# Vantage Prevent

Intelligence Directed Dynamic Application Security Testing

## Organizations need an automated and an accurate way to test their applications for security vulnerabilities

Organizations need to deliver new applications and API's, fast. Unfortunately, this "need for speed" requirement can lead to vulnerabilities in software code and "At-Risk" applications. While these vulnerabilities can be identified once in production, so begins the process by which developers must stop working on new projects to fix the vulnerabilities in released applications. To not do so could open their organization up to the myriad of threats that these vulnerabilities expose.

DevOps are not security experts. Nor should they be. Organizations need an automated and accurate way to test applications for security vulnerabilities earlier in the development process, one that is without cumbersome configurations or time-outs as software engineers come up to speed on security expertise.

## Vantage Prevent is a revolutionary new application security testing solution

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 on what's 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.

## Key Features & Functionalities

- ✓ Dynamic testing completed in minutes — not days — everywhere throughout the SDLC
- ✓ Developer-directed DAST integrates security testing with functional and QA testing
- ✓ Native API testing
- ✓ Language and platform agnostic
- ✓ Quickly test incrementally or scan an entire application in local developer environments

# How Does Vantage Prevent Work?

**STEP 1**
Customer creates or reuses existing functional tests

**STEP 2**
Vantage Prevent uses functional testing to discover vulnerabilities in a running application

**STEP 3**
User views vulnerability report and remediates vulnerabilities

## Technical Features

### SUPPORTED VULNERABILITIES

**+ Broken Access Control**
- » Acess-Control-Allow-Origin & Cross-Origin Resource Sharing (CORS)
- » Cross-Site Request Forgery (CSRF)
- » Directory Listing & Path Traversal
- » Improper or Missing Authorization
- » Unvalidated Redirect

**+ Cryptographic Failures**
- » Broken or Risky Cryptographic Algorithms
- » Insecure Transport
- » Sensitive Information Disclosure
- » Bad Cipher Suites (CBC), TLS Protocols, and Weak SSL (POODLE)

**+ Injection**
- » Blind/Hibernate and Error-based SQL Injection
- » Content Spoofing
- » OS Command Injection
- » PHP Code Injection and Execution
- » XSS: Reflected, Stored, and DOM

**+ Insecure Design**
- » Arbitrary HTTP Method
- » Cross Frame Scripting
- » Improper Control of Interaction Frequency
- » Password in Cleartext, and Autocomplete Attributes

**+ Security Misconfiguration**
- » ASP .NET Misconfiguration
- » Cookie Vulnerabilities (HTTPOnly, Secure)
- » Configuration File Search
- » Directory Listing & Search
- » Internal Path Disclosure
- » Server Error & Stack Trace
- » XXE

**+ Vulnerable and Outdated Components**
- » Apache Struts
- » Heartbleed
- » Server Fingerprinting
- » Shellshock

**+ Identification and Authentication Failures**
- » Hard-coded & Weak Passwords
- » Improper and Missing Authentication
- » Session Token in URLReflected, Stored, and DOM XSS

**+ Software and Data Integrity Failures**
- » Insecure Deserialization
- » Insecure Object Usage

**+ API Broken Object Level Authorization**
- » APIBA

**+ API Lack of Resources & Rate Limiting**
- » APIRL

## Integrations with CI/CD

Jenkins

GitLab Pipeline

GitHubActions

AzureDevOps

## Sources of Intelligence

Functional testing inputs with credentials

Postman

HTTP Archive

## Intelligence Directed DAST

**Leverage functional tests to shift security testing to the left.**

Traditional DAST scanners can't be used in development environments due to the nature of how they work. Scanners usually crawl applications to discover (attack vectors) the targets that need to be attacked. Crawling a site takes a long time and, in most cases, is too long within development environments. Instead of crawling, Vantage Prevent uses functional tests to discover targets within the application to attack.

- ✓ Eliminates the need to crawl, resulting in scans that take minutes, not hours
- ✓ Runs standalone in your development environment on Windows, Mac, or Linux
- ✓ Accurate results, focusing on high impact, actionable vulnerabilities

Vantage Prevent reduces the chance for vulnerabilities to appear in production as well as ensures that development / engineering organizations adhere to security policies.

## Session and Credential Manager

**Automatically manages session authentication with no configuration.**

- ✓ User does not have to manage credentials
- ✓ Automatically detects authentication state
- ✓ Supports most forms of authentication

Eliminates the hassle of managing and updating credentials within the tool.

## Intelligent Attacks

**Efficiently tests your system of vulnerabilities.**

Traditional DAST tools take a brute force approach to testing. The downside to a brute force test is that it takes a long time. Instead of trying everything, Vantage Prevent intelligently tests just a few payloads at first. If there is an indication of a vulnerability, Vantage Prevent will try more tests.

- ✓ Only spends time attacking what is vulnerable
- ✓ Covers OWASP / API Top 10
- ✓ Provides detailed evidence and remediation information

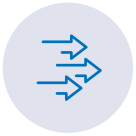
Vantage Prevent provides you the ability to run faster scans that produce rapid but accurate results that results in quick resolution of vulnerabilities.

## Why customers want Vantage Prevent?

Powered by its patented and revolutionary Directed-DAST technology, Vantage Prevent brings next-gen dynamic security testing to every stage of the SDLC. Vantage Prevent 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.

- Empower developers, QA, and DevOps to test for security
- Does not require security subject matter expertise
- Requires little to no configuration
- Performs a scan in minutes
- Focuses on high impact and actionable vulnerabilities

# Vantage Prevent is Built to Provide



### Speed

IDD scan times are measured in minutes, not hours or days. This enables security testing to be part of the CI/CD pipeline and deliver real-time vulnerability findings.

### Accuracy

Focus on accuracy is incredibly important in today's DevOps world. False positives are as crucial as false negatives, and noise in a scan result can slow down the entire process. This is why evidence is included with IDD's vulnerability results.

### Ease

IDD is easy to use with no dependencies and minimal configuration. It includes intelligence that automatically handles common challenges such as logins and complex session states.

### Automation

Collapse the configuration paradigm by integrating cutting-edge security vulnerability testing during development.

### Universal Workability

Test wherever you work. Locally, remotely, or in the cloud.

# License Capability Matrix

| | FOR DEVELOPERS | FOR DEVOPS | FOR SECURITY |
|---|---|---|---|
| Unlimited Scans | ✓ | ✓ | ✓ |
| Unlimited Applications | ✓ | ✓ | ✓ |
| Attack Selection | ✓ | ✓ | ✓ |
| Remediation Advice | ✓ | ✓ | ✓ |
| Testing Local and Remote Applications | Local Only | Yes, but only from CI/CD pipelines | ✓ |
| Ticketing Integration | | ✓ | ✓ |
| CI / CD Integration | | ✓ | |

**NTT APPLICATION SECURITY** 1741 Technology Dr. #300, San Jose, CA 95110 • 1.408.343.8300 • www.whitehatsec.com


NTT Application Security