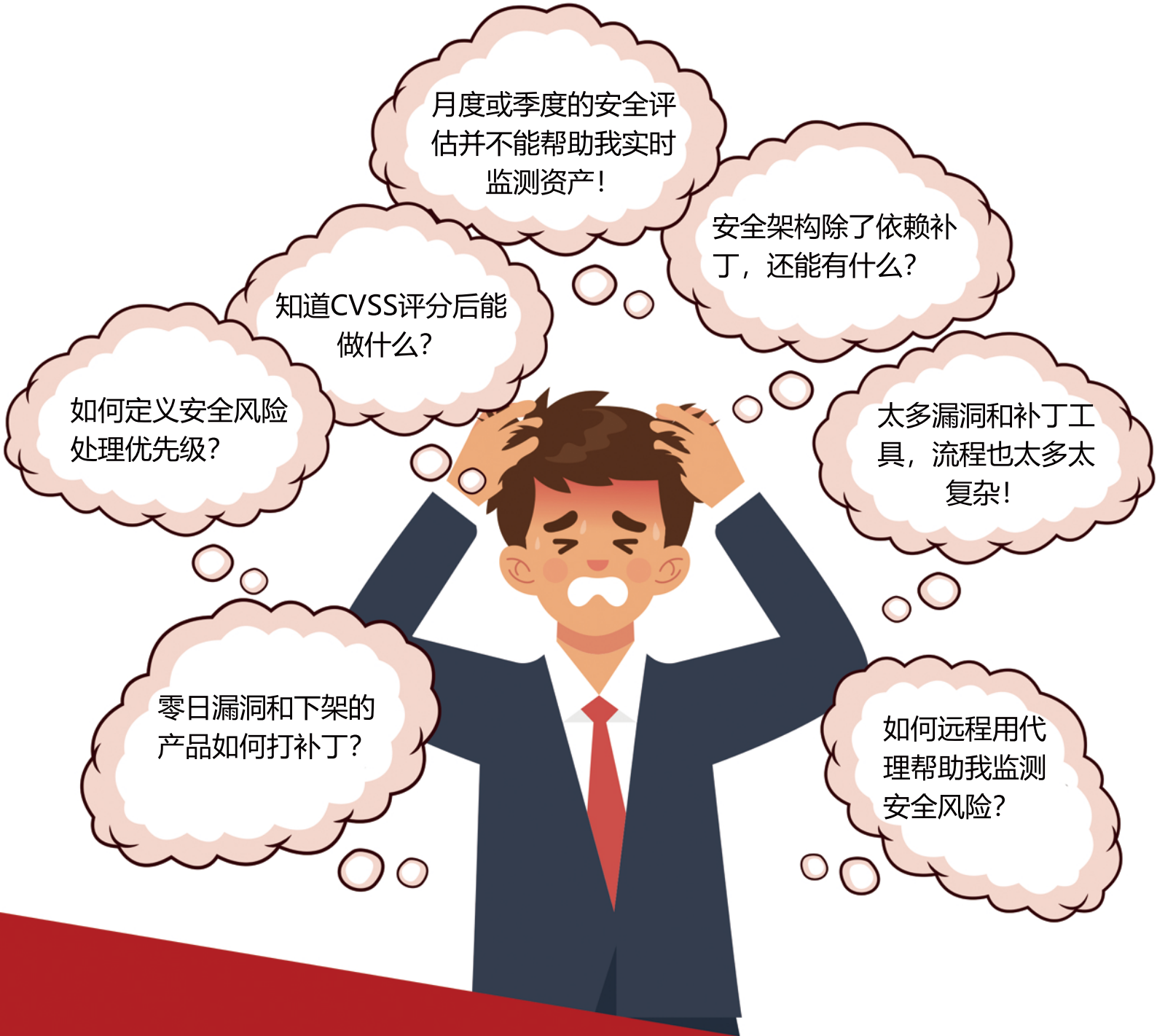
7个安全管理重大问题的答案



ManageEngine
Vulnerability Manager Plus

过去，在“周二补丁日”后，系统管理员仅需一两周就能更新完网络中所有补丁。而今，IT环境日趋复杂化，这种补丁管理模式已经不再适用。随着全球网络终端、应用和操作系统的多样化，以及漏洞的不断激增，组织正面临着更大的网络风险。

