# Continuous Dynamic

## Web application security for modern and traditional web frameworks and applications

Modern organizations deploy a plethora of web applications, ranging from external-facing corporate websites, customer portals, shopping carts, and login pages to internal-facing HR portals. Web applications are an appealing target for hackers, because they can exploit vulnerabilities in these business-critical applications to gain access to back-end corporate databases.

## Continuous Dynamic

Continuous Dynamic™ is a software-as-a-service (SaaS) dynamic application security testing (DAST) solution that allows your business to quickly deploy a scalable web security program. No matter how many websites you have or how often they change, Continuous Dynamic can scale to meet any demand. It provides security and development teams with fast, accurate, and continuous vulnerability assessments of applications in QA and production, applying the same techniques hackers use to find weaknesses, so you can remediate them before the bad guys exploit them.

Continuous Dynamic is a cloud-based solution that requires no hardware or scanning software to be installed. It provides

- Unlimited, continuous, and concurrent assessments
- Automatic detection and analysis of code changes in web applications
- Open API integration to security information and event management solutions, bug-tracking systems, and web application firewalls

Continuous DAST fits into any environment and is highly scalable, with the ability to assess thousands of websites simultaneously. Furthermore, all vulnerabilities are verified by Black Duck® security experts, virtually eliminating all false positives.

### Powered by artificial intelligence and machine learning

Continuous Dynamic brings together machine learning (ML), artificial intelligence (AI), and expert vulnerability analysis to deliver the most accurate dynamic application security testing results, so you can verify the security of your web applications without slowing down developers with false positives.

Years of valuable data gathered by our highly trained security experts is used to develop our proprietary AI/ML models. This approach provides fast, automated results augmented by expert validation, enabling earlier detection and faster response to cyberattacks.

## How Continuous Dynamic works

Continuous Dynamic combines automated application scanning with the world's largest security expert team to provide you with verified vulnerabilities and actionable reports.

**Onboarding**

Customer provides URLs, logins, and schedule

**Initial scanning**

Discovery, fine-tuning, and configuration

**Website assessment**

Unlimited assessments, vulnerability detection, and verification

**Reporting**

Results displayed in a portal with customizable reports

## Choose the Continuous edition best suited to your needs

| Continuous PE (Premium Edition) | Continuous SE (Standard Edition) | Continuous BE (Baseline Edition) |
|---|---|---|
| • For mission-critical permanent websites with multistep forms and rigorous compliance requirements<br>• Includes all SE features and business logic testing | • For permanent websites that are not necessarily mission-critical<br>• Includes all BE features and tests for issues involving multistep forms and logins | • BE is the foundational solution for basic, less-critical websites<br>• Includes automated scanning and vulnerability verification, ideal for lower-risk websites |

| FEATURE | DESCRIPTION | PE | SE | BE |
|---|---|---|---|---|
| **Continuous assessment** | Websites are scanned continuously to automatically detect code changes to web applications. | ● | ● | ● |
| **Vulnerability verification** | All vulnerabilities are manually verified by security experts and augmented by AI, virtually eliminating false positives. | ● | ● | ● |
| **On-demand retests** | Websites can be retested on demand after detected vulnerabilities are remediated to confirm that they have been fixed. | ● | ● | ● |
| **Production safe** | Only production-safe payloads are used, ensuring no degradation in performance. | ● | ● | ● |
| **Access to Continuous security engineers** | Unlimited and direct access to security experts via the portal to provide remediation guidance. | ● | ● | ● |
| **Continuous Security Index (WSI)** | A single score provides an instant, visual overview of the robustness of your website security. | ● | ● | ● |
| **Testing internal QA/staging environments** | Internal preproduction/staging environments can be rigorously tested to catch vulnerabilities before they reach production. | ● | ● | ● |
| **Flexible reports, analytics, and peer benchmarking** | Enterprise-class reporting and analytics with business-unit-level aggregation of data in flexible formats provides an overview of security trends for all your websites, and benchmarks your score against industry averages. | ● | ● | ● |
| **Single-page applications** | Single page applications scanned in a production-safe and fully automated manner. | ● | ● | |
| **Full configuration and form training** | Scanners can be configured to safely scan websites with forms and logins. | ● | ● | |
| **Authenticated scanning** | Automated and authenticated site scanning, including those that require multifactor authentication. | ● | ● | |
| **Business logic assessments** | Business logic assessments find complex business logic and workflow vulnerabilities that require a deeper understanding of an application's intended behavior and that cannot be discovered by automated scanners alone. | ● | | |

# What Makes Continuous Dynamic Unique

### Easy to deploy, concurrent, and scalable

Continuous Dynamic is an easy-to-deploy cloud-based dynamic security testing solution that can onboard and test over 10,000 websites concurrently without slowing you down. It is scalable to fit any environment and matches your pace of development.

### Continuous assessment methodology

Continuous Dynamic offers true continuous analysis, constantly scanning your website as it evolves. Automatic detection and analysis of code changes to web applications, alerts for newly discovered vulnerabilities, and the ability to retest a vulnerability without having to test from the beginning offer an "always on" risk assessment.

