勒索软件防御战：Veeam培训、实施和修复

Rick Vanover
产品战略高级总监
Veeam Software

Contents

勒索软件威胁现状

勒索软件构成的威胁大家有目共睹，经常有勒索软件攻击致使组织停摆的事件曝出。ZDNet 在最近发表的一篇文章中指出，勒索软件攻击活动日益猖獗，态势愈发严峻。[1]组织必须对此加强重视，制定详细的准备、防御和补救措施，以备不时之需，防止临阵而乱。

我经常在参加活动时询问现场的朋友们，有多少人遭遇过勒索软件攻击，大家的答复令人震惊。如果您不曾有过这样的经历，那么您很幸运。接下来我们将介绍一下如何免受勒索软件影响，有效保障数据安全。

[1] ZDNet：https://www.zdnet.com/article/the-ransomware-crisis-is-going-to-get-a-lot-worse/

防范勒索软件的 3 个终极策略

如果您想打赢勒索软件防御战，可以通过以下三种策略获得所需的弹性：**培训、实施和补救**。

每一种策略都有各自的专长，组织需要通过不断地重新评估，调整实施方案，从而提高弹性。每个领域也都有各自的专长、工具，并且在许多 IT 部门中，还会涉及到不同的角色。卓越弹性离不开 IT 部门的精心谋划和管理层的鼎立支持。接下来本文将结合 Veeam 技术的实用技巧和更多 IT 技术来解释这三种策略，让您更清晰地了解当今和未来实现弹性所需的功能。

许多“劫后余生”的勒索软件攻击亲历者就如何预防攻击或如何从中快速恢复提供了针对性的反馈意见。本文也对这些意见进行了介绍，并整理成了普遍适用的技巧。

培训

在开展培训前，您需要先确定威胁因素的风险，明确需要实施的 IT 实践，以防在意外遭到勒索软件攻击时处于被动地位。

培训应主要针对两类受众：IT 人员和组织用户。这两类人员缺一不可，因为威胁可能会从其中任何一方下手。据报道，截至 2019 年第四季度[2]，超过 57% 的勒索软件攻击载体通过远程桌面协议 (RDP) 漏洞切入，超过 26% 通过网络钓鱼攻击传播，还有超过 12% 是来自软件漏洞。

攻击载体识别培训

从培训的角度来看，让用户了解 RDP、网络钓鱼和软件更新是攻击切入的三大机制，则有助于在攻击载体方面找准应对勒索软件攻击的着力点。

大多数 IT 管理员都在日常工作中使用 RDP。在后面有关 Veeam 实施的部分，我们会在介绍备份组件时介绍帐户分离。帐户分离可有效提升 RDP 访问的安全性。令人难以置信的是，当今 IT 界中仍然有许多 RDP 服务器直接连接到互联网。我们迫切地需要摒弃这种做法。[3]虽然 IT 管理员可以使用特殊 IP 地址、重定向 RDP 端口或者复杂的密码等方式来提高安全性，但是数据不会说谎：一半以上的勒索软件通过 RDP 潜入系统。这一事实告诉我们，将 RDP 暴露在互联网中的做法有违预防勒索软件的弹性策略。稍后我们将分享一些有关 RDP 的建议，帮助您增强抵御勒索软件攻击的能力。

另一种最常见的切入方式是利用网络钓鱼邮件。我们都收到过莫名其妙的电子邮件。遇到这种情况，直接删除便可。但并不是每位用户都能做到。有两种常用工具可帮助组织评估网络钓鱼得逞后带来的威胁风险：Gophish 和 KnowBe4。

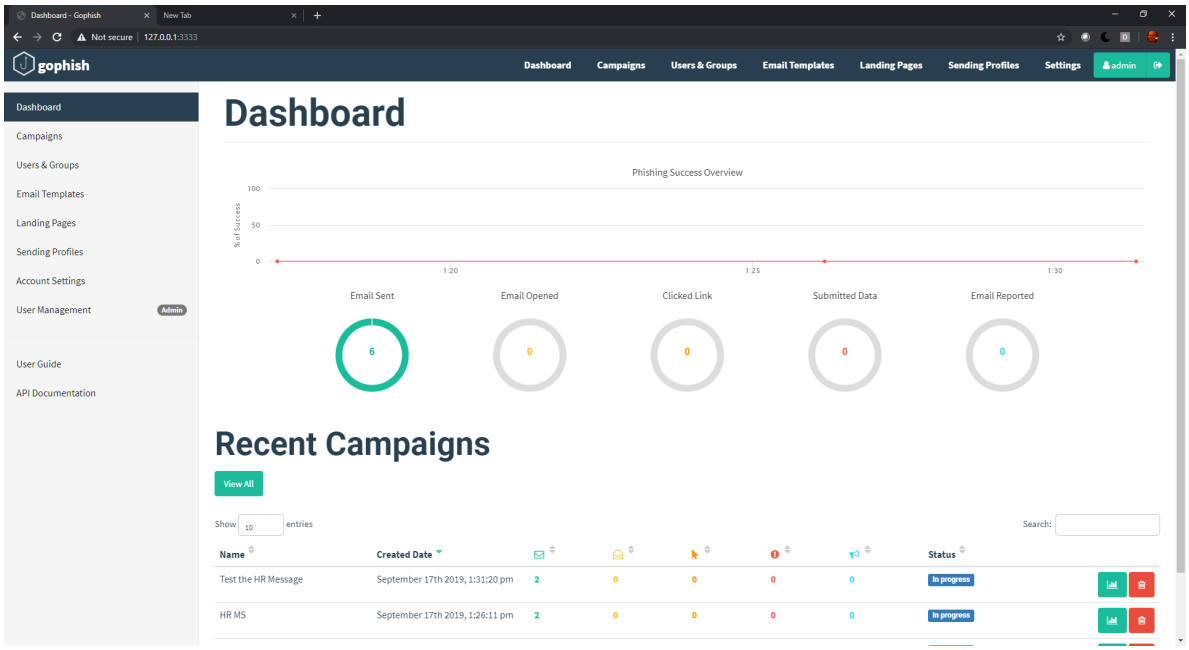
KnowBe4（https://www.knowbe4.com）可帮助增强最终用户和管理员的安全意识。KnowBe4 服务支持公司提供安全意识培训，而且还会模拟网络钓鱼攻击。

除了 KnowBe4 之外，还有一些开源资源可以帮助应对网络钓鱼攻击，比如 Gophish（https://getgophish.com/）。Gophish 支持您创建仪表板并发送电子邮件，测试收件人是否会点击网络钓鱼电子邮件。设置这种网络钓鱼测试只需几分钟。

邮件发送成功以后，您可以查看已发送邮件数量、打开的邮件数量以及单击链接的用户数量等一系列统计数据。这种方法可以轻松测试组织内用户安全意识。Gophish 仪表板如下所示：

[2] Coveware 报告：https://www.coveware.com/blog/2020/1/22/ransomware-costs-double-in-q4-as-ryuk-sodinokibi-proliferate

[3] ESET：https://www.welivesecurity.com/2019/12/17/bluekeep-time-disconnect-rdp-internet/



这些工具可以有效地帮助组织自我评估网络钓鱼电子邮件和附件等方面的风险。

此外，漏洞带来的风险也很高。及时更新系统是 IT 人员最基本的职责，但重要性更甚以往。这项不起眼的工作可以防止勒索软件从已知和已修补的漏洞下手。因此，切勿忘记更新操作系统、应用程序、数据库和设备固件等关键 IT 资产。一些勒索软件就是从一些已经发现并修复的漏洞入手，比如 WannaCry、Petya 和 Sodinokibi。[4]这些漏洞还包括非操作系统服务，比如适用于 Adobe Flash 的 njRAT[5]。

此外，建议您也高度重视终端更新。作为攻击的“宿主”，终端的面临风险不亚于数据中心系统，尤其是在面对一些喜欢驻留在目标上收集信息的威胁时。这一驻留时间平均约为三天[6]。

准备与培训相辅相成

组织还需要采取一些额外的准备措施，包括学习如何使用现有工具。例如，IT 部门可以先熟悉不同的还原场景，以便能够在发生勒索软件攻击并需要还原数据时，更好地应对。这可以使 IT 专业人员熟悉相关流程、合理预计投入的时间，最重要的是，提高对还原流程的信心。培训实践步骤的一些示例总结如下：

[4] ZDNet：https://www.zdnet.com/article/sodinokibi-ransomware-is-now-using-a-former-windows-zero-day/

[5] TrendMicro：https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/lord-exploit-kit-rises-delivers-njrat-and-eris-ransomware

[6] ZDNet：https://www.zdnet.com/article/most-ransomware-attacks-take-place-during-the-night-or-the-weekend/