此外，超出漏洞范围的攻击方式也在不断增加。漏洞管理开始逐渐受到组织的重视，但通常组织会有一系列疑虑。

我应该多久扫描一次网络？需要重点关注哪些方面？漏洞管理真的会降低风险吗，还是仅为了合规而做的繁琐工作？确定安全风险处理优先级需要考虑哪些因素？我如何挑选一个全面的漏洞管理解决方案？安全架构应该完全依赖于补丁吗？如果我的网络中出现零日漏洞怎么办？

在这个电子书中，我们将探讨7个漏洞管理难题，一次性解答您的所有疑虑。除了回答常见的漏洞管理问题外，我们还提供了漏洞管理各个阶段的最佳实践指南。另，阅读此电子书，需要对漏洞管理的基础知识有一定了解。

本书各章节内容独立，读者可根据自己的需求，按顺序阅读，或随意翻阅，点击目录中的链接，可跳转到您感兴趣的部分。

目录

使用代理进行漏洞管理有什么优势？如果是远程工作环境呢？

有效的漏洞管理产品的关键在于消除盲点，而终端代理能很好地解决这个问题。基于代理的扫描所提供的可见性、准确性和效率性，是无代理扫描无法实现的。

无代理扫描会对网络造成影响，每一次基于网络进行扫描以获取网络资产的漏洞状态，都可能产生流量阻塞问题。另外，要想访问和运行针对资产的全面扫描，检查文件系统、注册表和配置，还需要提供主机凭证。这就带来了更多的管理问题，既要确保凭证的持续更新，又要确保存储安全，以防止凭证泄漏。

而安装在终端的代理则是一款轻量级、多用途工具。无需凭证，即可持续监视并发现新新漏洞、错误配置和其他问题，也不会有扫描时间限制或阻塞网络带宽的情况。

现代代理连接到漏洞管理服务器的IP地址，因而可以通过网络终端的动态IP来实现持续追踪网络资产。此外，代理可以直接从服务器复制补丁二进制文件到客户端机器，无需每个客户端机器都下载补丁，大大降低了总体带宽消耗。

自从为应对COVID-19而迅速转向远程工作模式以来，许多组织一直依赖VPN网关进行漏洞扫描和补丁管理。但这种做法通常会导致更新进程缓慢。另外，并不是所有使用VPN的设备都能与网络保持稳定连接。

终端的网络连接经常会出现断开的情况，在扫描时，如果这些设备未连接到网络，无代理的扫描可能会漏掉这些终端，从而使终端积累大量的漏洞，尤其是这些漏洞中很大一部分超出了边界安全的范围，暴露于危险的网络环境中，对系统安全构成了威胁。

根据国际数据公司（IDC）的数据，“70%的成功入侵都是从终端开始的。”

除边界安全问题外，无论是移动设备、远程设备还是外网设备，组织都需要掌握这些资产的位置，并确保每个资产的安全。面对全球多样化的IT环境，终端代理可以实现对远程终端的持续监视和控制。

在远程终端上安装代理后，通过代理，您可以直接从受信任的厂商下载需要的补丁到远程机器上，远程用户无需通过VPN登录到内部网络，从而避免了VPN带宽不足问题。终端代理不受位置限制，从扫描风险和漏洞到部署修复方案，所有操作都可以通过远程终端代理无缝执行。

根据合规性需求，月度或季度的安全评估是否足够？

尽管在全球范围内，由于未打补丁和不安全的系统导致了大量网络侵入事件，并且让组织损失惨重，但仍有很多组织尚未意识到，他们网络中的漏洞随时都可能被利用。事实上定向攻击并不常见，绝大多数攻击都是利用已知的漏洞，而这些漏洞广泛存在于全球数以百万计的终端上。

