BLACKDUCK®

Continuous Dynamic

面向现代及传统Web框架与应用的安全解决方案

现代企业部署了大量的Web应用，包括面向外部的公司网站、客户门户、购物车和登录页面，以及面向内部的HR门户。对黑客而言，Web应用是很有吸引力的目标，因为他们可以利用这些关键业务应用中的漏洞来访问后端企业数据库。

Continuous Dynamic

Continuous Dynamic™是一款软件即服务 (SaaS) 形式的动态应用安全测试 (DAST) 解决方案，旨在使企业能够快速部署可扩展的Web安全程序。无论您有多少个网站，或者更新频率是多快，Continuous Dynamic都可以通过扩展而满足您的需求。它允许安全和开发团队在QA和生产阶段进行快速、准确和持续的应用漏洞评估，并且采用与黑客发现漏洞相同的技术，因此，您可以在这些漏洞被黑客利用之前就修复它们。

Continuous Dynamic是一款基于云的解决方案，无需安装硬件或扫描软件。它提供：

- 无限制、连续和并发评估
- Web应用中代码变更的自动检测和分析
- 采用开放式API与安全信息和事件管理（SIEM）解决方案、缺陷跟踪系统及Web应用防火墙（WAF）集成

Continuous DAST适用于任何环境，具有高可扩展性，能够同时评估数千个网站。此外，所有漏洞都经过Black Duck安全专家的验证，几乎消除了所有误报。

依托人工智能和机器学习技术

Continuous Dynamic将机器学习 (ML)、人工智能 (AI) 和专家漏洞分析结合在一起，以提供最准确的动态应用安全测试结果，因此，您可以即时验证Web应用安全性，避免因为误报而减慢开发人员的速度。

我们训练有素的安全专家多年来收集了大量的宝贵数据，我们利用这些数据开发了专有的AI/ML模型，用于快速、自动生成结果。我们还通过专家验证来增强这些结果，以便更早地检测到网络攻击并更快地做出响应。

Continuous Dynamic 如何发挥作用

Continuous Dynamic具有自动应用扫描功能，并由世界上最大的安全专家团队提供支持，能够为您提供经过验证的漏洞和可操作的报告。

客户引导

客户提供URL、登录数据和时间表

初始扫描

发现、微调和配置

网站评估

无限制的评估、漏洞检测和验证

生成报告

在门户中通过可定制的报告来显示结果

选择最适合您需求的Continuous版本

Continuous PE（高级版）	Continuous SE（标准版）	Continuous BE（基础版）
• 适用于具有多步骤表单以及严格合规要求的关键任务型永久网站 • 包括SE版本的所有功能，外加业务逻辑测试	• 适用于不一定属于关键任务的永久网站 • 包括BE版本的所有功能，外加多步骤表单和登录问题测试	• 面向非关键任务型基本网站的基础解决方案 • 包括自动扫描和漏洞验证功能，非常适合低风险网站

功能	说明	PE	SE	BE
持续评估	持续对网站进行扫描，以自动检测Web应用的代码变更。	●	●	●
漏洞验证	所有漏洞都由安全专家手动验证，并通过AI进行增强，几乎能够消除所有误报。	●	●	●
按需重新测试	在检测到的漏洞得到修复后，可以根据需要对网站重新测试，以确认漏洞是否已被修复。	●	●	●
生产安全	仅使用生产安全型有效载荷，以确保性能不会降低。	●	●	●
联系Continuous安全工程师	通过门户网站无限制直接联系安全专家，以提供补救指导。	●	●	●
Continuous安全指数 (WSI)	这个分数可以即时、直观地显示网站安全性的稳健程度。	●	●	●
测试内部的QA/暂存环境	可对内部的预生产/暂存环境进行严格测试，以便在漏洞进入生产环境之前发现它们。	●	●	●
灵活的报告、分析和同行对标	企业级报告和分析，可通过灵活的格式来汇总业务部门级数据，以针对您的所有网站提供安全趋势概览，并将您的得分与行业平均水平对标。	●	●	●
单页面应用	以生产安全的全自动方式来扫描单页面应用。	●	●	
完整配置和表单训练	扫描工具可通过表单和登录计划进行配置，以安全地扫描网站。	●	●	
身份验证扫描	经过身份验证的自动网站扫描，包括需要多因素验证的扫描。	●	●	
业务逻辑评估	应用层手动渗透测试可以发现仅靠扫描工具无法发现的复杂业务逻辑漏洞。	●		

Continuous Dynamic缘何与众不同

易于部署，支持并发测试，并且可扩展

Continuous Dynamic是易于部署的基于云的动态安全测试解决方案，可同时测试超过1万个网站，而不会减慢运行速度。它具有扩展性，能够适应任何环境，并与您的开发速度保持一致。