- **Veeam 安全恢复**：在安全恢复期间，Veeam Backup & Replication™ 会挂载您计划还原的机器的磁盘，然后触发杀毒软件，扫描已挂载磁盘中的文件。如果杀毒软件在扫描期间检测到恶意软件，则 Veeam Backup & Replication 将中止还原流程，或者根据安全恢复设置中的限制条件还原机器或还原磁盘。虽然这只是还原流程中的一个小步骤，但它会为避免（因新定义）再次引入威胁添加一层额外的保障。
- **Veeam DataLabs™**：Veeam DataLab 是一项 SureBackup® 作业，可在隔离的环境中执行并打开虚拟机（VM）备份。此功能旨在验证系统是否确实可恢复，也可用于测试应用程序或操作系统更新等。DataLabs 可用于获取还原点，并在还原之前确保系统按预期运行。另一个用例是在不连接网络的情况下打开 DataLab 中的一个或多个系统，以执行一些可能的修复活动。

  一般情况下，建议您掌握 Veeam SureBackup 的使用方法。如果系统由于勒索软件威胁或其他原因而无法恢复， 则 Veeam SureBackup 可提前发出指示。在进行勒索软件修复时，您可以轻松运行 SureBackup 作业，以确保系统可以正确还原，并且应用程序按预期运行。您还可以选择在 SureBackup 作业完成后继续运行该作业，从而在还原前手动检查系统中是否还存在勒索软件威胁。有关 Veeam DataLabs 的更多信息，请参见本白皮书的“实施”部分。

- **多种还原场景**：组织应根据事件类型执行不同类型的还原。例如，复制副本故障切换可能是解决勒索软件攻击最合理的方法。文件级还原可能是最有效的方式。其他场景可能更适合使用虚拟机整机还原或 Veeam Agent 还原。了解各个还原场景可帮助组织对遭遇勒索软件攻击后成功修复充满信心。

培训不得有半点松懈，无论是评估组织的网络钓鱼风险，还是消除最常见的攻击载体，又或者是及时升级系统和软件，这些都是防止勒索软件攻击的必要措施，否则勒索软件的风险就会增加。衡量培训投资的一种方法是将其与毫无准备地应对勒索软件攻击的风险、成本和压力进行比较。

在任何情况下，一旦遭到勒索软件攻击，唯一的应对措施就是还原数据。从培训的角度来看，只有提高这一方面的意识，才能更好地实施下文提到的 Veeam 备份产品实施和修复。没有人愿意看到数据丢失，也没有人愿意支付赎金，最好的选择就是可靠恢复。以下技巧可帮助组织提高抵御威胁的弹性。

实施

Veeam 备份产品以简单、灵活和可靠而著称，这对想要尝试新功能的用户来说是重要的考虑因素。从弹性抵御勒索软件的角度来说，备份解决方案的实施与合规性审计十分相像。产品合规性可能并不在于产品本身，而是完全由产品的实施和审核方式来决定。当遭到勒索软件攻击时，组织弹性完全取决于备份解决方案的实施方式、威胁行为和修复过程。

在勒索软件事件中，实施 Veeam 备份基础架构是至关重要的一步，也是获取弹性的关键一环。有关弹性抵御勒索软件的实施建议，请见以下部分：

- 保护 Veeam Backup & Replication 服务器和组件
- 实现检测勒索软件的 Veeam 功能
- 超弹性备份存储和 3-2-1 原则
- 多种恢复技术配置
- 终端保护
- NAS 保护
- Veeam 备份数据加密
- 编排式备份和副本恢复

保护 Veeam Backup & Replication 服务器和组件

从勒索软件的角度来看，Veeam Backup & Replication 服务器是解决方案中的关键一环，尽量保持隔离也很重要。以下是一些值得考虑的重要实施技术：

不联网的 Veeam 服务器：隔离备份服务器（不联网）十分重要，可防止威胁入侵或传播。如果使用 Veeam Cloud Tier 或 Veeam Cloud Connect，则应特别注意不要忘记提供访问云资源的明确权限。

Veeam 部署帐户：弹性最强的方法是尽量使用不同的帐户部署 Veeam 解决方案。考虑将 Veeam 备份代理、存储库、广域网加速器和其他组件的关联到具体的帐户，以映射对应的权限。有些组织可能倾向于针对这些组件使用一组隔离的帐户（非域），还有些组织更倾向于使用不同的 Microsoft Active Directory 域来访问尽量分隔开来的 Veeam 和相关基础架构工具。特别需要注意的是，不要在不同的生产数据源和备份基础架构之间使用共享帐户。最糟糕的做法是全部以 DOMAIN\管理员的身份登录，并授予该帐户访问关键基础架构资源（如 Veeam、vSphere 和 Hyper-V）的权限。如果该帐户通过 Veeam 组件使用，那么一旦遭到入侵，许多弹性技术将面临风险。

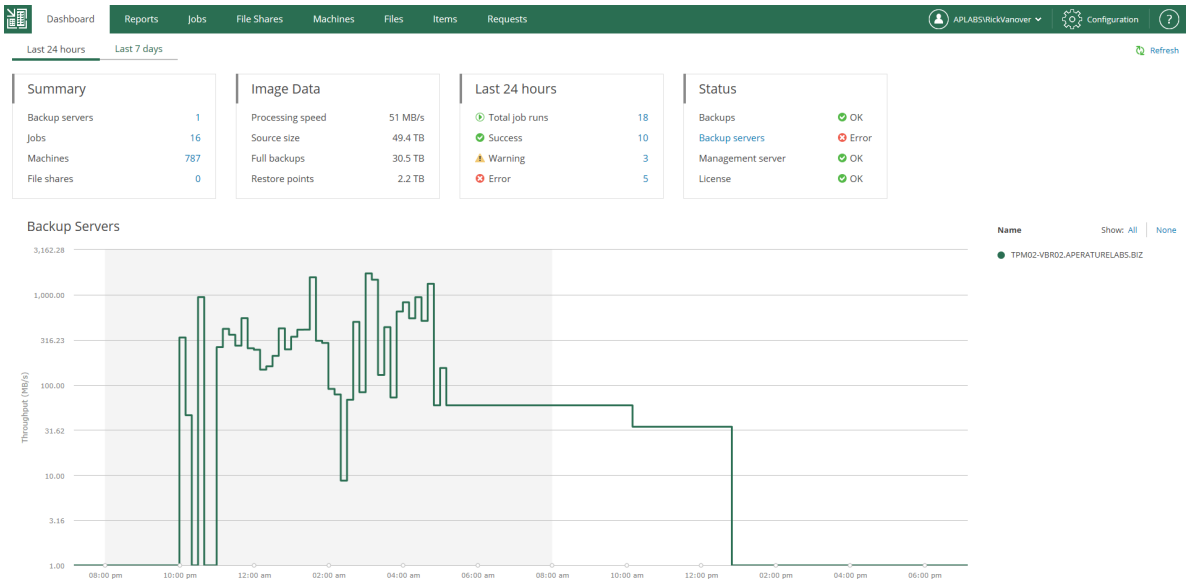
阅读推荐

所有 Veeam 产品所需的权限（以及每个角色的端口要求）都有书面记录，请参见：
https://helpcenter.veeam.com

此外，如需查看有关基础架构强化的 Veeam 最佳实践指南，请访问：
https://www.veeambp.com/infrastructure_hardening

设置明确的存储库访问权限：如果我们在上文建议的基础上更进一步，那么由于在弹性抵御勒索软件的过程中，备份存储库是最关键的存储资源，建议您禁止组织内的任何人访问和浏览 Veeam 备份存储库（以防备份外泄）。此外，您还以实施微分割，并将内部网络防火墙设置为允许明确连接（和访问）所需的源和目标。

使用 Veeam Backup Enterprise Manager：通过将 Veeam Backup Enterprise Manager（BEM）用于相关任务，组织可以大幅减少对 Veeam 基础架构主控制平面的访问。文件级还原、虚拟机整机还原、快速备份、作业克隆、作业编辑、请求主动完整备份等常见任务均可在 BEM 中完成。BEM 的强大之处在于，它可以在组织内部署的所有 Veeam Backup & Replication 服务器上提供这些操作。BEM 主界面如下图所示：



此外，要想减少全权限登录 Veeam 备份服务器的频率，还可以使用内置角色。这些角色可同时用于 BEM 和 Veeam Backup & Replication 本身，包括还原操作员、门户网站用户和门户网站管理员。有关角色的更多信息，请访问 Veeam 用户指南或 Veeam 帮助中心（https://helpcenter.veeam.com/docs/backup/hyperv/users_roles.html?ver=100）。

