VERACODE

# Veracode Dynamic Analysis

Technical Paper

VERACODE

# Reducing your risk of a breach with dynamic analysis

## APPSEC COVERAGE ACROSS THE ENTIRE SDLC

The adoption of DevSecOps in application security testing (AST) has increased the number of flaws identified in the earliest stages of application development, when flaws are less expensive to fix. Not only does this approach assist developers in learning to write secure code, but it also prevents a number of flaws from being introduced into later stages of the SDLC. It has substantiated the need for later-stage dynamic application security testing (DAST), as organizations are looking to further reduce the risk of breach by fixing flaws that can only be detected at runtime. Further, development teams use DAST results to validate the proposed mitigations of vulnerabilities found through other AST techniques in order to more effectively prioritize policy-violating flaws.

According to the Verizon 2020 Data Breach Investigations Report, web applications are the most highly-targeted assets within an organization, with 43 percent of breaches resulting from attacks on web applications – more than double the results from 2019. Ensuring that your web applications are sufficiently protected and continue to be monitored once they are in production is vital to the security of your customers and your organization. Attackers are constantly looking for new ways to exploit vulnerabilities and to breach web applications, which means that as their methods mature and they become more aggressive, even the most securely developed applications can become vulnerable. Organizations that only perform annual penetration tests on their web applications may be leaving themselves open to a breach that could be easily prevented with regular production scanning.

While using a mix of testing types is the only way to ensure stronger security of your application layer, web application discovery and dynamic application security testing (DAST) are critical baseline solutions for your application security program.

### What is dynamic application security testing (DAST)?

Dynamic application security testing (DAST) evaluates applications that are in runtime. Dynamic analysis instruments a browser to actively attack the running application. This means that the vulnerabilities it finds are provably exploitable, rather than theoretical, which significantly reduces false positives. Dynamic analysis is also the only assessment type that can find security misconfigurations on the server because it assesses the running instance rather than the code. While other forms of AST can evaluate the quality of the code, including if there are any known vulnerabilities in the third-party libraries that your developers use, DAST scanning can check for configuration errors, certificate issues, deployment issues, and exploitable vulnerabilities instead of just flaws that may turn into a vulnerability.

### DAST leverages crawl and audit technology to uncover all exploitable vulnerabilities

The DAST scanner interacts with the application similarly to how a user or attacker would. To find these vulnerabilities, the DAST scanner first performs an exhaustive crawl of the application to understand the application's architecture. The crawl will find all links, text, form fills, and other page elements that a user

could interact with, as well as attack points that are less visible to the user, such as header values, cookies, and URL parameters. Once the crawl is completed, the scanner then audits all the objects or attributes the crawl discovered. The audit will send multiple attacks at the specific object/attribute to see if there are vulnerabilities that could be exploited. These attacks include, but are not limited to:

- Cross-Site Scripting
- SQL injection
- Misconfiguration errors
- XML External Entities (XXE)
- Server-Side Request Forgery (SSRF)
- Broken authentication

### How can Veracode help secure your web applications

Applications power the modern world and the global economy, and insecure applications can bring it all to a grinding halt. In order to combat the ever-present risk of attack, Veracode provides application scanning solutions for each stage of the SDLC. Veracode Dynamic Analysis delivers DAST scanning that meets the needs of security and development teams that require a solution that can be easily automated, provides accurate and actionable results, and returns results in a timely manner. Veracode Dynamic Analysis complements a shift-left approach to application security testing by verifying in production that vulnerabilities were addressed or mitigated before application release, testing for vulnerability classes that require examining a deployed application like configuration issues, and identifying applications that may have missed the SDLC processes.

## Veracode Dynamic Analysis

Veracode Dynamic Analysis focuses on four distinct areas:

- Rapidly delivering high-quality results
- Ease of onboarding, use, and automation
- Scale
- Coverage