然而，许多组织仍然认为，漏洞评估只是为了应付审计要求，基本上每月或每季度才扫描一次，更有甚者，每年一次。 这些时间点快照，对掌握网络安全状况没有任何意义。

首先，过长的扫描周期导致一次性扫描的数据量过大，生成的报告多达数百页，需要花费几周到几个月的时间来查看。这种扫描无意义的一个主要原因是，系统每90分钟就需要识别一次新的漏洞，并且定期提供这些漏洞的补丁。可能在您分析完扫描结果之前，网络中已经出现了新的漏洞。

近年来，漏洞从披露到主动利用之间的时间差越来越短，凸显了定期进行漏洞扫描的紧迫性。仅仅一个高风险漏洞，就足以摧毁您的企业。因此，要确保持续的漏洞管理，基于月度或季度审计的评估远远不够。

互联网安全中心（CIS）在其十大安全控制措施中强调了持续的漏洞管理。

然而，手动扫描可能无法保证风险识别的及时性。现代企业与合作伙伴和客户之间联系紧密，当来自合作伙伴或客户的新设备或软件实例进入您的网络时，就可能产生新的漏洞，从而增加网络安全风险。

除此之外，系统环境也在不断变化。开发人员在开发软件时，可能会为了方便而编写灵活的防火墙规则，创建网络共享，但在完成工作后未修改回安全设置。有时管理员为了测试或故障排除，会允许配置更改操作，但在结束后却忘记恢复限制。对于这样不断变化的IT生态系统，应该定期扫描系统以确保网络安全。

基本上，任何未作记录的更改都可能导致错误配置，从而损害网络安全。针对这种情况，组织需要使用自动化漏洞管理工具，持续监视网络资产，跟踪并处理新发现的漏洞和错误配置。毕竟，知己知彼，才能百战不殆。

根据Forrester全球安全调查结果指出，49%的公司都被攻破过，软件的安全漏洞是主要的突破口。

没有基于风险的评估，漏洞管理工作是否徒劳无功?

无论组织的规模如何，都面临着同样的漏洞管理难题，那就是需要修复的漏洞太多了。

随着攻击者针对公开漏洞开发攻击程序的时间缩短，组织也应加快修复漏洞的响应速度。但由于漏洞数量过多，且时间紧迫，难免令组织应接不暇。

在资源有限、时间不足的情况下，手动为网络中所有的漏洞打补丁是不切实际的。即使您能够增加系统管理员的人数，要使得所有Windows机器在"周二补丁日"后的第二天就更新到最新补丁也是不现实的，因为补丁管理是一项会耗费大量时间的工作，受到系统数量、应用数量、要打补丁的资源类型、补丁工具的负载处理能力、部署补丁时间段，以及与打补丁相关的测试过程等等方面的影响。此外，由于服务器预留的补丁时间非常短，在为服务器打补丁时必须格外谨慎。一个错误就可能导致长时间的停机，中断正在进行的业务活动。

虽然自动化可以极大地缩短打补丁时间，但盲目地将所有机器都自动打上补丁，而不考虑补丁的优先级也是没有意义的。如果攻击者试图利用高风险漏洞窃取数据，而您正在修复的却是低风险漏洞，那么即使借助自动化加速修复进程，也是徒劳。

并非所有漏洞的风险等级都是一样的。攻击者会挑选便于利用达到目的的漏洞。所以就企业安全而言，区分哪些是高风险漏洞，哪些是低风险漏洞，对于有效抵御网络攻击，确保网络安全至关重要。

例如，假设一次漏洞扫描识别出网络中有1000个漏洞。
显然，所有漏洞无法同时修复，但是随机修复这些漏洞可能会让关键漏洞排在队列的最后，而非关键的漏洞却被优先修复。如果您能从中挑出100个高风险漏洞，及时打上补丁，就能有效抵御网络攻击。

