Acronis

白皮书

Acronis 执行备份扫描以查找恶意软件

在不牺牲安全性或可用性的情况下获得无中断的性能

备份技术和防恶意软件是现代终端安全态势的两个重要组成部分。虽然通常是在备份之前扫描恶意软件，但在许多情况下，恶意软件也会入侵到备份镜像。导致这种情况的原因有两个，一个是普通的防恶意软件解决方案的检测能力有限，另一个是在防恶意软件扫描之前进行了备份。

完整扫描大型存档（包括备份）来检测恶意软件，通常需要大量的时间和计算资源。因此，这类扫描往往不能有效利用时间和资源。也就是说，如果存档不是存储在本地，而是存储在云存储中，扫描存档就变得尤为重要，因为访问云中存档的速度可能比访问本地存储设备的速度慢得多（具体取决于所用的网络或通信通道的速度和/或通道的负载量）。此外，如果在存档中发现任何病毒和/或恶意文件，则认为该存档已损坏或已感染，可能不适合用于系统恢复或文件和数据提取。

在过去，为了避免还原受感染的数据，在存储期间、向存档中添加新切片时和/或在还原数据之前，会使用防病毒扫描程序定期扫描存档。但是，目前还没有一种解决方案能够在时间或范围方面自定义存档扫描。相反，所有解决方案都强制要求扫描整个存档。而且，它们无法修复存档中受损或受感染的数据。

Acronis 技术解决了所有这些问题

系统管理员通常需要处理大量的计算机及其对应的备份。在工作过程中，他们不仅需要处理上述的所有问题，还需要准备应对其他挑战。例如，备份的系统驱动器并不是唯一易受恶意软件攻击的组件。设备的操作系统和第三方应用程序也可能成为感染的入口。

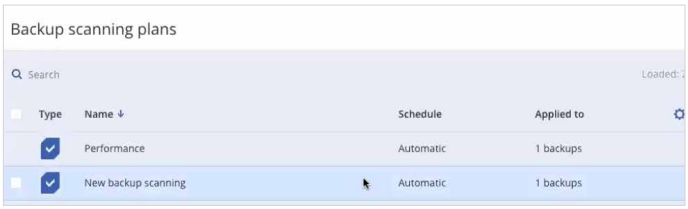
通过修补计算机并应用最新的防恶意软件定义，系统管理员可以还原操作系统镜像，以防再次发生感染。为确保安全还原和安全数据存储，另一个必要步骤是在一个集中位置正确有效地扫描备份以查找恶意软件。这正是 Acronis Cyber Protect 所提供的功能。

通过 Acronis Cyber Protect，用户可以在一个集中位置（Acronis Cloud 或其支持范围未来可扩展到 Amazon、Google、Microsoft 或任何其他常用云存储环境的本地服务器）扫描完整磁盘备份，以发现潜在的漏洞和恶意软件感染文件，从而确保在必要时可以使用无恶意软件的备份进行无恶意软件的还原。

Acronis 工程师不仅可以检查大型备份，还可以检查存档的切片是否存在恶意软件。可以将备份存档中众多切片中的第一个切片装入到磁盘中，这个切片便是首次建立的用户数据镜像。Acronis 技术可以检测所装入的切片中的修改块，识别所装入的第一个切片中与检测到的修改块相对应的文件，并扫描特定文件以查找病毒和其他恶意软件。使用这种方法，Acronis 还会生成一个修复切片，其中包含所装入的第一个切片的用户数据但不包含恶意文件。通过在集中位置进行扫描，Acronis Cyber Protect 允许用户：

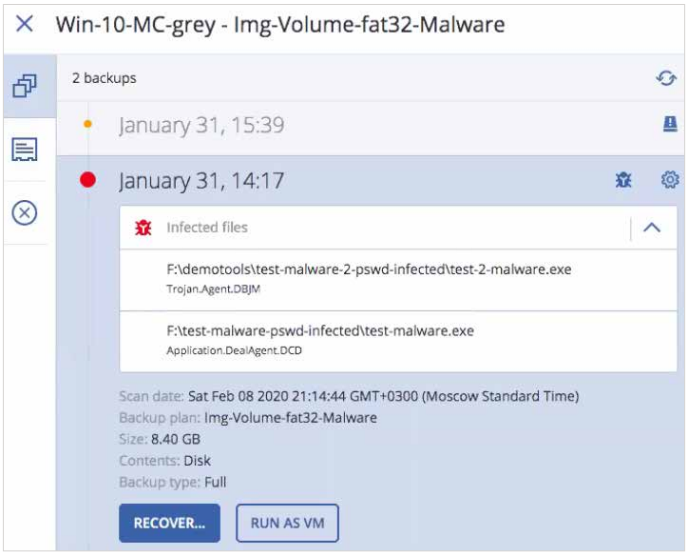
- **减少客户终端上的负载**
- **仅还原干净数据**
- **提高 Rootkit 和 Bootkit 检测率（在首次“访问时”扫描或按需求扫描期间不容易检测到 Rootkit 和 Bootkit）**

这意味着管理员可以执行定期备份扫描，在一个集中位置扫描每个客户的备份增量部分以查找恶意软件。在第一版的 Acronis Cyber Protect 中，仅支持 Acronis Cloud Storage 作为集中位置。在未来的迭代版本中，支持范围将扩展到 Amazon、Google、Microsoft 和其他常用云存储环境。



