Fortify Static Code Analyzer

编写更严谨的代码，确保软件万无一失

应用程序会带来风险和安全漏洞

软件开发人员面临的现实

- 构建新特征与新功能
- 日益加剧的复杂性
- 数不胜数的交付日期
- 日渐萎缩的预算
- 产品延期

这些词语无时无刻不在软件开发人员的耳边萦绕，因为这些正是他们在开发重要业务应用程序时所面临的需求。当今的应用程序构建需要满足不计其数的复杂需求，开发人员因此感到顾此失彼，安全性考虑只能退居其次。与此同时，各种威胁不断演变，对手也越来越擅长利用应用程序这一软肋。Fortify Static Code Analyzer (SCA) 可帮助组织抵御当今最大的安全风险，即运行于企业内部的应用程序。

Fortify Static Code Analyzer

Fortify SCA 是一款静态应用程序安全性测试 (SAST) 产品，可供开发团队和安全专家分析源代码，检测安全漏洞。该功能可检查代码，能够帮助开发人员更快更轻松地识别问题并排定问题优先级，然后加以解决。

Fortify SCA 可助力开发人员：

- 提前并经常性地扫描源代码
- 将漏洞的根本原因锁定到代码行
- 关联结果并对其进行优先级排序
- 加快开发速度并缩短扫描时间
- 快速修复安全漏洞
- 审视最佳实践，帮助开发人员以更安全的方式进行编码

什么是静态代码分析？

静态代码分析可有效识别源代码中的安全漏洞。静态代码分析应当在开发生命周期的前期完成，并且应持续贯穿应用程序的整个生命周期。它能够在开发过程中就代码中出现的问题快速向开发人员提供反馈。

为何 Fortify SCA 非常适合您

全面

Fortify SCA 支持丰富的开发环境、语言、平台和框架，可对开发与生产混合环境进行安全检查。

- 25 种编程语言
- 超过 911,000 个组件级 API
- 可检测超过 961 个漏洞类别
- 支持所有主流平台、构建环境和 IDE

统计信息

- 超过 84% 的安全漏洞发生在应用程序层[1]
- 重大 Web 安全漏洞可影响近乎半数的 Web 应用程序[2]
- 52% 的 Web 应用程序会遇到输入验证、跨站点脚本编写和 SQL 注入等问题[3]
- 33% 的应用程序从未经过安全漏洞测试。[4]

1 Gartner 魔力象限报告
2 Micro Focus 网络风险报告
3 同上
4 调研：未进行安全性投资的移动应用程序开发人员

准确
Fortify SCA 可提供准确的结果，并且能检测出大量其他静态测试技术所无法检测的问题。Fortify SCA 可对漏洞进行优先级排序，从而提供准确的操作计划，交付已按风险划分等级和分类的问题。该产品遵循由 Micro Focus® Security Fortify 软件安全研究团队扩展和更新的一套最大且最全面的安全编码规则。

灵活
Fortify SCA 可融入您的现有开发环境。它是一款灵活的命令行静态代码分析器，可通过脚本、插件和 GUI 工具集成到任何环境，便于开发人员快速轻松地启动运行。

高效
那些需要加速实现应用程序安全计划的组织将从更短的扫描时间中获益浅。Fortify SCA 可通过提供增量扫描，帮助开发人员提升编程效率。通过只分析自上一次完整扫描之后变更的代码部分，增量扫描可缩短运行扫描所需的时间。这将显著缩短扫描时间，从而让开人员加速获得结果，该产品还能通过支持更加频繁的扫描来提高工作效率，并可以更快地将软件投入到生产当中。

可扩展
由于应用程序来自于公司内部、外包、第三方、开源、移动等多个来源，再加上这些应用程序具有惊人的数目和复杂性，因此想要测试并保持企业中的所有这些应用程序类型的安全无虞便显得困难重重。Fortify SCA 支持业内大部分编程语言，能够识别所有类型应用程序中的风险，并可根据不断增长的企业需求进行扩展。

内部部署或按需部署
Fortify SCA 能够以多种交付模式运行，旨在适应不断变化的需求和要求。

- 内部部署 — 适用于部署、管理及现场运行静态应用程序安全性测试计划的 Fortify SCA。
- 按需部署 — Fortify on Demand 是一项托管应用程序安全性测试服务，它能以一种简单、准确的方式启动静态、动态和移动测试，同时无需前期投资、额外的资源和时间。

支持的语言

- ABAP/BSP
- ActionScript/MXML (Flex)
- ASP.NET、VB.NET、C# (.NET)
- C/C++
- Classic ASP （带 VBScript）
- COBOL
- ColdFusion CFML
- HTML
- Java（包括 Android）
- JavaScript/AJAX
- JSP
- Objective-C
- PHP
- PL/SQL
- Python
- T-SQL
- Ruby
- Swift
- Visual Basic
- VBScript
- XML
- Scala

支持的 IDE

- Eclipse
- IntelliJ Ultimate
- IntelliJ Community Android Studio
- IBM Rational Application Developer (RAD)
- IBM Rational Software Architect (RSA)
- Microsoft Visual Studio

支持的构建工具

- Ant
- Jenkins
- Maven
- MSBuild
- Xcodebuild

Fortify 的软件安全漏洞分类

漏洞类别
谈到软件安全，目前对何谓重大漏洞尚没有统一的标准。众多组织都发布了自己对严重漏洞的解读，这导致对标准产生了认知差异和疑惑。为了帮助开发人员了解导致安全漏洞的常见编码错误类型，Fortify 编写了软件开发七宗罪（The Seven Pernicious Kingdoms），在其中统一了漏洞的组织分类，并将它们对应到 OWASP、SANS、CWE 和 FISMA 等标准中。

作为一家业界公认的顶尖安全组织，Fortify 安全研究团队是一支监控新型威胁全球团队。他们会以漏洞检查的形式将收集到的知识输送到 Micro Focus Security Fortify 产品套件中，确保及时检测出最新的威胁。该团队创建了一套漏洞类别分类规则，力求帮助开发人员了解各种影响应用程序的安全漏洞。

了解详情：分类的演化过程 **vulncat.fortify.com/en**

关于 Micro Focus Security

Micro Focus 是一家业界领先的提供商，为现代化企业提供安全及合规性解决方案，帮助他们降低混合环境中的风险并抵御各种高级威胁。Micro Focus 安全智能平台建立在 ArcSight、Fortify 和 Data Security 等市场领先产品的基础之上，独家提供高级关联、应用程序保护和网络防御等功能，能够保护当今的混合 IT 基础设施免遭复杂的网络威胁。

如需了解 Micro Focus Security 产品详情，请访问 **microfocus.com/securitysolutions**。

了解更多信息

Micro Focus Security Fortify 解决方案将帮您打造值得信赖的软件，让您放心地开展业务。如需了解 Fortify Static Code Analyzer 详情，请访问 **microfocus.com/ fortifysca**。

有关详细信息，请访问
microfocus.com/fortifysca

www.microfocus.com

Micro Focus 英国
总部 英国
+44 (0) 1635 565200

美国 总部
马里兰州罗克威尔
301 838 5000
877 772 4450

有关其他联系信息及办公地点，请访问：
www.microfocus.com

扫描二维码
关注 Micro Focus 微信公众号

销售咨询：400 670 6101
网址：https://www.microfocus.com/zh-cn/