这里要说明一下，我们并不是反对修复所有的漏洞。在如今的网络环境中，新漏洞层出不穷，因此，漏洞管理是一个持续的过程。而在有限的时间内，修复漏洞最有效的方法，是先消除高风险漏洞，然后再自动化部署其余补丁。

这也是需要评估漏洞风险的原因，预测漏洞被利用的可能性，以及可能造成的损失，对有效保护网络安全至关重要。这样，IT安全团队就可以将时间精力投入到易被利用的漏洞上，避免在非关键问题上浪费过多资源，要知道，这些非关键漏洞所需的修复成本，有时会大于其造成的损失。

以下是更多评估漏洞风险带来的好处：

- 尽早识别易被利用的、影响严重的漏洞。因为大部分漏洞是蠕虫级漏洞，这意味着漏洞的利用，无需任何管理员或用户交互，即可在网络中传播。
- 提供漏洞详细信息，评估漏洞的优先级、紧急程度和潜在风险。
- 打补丁通常会干扰企业的正常运营，因为会消耗大量的网络带宽，而且补丁部署完成后，通常需要重启，从而导致不可避免的停机时间。优先处理高风险漏洞，可以在降低风险和强制停机之间取得平衡。

要确定安全风险处理优先级，除了CVSS评分，我还需要跟踪哪些指标？

通用漏洞评分系统（CVSS）的分数常用作确定漏洞优先级的评判标准。漏洞的CVSS评分从1到10不等（10分最严重）。然而，却没有组织基于CVSS做风险评估。如果您仅靠CVSS评分来保护网络安全，可能远远不够，原因如下。

由于CVSS是一个行业公开标准，在漏洞数量激增的大环境下，组织倾向于以CVSS评分为基础，确定漏洞优先级。但是CVSS评分有许多缺陷。例如，组织中普遍将严重程度在7分以上的漏洞视为高风险，但是在往年发现的漏洞中，大部分漏洞的评分都高于7分。

在一次微软产品发布的787个CVE中，有731个CVE的严重程度评分在7分以上。

而且网络攻击仅利用了其中一小部分漏洞。这是因为，攻击者是否利用漏洞，主要取决于漏洞是否可以帮助其达到目的，也就是漏洞对组织造成的影响。此外，漏洞利用的技术可行性，以及概念验证的公开可用性等因素，也会影响攻击者对利用漏洞的选择。

CVSS分数是在发现漏洞后的两周内评定的，并且评定后不会再做修改。那么当时评分严重程度较低，但在披露后被广泛利用的漏洞，将无法反映在CVSS报告中。

你知道吗？微软曾报告过，其Windows操作系统及应用程序中，存在12个被广泛利用的漏洞，而其中有9个漏洞仅被评为高风险，但它们实际应该属于严重级别。

如果组织仅基于CVSS的评分确定漏洞优先级，将要处理大量的漏洞，而这些漏洞虽然评级为严重级别，但实际几乎没有风险，这就违背了确定漏洞优先级的初衷——及时处理高风险漏洞。

而结果就是，大量精力消耗在无关痛痒的漏洞上，而需要立即采取措施的高危漏洞却仍未修复，这种建立起来的虚假安全屏障，实则一攻即破。

要想使漏洞管理工作取得成效，组织应以风险评估为基础，根据漏洞潜伏时间、可利用性、当前利用活动、受影响的资产数量、受影响的资产关键性、影响类型和补丁可用性等因素，多维度分析，优化基于CVSS评分的评估，最终制定综合的优先级评估方法。

风险评估变量确定后，下面让我们探讨一下，如何聚焦关键漏洞，以及应对的最佳实践。

了解漏洞的可利用性和利用活动

漏洞是否已有利用程序，是确定漏洞优先级需要考虑的一个重要因素。如果漏洞已被广泛利用，无论这些漏洞安全等级如何，都需要立即处理，因为任何人都可能利用其侵入您的网络，窃取敏感数据。

