tenable

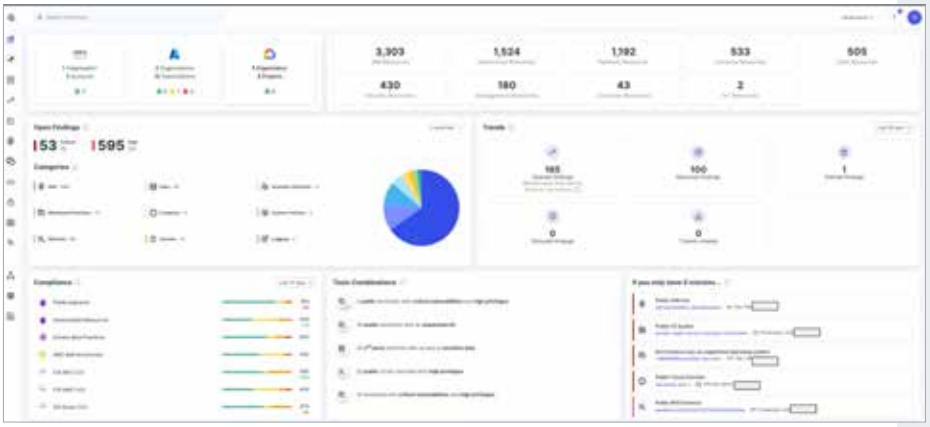
产品资料

云原生应用程序保护平台 (CNAPP)

Tenable Cloud Security：覆盖基础设施、身份与工作负载的安全之网

对云服务的快速采用让环境变得愈发复杂与分散，攻击面也随之扩大。与此同时，大量各自为政的工具、快速的变化以及缺乏云安全和合规性专家来保护业务安全，这些问题已经让企业举步维艰。

借由在一个集成式解决方案中提供统一的云应用程序安全平台 (CNAPP)，由此查看并保护多云环境的所有云资产，Tenable Cloud Security 便可以解决上述所有难题。Tenable Cloud Security 支持从全面的资产发现和深入风险分析到运行时威胁检测和合规的所有功能，通过提供富有参考价值的可视化信息与分步式指南，可以将复杂难懂的安全操作自动化。利用对身份和基础设施依赖项的深入理解，这一解决方案可以对安全缺口进行优先级分析与修复，不仅有助于缩小云攻击面，还能规模化实施最低权限。



关键优势

全面可见性
获得所有云的全方位资产和风险暴露视图

减少风险暴露
了解安全缺口的优先级分析并立即实施修复措施

持续治理
为开发到部署的整个生命周期保驾护航

简化合规
利用自动化的合规报告，最大限度地缩短报告时间与减少相关工作量

加速修复
利用有价值的可视化信息与分步式修复措施

扩展安全运营
让所有人都可获得见解，提高企业的安全工作效率

Tenable Cloud Security 是一种可在几分钟部署完毕的无代理式解决方案，可以在几小时内提供切实可行的见解，让利益相关者借由精准的风险优先级分析信息，修复从代码到云的所有安全问题

关键功能

多云资产管理和统一的可见性

覆盖云环境所有身份、数据、基础设施和工作负载的深入集中可见性，为企业带来诸多益处。

云安全态势管理 (CSPM)

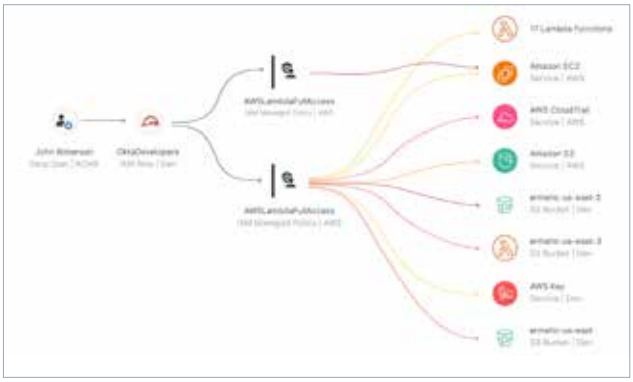
利用一种解决方案来简化云合规事宜。这种解决方案不仅可以持续扫描所有云的配置与资源，还能够识别违规行为与进行自动化修复。

云工作负载保护 (CWP)

扫描和检测关键风险，识别虚拟机、容器和无服务器功能中的漏洞、泄露的机密/敏感数据、恶意软件和错误配置。

云基础设施授权管理

揭示手动检测几乎无法发现的问题，充分利用精准且自动化的修复措施。



Kubernetes 安全态势管理 (KSPM)

确保 Kubernetes 集群处于默认安全状态。如果检测到错误配置，则会主动告知问题，以便相关的利益相关者快速缓解与解决这些错误配置。

保护基础设施即代码的安全

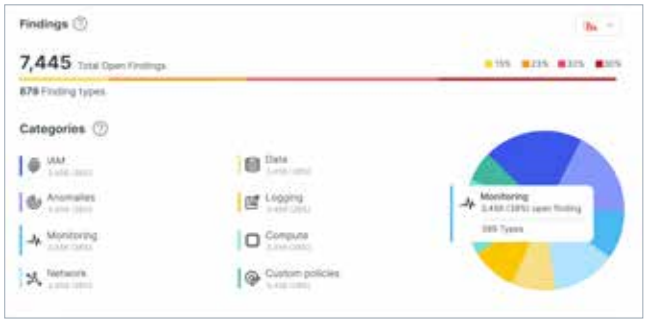
发现基础设施即代码 (IaC) 中的错误配置与其他风险，在 CI/CD 管道中加固云基础设施环境的安全，避免因部署而产生风险。

云检测和响应 (CDR)

采用持续行为分析与异常检测，快速识别与调查云威胁。

全堆栈式风险分析与优先级分析

利用全堆栈式分析揭示如可能会泄露敏感数据等风险情况，从而提供切实可行的见解。



自动修复

自动执行可修复问题的响应措施，加速修复云基础设施风险的速度。

自助式即时访问权限

根据需要，快速批准访问权限，最大限度地缩小云攻击面，避免因无法及时撤销特权所带来的风险。

关于 Tenable

Tenable® 是一家风险暴露管理公司。Tenable 帮助全球约 43000 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。

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