公司概况

我们致力于解决的问题

现代攻击面正在不断扩大，并持续变化，相互之间的关联比以往任何时候都更复杂。为了应对这种情况，安全团队部署了多种安全技术，每种技术都有各自的分析，缺乏一致的报告。不同的工具可能导致重复工作和无效程序，没有明确的前进道路来切实降低风险或简洁地传达企业安全态势。更糟糕的是，这种对网络安全采取被动灭火的做法，使防御者处于严重劣势。

网络安全团队需要一种统一、预测和主动的方式来管理其整个攻击面的风险暴露。Tenable One 风险暴露管理平台可以提供上下文风险意识，以及从被动方法转变为预防方法所需的能力，使得安全团队可以在威胁造成损害之前预测和阻止威胁。

简介

创立
2002

总部
- 美国马里兰州哥伦比亚
- 国际总部位于爱尔兰都柏林
- 在 40 多个国家和地区设立分公司

市场覆盖
- 超过 40,000 家客户
- 超过 60% 的财富 500 强公司
- 超过 40% 的全球 2000 强上市公司

领导层
董事长兼首席执行官 **Amit Yoran**
首席产品官 **Nico Popp**
首席技术官 **Glen Pendley**
首席财务官 **Steve Vintz**
首席人才和文化官 **Bridgett Paradise**
首席运营官 **Mark Thurmond**
首席营销官 **Brian Goldfarb**
首席营收官 **Dave Feringa**
运营、全球业务拓展和渠道执行副总裁 **Terry Dolce**
首席传播官 **Michela Stribling**
首席安全官 **Robert Huber**
首席信息官 **Patricia Grant**
企业发展与战略高级副总裁 **Matt Olton**

关于 TENABLE

Tenable® 是一家风险暴露管理公司。Tenable 帮助全球约 40000 家企业了解和减少网络安全风险。Tenable 是 Nessus® 产品发明者，凭借在漏洞方面的专业技术，推出了全球首个检查和保护各种计算平台上数字资产风险的平台。Tenable 的客户包括 60% 左右的《财富》500 强企业、40% 左右的全球 2000 强企业和大型政府机构。
详情请访问 zh-cn.tenable.com。

Tenable One 风险暴露管理平台

Tenable One 旨在帮助企业在整个现代攻击面上获得可见性，集中精力预防可能发生的攻击，并准确传达网络安全风险，以支持企业达到最佳绩效。Tenable One 平台提供了广泛的漏洞覆盖范围，涵盖 IT 资产、云资源、容器、Web 应用程序和身份系统。

TENABLE 提供的功能有：

云安全
Tenable 提供完整的多云环境可见性和安全性，可以在单一管理平台提供漏洞、错误配置和漂移的统一视图。通过基于风险的评分、合规性报告和自动修复，快速对措施进行优先级分析，将平均响应时间 (MTTR) 提高到 99%。

Web 应用程序安全
Web 应用程序无处不在，对业务至关重要，同时又不断变化。Tenable 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。用户可以配置和管理 Web 应用程序扫描，并在几分钟内即可收到可操作的结果。

Active Directory 安全
几乎每个重大数据外泄事件的背后都是一起针对 Active Directory (AD) 的攻击，使得攻击者能够提升特权并促进横向移动。Tenable 支持用户查看其 AD 环境中的所有资产，预测重要风险，并在攻击者利用风险之前解决风险，以阻断攻击路径。

基于风险的漏洞管理
传统的漏洞管理 (VM) 工具已完全跟不上当今的 IT 环境。基于风险的漏洞管理对于优先对哪些漏洞进行修复而言，杜绝了主观臆断。

外部攻击面管理
可见性是网络安全的基础，但很少有企业能够掌握。外部攻击面管理 (EASM) 会挖掘整个互联网，从而发现企业的所有域。识别并保护以前未知的连接互联网的资产，以消除盲点。

运营技术安全
工业数字转型提高了控制力、效率、产量和安全性，但这并非没有风险。Tenable 提供了完整的可见性、统一的安全和对威胁管理的优先级分析功能，以帮助缓解 IT 和 OT 集成环境中的风险。

基于 Nessus，漏洞评估领域的黄金标准
了解漏洞是风险暴露管理的基础，而 Nessus 正是 Tenable One 的核心。Nessus 可以帮助用户评估其现代攻击面，提供准确环境状况，以便用户能够快速有效地采取措施。