安全团队应随时掌握攻击者的最新动态，积极利用新披露的漏洞信息，集中时间精力，消除终端高风险漏洞。

将受影响资产的数量和关键性纳入漏洞优先级排序因素

资产的重要程度是不同的。比如Web服务器位于网络边界并暴露于互联网中，很容易成为黑客的目标。定义评估标准时，数据库服务器（记录着大量信息，如客户的个人资料和付款明细）的比重也应大于其他资产，因为对于像这样的业务关键资产来说，即使是较低风险的漏洞，造成的损害也等同于高风险漏洞。此外，如果发现中等到严重级别的漏洞正在影响一大部分IT资产，那么，立刻采取应对措施以降低整体风险，才是明智之举。

此时，您需要一个高级漏洞管理工具，通过敏捷的补丁部署任务，轻松修复多个终端中的漏洞。

确定漏洞在终端中的潜伏时间

漏洞信息披露之后，安全团队和攻击者之间的竞赛就开始了。了解高风险漏洞在终端的潜伏时间非常重要。如果漏洞长时间存在于网络中，那么就意味着安全体系架构是及其脆弱的。

有些漏洞最初看上去并不那么严重，但一段时间之后可能会变成高风险漏洞，因为攻击者最终会开发出利用程序。最佳实践是立即修复已知漏洞或被广泛利用的漏洞，然后再修复标记为关键的漏洞。较为严重的漏洞通常也较难利用，但一般来说，也应在30天内修复。

根据影响类型对漏洞进行分类

尽管漏洞被利用的容易程度在风险评估中占着很大比重，但并不是所有可利用的漏洞都会遭到攻击。事实上，攻击者并不会仅因为漏洞已有利用程序，或易于攻击就对系统发起攻击，而是为了达到某种获益目的才会发起漏洞攻击。只有在此前提下，攻击者才会考虑利用程序的可用性和易用性。

漏洞的影响包括但不限于拒绝服务、远程代码执行、内存损坏、特权提升、跨站点脚本和敏感数据泄露。蠕虫级漏洞则更为严重，在没有用户干预的情况下，任何恶意程序都能利用蠕虫级漏洞，在各个脆弱的计算机之间传播。

基于上述风险因素的漏洞分类，结果更加精准，利于组织采取适当的响应措施。

太多漏洞和补丁工具，流程也太多太复杂怎么办？

ESG曾针对网络风险管理做了一项研究，研究中调查了340位网络安全专家，其中40%的人认为长期的漏洞跟踪和补丁管理是他们最大的挑战。

对于漏洞修复工作，各组织更倾向于在漏洞评估软件中集成一个专业修复工具。各个组织的情况各不相同，有些组织希望补丁和漏洞管理都采用一流的解决方案，认为这样以达到最佳效果。有些组织则是因为他们的漏洞评估工具没有内置的补丁管理功能，没有其他的选择。

漏洞管理应该是一个整体的解决方案，而不是各种产品的集成。组织使用多种漏洞评估和补丁管理工具，会导致各工作流程孤立且低效。各部门员工对这些工具混乱无章的使用，造成了漏洞扫描和评估、提交工单及补丁部署等流程复杂、管理问题多。

当安全团队识别漏洞并确定其优先级时，需要向IT团队发送工单，详细说明为什么该漏洞是高优先级，以及修复漏洞所需的操作。当漏洞修复完成，修复/IT运营团队会将完成状态反馈给安全团队，安全团队进行验收，至此整个漏洞管理流程结束。

如果两个团队各自使用独立的产品，则不仅会造成漏洞修复的延迟，还可能导致集成解决方案之间存在数据差异，难以从一个集中位置跟踪整个漏洞管理流程（从检测到完成）的准确性，降低漏洞管理工作效率。

此外，安装多个来自不同厂商的代理会影响系统资源利用率，降低生产力。在以资产频繁进出为特点的动态环境中，新资产漏装其中任何一个代理，都会为工作流程带来阻碍。

而且，独立的漏洞评估和补丁管理解决方案还会增加成本投入。

对于上述问题，最好的办法是找到一个漏洞管理解决方案，具备内置补丁功能，在检测到漏洞后自动关联补丁，并且从单一控制台就能监管漏洞修复的全流程。

组织如何应对零日漏洞、公开披露漏洞和其他没有补丁漏洞?

