tenable Vulnerability Management

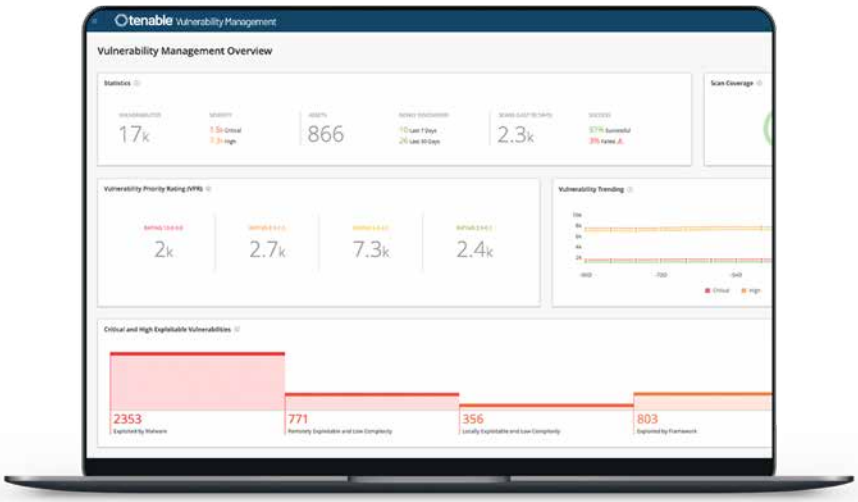
产品资料

掌握风险暴露情况并获悉修复漏洞的优先顺序

发现漏洞并对漏洞进行评估与优先级分析

Tenable Vulnerability Management 有两种使用方式：一是作为 Tenable One 风险暴露管理平台的一部分，二是作为一款独立的产品。Tenable Vulnerability Management 提供了整个攻击面（从 IT 到云，再到 OT 和容器）基于风险的视图，可以快速识别、研究漏洞，并进行优先级分析。企业可以立即获得可见性，从而了解风险并知晓哪些漏洞需要优先修复。

Tenable Vulnerability Management 由 Nessus 提供技术支持，并在云端进行管理，提供业界最全面的漏洞覆盖范围，并且能够预测哪些安全问题需要优先修复。Tenable Vulnerability Management 利用先进的资产识别算法，可以精准掌握处于瞬息万变环境中的动态资产与漏洞等相关信息。作为一款基于云交付的解决方案，Tenable Vulnerability Management 拥有界面直观的可视化仪表盘，综合全面的风险型优先级分析功能，还支持与第三方解决方案的无缝集成，帮助安全团队最大程度地提高效率，实现更高的生产力。



Tenable Vulnerability Management 可针对整个环境中的资产与漏洞提供精准视角，有助于企业根据实际网络安全风险确定修复优先级。

主要优势

- **洞察一切**
  持续追踪已知和未知资产及其漏洞。识别出有可能演变成漏洞的威胁及意外的网络更改。
- **提高生产效率**
  利用解决方案建立在软件即服务 (SaaS) 基础上的优势，首次评估运行时间不超过 5 分钟，且不会对 IT 硬件或维护造成额外负担。
- **漏洞优先级分析**
  将漏洞数据、威胁情报与大数据分析相结合，以便于了解风险评分，从而快速识别出会对业务带来最大影响的风险。
- **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。
- **ROI 最大化**
  借助业内首个基于资产的许可模型，消除因资产拥有多个 IP 地址而导致的双重或三重计数问题。

主要功能

客户友好的弹性资产许可

Tenable Vulnerability Management 带来了业界首个基于资产的许可模型，其中单个资产仅占用一个许可单位，即使该资产拥有多个 IP 地址也一样。该解决方案的弹性模型允许在许可数量暂时超额时，也能继续进行扫描，并自动回收极少扫描资产或一次性扫描所占用的许可。

全面的评估选项

Tenable Vulnerability Management 可以针对整个攻击面，提供统一可见性。该产品采用的 Nessus 传感器结合了主动扫描程序、代理程序、被动网络监控、云连接器和 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。这种不同数据传感器类型相结合的方式，有助于追踪并评估已知和未知的资产及其漏洞，包括难以扫描的资产（如由代理分析的瞬态设备）和敏感系统（如工业控制系统）。

基于资产精准追踪漏洞

Tenable Vulnerability Management 支持跟踪资产和资产漏洞，其准确度优于行业内任何其他解决方案。先进的资产识别方式涵盖了大量属性（如 Tenable ID、NetBIOS 名称、MAC 地址及其他众多属性），无论资产以何种方式漫游或接入时间多长，均能准确识别并追踪资产更改。

基于实际风险进行漏洞优先级分析

Tenable Vulnerability Management 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

Tenable Vulnerability Management 通过现代化的界面以及一目了然的仪表盘，将扫描配置、运行评估以及分析结果等常规任务，变得前所未有的简单。凭借预先按照最佳实践框架（如 CIS 和 DISA STIG）定义的扫描模板以及配置审查功能，保护企业安全轻而易举，不需要像之前一样大费周章。可通过预先配置的现成仪表盘，自定义专属报告与分析，也可以从零开始快速创建自定义报告与分析，满足企业需求。

联系我们：请发送电子邮件至 sales@tenable.com 或访问 zh-cn.tenable.com/contact

自动化的云可见性

Tenable Vulnerability Management 能够持续评估公有云环境并提供全面可视性。云连接器可自动识别 Amazon Web Services、Microsoft Azure 以及 Google Cloud Platform 中的资产，并实时监控资产状态。借助 Nessus 传感器检测漏洞、恶意软件，以及配置和合规性问题，全面评估云环境。

运营技术 (OT) 可见性

将 Tenable Vulnerability Management 与 Tenable OT Security 集成，即可获得针对融合式基础设施的统一风险视图。获得持续可见性、威胁检测和缓解、自适应评估、漏洞管理和配置控制，抵御可能使企业陷入风险的 OT 和 IT 威胁。

预先构建集成、文档化 API 和集成式 SDK

Tenable Vulnerability Management 已预先构建了集成（即插件），可用于常见的凭证管理、SIEM、工单系统和其他互补性解决方案，让您轻松创建高效的漏洞管理流程。请在此处查看完整列表。另外，也可以使用完全文档化的 API 集和 SDK 在 Tenable Vulnerability Management 中轻松创建自己的集成。使用这些工具无需支付额外成本，即可充分发挥漏洞数据的价值。

SLA 正常运行时间保证

Tenable 通过强大的 Tenable Vulnerability Management 服务级别协议 (SLA)，提供漏洞管理业界首例也是唯一的正常运行时间保证。如果未达到 SLA，我们将提供服务积分补偿，这也是一些全球领先的云服务提供商（如 Amazon Web Services）一贯的做法。

得到 PCI 认证的授权扫描供应商

Tenable Vulnerability Management 是一款得到 PCI 认证的授权扫描供应商 (ASV) 解决方案，使商户和服务提供商能够根据 PCI 数据安全标准 (PCI DSS) 外部网络漏洞扫描要求，证明其面向网络系统的安全性。

以 Tenable Research 为后盾

Tenable Vulnerability Management 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、预警以及安全公告。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，有助于保障客户所在企业的安全。