tenable Security Center Plus

产品资料

通过本地基于风险的漏洞管理升级安全计划

洞察秋毫、精准预测、本地管理，尽在 Tenable Security Center Plus。

> “这套多功能的 Tenable 解决方案非常棒，有了它，我可以随时根据业务目标对安全风险进行优先级分析，并评估企业的安全态势。”
> - 某医疗服务提供商

随着信息技术的不断变化和网络威胁的持续演进，定期扫描和合规性审查已不足以保护企业免受现代网络攻击。要确保企业安全无虞，就需要一个漏洞管理解决方案，可供全面了解攻击面，以便有效管理及度量网络安全风险。

以强大的 Nessus 技术为构建基础，Tenable Security Center Plus 是一款领先于市面其他产品的漏洞管理平台，助力企业在本地实施新一代的漏洞管理。借由高级分析、自定义仪表盘、报告和工作流，Tenable Security Center Plus 可帮助企业透彻了解漏洞管理并降低企业风险。

利用可以结合多种数据和威胁情报来源的预测优先级分析功能，预测某个漏洞遭到利用的可能性，并与动态资产在不断变化环境中的重要性对应匹配。企业由此可以查看与其重要资产密切相关的漏洞并对漏洞进行优先级分析，获得行之有效的见解，最终让企业免遭会对业务造成影响的泄露事件。

图 1: 可高度自定义的仪表盘、报告、工作流以及安全策略，可满足特定的业务需求。

Tenable Security Center Plus 包含超过 350 个可高度自定义的预置仪表盘和报告，有助于企业迅速了解安全合规性、有效性和风险。企业可基于高管层所关心的高级别业务目标和底层可自定义的基本策略，持续度量、分析及查看安全计划的有效性。

主要优势

- **持续可见性**

  持续追踪已知和发现未知资产及其漏洞。识别出有可能演变成漏洞的威胁及意外的网络更改。

- **被动漏洞检测**

  使用针对资产的被动漏洞检测不仅可以执行时间点扫描功能，还可以执行日志发现及进一步分析以检测资产是否发生更改，从而消除盲点。

- **资产和漏洞优先级分析**

  将资产和漏洞数据、威胁情报与大数据分析相结合，以便于了解风险评分，快速识别漏洞以及与其密切有关，并会对业务造成严重风险的重要资产。

- **覆盖广度与深度**

  Tenable Research 与安全社区密切合作，不断发现新漏洞，并提供分析见解，帮助企业展开更健全的漏洞评估实践。Tenable 涵盖超过 79000 个漏洞，拥有业界最为广泛的 CVE 和安全配置支持，帮助您了解所有风险暴露情况。

- **自动化的流程**

  通过充分文档化的 API 以及预建集成，导入第三方数据、自动进行扫描，并与企业 IT 系统共享数据。

主要功能

按需管理数据

Tenable Security Center Plus 是业内领先的本地漏洞管理工具。通过本地或混合部署选项（可以满足最复杂的部署要求）按所需方式管理数据，同时降低企业的风险。

全面的评估选项

Tenable Security Center Plus 可以针对整个攻击面，提供统一可见性。该产品采用的 Nessus 扫描器结合了主动扫描程序、代理程序、被动网络监控和 CMDB 集成，能够最大限度地扫描企业基础设施，从而减少漏洞盲点。混合配置不同类型的数据扫描器可以帮助企业同时追踪和评估已知和未知资产及相关漏洞。

被动漏洞检测

使用针对资产的被动漏洞检测不仅可以执行时间点扫描功能，还可以执行日志发现及进一步分析以检测资产是否发生更改，从而消除盲点。

基于实际风险进行漏洞优先级分析

Tenable Security Center Plus 将漏洞数据、威胁情报和大数据分析相结合，提供易于理解的风险评分，有助于对漏洞进行优先级分析，并了解哪些漏洞需要优先修复。企业可以快速评估风险并识别对企业影响最大的漏洞。

简化漏洞管理

搭配直观的报告、仪表盘外观和易于使用的界面，Tenable Security Center Plus 能帮助您轻松完成配置扫描、运行评估以及分析结果等常规任务。凭借预先按照最佳实践框架定义的扫描模板、配置和合规性审查，保护企业安全变得轻而易举，不像传统漏洞扫描流程那样费时费力。可通过预先配置的开箱即用仪表盘，自定义专属报告与分析，也可以从零开始快速创建，满足企业需求。

了解资产重要性

利用 Tenable 内置于 Tenable Security Center Plus 的资产重要性评级（ACR）功能，可以根据业务价值和重要性指标，预测资产优先级。资产重要性与预测优先级分析共同打造了一种独有漏洞管理方式，让企业可以了解需要优先修复哪些漏洞及其相关资产。

想要了解更多信息：请发送电子邮件至 sales@tenable.com 或访问 zh-cn.tenable.com/contact

Tenable One 集成

Tenable Security Center 数据可与 Tenable One 轻松集成，即刻开启风险暴露管理之旅。充分利用 Lumin Exposure View、Attack Path Analysis 和 Asset Inventory 等高级功能，获得现代攻击面的统一可见性，并主动管理网络安全风险。

简化合规性

通过预定义检查、指标和主动警示违反行业标准和监管规定的行为，掌握并报告合规情况。覆盖 CERT、NIST、DISA STIG、DHS CDM、FISMA、PCI DSS、HIPAA/HITECH 等多种行业标准。

本地 Web 应用程序扫描

使用本地的 Tenable Web App Scanning，轻松集成 Tenable Security Center 数据。在 Tenable Security Center UI 中配置新扫描并分析 Web 应用程序的风险暴露情况。Tenable Web App Scanning 为现代 Web 应用程序提供了简单易用、全面且自动化的漏洞扫描功能，从而让企业可以在无需过多投入人力成本的情况下，快速评估 Web 应用程序。

Tenable Research

Tenable Security Center Plus 以 Tenable Research 为后盾，提供一流的网络风险暴露情报、大数据分析见解、警示以及安全公告。Tenable Research 的高频次更新确保即时提供最新的漏洞检查、零日漏洞研究以及配置基准，有助于保障企业安全。

善用 Tenable Security Center Director

Tenable Security Center Director 是一款附件组件，可以提供集中式管理和风险态势视图，实现化繁为简，并且可以针对整个部署提供多个控制台的完整可见性。

预先构建集成、文档化 API 和集成式 SDK

Tenable 漏洞管理具备开箱即用的集成，可用于授权扫描、SIEM、SOAR、工单和修复系统以及其他辅助解决方案，帮助企业轻松简化漏洞管理流程。请在此处查看完整列表。另外，借助完全文档化的 API 接口，企业可以使用 Tenable Security Center Plus 轻松创建自己的集成。使用这些工具无需额外成本，即可充分利用特定漏洞管理使用案例的价值。