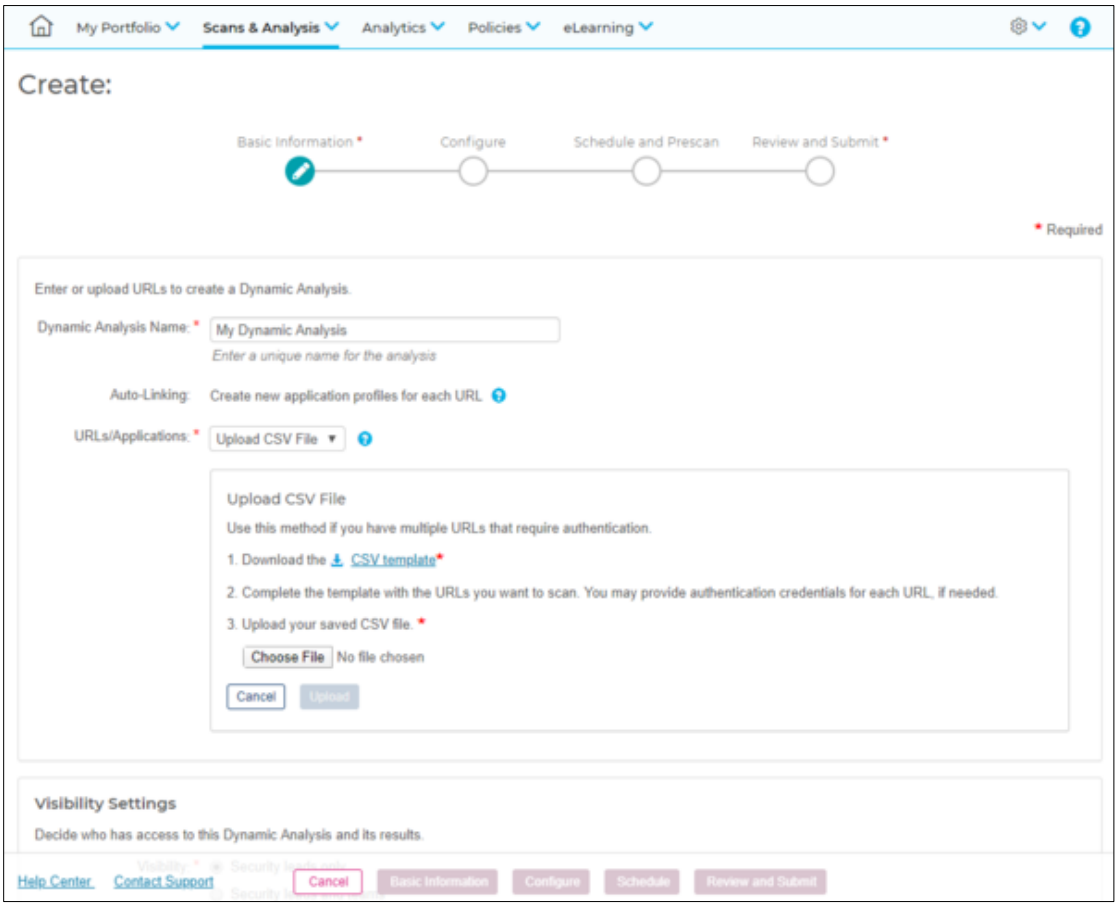
### Rapidly delivering high-quality results

Dynamic testing has not historically been known for how quickly it returns scan results, and if you're getting results quickly, then there must be a tradeoff in the quality of the results. With Veracode Dynamic Analysis, security and development teams benefit from both speed and accuracy, with 65 percent of scans finishing in 5 hours and 70 percent of scans finishing in 8 hours. Thanks to the accuracy of our automated scanner and limited manual results review, the results include fewer than 1 percent false positives, which means development teams spend less time sorting through a multitude of results and can get to work on remediation immediately.

