SYNOPSYS®

Coverity
靜態分析

在編寫程式碼的同時，高速尋獲並解決關鍵性安全與品質問題

優勢

- **提升安全性風險的能見度。**橫跨不同產品的回報機制，利用業界最佳的AppSec工具，針對整個專案的風險提供整體而全面的視野。
- **彈性資源調度。**您可以決定您的專案之中有哪些部分要在本地部署進行AppSec測試，或者是在雲端上進行。
- **提前進行安全性測試。**在編寫程式碼的同時，開發人員就可以在短時間內獲得可以高度反應真實狀況的增量分析結果，使開發人員可以在進入組建測試的階段之前就解決當下發現的問題。
- **為開發人員提供輔助。**為您的團隊提供在解決問題時所需要了解的整體背景資訊、詳盡資訊與建議，讓他們可以迅速、簡單而正確地解決軟體瑕疵。
- **針對特定背景環境的數位學習(僅限eLearning客戶)**
  針對開發人員自有的程式碼裡所定義的CWE，在有需要的時候提供即時的安全性訓練。開發人員本身不需具有安全性專業人士的專業能力。

概觀

Coverity®為您提供在開發高品質而安全的系統的過程裡所需要的速度、便利性、準確性、符合業界標準的合規性以及擴展性。Coverity可以在開發過程的早期，在程式碼的編寫過程中就辨識出關鍵性的軟體品質瑕疵以及安全性漏洞，這時候進行修改是最輕鬆也最不耗成本的。

精準而可以實行的彌補措施建議以及針對特定環境的數位學習功能可以幫助您的開發人員了解要怎麼迅速地為問題區分優先排序，而這不需要讓他們真的變成安全方面的專家。Coverity與自動安全測試無縫整合，深入您的CI/CD流程，並且可以輔助您既有的開發工具與工作流程。您可以選擇要在什麼平台上利用什麼方式進行開發：在本地部署的電腦上，或者是利用Polaris Software Integrity Platform™ (SaaS)在雲端空間進行，這是一個高度安全、建立在雲端空間的應用程式安全平台。Coverity支援22種語言，並支援70種以上的架構與模板。

Coverity之中包含了Rapid Scan，這是一種高速而不佔用太多資源的靜態分析引擎，可以用來掃描網路與行動裝置上的應用程式、微服務以及基礎架構即代碼(infrastructure– as–code：IaC的組態設定。Rapid Scan會自動執行，不需要另外設定程式組態，可以與所有Coverity的掃描功能一起執行，也可以在進行完整CI組建時將Rapid Scan納入為其中一部份，所需要的掃描時間則等同於傳統掃描的時間。在Code Sight™之中或利用命令列介面時，也可以把Rapid Scan當作獨立的掃描引擎，就如同在自動化建置流程中一樣。在此種用途下，Rapid Scan可以在幾秒鐘以內為大多數的專案提供可以及早予以因應的結果。它使用起來十分簡單：只要指定一個目錄或是Git儲存庫就好，不需要任何設定。它可以支援範圍廣泛的平台與檔案格式，這讓它可以輕鬆地掃描IaC組態設定檔案。API與組態設定檢查工具可以幫助您在設定檔案中辨識API的錯誤使用以及具有安全漏洞的組態設定。對於那些想要在編寫程式碼的過程中針對他們所使用的所有程式碼獲取即時的回饋的開發人員來說，它的功能十分理想。它對於多種分析輸出格式(如：SARIF、JSON以及console)以及GitHub Actions與GitLab CI的支援讓對於掃描流程可以自動化，並且可以發行管理報告。Rapid Scan也可以針對問題指派政策，以便自動中斷程式組建。

關鍵性功能

快速而準確的分析

- 搭配Code Sight™整合開發環境(IDE)外掛程式，開發人員可以在他們編寫原始碼的同時，在他們所使用的IDE裡迅速地獲取準確的分析結果。在解決已知問題時，Coverity可以為開發人員提供他們所需要的一切資訊，包含問題說明、類別、嚴重性、CWE數據、瑕疵所在位置、補救措施相關詳盡指示、數據流追蹤資料，以及包含在開發人員所使用的IDE內部的問題分類管理系統。
- 只要把游標指向原始碼，Coverity的Point and Scan桌面應用程式就可以讓使用者載入應用程式(包含IaC組建擷取功能)。對於比較偏好命令列介面的開發人員，Coverity CLI也可以提供類似的功能。

