours/week of technical account management (unused hours do not carry over from month to month). For information on purchasing additional program management, security consulting, or advanced support solution packages, please contact Veracode sales.
CS-SPW	Veracode's Secure Programming Workshop provides a one (1) day onsite training conducted by a Veracode application security consultant. This workshop is targeted at customer developers who are seeking to obtain "real world" experience interacting with flaws in code. This workshop can be used to help these individuals obtain knowledge pertaining to secure coding and to satisfy professional development requirements.

	This session is for twenty (20) or fewer attendees and covers a specific set of CWE IDs as well as advanced application security topics. Learning materials are reinforced with live examples in a Veracode-supplied demonstration application and environment. During the session, attendees are encouraged remediate flaws in the demo application's source code. Veracode provides a cloud-hosted IDE preloaded with the demo application and Veracode Greenlight, which can be used to verify flaw fixes. The workshop covers an array of flaw types including: cross-site scripting, SQL injection, OS command injection, SQL injection, CRLF injection, unsafe reflection, information leakage, code quality, credentials management, cryptographic issues, directory traversal, etc. Each workshop purchased consists of an instructor-led session delivered by one (1) Veracode application security consultant at the customer site. Sessions are approximately one (1) business day and will leverage Veracode's existing content without customization. Please allow Veracode up to four (4) weeks lead time.
--	--

MANUAL PENETRATION TESTING

CS-MPT-SUBSCR	During an annual purchased Subscription Term, Veracode will perform one annual baseline penetration test upon the customer's request and provide a report thereafter. Should the customer choose to remediate findings outlined in the baseline test report, Veracode will perform one penetration retest of such findings. Additionally, on mutually agreeable dates on a quarterly basis, Veracode will perform a single penetration test as follow up to the baseline penetration test and provide an associated report. Any unused baseline or single penetration tests shall expire at the end of the applicable Subscription Term.
CS-MPT	Veracode will perform a MPT based on the MPT type and number of days noted in the order form: • Single = custom scoped MPT for a single application based on information provided in the scoping document. • Time-Boxed = time-boxed MPT for a single application • DevOps = infrastructure or network penetration test scoped according to the number of IP addresses or systems • Declining = declining balance of days to be used for multiple MPTs If applicable, each MPT will build upon and extend the findings identified by automated scans of the application conducted on the solution platform. Veracode will provide oversight to facilitate the scheduling, logistics verification and related activities associated with conducting the MPT. For details on the MPT testing methodology, testing type descriptions, customer responsibilities, and other MPT engagement information see: https://www.veracode.com/resources/customers/mpt. Notwithstanding the subscription term of the automated solutions included herein, any manual services will be completed within the start and end date noted on the sales order form for these services.
CS-MPT-RETEST	Veracode will provide up to four (4) hours of post-test remediation validation (retest) time for MPT services previously performed by Veracode. To schedule a retest of specific remediated findings, please contact support@veracode.com. Veracode will work with the customer to schedule a retest. In some cases, expedited testing can be arranged by contacting Veracode sales.

DEFINITIONS

analysis size	is the compressed size of the software components of the application selected for analysis. The method for determining which components of the application are analyzed varies based on the language of the application submitted.
application	is a collection of logically related software components performing a coordinated set of functions; or a single URL that supports a single business process that is accessible via a desktop or mobile web browser
application profile	is a profile used to organize assessments of an application within the Veracode Platform
application programming interface	is also referred to as API
contributing developer	is used to measure the number of employees or contractors who, during the term of the agreement, access or use Veracode SCA within the Veracode Platform, or any engineer, developer, or other person that writes, develops, or modifies the Customer's code, application profile, or project being scanned by Veracode SCA in the previous 30 days.
IDE scan assessments	assessments performed on individual files or small software packages using Veracode's IDE plugins.
integrated development environment	is also referred to as IDE
manual penetration test	is also referred to as MPT
pipeline scan assessments	assessments of applications submitted using Veracode's pipeline scan service
project	is a single code repository of an application that is scanned by the Veracode SCA Agent.
remediation assessments	static analysis assessments after the initial assessment, to test the policy compliance of the third-party application.
security policy	is a standard for application security assessment defined in the Veracode Platform
software composition analysis	is also referred to as SCA
software composition analysis assessments	software composition analysis assessments of an application performed as a policy or sandbox scan, initiated via the Solution Platform UI, API, or IDE plugins. If included in third party program, a software composition analysis will assess open source risk contained within the application.
static analysis assessments	static analysis assessments of an application performed as a policy or sandbox scan, initiated via the Veracode platform UI, API, or IDE plugins.
third-party	a vendor of the Customer that will enter into a license with Veracode for the static analysis and software composition analysis Assessments.
uniform resource locator, also referred to as URL	is a unique URL that supports a single business process that is accessible via a desktop or mobile web browser. URLs can include but are not limited to the following examples: http://www.example.com , https://www.example.com , http://www.example.co.uk , http://businessA.example.com , and http://www.example.com/businessA , http://devURL.example.com , http://prodURL.example.com

user interface	is also referred to as UI
---------------------------	---------------------------

Veracode is a leading AppSec partner for creating secure software, reducing the risk of security breach, and increasing security and development teams' productivity. As a result, companies using Veracode can move their business, and the world, forward. With its combination of process automation, integrations, speed, and responsiveness, Veracode helps companies get accurate and reliable results to focus their efforts on fixing, not just finding, potential vulnerabilities.

Learn more at [www.Veracode.com](https://www.veracode.com), on the [Veracode blog](#) and on [Twitter](#).

Copyright © 2022 Veracode, Inc. All rights reserved. Veracode is a registered trademark of Veracode, Inc. in the United States and may be registered in certain other jurisdictions. All other product names, brands or logos belong to their respective holders. All other trademarks cited herein are property of their respective owners.



Veracode Headquarters
65 Blue Sky Drive
Burlington, MA 01803

Phone 339.674.2500
Email hq@veracode.com

EMEA Headquarters
36 Queen Street
London, EC4R 1BN, United Kingdom

Phone +44 (0)20 3761 5501
Email emea@veracode.com