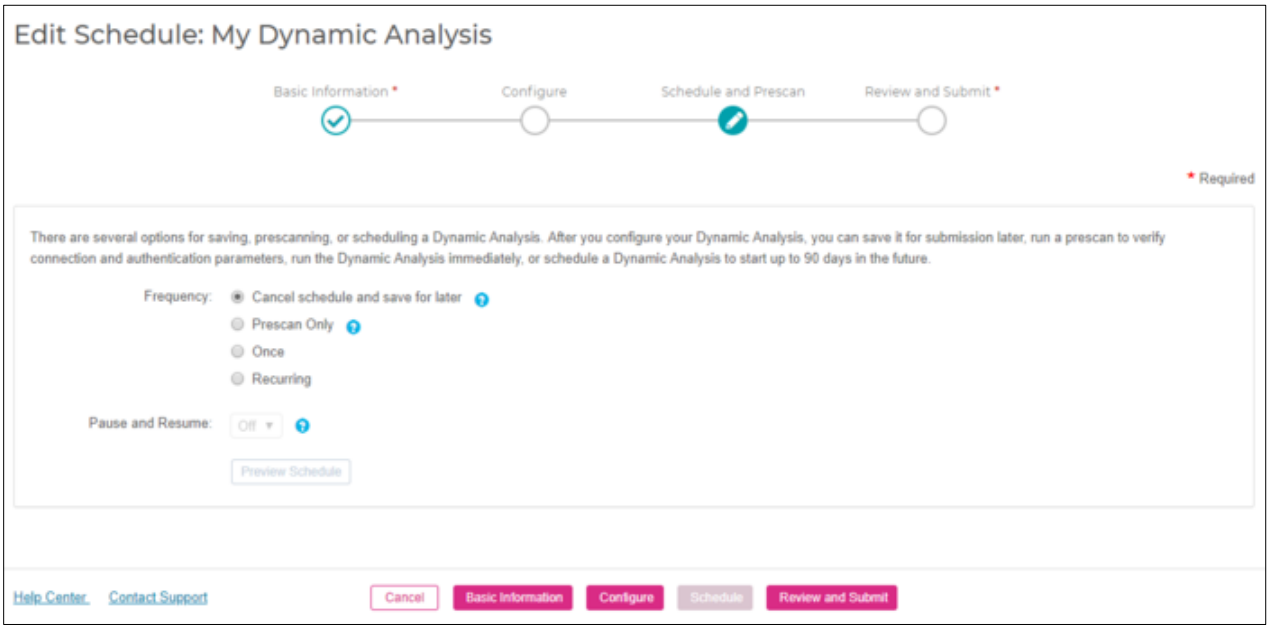
Veracode Dynamic Analysis covers a wide variety of application frameworks, including but not limited to Single Page Applications, JavaScript apps, HTML5, Angular, VueJS, and ReactJS. This gives you the reassurance that Veracode Dynamic Analysis will be able to return actionable results on your applications.

### Ease of onboarding, use, and automation

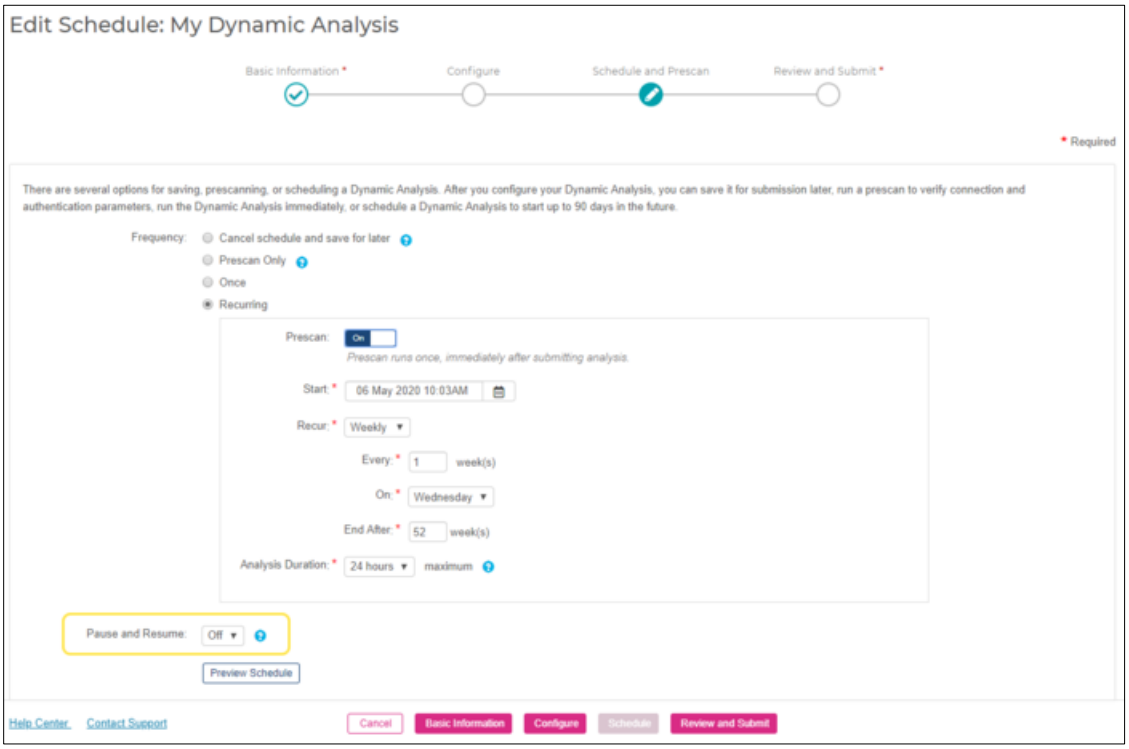
With Veracode Dynamic Analysis, configuring and kicking-off scans is much faster, ensuring that your team is not spending valuable time managing every scan on a case-by-case basis. We do this through scheduling automation as well as a single upload that allows you to batch upload multiple applications into the same analysis.




