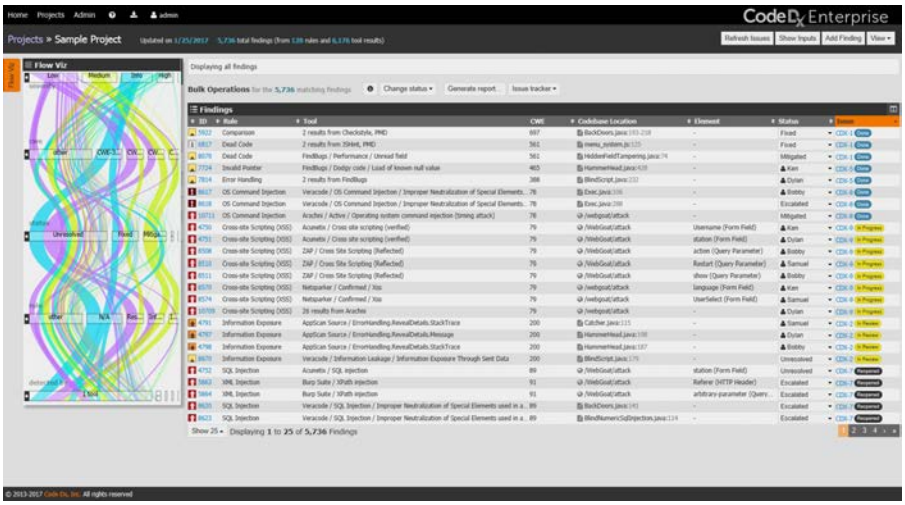
Code Dx Enterprise
Application Vulnerability Manager

FACT SHEET

Find and fix more vulnerabilities, with fewer false positives, automatically and in less time, with less work, and reduced labor costs.

Amplify your investment in SAST, DAST, and IAST tools with automatic consolidation, correlation, and de-duplication of findings, integrated into your AppSec processes, saving weeks of time.



Code Dx Enterprise is a comprehensive Application Vulnerability Manager featuring:

Correlation Create a unified, de-duplicated set of findings from *multiple techniques*: static (SAST), dynamic (DAST), interactive (IAST) application security testing, third-party component analysis, and manual review. Results of *multiple and diverse commercial and open source tools* are normalized to common nomenclature and severity ratings.

Analysis *Triage and prioritize* flaws and vulnerabilities based on industry standards, *regulatory compliance*, and your own rules and best practices.

Management A central console where you assign vulnerabilities for remediation, track progress, collaborate across security and development teams, and *report vulnerability trends* within your organization.

PROBLEM To properly secure your application you *must use multiple techniques, and combine the results*. You need to thoroughly analyze your source code, and then attack your running application. Each technique—static, dynamic, interactive, library analysis, manual review—yields different results for different categories of weaknesses. *Consolidating the results from these techniques is tedious and time-consuming*. Then, for each technique, such as static analysis, you must run and correlate results from *multiple tools*, because no one tool—commercial or open source—covers all programming languages or offers enough coverage to find every issue. The work to *consolidate, correlate and de-duplicate the results is labor-intensive and time-consuming*.

SOLUTION **Code Dx Enterprise** automatically consolidates, correlates, and de-duplicates results of multiple tools and multiple techniques, improving vulnerability coverage with fewer false positives. Since more tools mean better results, we even bundle and install for you a collection of open source SAST tools. Code Dx Enterprise identifies those vulnerabilities considered most-critical based on industry standards and *regulatory compliance*. It also helps you manage the consolidated results with easy ways to assign and track vulnerabilities for remediation, and report progress. Enterprise does this while seamlessly integrated into your development environment; it works smoothly with popular build servers and issue trackers, and adds security to your DevOps process.

The result is better *vulnerability coverage, less manual work, better collaboration across the development and security teams, and greater management insight* into the status of vulnerability remediation.

KEY BENEFITS

More effective software testing
- Better vulnerability coverage by combining multiple *tools* and *techniques*
- Fewer false positives
- Removes duplicate findings

Saves time and resources
- Automates the tedious process of combining results of multiple techniques
- Automates laborious work of correlating results of multiple tools within a technique
- Automatically selects and runs a collection of open source SAST tools and third-party library analyzers against your code

Analysis tools help you focus
- Identifies most-critical vulnerabilities based on industry standards, and on *potential for violation of regulatory compliance*
- Rapidly triage thousands of vulnerabilities into a manageable set to fix first

Helps you manage and track remediation
- Takes you directly to specific lines of code where vulnerabilities exist, and identifies neighboring flaws and vulnerabilities
- Centralized console to assign, track and monitor progress of remediation
- Vulnerability status across releases
- Reports on time taken to remediate vulnerabilities

Improves collaboration and communication
- Shared tool for security and development teams to communicate findings and discuss remediation
- Provides application security results in SIEM format for use by network security team
- Reports using a common nomenclature and severity rating across multiple tools