持续评估方法

Continuous Dynamic提供真正的持续分析，可以不间断地扫描您的网站，以洞悉其变化。它能够自动检测和分析Web应用的代码变更，对新发现的漏洞发出警报，并在中途对漏洞进行重新测试（无需从头测试），从而实现“永不间断”的风险评估。

生产安全

Continuous Dynamic对生产型网站来说是绝对安全的，不会降低其性能。它使用良性注入来代替实时代码，以确保数据完整性。此外，自定义扫描调优可在不影响性能的情况下实现全面覆盖。

结果经过验证且可操作，误报几乎为零

每个漏洞都经过安全专家的验证，并通过AI进行增强，几乎消除了误报。这使您能够简化补救过程，根据严重程度和威胁对漏洞进行优先级排序，并专注于补救和整体安全状况。

灵活格式的企业级报告

强大的内置报告有助于了解安全程序的性能并改善应用的安全状况。高级分析功能可以监测趋势和关键统计数据，如修复率、修复时间和漏洞的年龄。趋势分析可以跟踪实时和历史数据，以评估风险随时间的变化情况，并允许您一眼就能看到最安全和最不安全的网站。

无限制联系网络安全专家

使用Continuous Dynamic，您可以无限制联系Web应用安全测试专家并查看定制的修复指南。“提问”(Ask a Question)功能则允许您随时从门户网站联系到安全专家。

开放式API集成

Continuous Dynamic可与常用的漏洞跟踪系统，安全信息和事件管理解决方案，治理、风险和合规产品以及Web应用防火墙(WAF) 集成。

全自动单页面应用扫描

Continuous Dynamic提供对单页面应用和传统应用的全自动扫描和测试。它可将Web应用加载到浏览器中，并像与用户交互一样与之交互。生产安全型评估可以发现其他传统扫描工具遗漏的漏洞。

PCI合规

Continuous Dynamic允许对内部和公共网站进行持续、经过验证的漏洞评估，超越了PCI DSS 3.1的要求。Continuous PE包含PCI DSS所要求的业务逻辑评估和渗透测试。与WAF的集成则支持创建虚拟补丁来修复漏洞，同时提供审计人员开展检查工作所需的报告。

Continuous安全指数

Continuous安全指数 (WSI) 通过一个分数来表明应用的整体安全状况，以即时、直观的方式来示网站安全性的稳健程度。该分数根据一组全面的指标数据计算得出，并基于我们在智能指标方面的丰富经验以及我们在各行业的广泛客户群，WSI真实反映了您公司所有网站的应用安全状况。借助WSI洞察，您可以降低风险、节省时间、确定活动的优先级并提高整体安全性。

Continuous Dynamic | 可检测的漏洞

技术漏洞

威胁分类

- 功能滥用
- 应用代码执行
- 应用配置错误
- 自动完成属性
- 暴力破解
- 缓冲区溢出
- 可缓存敏感响应
- 点击劫持
- 内容欺骗
- 跨站请求伪造
- 跨站脚本攻击
- 拒绝服务
- 目录索引
- 指纹
- 框架资源
- HTTP响应拆分
- 输入处理不当
- 信息泄露
- 不安全索引
- 反自动化不足
- 授权不完善
- 密码策略执行不完善
- 密码恢复不完善
- 流程验证不完善
- 会话老化不完善
- 输层保护不完善
- LDAP注入
- 邮件命令注入
- 缺少安全报头
- 非HttpOnly会话Cookie
- 操作系统命令注入
- 操作系统命令
- 路径遍历
- 可预测的资源位置
- 查询语言注入
- 远程文件包含
- 路由绕行
- 服务器配置错误
- 会话固定
- 会话预测
- SQL注入
- SSI注入
- 未修补的软件
- 不安全的会话Cookie
- URL重定向器滥用
- XML外部实体
- XML注入
- XPath注入
- XQuery注入

OWASP Top 10

- A1 -访问控制中断
- A2 -加密机制失效
- A3 - 注入
- A4 - 不安全的设计
- A5 - 安全配置错误
- A6 - 易受攻击和过时的组件
- A7 - 认证和验证机制失效
- A8 - 软件和数据完整性机制失效
- A9 - 安全日志记录和监控机制失效(不在范围内)
- A10 - 服务器端请求伪造 (SSRF)

注:每个产品线的兼容列表均可按需提供

Black Duck与众不同

Black Duck® 提供业界最全面、最强大、最值得信赖的应用安全解决方案组合。我们拥有无与伦比的专业知识和经验,来帮助世界各地的组织机构快速保护其软件,在其开发环境中高效集成安全性以及使用新技术进行安全创新。作为软件安全领域公认的领导者、专家和创新者,Black Duck拥有您构建可信软件所需的一切。如预了解更多信息,请访问www.blackduck.com。