部署补丁，修复漏洞，一劳永逸。尽管这听起来很不错，但也有漏洞信息已经公布，可厂商尚未发布修复程序的情况。网络安全也因此处于脆弱状态，攻击者会抓住等待补丁的时间间隙开发利用程序。下面让我们来看看几种可能的场景，以及应对措施。

零日漏洞

如果漏洞的概念验证（PoC）代码在厂商修复安全漏洞之前暴露，就会出现零日漏洞。这些漏洞在被广泛利用时，仍未被披露或修复，甚至尚未被厂商发现。

“零日”，即代表软件开发人员或厂商没有修复漏洞的时间，因为往往在漏洞受到攻击之前，他们并没有发现漏洞的存在。

通常情况下，安全研究员和攻击者都会不断地探测操作系统和应用程序，使用一系列自动测试工具和逆向工程技术，寻找基础设施中可能存在的漏洞。如果安全研究员、互联网安全公司等先发现漏洞，就会告知厂商，同时将漏洞信息保密，直到厂商发布修复方案。然而，如果网络罪犯抢先发现漏洞，他们就会利用漏洞侵入系统。

针对零日漏洞，并没有什么万能的解决方案。但只要遵循基本的网络安全原则，企业就能够提高网络安全性，避免网络攻击。

保持最新补丁的更新：尽管为所有系统更新到最新的补丁，并不意味着绝对的安全，但至少可以降低攻击成功的概率。随着现代操作系统防护措施的强化，攻击者要想成功发起零日攻击，可能至少需要利用两个以上的已知漏洞。因此，保持所有操作系统和应用程序补丁的最新更新，可显著提升网络安全性。

执行最小特权原则（POLP）：限制用户的访问权限，只授予工作所需的最低权限。如此一来，即使零日漏洞攻击成功，也能将其造成的影响降到最低。

阻止易受攻击的端口，禁用遗留协议：Wannacry勒索软件的攻击在微软提出修复方案之前，给数千个组织造成了严重的损失。但如果提前禁用SMB V1，并设置防火墙规则，阻止端口445，就可以轻易阻止这种攻击。

还要确保防火墙阻止NetBIOS trio连接，并检查Telnet、服务器信息块（SMB）、简单网络管理协议（SNMP）和小型文件传输协议（TFTP）等不安全协议是否被禁用。

针对这种情况，最好的办法是加强IT生态系统的安全性（下一节将详细讨论），隔离受影响的系统，并将受影响的应用程序列入黑名单，直到发布补丁或提供解决方案。同时，需要掌握强化网络环境，抵御**零日漏洞**的最佳实践。

公开披露漏洞

公开披露，在极少数情况下，可能是软件用户偶然发现一个漏洞，并将其发布在网上。另一种情况就是网络安全研究员发现了漏洞，并告知厂商，但厂商对警告置之不理，不满的网络安全研究员遂将漏洞信息发布到公共论坛上。还有一种情况是，在发布补丁之前，厂商无意中在安全公告中透露了漏洞的信息。2020年3月，被不经意泄露信息的微软 SMB v3中的EternalDarkness（永恒之黑）漏洞就是一个例子。通常，厂商会尽快提供缓解漏洞利用的应急方案。组织需要一个工具，在永久修复漏洞的补丁发布之前，高效地将此应急方案应用到所有终端，保护网络免受新漏洞的威胁。

永久漏洞

暂且不谈最新版本软件上的零日攻击。厂商将不再对已经下架的软件进行安全更新，任何新发现的漏洞都可以被轻易利用。使用下架软件利大于弊。遗留的操作系统通常不能运行最新的应用程序，这意味着这些系统只能使用遗留的应用程序，而遗留的应用程序最终会下架，如此便扩大了网络攻击面。