Batch upload enables your team to upload multiple applications (both authenticated and unauthenticated) into the same analysis in a single step. By inputting your applications' URLs into the provided .CSV template and attaching the completed file during the configuration steps, the applications will be automatically added to the analysis. Veracode Dynamic Analysis also supports scanning for applications that require authentication by including the login information in the same .CSV template, which will be automatically added to the corresponding application during the upload process.




Scheduling automation is especially important for teams that work in an Agile or DevOps fashion, and setting up a recurring scan to run on whatever timeframe you want is fast and easy. You are able to set the day and time that the scan will kick off as well as how long you would like the scan to run. Do you have a period of time that you do not want the scan to run? With Veracode Dynamic Analysis' automated pause and resume function, the scan will pause during the do-not-scan period and resume where it left off during the next available scan window. This ensures that you do not disrupt IT maintenance windows or other critical business activities.




Veracode Dynamic Analysis integrates with Jira and Jenkins and provides a full suite of publicly facing RESTful APIs delivering programmability and automation into your existing workflow.

## Scalability

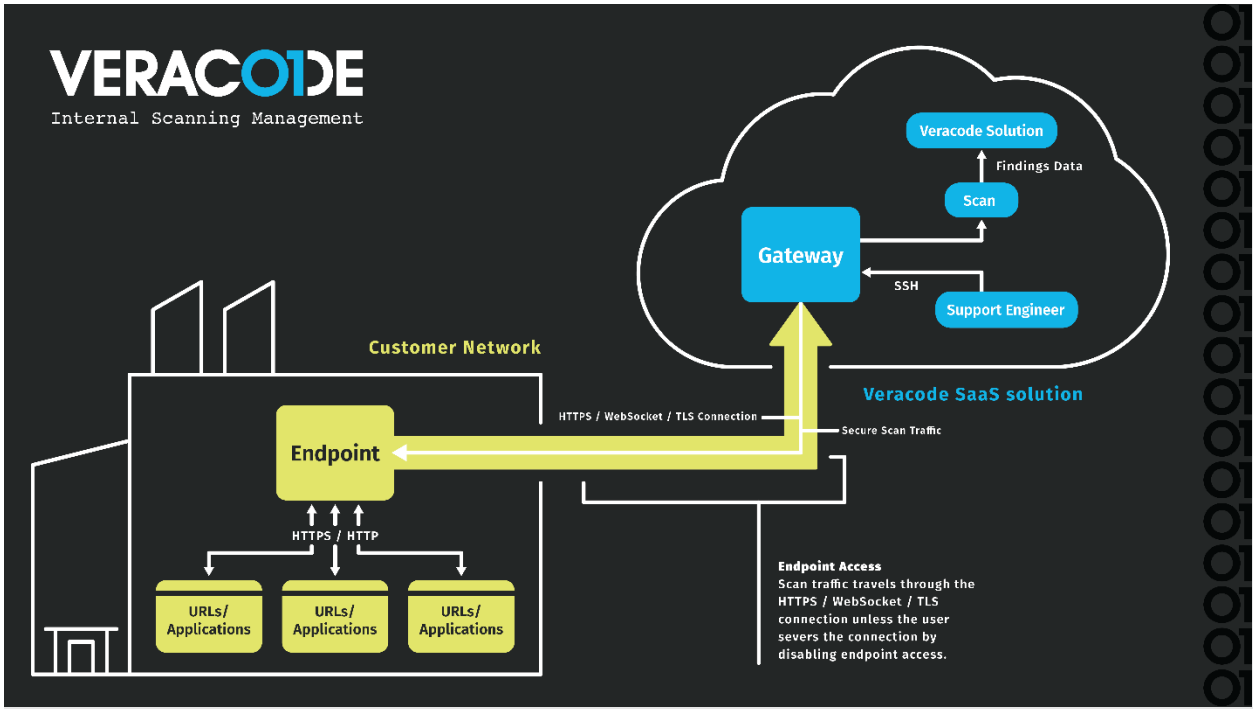
A solution is only as good as its ability to cover all of your applications, and Veracode Dynamic Analysis was built to provide a high level of scalability. As a SaaS solution, Veracode Dynamic Analysis can kick off a scan for hundreds of applications at the same time. Unlike other solutions on the market, Veracode Dynamic Analysis can concurrently scan both authenticated and unauthenticated applications in front of and behind a firewall, ensuring full coverage of your applications.