为远程桌面访问 Veeam 实施双重身份验证：对于运行 Veeam Backup & Replication 控制台角色的系统，建议您要求用户执行双重身份验证后再启动远程桌面（RDP）会话。通常，RDP 是最常见的攻击载体之一（57.4% 的攻击来自 RDP[7]）。即使是不连接互联网的网络，也应该考虑这种攻击载体。常见的双重身份验证方法需要借助 Microsoft 原生工具或外部工具（例如 Duo）。

[7] https://www.coveware.com/blog/2020/1/22/ransomware-costs-double-in-q4-as-ryuk-sodinokibi-proliferate

Microsoft 远程桌面服务双重身份验证：
https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/rds-plan-mfa

Duo 多重身份验证
https://duo.com/product/multi-factor-authentication-mfa

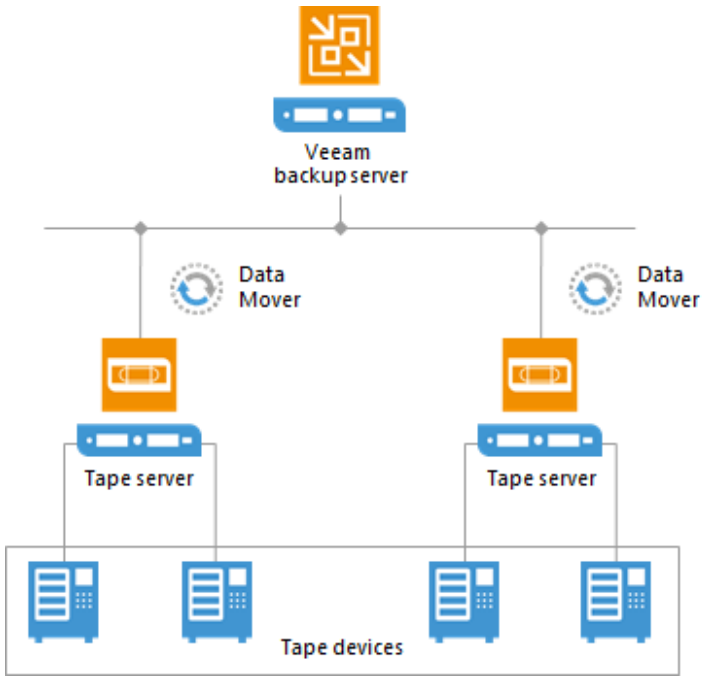
超弹性备份存储和 3-2-1 原则

组织应该具有一种超弹性备份存储形式，这也是本文的要点之一。超弹性备份存储要求您在以下介质上存储一个或多个备份数据副本：

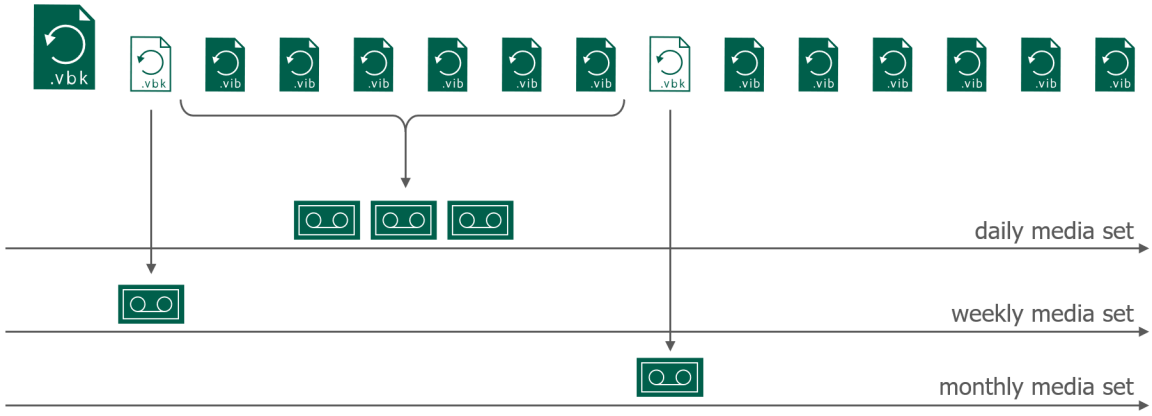
- 磁带备份
- S3 或兼容 S3 的对象存储中的不可变备份
- 物理隔离和离线介质（即移动硬盘、轮转驱动器）
- 带内部保护功能 Veeam Cloud Connect 中的备份

超弹性存储备份是弹性抵御勒索软件攻击的最关键措施之一。每种特性、每个组织都应根据特定情况选择最适合的方法。除了抵御勒索软件外，这些选项还可以利用其他保护技术提高备份数据的弹性，例如减少内部威胁和意外删除。下面详细介绍了这些超弹性介质类型：

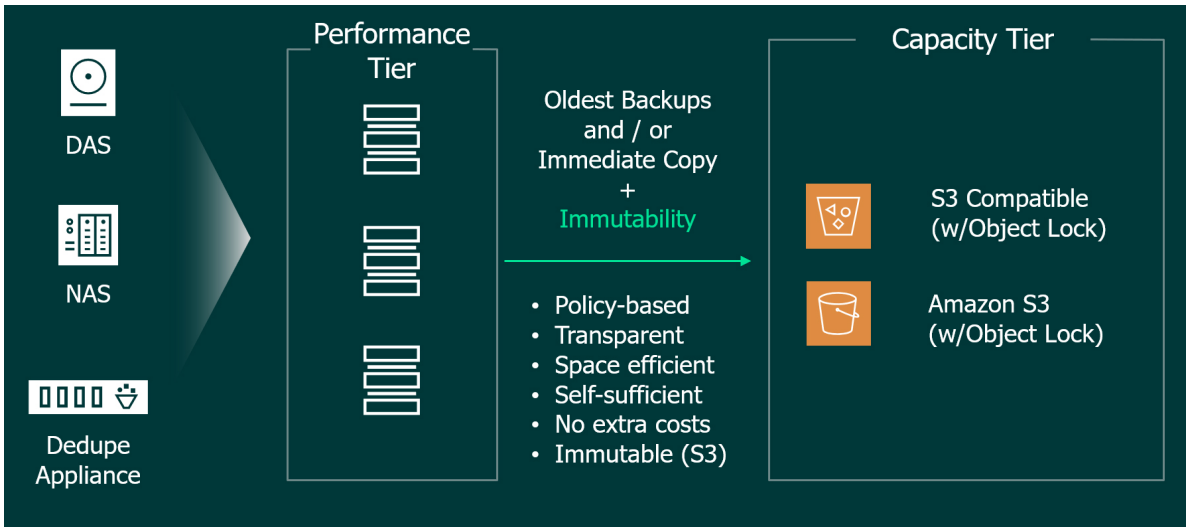
磁带备份：IT 部门对磁带介质的看法各不相同，但都认可磁带在购置成本、离线功能和可移植性方面的显著优势。除了在读写过程中，从库中弹出或移出的磁带介质将自动离线。Veeam 支持一写多读（WORM）介质，以增强抵御勒索软件的弹性。Veeam 还支持各种磁带介质操作，包括将文件写入磁带以及在磁带上进行完整备份。Veeam 磁带对虚拟机和物理服务器备份的支持可简单表示为下图模式：



