NTT | Application Security

Vantage Prevent

Bridging the Gap Between DevOps and SecOps

Vantage Prevent – Bridging the Gap Between DevOps and SecOps

Organizations need to deliver new applications and APIs fast. Regrettably, this "need for speed" requirement can lead to software vulnerabilities in and pushing "At-Risk" applications in production. When these vulnerabilities are identified in production, so begins the process by which developers must stop working on new projects to fix the vulnerabilities in previously released applications. Ultimately, this approach is no longer sustainable as application development practices, tools and environments in which they work have evolved. Simply put, traditional security testing methodologies are not keeping up.

According to NTT AppSec Stats Flash Report, **85% of vulnerabilities that organizations find this year will never be remediated**. When we add the current COVID Pandemic related, digital requirements of remote and hybrid work environments, this focus on speed over security creates a perfect storm where minor vulnerabilities missed early in the SDLC create a perfect opportunity for threat actors once these applications are in production. Almost daily we are treated to headlines where functional software vulnerabilities wreak havoc on global supply chains or offer threat actors apocalyptic opportunity.

According to the 2021 Gartner® Magic Quadrant™ for Application Security Testing, **"...the major driver for the evolution of the application security testing market is the need to support enterprise DevOps initiatives.** Customers require offerings that provide high assurance, high-value findings, whilst not slowing down development efforts. Clients expect offerings to fit earlier into the development process, with testing often driven by developers rather than security specialists. As a result, this market evaluation focuses more heavily on the buyer's needs when it comes to supporting rapid and accurate testing capable of being integrated in an increasingly automated fashion throughout the software development life cycle (SDLC)."[1]

Overcoming these obstacles has not been easy. DevOps are not security experts. Nor should they be. However, testing for security earlier while code is being written would save time and cross-functional headache. To achieve this goal, there are two challenges that must be addressed: The evolution of DevOps and the environments where they work and overcoming the traditional application security barriers.

DevOps Environments

To be effective in today's organizations, modern DevOps requires security to fit seamlessly into its own processes and environments. This includes shortening the turnaround time for application security testing (AST) and its results. Application security should also fit earlier in the development process, enabling developers to drive the application security testing function in an automated way, operating natively where they work and without requiring DevOps to become security experts. To achieve this, AST should be integrated into modern, global cloud-based DevOps communities such as GitHub and Postman. This will allow DevOps to continue operating within their universal and unified workspaces throughout development, testing and deployment of an application.

[1] Gartner, "Magic Quadrant for Application Security Testing" Dale Gardner, Mark Horvath, Dionisio Zumerle, 20 December, 2021

GARTNER and MAGIC QUADRANT are the registered trademarks of Gartner Inc., and/or its affiliates in the U.S. and internationally and has been used herein with permission. All rights reserved. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

The Challenge of Traditional Application Security Testing

Traditional AST technologies cannot cover the entire SDLC. While traditional AST technologies can test physical increments, such as a range of IP addresses or a range or URLs, they are unable to test critical business functionality.

Traditional AST technologies are heavily human-dependent. They require specialized security skills, which DevOps personnel do not often possess. These technologies require application security expertise and cannot be handed over to DevOps persons. Therefore, they are seldom run, and not when needed by DevOps. Additionally, these technologies are slow. It often takes many hours, days, and even weeks before users can get AST results. For all these reasons, traditional AST technologies are not well-fit for plugging into CI/CD pipelines.

Most if not all traditional AST products have been built for their vendors' proprietary platforms. They are not platform-agnostic and not native to modern DevOps platforms such as GitHub or Postman.

Traditional AST solutions do not cover cross-community workspaces: they require different tools, different user experience, and different skills for different SLC phases. Therefore, they offer vastly different user experience and skill requirements for DevOps and for SecOps.

Vantage Prevent Addresses the Needs of Modern AST

Powered by its patented and revolutionary Intelligence-Directed DAST technology, Vantage Prevent brings next-gen dynamic security testing to pre-production stages of the SDLC and empowers developers with the ability to simultaneously run dynamic security scans alongside functional testing as applications are built and integrated into DevOps' CI/CD pipeline.

