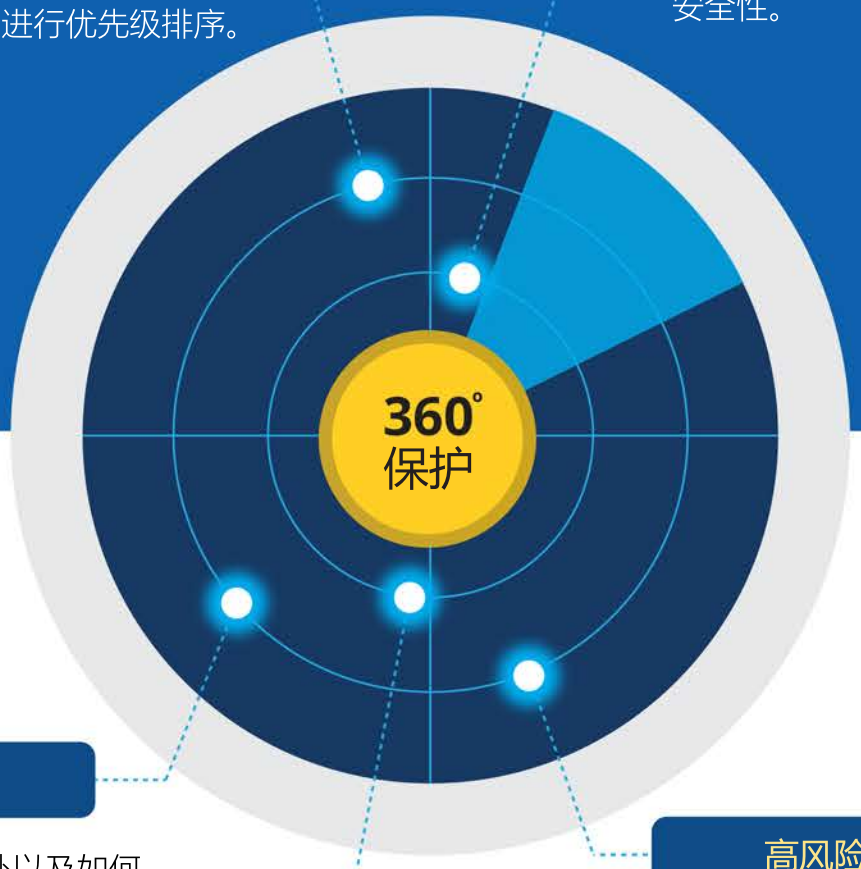
ManageEngine
# Vulnerability Manager Plus

## 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。

## 当前挑战

Gartner预测，“到2020年年底，99%被利用的漏洞仍将是安全和IT专业人员已知的漏洞。”网络安全意识和集中化管理方式的欠缺使许多组织容易受到网络攻击，例如，2019年披露的22316个新的安全漏洞中，超过三分之一的漏洞可被用于攻击。随着这些数字的飙升，组织需要实施一种战略方法来确定优先级并管理漏洞，因为并不是所有的漏洞都构成相同的风险。

## 解决方案

ManageEngine Vulnerability Manager Plus是面向企业的、聚焦优先级的漏洞管理软件，提供内置补丁管理。它是针对您的安全团队的战略解决方案，可以从一个控制台提供对所有IT资产（服务器、台式机、笔记本电脑、虚拟机、DMZ服务器和漫游设备）的威胁和漏洞的全面可见性、评估和修复。

检测 800+ 应用程序的漏洞

支持18 种 语言

1 个平台 集中管理补丁和漏洞

可扩展到 50000 台计算机

30 天 全功能免费试用

# Vulnerability Manager Plus如何增强您的网络安全性

## 漏洞评估

- 识别漏洞及其上下文，如CVSS和严重性，以确定优先级、紧急性和影响程度。
- 实时掌握漏洞攻击代码是否已公开披露。
- 密切关注漏洞在网络中存在的时间。
- 根据影响类型和补丁可用性过滤漏洞。
- 获得基于上述风险因素的重点漏洞修复建议。
- 对于公开披露的漏洞和零日漏洞，在修复发布前利用规避方案来降低漏洞的影响。
- 隔离并识别关键资产（即保存关键数据并执行关键业务操作的数据库和web服务器）中的漏洞。

## 安全配置管理

- 识别操作系统、应用程序和浏览器中的错误配置，并使其恢复合规性。
- 审计防火墙、杀毒软件和BitLocker状态。
- 强制执行复杂密码、账户锁定和安全登录策略，防止暴力破解。
- 确保已启用内存保护设置，如结构化异常处理覆盖保护(SEHOP)、数据执行防护 (DEP) 和地址空间布局随机化(ASLR)。
- 终止弊大于利的遗留协议。
- 管理共享权限，修改用户账户控制并禁用遗留协议，以减小攻击范围。
- 通过查看关键部署警告，在不中断业务操作的情况下安全地更改安全配置。