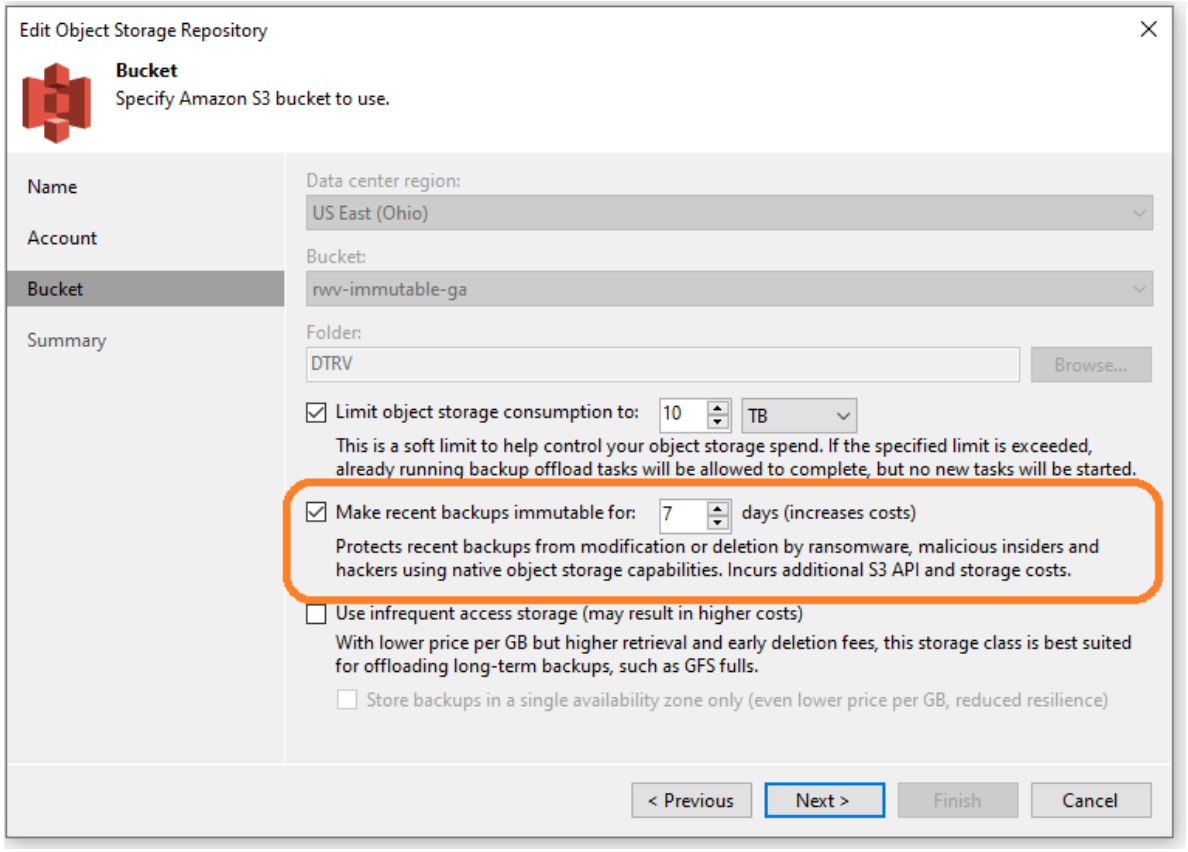
Veeam 对磁带的支持适用于现代 LTO 磁带设备和库的大多数配置。组织可以通过多种方式来利用磁带支持增强弹性抵御勒索软件的能力。其中一种方法是仅在较短的时间内将固定数量的数据放到磁带介质上，比如只需要保留几周的备份数据。人们对磁带基础架构的固有印象就是储有多年海量数据的大型介质库。但是，磁带也可以用作超弹性存储介质，以支持相对较近的还原点。以下是 Veeam 中的介质集图示，包括每日、每周和每月的介质集示例：



S3 或兼容 S3 的对象存储中的不可变备份Veeam Cloud Tier 支持功能强大的不可变备份，可有效抵御勒索软件和其他威胁。这种支持是通过利用启用了容量层（又称为云分层）的 Veeam 扩展式备份存储库（Scale-Out Backup Repository™）来实现的。容量层是一种基于策略的功能，可将备份数据写入对象存储。不可变备份支持 IBM Cloud、Azure、AWS 和兼容 AWS S3 的对象存储目标，但是仅公共 AWS S3 和兼容 S3 的特定存储系统支持具有合规模式的对象锁功能，有了这一功能才可以将 Veeam 备份数据作为不可变备份放到存储桶中。



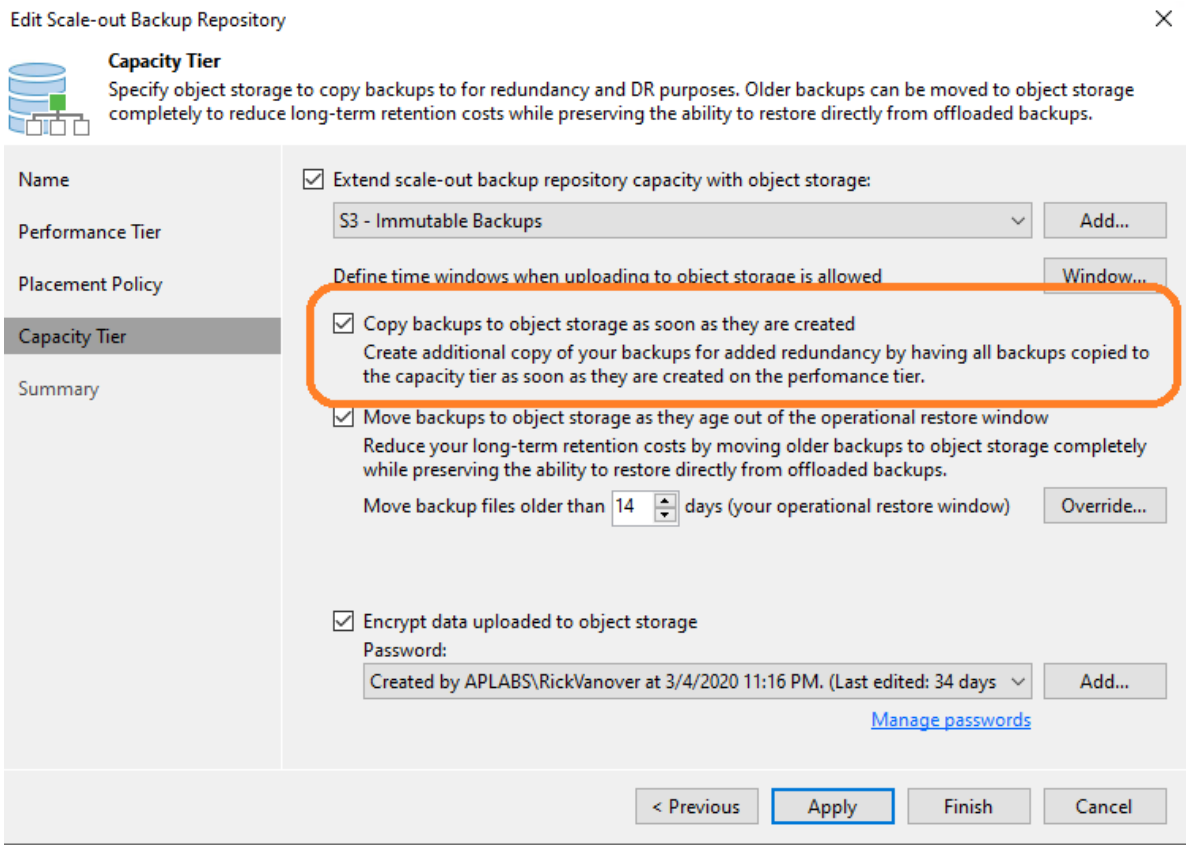
S3 不可变备份的优势在于，它在 Veeam Backup & Replication 中的配置非常简单。为充分发挥使用 Veeam 容量层时的弹性，用户应配置两个属性。第一个是 AWS S3 或兼容 S3 的存储桶，可以从这一属性中选择让备份在指定天数内不可变。这适用于通过扩展式备份存储库（Scale-Out Backup Repository™）分层流程进入存储桶的所有备份数据，分层流程发生在在备份完成后（复制模式）或一定间隔之后（移动模式）。存储桶的不可变期限设置如下所示：



所描述的不可变设置是对象存储桶的一个属性。为了最有效地使用对象存储弹性抵御勒索软件，用户还应使用另外一项设置来作为扩展式备份存储库（Scale-Out Backup Repository™）的属性。然后，容量层对象存储将通过将备份数据移动到对象存储（其中的备份文件早于指定的操作还原窗口，如14天或更早）中来接收备份数据。还有一个选项是在创建备份后立即将备份复制到对象存储（即复制模式）。

复制模式是勒索软件防范措施中的一个重要附加步骤，因为它会在备份作业完成后立即在对象存储中制作备份数据副本。随着备份的老化，移动模式仍将从性能层的内部删除备份数据或对其进行分层。在创建备份和操作还原窗口之间的期限内，备份将同时存在于内部和对象存储中。再加上不可变设置，这就是一项抵御勒索软件的弹性技术。

这一点十分重要，因为在许多情况下，从最近的点还原是最理想的选择，可以实现最近的恢复点目标（RPO）。下图显示了如何为扩展式备份存储库（Scale-Out Backup Repository™）配置复制模式：