Works within your development process
- Developers can process vulnerabilities directly from their IDEs
- Fits into continuous integration environments, giving you continuous security assessment
- Integrates with version control systems and issue tracking systems

Who uses Code Dx Enterprise?
- Software Developers & Managers
- Security Analysts
- Quality Assurance Professionals
- Compliance Auditors
- Accreditors

How do they use it?
- Secure software development
- Security & Quality Assurance reviews
- Verification & Accreditation support
- Compliance reviews
- Code audits
- Pre-procurement software evaluations
- Process improvement

Comprehensive application vulnerability correlation and management for the enterprise

Code Dx Enterprise gives you the power to build secure applications quickly and efficiently. Start by loading your source code into Enterprise, which will automatically select and run a pre-configured set of open source SAST tools and third-party vulnerability analyzers to find flaws and vulnerabilities based on the languages in your code. Then add in the results from the commercial and other SAST tools that you've run. Next, feed in the results of any dynamic and interactive (DAST and IAST) tools. Enterprise will automatically combine these results with the static findings to provide a comprehensive application security picture. And if you do manual code reviews, Enterprise can incorporate those findings as well.

The Analysis and Management console helps you triage and prioritize vulnerabilities, assign and track their remediation, and monitor the progress of that remediation. All of this is integrated into the development environment, to work seamlessly with popular build servers and issue trackers.

KEY FEATURES

- Integrates results from more than 40 commercial and open source application security testing tools
- Tool connectors to automatically pull results from specific tools
- Automatically combines and normalizes output of multiple SAST, DAST and IAST tools, third-party vulnerability scanners, and manual findings into a single set of results using common nomenclature and a common severity scale
- Automatically installs, configures and runs many open source SAST tools
- Automatically installs and runs open source SAST tools to check vulnerabilities in third-party libraries
- Maps results to Common Weakness Enumeration (CWE) and industry standards including OWASP Top 10, SANS Top 25
- Identifies vulnerabilties that are potential violations of regulatory compliance including PCI-DSS, HIPAA, DISA STIG
- Provides easy way to triage and prioritize findings
- Manages remediation with tools to assign, track, and report on vulnerability fixes
- Integrates with the popular JIRA issue tracker to automatically create tickets
- Integrates with popular development tools (Eclipse/Visual Studio) to put findings into the hands of developers who can fix them
- Integrates with the Git version control system for easy access to your code, and its history
- Embeds in continuous integration environments to build security into your process; enables integration to other build servers with its REST API
- Supports XML input for integration to custom or proprietary analysis tools
- Provides results in SIEM format for use by network security team

Specifications

Code Dx Enterprise is a server application that supports teams of any size. Enterprise runs on Windows, Linux, and MacOS, and supports all modern browsers.

About Code Dx, Inc.

Code Dx is committed to making security part of the software development process, regardless of organization size. Our family of products grew from research funded by the Department of Homeland Security Science & Technology (DHS S&T) Directorate, an organization dedicated to securing the nation's software supply chain.

Code Dx is proud to be a part of the DHS S&T Software Assurance Marketplace (SWAMP), a collaborative marketplace for continuous software assurance.

FEATURE DETAILS

Operating system support

Windows (7, 8, 10 & Server 2012 R2+)	
Mac OS X 10.8+	
Linux (Ubuntu, Fedora, Debian, RHEL, and CentOS)	

Language support

C / C++	Java
Javascript	JSP
.NET (C#, VB)	PHP
Python	Ruby
Scala	

SAST tool support – open source

Android Lint	Clang
ErrorProne	Jlint
OCLint	
Brakeman	CAT.NET
PHPMD	PHP_CodeSniffer
CheckStyle	CppCheck
FindBugs	FxCop
Gendarme	JSHint
PMD	Pylint
ScalaStyle	

SAST tool support – commercial

Checkmarx	Coverity
HP Fortify	IBM AppScan
Parasoft	Veracode
Armorize CodeSecure	
GrammaTech Code Sonar	
WhiteHat Sentinel Source	

DAST tool support – commercial & open source

Acunetix	Arachni
Burp Suite	HP Webinspect
IBM AppScan	Netsparker
OWASP ZAP	Veracode
WhiteHat Sentinel Dynamic	

IAST tool support – commercial

Contrast Security Assess

Third-party software library checkers

OWASP Dependency-Check	
Sonatype Nexus	Retire.js

IDE support

MS Visual Studio	Eclipse

Issue tracking support

JIRA, JIRA Template Expressions

Continuous integration support

Jenkins
REST API for custom integrations

Version control system support

Git

SIEM & scanner support

AlienVault	Nessus

Code Dx

6 Bayview Avenue, Northport, NY 11768-1502
www.codedx.com • 631.759.3933 • info@codedx.com