全面性的報告功能與可見化的合規性

Coverity on Polaris為您提供在這個平台上的應用程式在不同的軟體開發生命週期(SDLC)階段裡的風險態勢。

- 安全團隊可以得到針對整個軟體組合進行中心化統整的風險概況。而API則可以把結果匯入到其他風險報告工具裡。
- 您可以在不同團隊與專案之間，依據類別來篩選已知的安全性漏洞、檢視趨勢報告、依據關鍵性程度為安全性漏洞的補救措施決定優先順序，並且管理安全政策的合規性(如：OWASP Top 10、CWE Top 25以及PCI DSS)。
- 「各時期問題」報告可以顯示不同時段下的嚴重程度分級，並讓您得以立刻了解有關您的專案的安全概況資訊。使用者可以下載PDF格式的報告，讓稽核人員得以保留詳盡的合規記錄。

此外，Coverity為C/C++語言提供業界最佳的程式碼品質問題分類功能，同時也支援範圍最為廣泛的安全性、資訊安全以及可靠性相關標準(如：MISRA®、CERT C/C++、CERT Java、DISA STIG、ISO 26262、ISO/IEC TS 17961以及AUTOSAR®)，同時也能涵蓋Nvidia's CUDA C++指南中所描述的品質問題。

商業擴充性與快捷性

- 使用Coverity on Polaris的時候，您就不需要安裝並維護成本高昂的作業現場設備，而是可以彈性地依據成長中的業務需求去調整應用程式的安全測試。
- Polaris的設定就像登入URL介面一樣簡單，設定完成之後，就可以下載並安裝命令列介面(CLI)，或者是在您的CI工作流程中開始分析您的原始碼。
- 由於Coverity分析引擎是在一個連線性能良好的雲端平台上運作，因此Coverity on Polaris可以輕鬆地配合數以千計的開發人員與專案，管理數以百萬計的問題，效率良好，而且節省時間。

軟體開發生命週期整合

- Code Sight外掛程式不需要進行任何組態設定，您可以從Visual Studio、Visual Studio Code、Eclipse、IntelliJ、WebStorm、PyCharm、PhpStorm以及RubyMine的網路商城中下載它。
- Coverity也具有傳統的IDE原生整合功能(如：Visual Studio、Eclipse、IntelliJ、RubyMine、Wind River Workbench以及Android Studio)、原始碼管理(SCM)解決方案、問題追蹤工具(如：Jira以及Bugzilla)、CI組建工具(如：Jenkins以及Azure DevOps)以及應用程式生命週期管理(ALM)解決方案。
- REST API可以用來支援其他自動化組建解決方案，並且匯入分析結果到其他的企業內部工具或客製化工具。
- Coverity on Polaris可以在開發階段以及實際運轉前的階段自動雲端安全性測試提供額外的外掛程式與整合功能。
- 您可以利用REST API來將分析結果匯入到安全性與風險報告工具之中。相關資訊請參照Polaris資料表。

完備的問題管理儀表板

- 開發管理人員可以產生「各時期問題」趨勢圖，顯示所有的安全性風險以及針對業界規格(如： OWASP Top 10以及CWE Top 25)的合規性，並且顯示各個開發人員或整個專案團隊針對需要優先解決的問題所做出的回應。
- 您可以輕鬆地在儀表板裡瀏覽業界已知優先列表、前五大問題類型、以及技術風險指標等資訊，讓您可以專注在對於您的組織影響最大的問題，並且對問題進行優先排序。
- 您可以利用預先設定的篩選工具篩選並為問題依據以下類別進行分類：CWE、標準分類、優先列表、風險指標、路徑、以及個別負責開發人員。