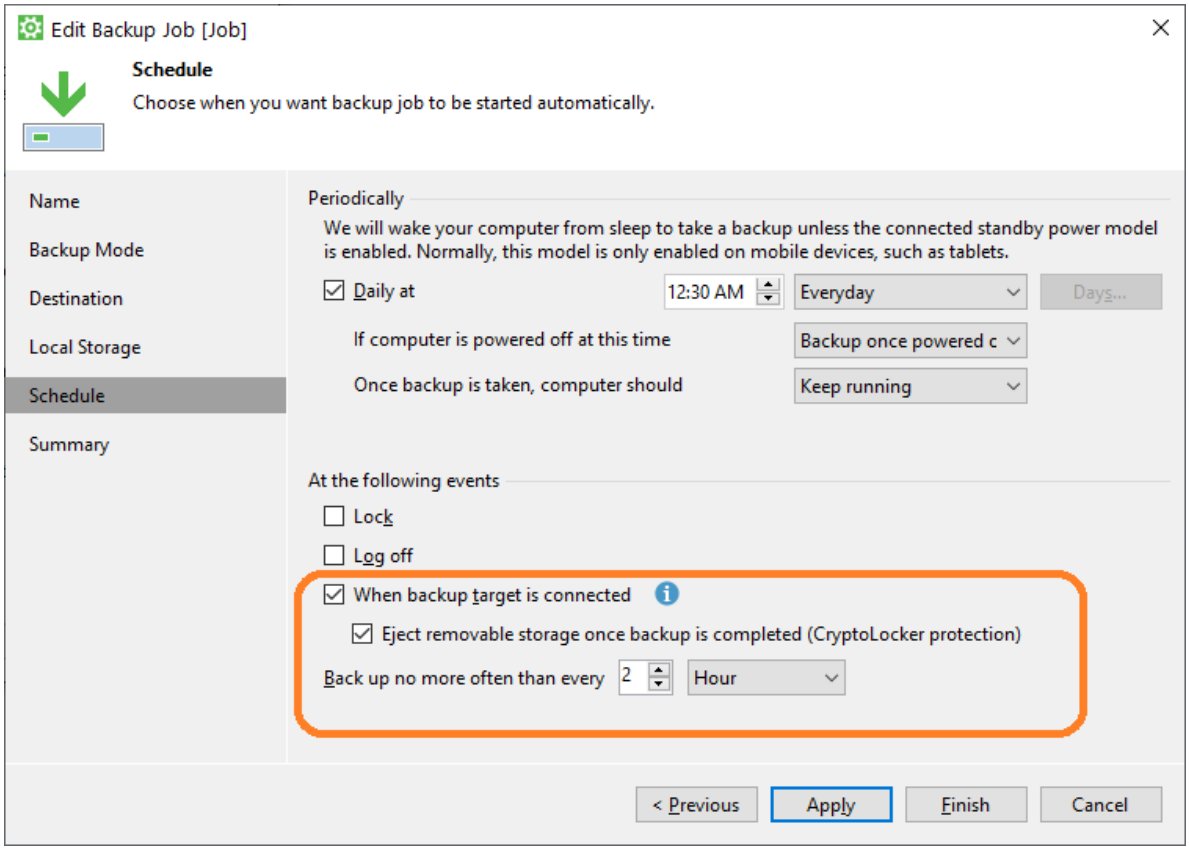
上图中还显示了在对象存储中加密备份数据的选项。毫无疑问，这是在云端备份数据的推荐配置。

阅读推荐

如欲了解有关 Veeam 不可变备份功能的更多信息，请参阅 http://vee.am/s3immutable

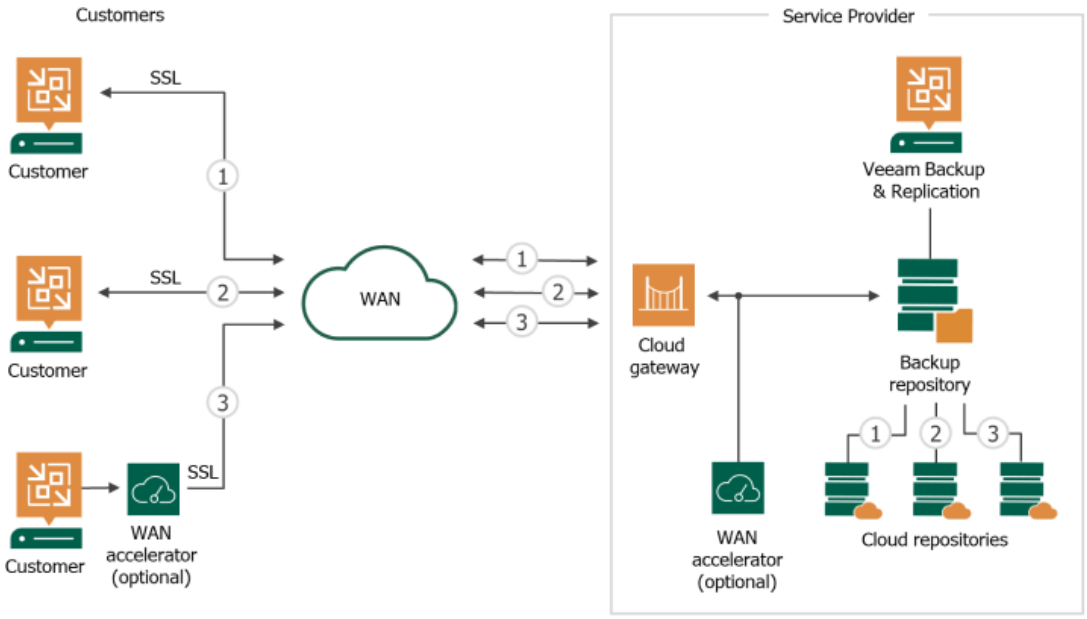
物理隔离和离线介质：轮转硬盘和移动硬盘也具有类似于磁带的离线特性。对于较大的数据配置文件，由于单个离线硬盘通常受容量的限制，管理起来有些困难，尽管硬盘容量在不断增加。这种方法可以根据具体情况灵活使用，比如用于终端和边缘位置（如 ROBO）。Veeam Backup & Replication 支持通过轮转介质来交换数据的存储库。

例如，Veeam Agent *for Microsoft Windows* 支持移动介质目标。对于终端，有一项附加功能支持在备份作业完成后弹出介质，将移动介质变成离线状态。该选项如下图所示：



带内部保护功能的 Veeam Cloud Connect 中的备份Veeam Cloud Connect 是目前市场上比较成熟的一项技术，可提供 Veeam 备份存储即服务以及基于 Veeam 复制功能的灾难恢复即服务（DRaaS）。Veeam Cloud Connect 由 Veeam 支持的服务提供商提供。该技术还提供了 Veeam Cloud Connect for the Enterprise 版，以便大型组织在内部使用此功能。

Veeam Cloud Connect 内部保护功能旨在增强的数据备份弹性，以抵抗勒索软件攻击、管理员恶意操作或意外删除带来的风险。借助内部保护功能，服务提供商可以保留额外的备份数据带外副本，并且通过人工介入（例如支持电话）提供这些副本。此流程支持将备份数据重新填充到 Veeam Cloud Connect 存储库中，然后在内部还原。Veeam Cloud Connect 备份如下所示：



您可以在此处查找提供支持内部保护的 Veeam Cloud Connect 服务提供商：http://vee.am/splookup

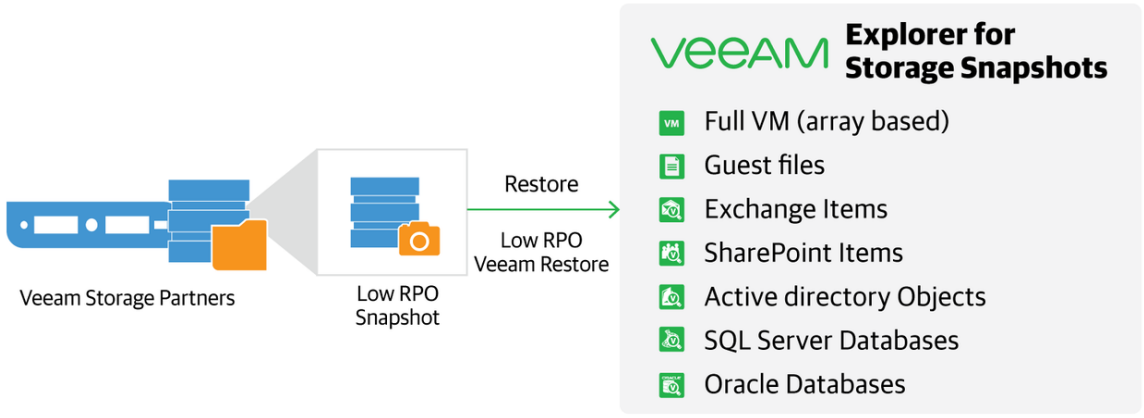
3-2-1 原则：多年来，Veeam 一直倡导将 3-2-1 原则作为通用数据管理策略。3-2-1 原则建议至少为重要数据保存三个副本，并保存在两种不同介质上，其中一个副本为异地存储。3-2-1 原则的优势在于，对硬件类型没有特别要求，并且具有普遍适用性，能够应对几乎任何故障场景。