### Production safe

Continuous Dynamic is completely safe for production websites with no performance degradations. Data integrity is assured by using benign injections in place of live code, and custom tuning of scans permits full coverage without performance impact.

### Verified, actionable results with near zero false positives

Every vulnerability is validated by security experts and augmented by AI, virtually eliminating false positives. This enables you to streamline the remediation process, prioritize vulnerabilities based on severity and threat, and focus on remediation and your overall security posture.

### Enterprise-class reporting in flexible formats

Understand the performance of your security programs and improve application security posture with powerful built-in reports. Advanced analytics capabilities monitor trends and key statistics such as remediation rates, time-to-fix, and age of the vulnerabilities. Trending analysis tracks real-time and historical data to measure your risk exposure over time and provide you with visibility into your most- and least-secure websites at a glance.

### Unlimited access to web security experts

With Continuous Dynamic, you have unlimited access to expert web application security testers and custom remediation guidance. The "Ask a Question" feature enables you to access security experts at any time, right from the portal.

### Open API integration

Continuous Dynamic can be integrated with popular bug-tracking systems; security information and event management solutions; governance, risk, and compliance products; and web application firewalls (WAFs).

### Fully automated single page application scanning

Continuous Dynamic provides fully automated scanning and testing of single-page applications as well as traditional applications. It loads your web application into a browser and interacts with it the same way a user would. Production-safe assessments find vulnerabilities other traditional scanning tools miss.

### PCI compliance

Continuous Dynamic exceeds the requirements of PCI DSS 3.1 by providing ongoing, verified vulnerability assessments for both internal and public websites. Continuous PE includes business logic assessments as required by PCI DSS. Integrations with WAFs support the creation of virtual patches to fix vulnerabilities while providing the reports needed for auditor inspections.

### Continuous Security Index

The Continuous Security Index (WSI) gives you an instant, visual overview of the robustness of your website security, providing one score that indicates overall application security. Calculated from a comprehensive set of indicator data and based on our extensive experience with intelligence metrics and our broad base of customers in a variety of industries, this score truly reflects the state of application security across all your websites. With WSI insights, you can reduce risks, save time, prioritize activities, and improve overall security.

# **Continuous Dynamic** | Detectable Vulnerabilities

## Technical Vulnerabilities

### Threat Classification

- Abuse of Functionality
- Application Code Execution
- Application Misconfiguration
- Autocomplete Attribute
- Brute Force
- Buffer Overflow
- Cacheable Sensitive Response
- Clickjacking
- Content Spoofing
- Cross Site Request Forgery
- Cross Site Scripting
- Denial of Service
- Directory Indexing
- Fingerprinting
- Frameable Resource
- HTTP Response Splitting
- Improper Input Handling
- Information Leakage
- Insecure Indexing
- Insufficient Anti-automation
- Insufficient Authorization
- Insufficient Password Policy Implementation
- Insufficient Password Recovery
- Insufficient Process Validation
- Insufficient Session Expiration
- Insufficient Transport Layer Protection
- LDAP Injection
- Mail Command Injection
- Missing Secure Headers
- Non-HttpOnly Session Cookie
- OS Command Injection
- OS Commanding
- Path Traversal
- Predictable Resource Location
- Query Language Injection
- Remote File Inclusion
- Routing Detour
- Server Misconfiguration
- Session Fixation
- Session Prediction
- SQL Injection
- SSI Injection
- Unpatched Software
- Unsecured Session Cookie
- URL Redirector Abuse
- XML External Entities
- XML Injection
- XPath Injection
- XQuery Injection

### OWASP Top 10

- A1 - Broken Access Control
- A2 - Cryptographic Failures
- A3 - Injection
- A4 - Insecure Design
- A5 - Security Misconfiguration
- A6 - Vulnerable and Outdated Components
- A7 - Identification and Authentication Failures
- A8 - Software and Data Integrity Failures
- A9 - Security Logging and Monitoring Failures (out of scope)
- A10 - Server-Side Request Forgery (SSRF)

*Note: A compatible list per product line available upon request*

phase pacific
A subsidiary of CoverTel Telecommunications Group

***Need Local Support?***

***Contact: Frank Cappellari***
***Email: frank.cappellari@phasepacific.com***
***Mobile: +61 449 205 670***
***Office: +61 (03) 9381 7818***

## About Black Duck

Black Duck® offers the most comprehensive, powerful, and trusted portfolio of application security solutions in the industry. We have an unmatched track record of helping organizations around the world secure their software quickly, integrate security efficiently in their development environments, and safely innovate with new technologies. As the recognized leaders, experts, and innovators in software security, Black Duck has everything you need to build trust in your software. Learn more at www.blackduck.com.

©2024 Black Duck Software, Inc. All rights reserved. Black Duck is a trademark of Black Duck Software, Inc. in the United States and other countries. All other names mentioned herein are trademarks or registered trademarks of their respective owners. August 2024