## 自动化补丁管理

- 自动关联漏洞情报和补丁管理。
- 自动修补Windows、macOS、Linux和300多个第三方应用程序。
- 定制部署策略，实现轻松部署。
- 在将补丁发布到生产机器前，测试并批准补丁。
- 根据实际情况，设置忽略补丁策略。

## Web服务器强化

- 持续监视Web服务器的默认配置和不安全配置。
- 基于上下文分析Web服务器错误配置，并获得安全建议。
- 确保已配置SSL证书并启用HTTPS，以保护客户端和服务器之间的通信。
- 验证是否已限制服务器根目录权限，以防止未经授权的访问。

## 高风险软件审计

- 对已结束或即将结束生命周期的遗留软件保持警觉。
- 获取被认为不安全的P2P软件和远程共享工具的实时信息。
- 持续查看系统中的活动端口，并找出占用该端口的恶意程序的进程。

## 代理硬件要求

| 处理器 | 处理器速度 | 内存大小 | 硬盘空间 |
|---|---|---|---|
| Intel Pentium | 1.0 GHz | 512 MB | 100 MB |

## 服务器硬件要求

| 管理的设备数量 | 使用的服务器 | 处理器 | 内存 | 硬盘空间 |
|---|---|---|---|---|
| 1 至 250 | Vulnerability Manager Plus Server | Intel Core i3 (2 core/4 thread) 2.0GHz 3MB cache | 2GB | 5GB |
| 251 至 500 | Vulnerability Manager Plus Server | Intel Core i3 (2 core/4 thread) 2.4GHz 3MB cache | 4GB | 10GB |
| 501 至 1,000 | Vulnerability Manager Plus Server | Intel Core i3 (2 core/4 thread) 2.9GHz 3MB cache | 4GB | 20GB |
| 1,001 至 3,000 | Vulnerability Manager Plus Server | Intel Core i5 (4 core/4 thread) 2.3GHz 6MB cache | 8GB | 30GB |
| 3,001 至 5,000 | Vulnerability Manager Plus Server | Intel Core i7 (6 core/12 thread) 3.2GHz 12MB cache | 8GB | 40GB |
| | SQL Server | Intel Core i7 (6 core/12 thread) 3.2GHz 12 MB cache | 8GB | 30GB |
| 5,001 至 10,000 | Vulnerability Manager Plus Server | Intel Xeon E5 (8 core/16 thread) 2.6GHz 20MB cache | 16GB | 60GB |
| | SQL Server | Intel Xeon E5 (8 core/16 thread) 2.6GHz 20MB cache | 16GB | 40GB |
| 10,001 至 20,000 | Vulnerability Manager Plus Server | Intel Xeon E5 (8 core/16 thread) 2.6GHz 40MB cache | 32GB | 120GB |
| | SQL Server | Intel Xeon E5 (12 core/24 thread) 2.7GHz 30MB cache | 32GB | 80GB |

如果您管理的计算机超过1000台，我们建议您在Windows Server上安装Vulnerability Manager Plus。

## 软件要求

| 服务器支持的操作系统 |
|---|
| Windows 7 / 8 / 8.1 / 10 / Servers 2003 / 2003 R2 / 2008 / 2008 R2 / 2012 / 2012 R2 / 2016 / 2019 |

## 代理支持的操作系统

| Windows 操作系统 | Windows Server 操作系统 | MAC 操作系统 | Linux 操作系统 |
|---|---|---|---|
| Windows 10 | Windows Server 2019 | 10.15 | Ubuntu 10.04 及以上 |
| Windows 8.1 | Windows Server 2016 | 10.14 | Debian 7 及以上 |
| Windows 8 | Windows Server 2012 R2 | 10.13 | CentOS 6 & 7 |
| Windows 7 | Windows Server 2012 | 10.12 | Red Hat 6 & 7 |
| Windows Vista | Windows Server 2008 R2 | 10.11 | SUSE Enterprise Linux 11 及以上 |
| Windows XP | Windows Server 2008 | 10.10 | |
| | Windows Server 2003 R2 | 10.9 | |
| | Windows Server 2003 | 10.8 | |

## 可选版本

**免费版**
20个工作站和5个服务器的完整漏洞管理
**专业版**
适用于局域网
**企业版**
适用于广域网和局域网

## 联系我们


https://www.manageengine.cn/vulnerability-management/
support@manageengine.cn
(86) 400-660-8680