由于勒索软件威胁不断加剧，Veeam 强调其中“一个”数据副本必须具有超强的弹性（即物理隔离、离线或不可变）。这是抵御勒索软件的必行之计。

多种恢复技术配置

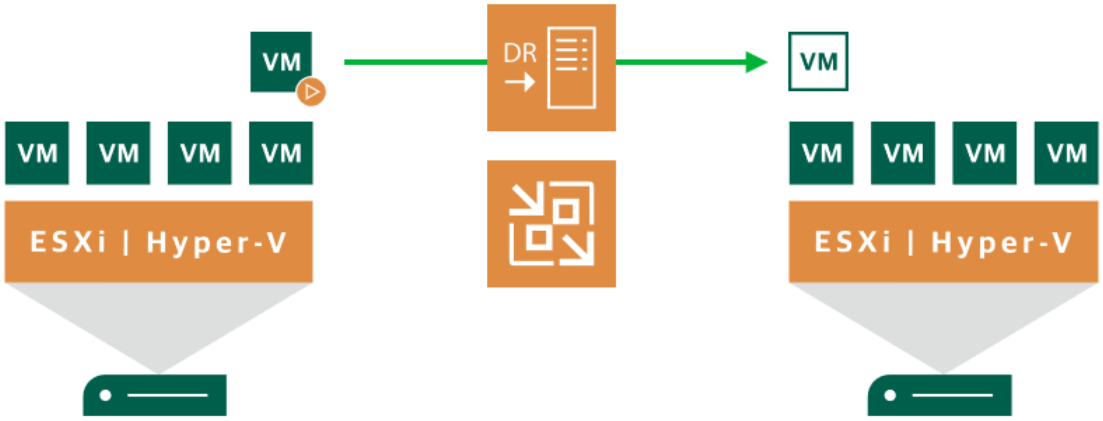
在实施 Veeam Backup & Replication 的过程中，您必然会连接其他各种系统。这些系统包括虚拟环境（例如 VMware vSphere、Microsoft Hyper-V 或 Nutanix AHV）、物理环境（例如 Windows、Linux、AIX 和 Solaris）以及存储阵列系统。在这种情况下，建议您灵活使用所有恢复选项。最常见的还原流程类型通常涉及整个系统（即虚拟机或服务器）恢复、文件级恢复或应用程序级恢复。除此之外，还有以下还原类型：

存储快照集成：如果主存储系统支持 Veeam 集成的存储快照，则这种高速恢复技术具备出色的通用性。Veeam Explorer™ for Storage Snapshots 可以从按时间表创建的存储级快照中快速恢复虚拟机。以下为 Veeam Explorer for Storage Snapshots 图示：



有了上述技术加持，还原技术就可以利用生产数据（即虚拟机），支持从主存储快照中还原数据。但是，我们还建议您备份主存储系统。Veeam 支持只读存储快照技术，例如 NetApp SnapVault 和 Pure Storage SafeMode 快照。

Veeam 复制：许多组织选择 Veeam 来帮助备份和恢复关键工作负载，但除此之外，复制引擎也是一项应对勒索软件攻击的强大技术。将复制的虚拟机放到同一站点或灾难恢复（DR）站点是一种高速恢复技术，可以帮助快速消除威胁。以下是 Veeam 复制的虚拟机的简化视图：



切记，在复制场景中，勒索软件可能也会瞄准目标端。在弹性抵御勒索软件的过程中，一般复制要考虑以下重要因素：

- 通过 vCenter 或 System Center 等虚拟机管理程序和管理软件，在源端和目标端使用不同的安全环境。
- 复制副本还原点与备份引擎非常相像，代表运行复制副本作业时的虚拟机。
- 在 VMware 环境中，用户可以为 Veeam 复制副本创建 SureBackup 作业，确保在从勒索软件事件中还原之前，复制副本可以正常启动和运行。

Veeam Availability Orchestrator（Veeam 的另一款产品）提供了可靠、可扩展、易于使用的编排和自动化引擎，这种引擎专为满足当前业务连续性/灾难恢复（BCDR）需求而构建。通过消除低效、冗长且易错的手动测试和恢复流程，Veeam Availability Orchestrator 提供了一种成熟、可靠的按计划灾难恢复策略（使用副本和备份），能够提升 IT 运营的弹性。Veeam Availability Orchestrator 还可确保复制副本和备份自动满足恢复时间目标（RTO）和 RPO，从而让您对全面的灾难恢复策略充满信心，并证明可以满足您的可用性 SLA。在弹性抵御勒索软件的策略中，只有对灾难恢复充满信心，才更有可能从勒索软件攻击事件中恢复。

多种选择：恢复方法不止有一种，具体取决于勒索软件攻击的性质。在许多情况下，虚拟机整机恢复或整个系统恢复都是非常有效的方式，但是考虑到可能需要还原特定数据，建议您让专家执行其他类型的还原，包括文件级恢复、应用程序级恢复或特定驱动器恢复（比如 VHDX 或 VMDK 文件）。

终端保护

许多组织都知道 Veeam 可为物理服务器和虚拟机等提供数据中心备份。但是，Veeam Agent 还可为台式机、笔记本电脑和 Windows 平板电脑提供备份。对于终端的 Linux 和 Windows 备份，组织可以在终端进一步增强弹性，以抵御勒索软件攻击。

从表面看来，终端备份策略提供了一种从备份中恢复的弹性技术。如果将 Veeam 数据集成 API 用到终端备份中，则还可以带来额外的好处，即对终端系统进行备份后扫描，这样可以压缩从威胁侵入系统到开始利用漏洞之间的时间。

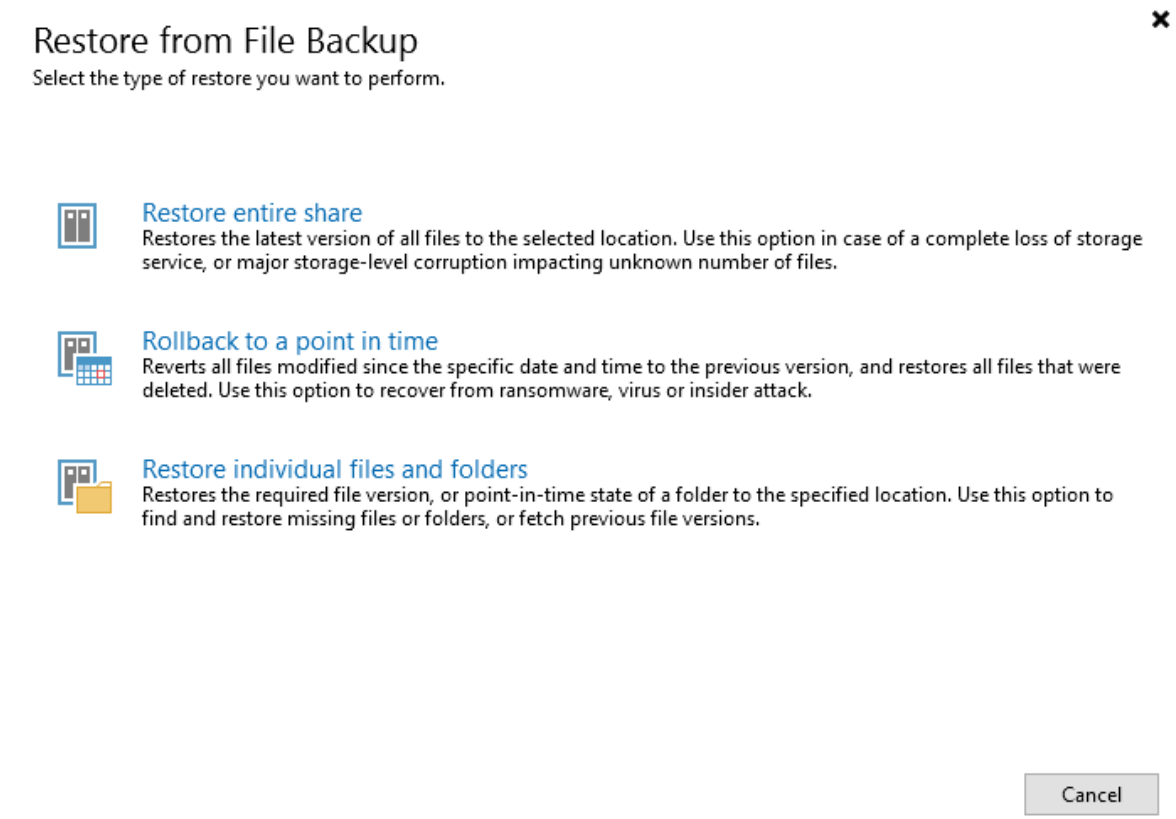
如上文所述，Veeam Agent *for Microsoft Windows* 支持在备份和离线备份后弹出移动介质，使其处于离线状态。备份和离线备份是弹性抵御勒索软件的两种关键技术。Linux 系统以及台式机、笔记本电脑和 Windows 平板电脑均支持此功能。