擴充對於標準的合規性以及對於安全性漏洞的偵測

Coverity Extend是一個簡單好用的軟體開發工具(SDK)，它讓開發人員可以偵測特定的瑕疵類型。SDK是一種用來編寫程式分析工具或檢查工具的架構，可以用來辨識特定的瑕疵或是特定領域的瑕疵。Coverity CodeXM是一個針對特定領域的功能性程式語言，開發人員可以用它來開發屬於自己的客製化檢查工具。這些客製化檢查工具可以幫助您的組織符合安全性需求以及業界標準或指導方針的需求。

Coverity 靜態分析 | 技術規格

支援的程式語言以及平台

- Apex
- C/C++*
- C#*
- CUDA
- Java*#
- JavaScript*#
- PHP*#
- Python*
- .NET Core
- ASP.NET
- Objective-C
- Go
- JSP
- Ruby*
- Swift*#
- Fortran
- Scala
- VB.NET
- iOS
- Android
- TypeScript#
- Kotlin

* 目前Coverity的Point and Scan桌面應用程式以及Coverity CLI功能有支援這些語言。
# 目前Rapid Scan有支援這些語言，針對原始碼的安全漏洞進行掃描。

有支援的IaC平台以及檔案格式

平台

- Terraform
- AWS CloudFormation
- Kubernetes
- Helm
- ELK

檔案格式

- JSON
- YAML
- HCL (Terraform)
- HTML
- XML
- plist
- TOML
- Properties
- Vue template
- JSX
- TSX

雲端平台支援

- 您可以在AWS與GCP公用雲端平台的容器中運行Coverity Connect
- 支援平台自有技術：Docker、Kubernetes

支援的架構

Coverity可以支援多達70種以上的不同架構，包含Java、JavaScript、C#以及其他程式語言。Coverity也可以在主要的雲端服務平台上，為與AWS服務(EC2、S3、DynamoDB、IAM)以及Google Cloud Storage APIs (GCP)互動的雲端自有JavaScript應用程式進行API架構的安全性建模。

Java

- Android SDK
- Apache Shiro
- Axis
- DWR
- Enterprise Java Beans (EJBs)
- GWT
- Hibernate
- iBatis
- Java Frameworks
- Java Persistence API (JPA)
- Javax.websocket
- JAX RS
- JAX WS
- JEE
- JSF/Facelets
- JSP 以及 JSP Standard Tag Library (JSTL)
- ReactiveX (RxJava, Reactor)
- Restlet
- Spring Boot
- Spring Framework
- Struts
- Terasoluna
- Tiles
- Vert.x
- WS XML-RPC

C#

- ASP.NET Core MVC/ASP.NET MVC
- ASP.NET Core Web API
- ASP.NET ASMX Web Services
- ASP.NET Web Forms
- Identity Server
- MassTransit
- Razor templates
- WCF Services

JavaScript/TypeScript

Client-side

- Angular
- Angular JS
- Apache Cordova
- Backbone
- Bootstrap
- Ember
- HTML5 DOM APIs/Ajax
- jQuery
- Mithril
- React/ Preact
- Socket.IO
- Swig
- Vue

伺服器端
- Angular server-side rendering (Express 以及 Hapi engines)
- Express
- Fastify
- Hapi
- Koa
- Mean.io
- Node
- Passport
- React server-side rendering (Next.js)
- Restify
- SAP XS Classic and Advanced
- Socket.IO
- Vue server-side rendering

模板引擎
- Consolidate
- doT.js
- EJS
- Handlebars
- Hogan
- Jade
- koa-views
- Lodash (templating)
- Marko
- Mustache
- Nunjucks
- Pug
- Swig
- Twig
- Underscore (templating)
- Vision

主要資料庫
- Axios
- Google Cloud APIs (Storage)
- Mongoose / MongoDB
- Request
- Sequelize
- Sqlx
- Swashbuckle
- Underscore / Lodash

GO
- Echo

PHP
- Symfony

Python
- Flask
- Django

Ruby
- Ruby on Rails

Rapid Scan IaC架構
- Android
- Apache Cordova
- Apache Kafka
- Apache Struts
- Apache Zookeeper
- Apollo GraphQL
- AWS Cloudformation
- Consul
- Express
- Grails® framework
- GraphQL
- Istio
- Jakarta Server Faces
- Java/Jakarta EE
- Kubernetes
- mybatis
- NodeJS
- OpenAPI
- Postman
- RabbitMQ
- React
- Socket.IO
- Spring
- Terraform
- Vue.j