## Internal Scanning Management with Veracode Dynamic Analysis

There are many reasons for an application to live behind a firewall, whether it is still in the development process waiting for test and quality assurance checks, is used for more sensitive financial operations or HR purposes, or is only used internally. DAST vendors often struggle with the most secure way to scan these applications. Instead of installing a virtual appliance that needs to be maintained by the end-user or using an on-premises scanner that is difficult to maintain and doesn't scale, Veracode has taken a different approach to accessing the applications behind a firewall. Veracode Dynamic Analysis continues to run in the cloud and is connected to an endpoint deployed in your environment called the Secure Scanning Gateway.

Giving you complete control of the gateway and your environment, you can open the Secure Scanning Gateway when you want to send your scan results from the endpoint back to the scanner in the cloud, and close it when you've completed scanning. This empowers you to not only scan applications that live behind the firewall but to apply dynamic testing to applications in the staging environment before they are pushed into production.

Below is a visual representation of this new scanning technology.




## Veracode Dynamic Analysis + Veracode Discovery

While many organizations may have a good understanding of the web applications that they own, others have a hard time keeping an up-to-date inventory of all existing web applications. This could be due to merger & acquisition activities, marketing promotion sites, rapid development of applications, or even just the fact that the organization has never had the time or ability to discover all of the applications on its attack surface. This could be a crucial mistake in the fight against cyberattackers since they will often look for the easiest way into an organization, which is most often through a long-forgotten web application.

Without a solution to help you discover these web applications, you can never be completely certain that you have scanned all of your web applications. This is where Veracode Discovery can help.

Veracode Discovery is a threat intelligence solution that leverages IP ranges, hostnames, keywords, and other inputs to scan the web for every web application that may be associated with your organization. The results are uploaded to the Veracode Application Security Platform where users can sort through the findings and create new Dynamic Analyses through an easy-to-follow workflow. This ensures that you have full visibility into what your organization owns and can easily set up scans to ensure that those applications are not vulnerable. Organizations that use Veracode Discovery typically find 30 percent more applications than they knew about and are able to either scan and fix those applications or sunset them, which improves the organization's overall security posture.

## Veracode Dynamic Analysis Technical Details

### Where does Veracode Dynamic Analysis fit into the SDLC?

Veracode Dynamic Analysis is most often used to scan applications that are in runtime, and through its internal scanning capabilities, can run scans on applications as early as the testing phase.

### What frameworks are supported?

Veracode Dynamic Analysis supports a wide variety of frameworks and application types, including:

- Angular 1-7
- Single Page Applications
- HTML5
- ReactJS
- JavaScript Heavy Applications

### Veracode's single-page application support

Single-page applications (SPAs) are becoming more widely used by development teams. Unfortunately, these applications can often be challenging for a DAST scanner. Unlike traditional web applications, single-page applications do not have a defined ending of the page; instead, they leverage APIs dynamically to update the page as a user interacts with it, without performing a complete page refresh. While this can be great if you are looking for the perfect shirt, it can be challenging for traditional scanning technologies since it could cause a scanner to infinitely crawl the application hoping to find the end.