NAS 保护

NAS 系统也经常成为勒索软件攻击的目标。再加上内部威胁或意外删除等众多原因，文件数据也需要作为保护对象。如果勒索软件攻击导致文件共享的内容受损，则可以通过 Veeam Backup & Replication 对 NAS 备份的支持获得有效的恢复选项。

Veeam 文件备份引擎具有三种恢复类型。第一种类型是在隔离环境中进行文件和文件夹恢复，根据上次运行备份的时间进行恢复。第二种恢复类型是将整个共享恢复到指定的还原点。第三种恢复场景是在设备丢失的情况下将整个共享还原到新设备。

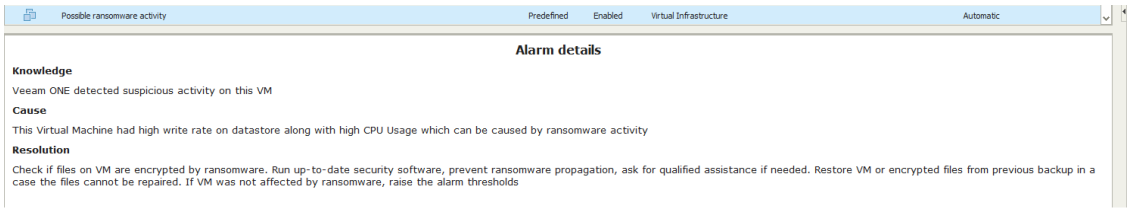
每种场景都可以用于在发生勒索软件攻击的情况下进行恢复，但是第二个场景能够在发生勒索软件攻击时高效恢复共享。如果威胁解除，但部分 NAS 共享已被加密或删除，则此还原类型可将共享的内容恢复到指定备份时间点的状态。对于具有数百万个文件和复杂文件夹路径的 NAS 系统，面向共享的 Veeam 缓存存储库可跟踪共享中的文件和文件夹更改。这种方法可以在无需了解受损共享内容的情况下还原到特定时间点。NAS 还原选项如下所示：



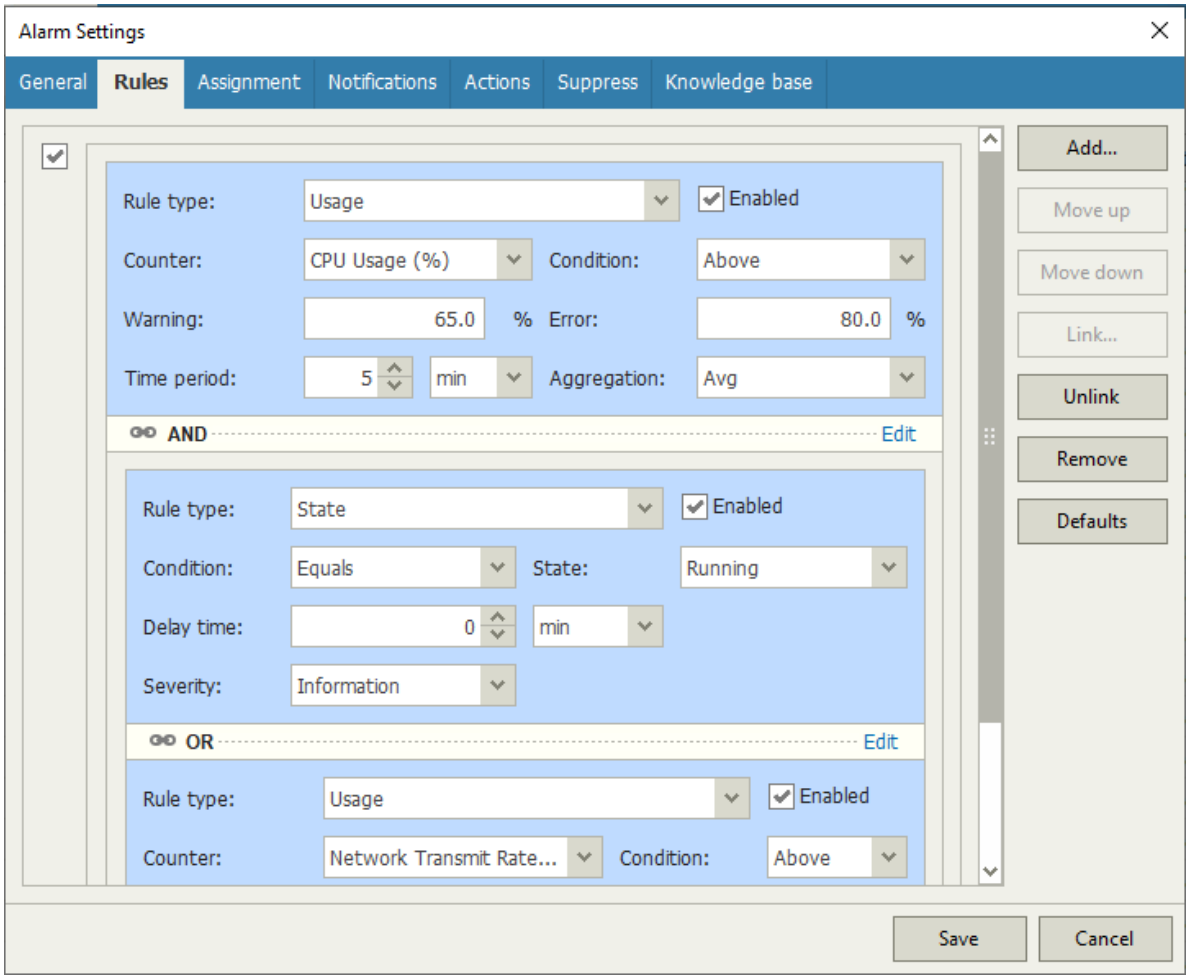
实现检测勒索软件的 Veeam 功能

对于 IT 部门来说，尽早发现勒索软件威胁会带来巨大的优势，这种潜力不可小觑。Veeam 实施了两种特定的检测技术来检测疑似勒索软件活动：

疑似勒索软件活动警报：Veeam ONE™ 警报可检测到 CPU 利用率高且硬盘持续写入 I/O 的情况。该警报如下图所示：

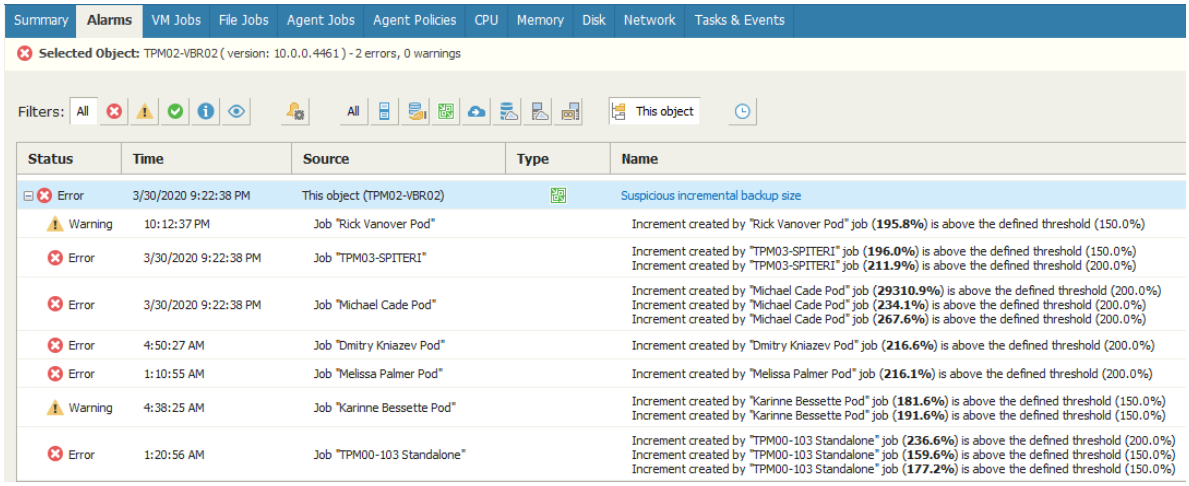


用户可以自定义该警报。默认值是一个会触发勒索软件警报的适中值，也可以调整得更为保守一些。自定义设置如下图所示：



使用 Veeam ONE 的组织应注意，下一条建议对解决触发此警报的问题至关重要。我建议执行一些特定的警报内置操作，这些操作可以向 IT 人员发出更紧急的通知。这包括发送短信提醒、警告安全团队甚至是一些极端的操作，例如通过 Veeam ONE 警报的操作步骤关闭虚拟机或断开网络接口。如果您同时安装了 Vmware 和 Hyper-V 系统，请务必对两种环境执行这些必要的操作。