支援的平台
- Windows
- Linux
- Mac OS X
- Solaris
- AIX
- NetBSD
- FreeBSD

SDLC原生整合功能

SCM
- AccuRev
- Apache Subversion (SVN)
- CVS
- Git
- Mercurial (Hg)
- Perforce Helix
- Team Foundation Server SCM

傳統IDEs
- IBM Rational Team Concert
- QNX Momentics
- Wind River Workbench

CI組建伺服器*
- Jenkins
- Azure DevOps Server

Code Sight支援的IDEs†
- Visual Studio for VB.NET, C#, C/C++, JavaScript, PHP, Python, Ruby, TypeScript
- Visual Studio Code for C# (.NET Core), C/C++, Java, JavaScript, PHP, Python, Ruby, TypeScript
- Visual Studio Code (Rapid Scan) for Java, JavaScript, and TypeScript
- Eclipse for Java, JavaScript, C/C++, PHP, Python, Ruby, TypeScript
- IntelliJ for Java, JavaScript, PHP, Python, Ruby, TypeScript
- WebStorm for JavaScript, TypeScript
- PyCharm for Python
- PhpStorm for PHP
- RubyMine for Ruby

問題追蹤
- Jira
- Bugzilla

支援的編譯器
- Analog Devices Blackfin
- Analog Devices SHARC
- Analog Devices TigerSHARC
- ARM C/C++
- Borland C++
- CEVA BXx
- CEVA XC16
- CEVA-X2
- CEVA-XC4500
- Clang
- Cosmic C
- Freescale CodeWarrior
- GNU GCC/G++
- GHS PowerPC on Windows
- Green Hills C/C++/EC++
- HI-TECH PICC
- IAR C/C++
- IBM AIX
- IBM XLC
- Intel C++ for Windows
- JDK for Mac OS X
- Keil compilers
- Marvell MSA
- MPLAB XC8
- Nvidia CUDA Compiler (NVCC)
- OpenJDK
- QNX C/C++
- Renesas C/C++
- SNC C/C++
- SNC GNU C/C++
- SONY PS4 SDK

- STMicroelectronics GNU C/C++
- STMicroelectronics ST Micro C/C++
- Sun (Oracle) CC
- Sun/Oracle JDK
- Synopsys MetaWare C and C++
- Tasking for ARM Cortex and TriCore
- TI Code Composer
- Visual Studio
- Wind River C/C++

(此列表僅為代表性列表)

關鍵性檢查

- API usage errors
- Best practice coding errors
- Buffer overflows
- Build system issues
- Class hierarchy inconsistencies
- Code maintainability issues
- Concurrent data access violations
- Control flow issues
- Cross-site request forgery (CSRF)
- Cross-site scripting (XSS)
- Deadlocks
- Error handling issues
- Hard-coded credentials
- Incorrect expression
- Insecure data handling
- Integer handling issues
- Integer overflows
- Memory—corruptions
- Memory—illegal accesses
- Null pointer dereferences
- Path manipulation
- Performance inefficiencies
- Program hangs
- Race conditions
- Resource leaks
- Rule violations
- Security best practices violations
- Security misconfigurations
- SQL injection
- Uninitialized members

* 有關其他Coverity on Polaris的CI組建伺服器與其他外掛程式整合功能，請參照Polaris資料表。

† 有關最新的CodeSight以及支援的IDE版本，請參照https://dev.sig-docs.synopsys.com/codesight/topics/support_matrix/r_code_sight_support_matrix.html 。

有關最新的Rapid Scan分析引擎的公告與更新(單獨使用時)，請參照此處。

此資料表適用於Coverity 2022.12.0與其之後的版本。

Synopsys與眾不同之處

Synopsys協助開發團隊組建安全而具有高品質的軟體，在最大化速度與產能的同時，將風險最小化。Synopsys是應用程式安全業界公認的領導者，提供靜態分析、軟體成分分析以及動態分析解決方案，讓開發團隊可以快速地發現並解決自有程式碼、開源組建以及程式在行為上的安全性漏洞。