Nessus NP™ Professional

全球有一百多万用户已经部署 Nessus® 以进行漏洞风险、配置和合规评估。

Nessus Professional Vulnerability Scanner

Nessus® Professional 是业界部署最广泛的漏洞风险评估解决方案，可帮助您缩小组织的攻击面并确保合规。Nessus 具有快速资产发现、配置审核、目标分析、恶意软件检测以及敏感数据发现等功能。

与竞争解决方案相比，Nessus 支持更多技术，可扫描操作系统、网络设备、下一代防火墙、虚拟机监控程序、数据库、Web 服务器以及关键基础设施的漏洞风险、威胁和不合规情况。

凭借着全球最大且不断更新的漏洞风险和配置检查库，以及 Tenable 专家漏洞风险研究团队的支持，Nessus 树立了漏洞风险扫描速度和准确性的标杆。

完整的漏洞风险覆盖范围

- 虚拟化和云
- 恶意软件和僵尸网络
- 配置审核
- 网络应用程序

主要优点

- **缩小攻击面**：通过识别需要解决的漏洞风险来防范攻击
- **全面性**：符合最广泛的合规和监管标准
- **可扩展性**：从 Nessus Professional 单用户许可证开始，然后随着漏洞风险管理需求的增加，转为 Nessus Manager 或 Tenable.io
- **低 TCO**（总拥有成本）：以低成本获得完整的漏洞风险扫描解决方案
- **不断更新**：Tenable 研究团队不断添加新内容

SC MAGAZINE ★★★★★

Nessus 功能

报告和监控

- 灵活的报告：自定义报告以便按照漏洞风险或主机分类，创建执行摘要，或比较扫描结果以突出显示变化
  - 原生（XML）、PDF（要求在 Nessus 服务器上安装 Java）、HTML 和 CSV 格式
- 对扫描结果、补救建议以及扫描配置改进提供有针对性的电子邮件通知

扫描功能

- 发现：准确、高速资产发现
- 扫描：漏洞风险扫描（包括 IPv4/IPv6/混合网络）
  - 非凭据式漏洞风险发现
  - 系统强化和缺失补丁凭据式扫描
  - 满足内部漏洞风险扫描的 PCI DSS 要求
- 覆盖范围：广泛的资产范围和分析
  - 网络设备：防火墙/路由器/交换机（Juniper、Check Point、Cisco、Palo Alto Networks）、打印机、存储器
  - 网络设备离线配置审核

- 虚拟化 VMware ESX、ESXi、vSphere、vCenter、Microsoft、Hyper-V、Citrix Xen Server
- 操作系统：Windows、OS X、Linux、Solaris、FreeBSD、Cisco iOS、IBM iSeries
- 数据库：Oracle、SQL Server、MySQL、DB2、Informix/DRDA、PostgreSQL、MongoDB
- 网络应用程序：Web 服务器、Web 服务、OWASP 漏洞风险
- 云：扫描云应用程序配置，例如 Salesforce 和云实例（如 Amazon Web Services、Microsoft Azure 和 Rackspace）
- 合规：帮助满足政府、法规和企业要求
- 帮助执行 PCI DSS 要求，以实现安全配置、系统强化、恶意软件检测、网络应用程序扫描和访问控制

- 威胁：僵尸网络/恶意进程/防病毒审核
  - 检测病毒、恶意软件、后门程序、与感染僵尸网络的系统通信的主机、已知/未知进程、链接到恶意内容的 Web 服务
  - 合规审核：FFIEC、FISMA、CyberScope、GLBA、HIPAA/HITECH、NERC、SCAP、SOX
  - 配置审核：CERT、CIS、COBIT/ITIL、DISA STIGs、FDCC、ISO、NIST、NSA、PCI
- 控制系统审核：SCADA 系统、嵌入式设备以及 ICS 应用程序
- 敏感内容审核：PII（例如，信用卡号、SSN（社会保险号码））

Nessus 优势

客户选择 Nessus，是因为它具有以下优势：

- 低误报率的高度准确扫描
- 综合的扫描性能和功能
- 可扩展到成千上万个系统
- 易于部署和维护
- 管理和运行成本低

部署和管理

- 灵活的部署：在内部或服务提供商的云中部署的软件、硬件、虚拟设备。
- 扫描选项：支持非凭据式远程扫描和凭据式本地扫描，以对在线及离线或远程资产进行深入、具体的分析。
- 配置/策略：现成可用的策略和配置模板。
- 风险评分：基于 CVSS 的漏洞风险分级、五个严重性级别（严重、高、中、低、信息）、可重新界定风险的自定义严重性级别。
- 优先顺序：与利用框架（Metasploit、Core Impact、Canvas 和 ExploitHub）相关，并根据可利用性和严重性筛选。
- 可扩展性：RESTful API 支持将 Nessus 集成到现有的漏洞风险管理工作流中。

培训

Tenable 可为不熟悉使用 Nessus 并希望掌握相关知识和技能以最大限度地利用本产品的用户提供培训，同时提供针对更高级用户的合规审核等重点主题培训。相关课程可通过 Tenable 网站按需提供。

更多信息：请访问 tenable.com
联系我们：请发送电子邮件至 subscriptionsales@tenable.com 或访问 tenable.com/contact
版权所有 © 2017 Tenable Network Security, Inc. 保留所有权利。Tenable Network Security 和 Nessus 是 Tenable Network