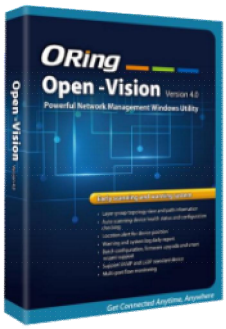
Open-Vision Pro 5.0

专为网络安全设计的网络管理软件



特性

- 基于网页的管理操作界面
- 通过防火墙收集安全相关的事件和日志
- 通过自动化分析来识别真实威胁与攻击
- 支持分级用户角色（如系统管理员、管理员、普通用户）分配特定权限
- 设备端口流量监控与告警功能，允许用户自定义阈值参数
- 通过 IP 扫描检测本地网络中的所有 Oring 交换机及第三方 SNMP 设备
- 自动绘制整个网络拓扑结构
- 动态拓扑视图可清晰展示网络连接状态及事件通知
- 支持包含端口号信息的多链路拓扑
- 支持环网状态信息显示（ORing 拓扑视图）

产品描述

在监控和管理网络中所有设备时，将网络安全与网络管理软件相结合对于管理员来说至关重要，基于此 ORing 正式发布 Open-Vision Pro 5.0 网管软件。Open Vision Pro 5.0 在三个核心领域比以前的版本有了重大改进：CyberSIEM、可视化管理和综合监控。我们将详细介绍这些增强功能，并解释高级监控功能和网络安全防御如何使用户能够及时检测和响应本地网络中的任何问题。

因此，Open Vision Pro 5.0 可以确保本地网络的稳定性和安全性。

CyberSIEM:

Open Vision Pro 5.0 是一款功能强大的网络安全集成网络管理软件，支持名为 cyberSIEM 的新功能，这是一种即时协作预防系统。它可以从防火墙收集与安全相关的事件和日志，以识别潜在的入侵或恶意行为并生成警报。当检测到恶意流量时，它可以立即采取行动阻止攻击并减轻潜在威胁。对现场自动化资产的持续监控有助于减少异常造成的运营损失。

可视化管理:

ORing 的拓扑视图可以显示复杂的拓扑，包括本地网络中所有 ORing 以太网交换机和第三方 SNMP 设备的多链路拓扑。

此外，不同的设备可以按不同的 IP 分组，并在不同的拓扑窗口中显示。因此，管理员不需要同时监控本地网络中的所有设备，这使得监控工作更容易、更高效。 另一方面，连接的健康状态将以不同的颜色显示。 ORing 拓扑视图帮助管理员以可视化、直观和更高效的方式进行管理。

综合监控:

ORing Vision Pro 5.0 具有多种机制来监控 ORing 交换机的状态，包括事件日志和 SNMP 陷阱。管理员将通过电子邮件收到任何异常事件的通知，事件日志列表可以导出为 excel 文件。此外，可以保存所有 ORing 交换机的配置，并定期扫描本地网络中所有交换机的配置状态，以检测配置的任何变化。因此，管理员可以知道交换机配置的任何意外更改。另一方面，ORing Host 监视器可以自动

ping 和检查局域网中所有基于 IP 的设备之间连接的健康状态。主机监视器还具有 IP 分类功能，所有基于 IP 的设备都可以按不同的 IP 分组并被监视。

规格

型号	Open-Vision 50	Open-Vision 100	Open-Vision 300	Open-Vision 500	Open-Vision 1000
设备数量	50	100	300	500	1000
	免费下载使用	使用许可证密钥解除数量限制			
架构	基于网页的操作界面				
语言	英语				
拓扑视图					
账户管理	支持账户创建与管理 具有特定权限的支持角色（系统管理员、管理员、普通用户）				
许可证管理	支持激活与停用许可证				
设备发现	支持 Oring 及第三方 SNMP 设备 支持连接至交换机的终端设备（需启用设备绑定功能） IPv4 地址范围扫描 支持手动添加新设备 支持从现有备份文件直接加载拓扑结构，无需重新发现				
链接发现	支持手动创建链接 支持拓扑中的冗余链路（虚线表示备用链路） 支持具有相对端口号的多种链路拓扑结构				
拓扑视图	显示设备信息（包括 IP 地址、系统名称、描述及端口号）；支持第三方 SNMP 设备（可自定义设备图标）。 显示网络冗余协议的设备角色 支持自定义设备图标 支持拓扑集中布局模式				
设备信息	设备名称、设备描述、IP 地址、MAC 地址 环网信息				
主机监控	支持持续监控指定主机的连接状态，并在检测到断线时触发警报或执行操作，以确保网络稳定性。				
流量分析	所有端口的流量信息 多端口性能监控 流量预算设置及流量告警 记录历史网络流量				
拓扑保存	支持将拓扑结构保存至拓扑备份文件；支持打印当前拓扑结构				
刷新	支持按特定时间间隔进行定期发现 支持手动刷新 支持在不稳定的网络环境中设置重试次数				
SNMP（简单网络管理协议）	支持数据捕获代理接收 SNMP 告警； 支持 SNMP V1、V2 及 V3 版本。				
系统日志	支持事件日志和 SNMP 陷阱 支持日志记录清除 支持将日志导出为 CSV 文件				
事件处理	支持断开连接事件处理，以确认事件状态				
CyberSIEM					
检测恶意行为	支持监控网络流量、识别潜在入侵或恶意行为，并生成警报				

实时威胁拦截	支持立即采取行动阻止攻击，从而减轻潜在威胁
系统要求	
操作系统	Windows 11 Windows 10
浏览器	谷歌浏览器、微软 Edge 和火狐浏览器
硬件要求	
中央处理器	英特尔酷睿 2 双核处理器，频率为 2.4 GHz 或更高
随机存取存储器	1G 或更高版本
硬盘空间	1G 或更高版本
终端设备要求	
网络协议	TCP /IP UDP 简单网络管理协议

订购信息

Open-Vision Pro v5.0

Open-Vision 50	强大的网络管理功能，基于Windows系统的网页操作界面，支持50台IP设备
Open-Vision 100	强大的网络管理功能，基于Windows系统的网页操作界面，支持100台IP设备
Open-Vision 300	强大的网络管理功能，基于Windows系统的网页操作界面，支持300台IP设备
Open-Vision 500	强大的网络管理功能，基于Windows系统的网页操作界面，支持500台IP设备
Open-Vision 1000	强大的网络管理功能，基于Windows系统的网页操作界面，支持1000台IP设备