在受监管行业中，企业还可能因运行过时的系统而面临巨额罚款。为什么必须跟踪有哪些应用和操作系统即将或已经下架？这就是原因。在软件下架后，建议您迁移到最新版本。

我的安全架构除了依赖补丁，还能有什么？

漏洞只是进入网络的一个入口，攻击者还会通过其他方式攻击网络。因此，除了关注未打补丁软件中的漏洞之外，组织应扩大监视范围，完善应对措施，加强终端安全。接下来，我们将提供一些切实可行的操作实践，帮助您有效地阻止攻击者的入侵。

确保您的杀毒软件已启动并使用最新的签名文件运行

如果杀毒软件阻碍了某些操作（如运行安装程序），员工通常会先将其禁用，但结束后却忘记重新启用杀毒软件。而杀毒软件为了应对层出不穷的漏洞，每天都会发布四到六次检测新病毒的签名更新。这就导致即使禁用杀毒软件时间很短，也会构成终端安全风险。

21%的终端 安装了过期的杀毒软件/恶意程序防护软件。

漏洞扫描工具的性能取决于已知缺陷和签名的数据库。该数据库必须不断更新，因为它是持续扫描和消除终端安全漏洞的基础。扫描您的网络中是否存在杀毒软件已禁用或已过期的终端，确保使用具有最新定义或签名文件的企业级杀毒软件。

调整用户账户控制

用户帐户控制（UAC）是保持访问控制及防止计算机未经授权更改的最佳途径之一。为充分发挥其功能，请将用户账户控制做如下设置：

- 提示提升权限时，切换到安全桌面
- 在安全桌面上提示管理员同意
- 在管理员批准模式下运行所有管理员
- 为内置管理员帐户启用管理员审批模式
- 在安全桌面上提示标准用户输入管理凭证
- 检测应用程序安装和提示提升权限
- 将文件和注册表写入错误虚拟化到每个用户位置

遵守强密码和账户锁定策略

使用易于记忆的名称或字典单词作为密码存在安全隐患。通常，黑客会购买以往入侵事件中使用的凭证和字典单词，以发起基于密码的暴力破解攻击。

62 %的用户 承认重复使用密码。

除了强制使用长密码之外，还应该确保用户遵守预定义的密码策略组合，如密码复杂度、最短密码有效期、最长密码有效期，以及必须使用多少个新密码后才可以重用旧密码。

账户锁定策略搭配强密码策略使用，达到设置的失败登录尝试次数后锁定账户，并设置锁定时长。帐户锁定策略有三种设置：

- “账户锁定阈值”，设置在用户账户被锁定之前，允许账户登录失败的次数。将账户锁定阈值设置为20。
- “账户锁定时间”，设置账户锁定时长（分钟）。将账户锁定时间设置为1440分钟。
- “重置帐户锁定计数器之前经过”，此选项允许您设置从第一次失败的登录尝试开始必须经过多长时间，才能将登录尝试失败次数计数器重置为0。设置重置帐户锁定计数器的值为30分钟。

通过安全配置管理建立安全基础

高危漏洞和零日漏洞层出不穷，组织必须建立安全基础，避免因一个漏洞而导致整个系统崩溃。恶意软件进入网络后，将利用**错误配置**向预定目标渗透。默认设置、记录不全的配置更改，甚至是技术疏忽都可能导致终端的错误配置。

部署安全配置以修复配置漂移，并使其恢复合规性是至关重要的。尽管在终端中需要处理的安全配置列表很长，但我们可以优先考虑一些重要的配置：

- 禁用加密算法较弱的不安全TLS/SSL 协议，启用最新且更安全的TLSv1.2。同时限制TLS通信使用默认、NULL或其他不安全的密码套件和算法。
- 禁用遗留协议，如Telnet、服务器信息块（SMB）、简单网络管理协议（SNMP）和小型文件传输协议（TFTP）。
- 启用安全浏览、限制不安全的插件和部署浏览器更新，强化浏览器。
- 启用操作系统内置的内存保护组件，如结构化异常处理覆盖保护（SEHOP）、数据执行保护（DEP）、地址空间布局随机化（ASLR）。
- 禁用匿名登录、共享和来宾登录。
- 启用BitLocker加密，加密整个磁盘卷。