Veracode Dynamic Analysis' scanning engine uses an embedded browser in order to record and replay a series of actions that a user is likely to take as they browse a single-page application. To do this, the application is mapped out in a three-stage pipeline consisting of execution, analysis, and derivation. This process is followed until the application has been successfully scanned. Without an embedded browser and application mapping, which is the case with traditional dynamic scanning, it is extremely difficult to achieve this same level of coverage.

### Automate dynamic analysis scanning with REST APIs

DAST scans crawl and attack the live application in the same way an attacker would, without bringing down the application. The Veracode Dynamic Analysis REST APIs offer the ability to integrate dynamic scanning into the SDLC, or to parallel security processes to automatically kick off scans.

Development teams can use these REST APIs to automate the core functionality of the solution, building their own integrations to create, configure, schedule, run, and link their results back to the application profile, which can aggregate their scan results across multiple assessment types. This means that development teams can kick off and return DAST scan results without ever needing to leave their unique workflows and environments. Veracode's YAML and Swagger files leverage these APIs to make SDLC integration easy, ensuring that they can be broadly leveraged regardless of the development tool.

The REST APIs, coupled with faster scan times, even allow you to integrate DAST scanning as a non-release blocking post-build action as a part of your CI/CD.

Through a complete API-driven approach to automating DAST scanning, teams with a high level of comfort writing custom scripts and using APIs for automation can use Swagger documentation, JSON templates, and possibly sequential API calls to drive intended code, configuration, and scan reuse behavior.

Another approach is the UI Configured, API Scheduled model. This hybrid model allows you to configure your scans within the Veracode Dynamic Analysis UI and then leverage that configuration when setting up automation through the APIs. This enables you to validate your configuration with pre-scan prior to integrating with the APIs and allows for more trial and error.

For further information on the Veracode APIs, visit the Veracode Help Center.

## Scanning authenticated applications

It's not always possible for an organization to track every single login credential, and some organizations do not want to record these credentials for security reasons. However, only running unauthenticated scans against your web applications could leave you vulnerable to breach: login screens can often be attacked and grant access either through brute force or some other means of entry.

In order to ensure that the application behind the login screen is not vulnerable, Veracode Dynamic Analysis offers several options for scanning authenticated applications:

- **Auto-Login:** This method is selected by default as it is the common method for most applications, including simple login forms that have a username, password, and login button. Auto-login also works for browser-generated logins, such as basic authentication and NTLMv2. For NTLMv2, you can include the NetBIOS domain separated from the username with a backslash, for example, DOMAIN\username. If your organization's applications require multiple forms of authentication, you can combine auto-login authentication with basic authentication.
- **Login Script:** If your application uses a customized or complex form for its login, you can add login script authentication to auto-login authentication by recording and uploading a login sequence that Veracode uses to automatically log in to your application. Use this method for multi-step login sequences that contain one or more authentication methods, such as username, password, and PIN. You can also combine login script authentication with basic authentication.
- **Client Certificate:** You can scan an application that requires a PFX or P12 certificate by uploading the certificate and associated password.
- **Basic Authentication (Browser-Generated):** The basic authentication method provides information for a site that uses basic or browser-generated authentication where the browser prompts you for credentials in its own pop-up window. Enter the username and password you want Veracode to use. Optionally, you can enter the domain name. You can use this method alone or in combination with the auto-login or login script methods.

For further information about how to run authenticated scans with Veracode Dynamic Analysis, visit the Veracode Help Center.

## Leveraging crawl scripts to target specific areas of an application

There may be times when your security needs only require that you scan a small portion of an application. In order to accomplish this, you need to limit the scope of your DAST scan. Veracode Dynamic Analysis allows you to do this by leveraging crawl scripts that tell the scanner exactly where to crawl and audit.

For further information about how to use crawl scripts to target specific areas of an application, visit the Veracode Help Center.

## Run an Integrated DevSecOps Program with Veracode

There are a number of different places where you could start your application security program, and many different paths to mature your program – but there are not many companies that can help cover your needs from end to end. When assessing your options for an AppSec partner, you need to look for a company that can cover the entire software development lifecycle (SDLC) with a strong focus not only on first- and third-party code, but that also has the ability to implement a mature program. Veracode is the market leader in application security, and our years of experience have shown that companies that evaluate their first-party code, plus open source libraries, and do so early, midway, and late in the SDLC have the best coverage. With Veracode, you can ensure a scalable, cost-effective AppSec program that helps make security part of your competitive advantage.