



Vulnerability Manager Plus

完整的漏洞管理解决方案

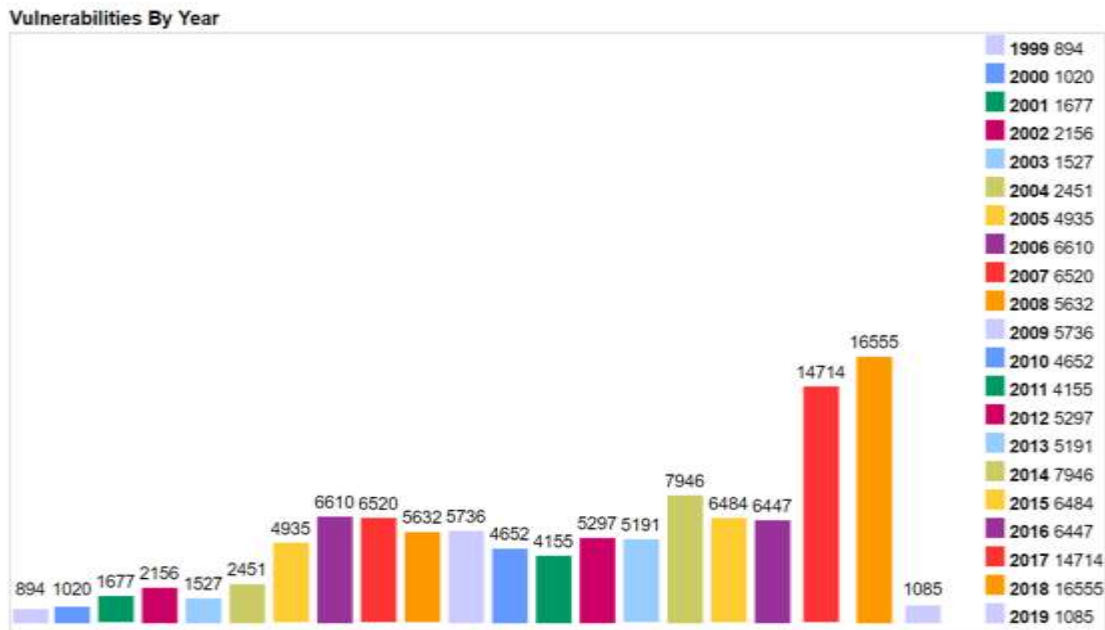
什么是 Vulnerability Manager Plus?

Vulnerability Manager Plus 是一个企业威胁和漏洞管理解决方案，可以从单一控制台对网络中的所有计算机进行漏洞的扫描、评估、修复。

为什么需要漏洞管理？

漏洞一直在上升

据报道，2018年大约有16555个漏洞，相较于2017年有12.51%的增长。



Source: [CVE details](#)

漏洞管理的挑战

- 漏洞在持续增长
- 缺少资源和时间去从大量的漏洞中预测真正的风险
- 无法掌握企业的整体安全态势
- 无法跟踪并修复网络中的安全漏洞

Vulnerability Manager Plus 是怎样工作的?