审计正在使用的活动端口

系统中的应用程序和服务，依赖端口在网络中运行。要发现每个端口正在监听的内容，保持对系统中活动端口的持续可见性至关重要。通过监视正在使用的端口和进程，您可以轻松识别可能被恶意软件实例激活的端口。

采用安全的远程桌面共享实践

为了便于操作，IT员工经常使用远程桌面共享软件，通过互联网远程访问并管理服务器、虚拟桌面、终端服务器和应用程序。远程桌面共享软件在提高工作效率的同时也扩大了攻击面，针对用于远程访问业务关键资产的计算机，攻击者一旦找到利用方法，他们就有机会对这些资产进行控制。

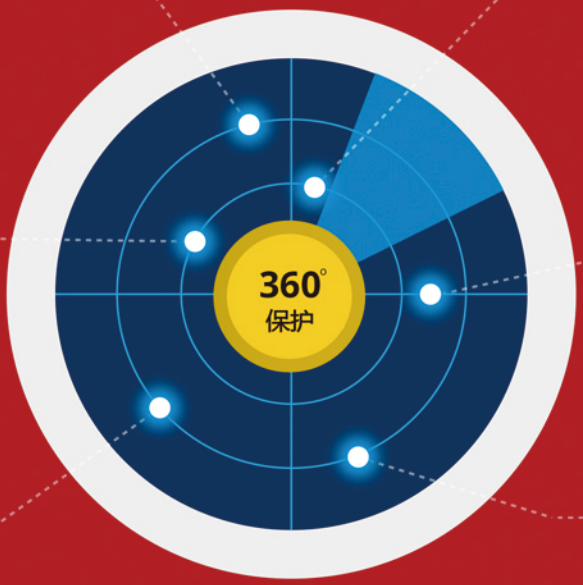
如果未对远程桌面共享会话进行加密，则可能增加中间人（MITM）攻击的几率。因此，应尽量避免使用远程桌面共享工具。如有必要，至少要用强密码来保护远程桌面连接，防止远程桌面服务器监听默认端口，进而阻止未经授权的远程连接。

看到这里，您是否已经开始头疼了？尽管上述内容能帮助您对漏洞管理有更深的了解，但要实现这里讨论的所有最佳实践可能需要投入大量时间精力。如果我们能为您提供一个解决方案，解决上述所有问题，您是否会感兴趣？

Vulnerability Manager Plus：
一站式解决方案，解决您所有的漏洞管理难题

Vulnerability Manager Plus是一款基于优先级排序的风险和漏洞管理软件，为企业提供内置的补丁管理功能。它是一个助力安全团队的战略解决方案，可以通过一个中心控制台对网络中的威胁和漏洞进行全面可视化、评估和修复。

除了漏洞管理之外，它还提供了一系列强大的安全功能。如安全配置管理、零日漏洞缓解、高风险软件审计、杀毒软件审计、端口审计、Web服务器强化、防火墙审计、密码策略管理、BitLocker加密、自动打补丁等，帮助您建立终端安全基础，确保安全可靠的网络状态。



漏洞评估

利用风险评估确定优先级，
识别高危漏洞。

安全配置管理

识别配置漂移和错误配置，
并使其恢复合规性。

高风险软件审计

一键审计并卸载网络中未经授权、
不受支持的软件。

Web服务器强化

帮助Web服务器抵御多种攻击，
如XSS和点击劫持。

补丁管理

自动化整个补丁管理过程，支持Windows、
Mac、Linux和350+个第三方应用程序。

活动端口审计

识别部分被恶意可执行文件激活的
活动端口和实例。

免费试用

注意：

Vulnerner Manager Plus的所有功能也可作为Desktop Central的选件模块使用。如果您已经是Desktop Central用户，建议将其作为选件使用。更多信息请访问官网 www.manageengine.cn