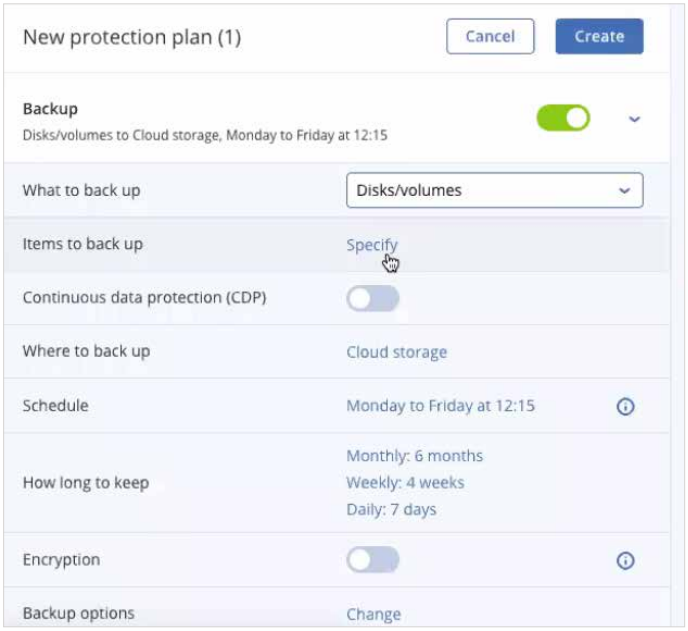
完成此操作后，管理员不仅拥有恢复点，而且这些恢复点还显示为未检测到恶意软件的“安全恢复点”。

管理员可以使用 Acronis Cyber Protect 管理中控台来详细查看发现了哪些受感染的文件，以及这些受感染文件的出现时间。在这里，他们可以从备份切片中消除恶意软件，并还原其数据的干净副本。通过 Acronis Cyber Protect 执行的所有备份扫描都会使用最新的恶意软件定义，因此，即使最初未检测到未知恶意软件，也会在下一次完整备份扫描中识别出这些恶意软件。



目前，Acronis 技术支持带有增量选项的完整磁盘或卷备份，但不支持文件备份。

其他产品只能装入和扫描整个镜像，但 Acronis 通过在扫描初始切片后快速扫描新切片来提供灵活性和高效率。这意味着它的扫描速度比同类竞争产品快几倍（实际结果取决于卷镜像的大小和同类竞争产品扫描引擎的性能）。Acronis 技术结合了 Archive 3 存储格式 API 和 NTFS 文件系统功能的优势，这也是操作性能极高的另一个原因。



如有必要，还可以在本地扫描备份。例如，当小公司使用网络共享来存储备份卷时。无需使用 Acronis Cyber Protect 代理程序，即可覆盖文件存储。在这种情况下，可以通过网络中任何可访问存储并安装了 Acronis Cyber Protect 代理程序的计算机来扫描文件存储。

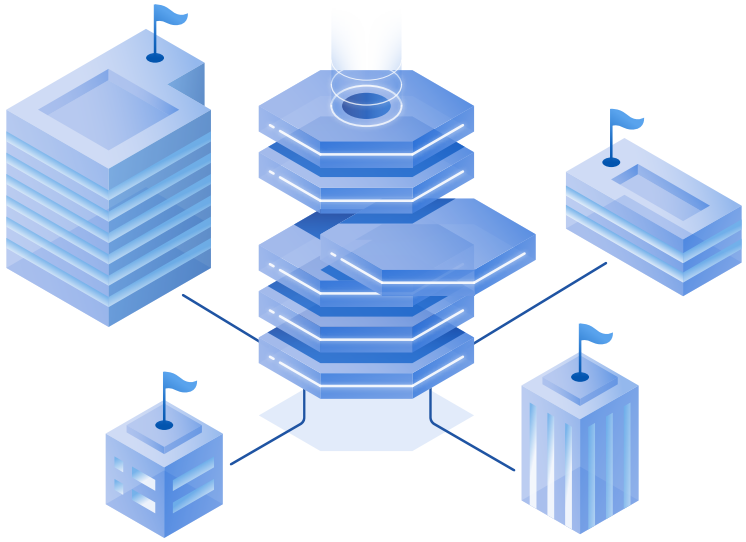
下一步是消除完整磁盘/卷备份中软件内部的潜在漏洞。在许多的实际案例中，恶意软件通过一个未打补丁的漏洞在本地网络和受感染的计算机上传播。计算机在还原后再次被感染，只是因为一旦操作系统工作环境恢复在线，很快就会再次感染恶意软件。为了避免这种危险情况，可以在完整计算机还原操作期间修补软件，使恶意软件无法再利用该漏洞。Acronis Cyber Protect 很快就能做到这一点，该功能还处于开发阶段，目前正在进行测试和质量保证。

阻止入侵。
信任顶级防恶意软件保护

恶意软件经常会感染备份。有些公司会在一个集中位置扫描备份，但执行连续的定期扫描需要花费大量时间。活跃的恶意软件还会再次感染未打补丁的磁盘镜像。每日甚至每周的完整磁盘按需求扫描会花费大量时间，而且通常无法在非工作时间内完成，这意味着员工经常会受到扫描的干扰，从而导致工作效率下降。

现在有一种更好的方法可以提供防恶意软件保护：对终端进行快速扫描，并在备份后在一个集中位置进行其余扫描。这样，您可以通过 Acronis Cyber Protect 提供安全保护，而无需牺牲性能。

在 Acronis 推出的这款创新产品中，将网络安全和顶级备份技术集成到一个代理程序中。因此，我们可以涵盖网络安全保护的这两个基本方面，从而消除现代威胁。管理员能够比使用其他解决方案更快地扫描备份，并且可以放心地在没有任何恶意软件或报告漏洞的情况下还原系统。



Acronis

要了解更多信息，请访问
www.acronis.com