扫描



扫描所有被管计算机

评估



基于攻击者的分析，优先
处理更可能被利用的漏洞

管理



避免网络中的安全漏洞的被利用，
防止进一步出现漏洞

功能概览

- 漏洞评估
- 安全配置管理
- 补丁管理
- 强化Web服务器
- 高危软件审计

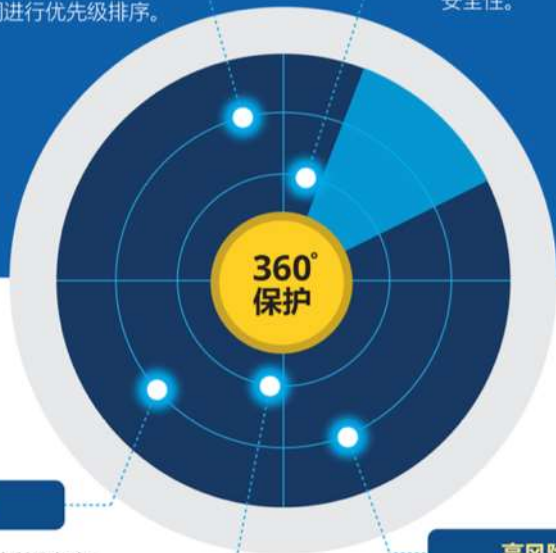
通过预防性漏洞管理减小攻击范围

漏洞评估

利用基于攻击者的分析，对可能被攻击者利用的漏洞进行优先级排序。

安全配置管理

删除不适当的安全配置，增强系统安全性。



补丁管理

决定修补什么、何时修补以及如何修补。更重要的是，实现自动化。

高风险软件审计

只需点击一下，即可审计并删除网络中未经授权、不受支持的软件。

Web服务器强化

保护面向互联网的服务器免受多种攻击，如XSS、Clickjacking等。

漏洞评估

- ❖ 通过持续监控和自动扫描随时了解新出现的漏洞。
- ❖ 根据漏洞的可利用性、严重性、存在时间、受影响的系统数量以及是否有修复程序等来评估并确定其优先级。
- ❖ 识别并评估0-day漏洞，比如Wannacry、Petya、meltdown和spectre等等。
- ❖ 深入洞察网络中的漏洞趋势，安全态势等。
- ❖ 实时获取到网络中前20高危漏洞列表。

安全配置管理

- ❖ 跟踪和识别配置变化。
- ❖ 审计防火墙策略、共享、未授权的用户、弱密码、过时协议和其他不当的配置。
- ❖ 在不中断业务操作的情况下，安全地发生安全配置告警。

补丁管理

- ❖ 自动部署补丁到Windows, Mac, Linux 以及超过250多种第三方应用程序。
- ❖ 自定义部署策略, 不影响业务操作。
- ❖ 在部署补丁到生产环境之前测试并批准补丁。
- ❖ 对指定的组设置忽略补丁策略。

强化Web服务器

- ❖ 持续地监控Web服务器和不安全的配置
- ❖ 根据上下文分析Web服务器的错误配置，并获得修复的详细信息
- ❖ 确保配置SSL证书，HTTPS被启用，从而保证客户端和服务器的通信安全

高危软件审计

- ❖ 持续监控网络中的终端，检测要下架的软件，P2P软件和远程共享工具。
- ❖ 获取关于软件过期日期和即将下架的软件。
- ❖ 实时获取受这些软件影响的计算机数量。
- ❖ 只需要在控制台点一下就可以清除这些软件。

防病毒软件审计

- ❖ 终端上安装了哪些杀毒软件。
- ❖ 已安装的杀毒软件是否启用，是否需要更新。
- ❖ 从控制台直接部署防病毒软件更新；

说明：部署防病毒更新支持：Windows Defender Antivirus和Mcafee Virusscan Enterprise

端口审计

- ❖ 持续监控终端活跃的端口
- ❖ 识别端口类型 (TCP还是UDP)
- ❖ 根据端口范围过滤端口
- ❖ 识别每个的端口的实例数量
- ❖ 查看端口对应的计算机、进程、进程路径、进程描述等

和传统漏洞管理的提升

- ❖ 无需额外的费用，对用每种漏洞都提供内置的补丁模块。
- ❖ 运行推荐的脚本来缓解0Day漏洞，无需等待厂商提供补丁。
- ❖ 洞察企业全网的杀毒软件保护状态。

智能报表

- ❖ 提供丰富的安全状态历史报表。
- ❖ 提供预置报表来追踪漏洞进展并持续关注。
- ❖ 按照自己的需求来通过SQL语句来定制报表。

版本对比

共有3个版本

免费版

管理至多25台电脑

- » 适用于中小型企业
- » 功能齐全
- » 最多25台电脑

专业版

适用于局域网中的计算机

- » 漏洞扫描和评估
- » 系统配置错误检测
- » 高风险软件检测
- » 检测和解决服务器错误配置
- » 漏洞报表

企业版

适用于WAN中的计算机

专业版功能+

- » 安全配置部署
- » 自动化补丁部署
- » 测试和批准补丁
- » 高风险软件卸载
- » 零日漏洞缓解

Vulnerability Manager Plus带来的收益

- ❖ 降低漏洞管理的成本和工作量。
- ❖ 获得漏洞管理集成的控制台和实时仪表板，简化漏洞管理。
- ❖ 排除安全死角，最大程度确保安全。
- ❖ 灵活且易用。

<https://www.manageengine.cn/vulnerability-management>

support@manageengine.cn