How it works

Vantage Prevent delivers dynamic application security testing (DAST) technology that tests running applications by executing attacks against those applications. However, it is substantially different than traditional DAST technology. Traditional DAST tests applications by crawling, or scanning a website in its entirety, gathering data that serves as input for running the test that produces findings. This method is extremely time consuming and provides little-to-no insight into an applications' runtime code, API's and/or microservices. Often deployed late in the SDLC, traditional DAST is labor intensive and often leveraged by highly trained security experts. This results in a process by which remediation is more costly and challenging as it cannot be leveraged by development, QA, or Operations.

Vantage Prevent is fundamentally different in that it does not crawl webpages. Instead, it leverages existing functional tests to direct the security testing of applications.   Vantage Prevent operates in a fully automated fashion, analyzing and identifying each web application or API request and tests them each individually. This allows Vantage Prevent to gain insight into interactions between server, browser/client, and microservices, and delivering highly accurate testing results.

A Revolutionary, Modern Approach to Application Security Testing

Vantage Prevent allows developers with no security domain expertise to discover and resolve vulnerabilities before they reach production. Additionally, security teams have visibility into the results which provides them with confidence that what is getting pushed into production is secure. This reduces the load and stress on the security team by reducing or eliminating the stress of finding critical vulnerabilities in production systems.

- **Start Testing in Minutes – No Security Expertise Required**
  Vantage Prevent is fully automated and runs without human interference. This means that it can be run without cumbersome application information or crawler configurations. Downloaded as a desktop application, Vantage Prevent integrates with tools such as Postman, Jenkins and Azure Pipeline, allowing for testing to be run locally, within the environments and tools where developers work. Additionally, testing can be run without needing to configure authentication login and credential handlers. Instead, Vantage Prevent automatically acquires credentials from the running applications themselves, and carries those credentials throughout the security test, thus assuring complete test coverage.

- **Testing Earlier in the SDLC**
  Vantage Prevent enables organizations to test earlier in the SDLC, from programming to build, to pre-deployment, thereby bridging the gap between development and security. Starting with developers, Vantage Prevent can conduct security testing where the code is written, compiled, and integrated into the (copy of) master build, thereby testing the individual build-unit. In doing so, Vantage Prevent can run in concert where Static Analysis Testing (SAST) is run, however incrementally, against single build-units, multiple build-units, or an entire application consisting of all build-units. Additionally, Vantage Prevent focuses on testing business functions to ensure security throughout the application. Unlike traditional DAST which tests an IP-address range or URL, Vantage Prevent tests the actual actions of the application processes, for example, the functional aspects of depositing money through an application. Easily integrated into CI/CD pipeline technologies such as Jenkins and Azure Pipelines, Vantage Prevent empowers DevOps by seamlessly enabling security testing within their processes and environments.

- **Natively Test Any Application Architecture**
  Vantage Prevent is application-architecture agnostic. No special or additional efforts are required by the user to test applications, regardless of their architecture. Leveraging application workflow insight (API calls, UI actions, Logins), as well as interactions between server, UI/Browsers and Microservices, Vantage Prevent can deliver comprehensive testing of Single-Page Applications (SPA), Multi-Page Applications (MPA), and Microservices (MS).

- **Native API Testing**
  Traditional application security testing requires that APIs' declaration to be compliant with associated regulations. Vantage Prevent simplifies API testing by automatically testing APIs without the need for DevOps personnel declaration. In doing so, Vantage Prevent delivers compliance agnostic API testing.

- **Location and Community Native**
  Vantage Prevent can be downloaded and run locally where developers and DevOps work - whether on a user's physical device or server (Linux, Mac or Windows), or in the cloud (AWS or Azure). Additionally, Vantage Prevent runs natively in the most popular community DevOps environments such as GitHub Actions and API testing tools such as Postman, allowing users to receive test results quickly and automatically, without ever needing to leave their environment.

Application Security Testing Accuracy and Speed - Delivered

Based on its patented, revolutionary Intelligence-Directed DAST technology, Vantage Prevent brings next-gen dynamic security testing to early stages of the SDLC and empowers developers with the ability to integrate functional and dynamic security testing at each step of the development cycle. Leveraging 20+ years of application security expertise, Vantage Prevent tests applications where they are being built, preventing exploitable vulnerabilities from reaching production.