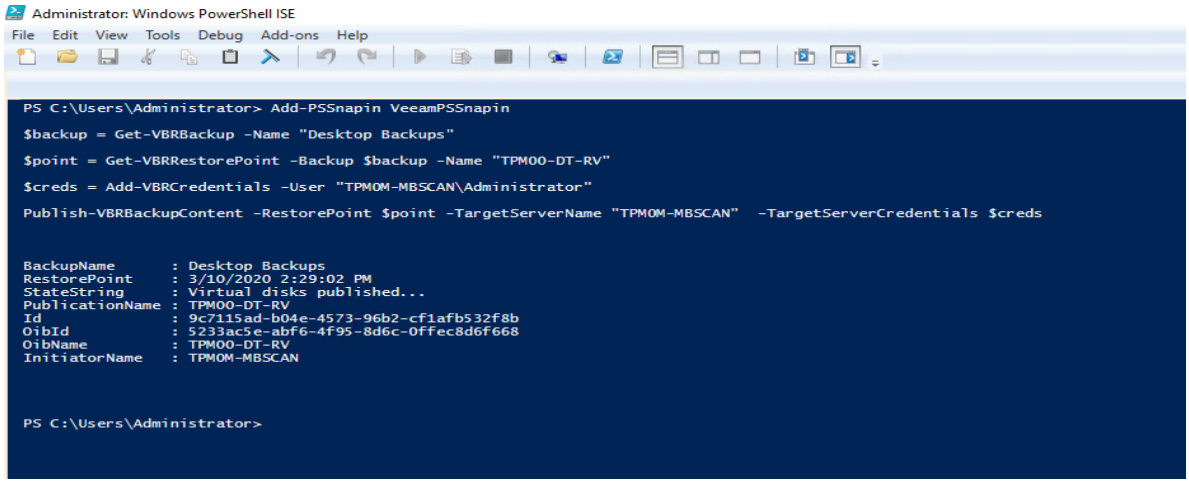
增量大小异常：该警报适用于 Veeam ONE 在数据保护视图中监控 Veeam Backup & Replication 的情况，是一种报告增量备份过大的有效方法。该逻辑基于正常的变化率以及源数据被加密的可能性，可以避免大多数存储效率问题。像大多数 Veeam ONE 警报一样，该警报提供一些可配置的规则来帮助您选择执行分析的深度。默认情况下，它分析三个还原点，当变化率为 150% 时指示警告，变化率为 200% 时指示错误警报。该警报如下所示：



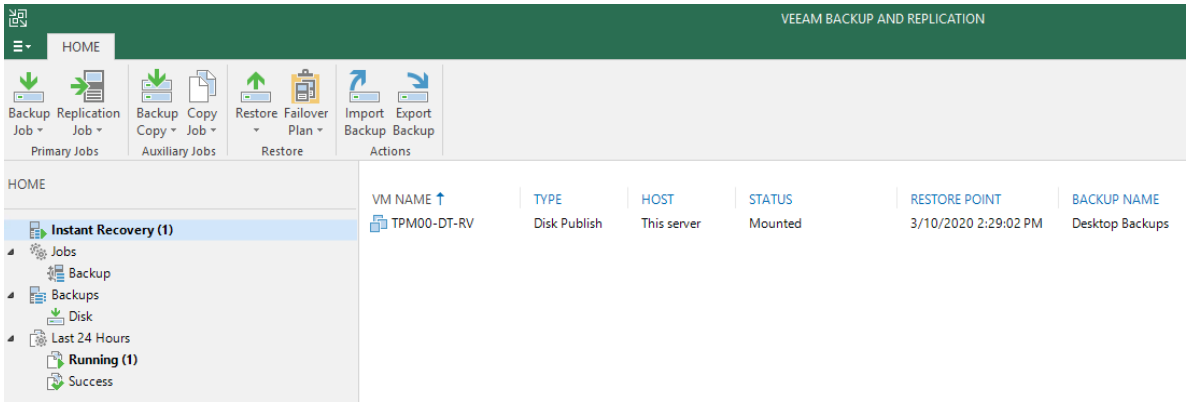
数据集成 API：Veeam 数据集成 API 是 Veeam Backup & Replication v10 的一部分，最好通过 PowerShell 使用。此功能允许将备份文件数据显示为已挂载的 Windows 文件夹，并支持您访问 Veeam Backup & Replication 创建的备份中的可用数据。此功能是一项新技术，能够有效防御勒索软件，可以对已经备份的数据执行额外的扫描。

这种抵御勒索软件的弹性技术可以额外扫描备份是否存在威胁，包括使用可能未在生产工作负载上使用的其他介入性更强的工具。此外，如果终端备份位于 Veeam 存储库中，则潜在威胁的分析范围会非常大。

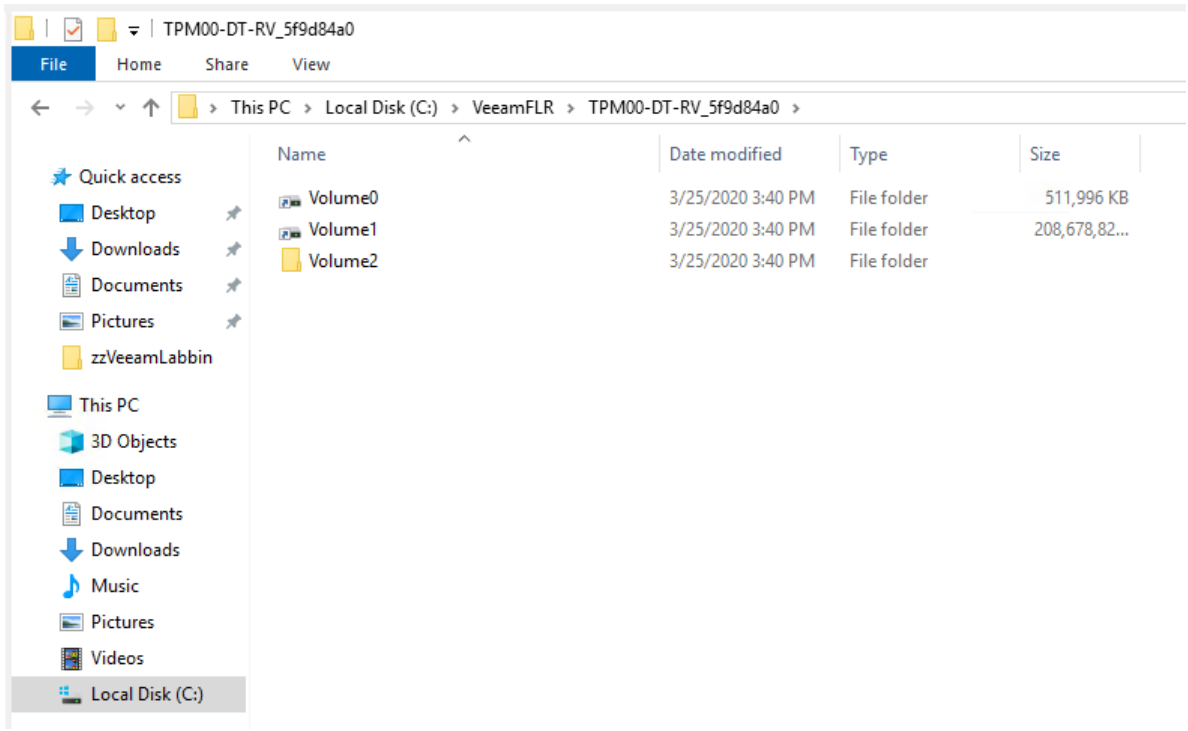
数据集成 API 的使用将从 Veeam 存储库中的备份开始。PowerShell 脚本示例将调用通过 Publish-VBRBackupContent Cmdlet 挂载的系统备份（TPM00-DT-RV），如下图所示：



这是一个挂载备份的 PowerShell 脚本示例，用户可以使用 Cmdlet 挂载多个备份。这一操作将在 Veeam Backup & Replication 中执行即时磁盘发布任务。这一特定的操作类似于 Instant VM Recovery®（即时虚拟机恢复），但它不是将备份虚拟机或代理的存储发布到 Vmware 或 Hyper-V 环境，而是从 Cmdlet 通过 iSCSI 透明发布到 Veeam Backup & Replication 服务器。此 Veeam Backup & Replication 服务器可显示作为磁盘发布而公开的备份，如下所示：

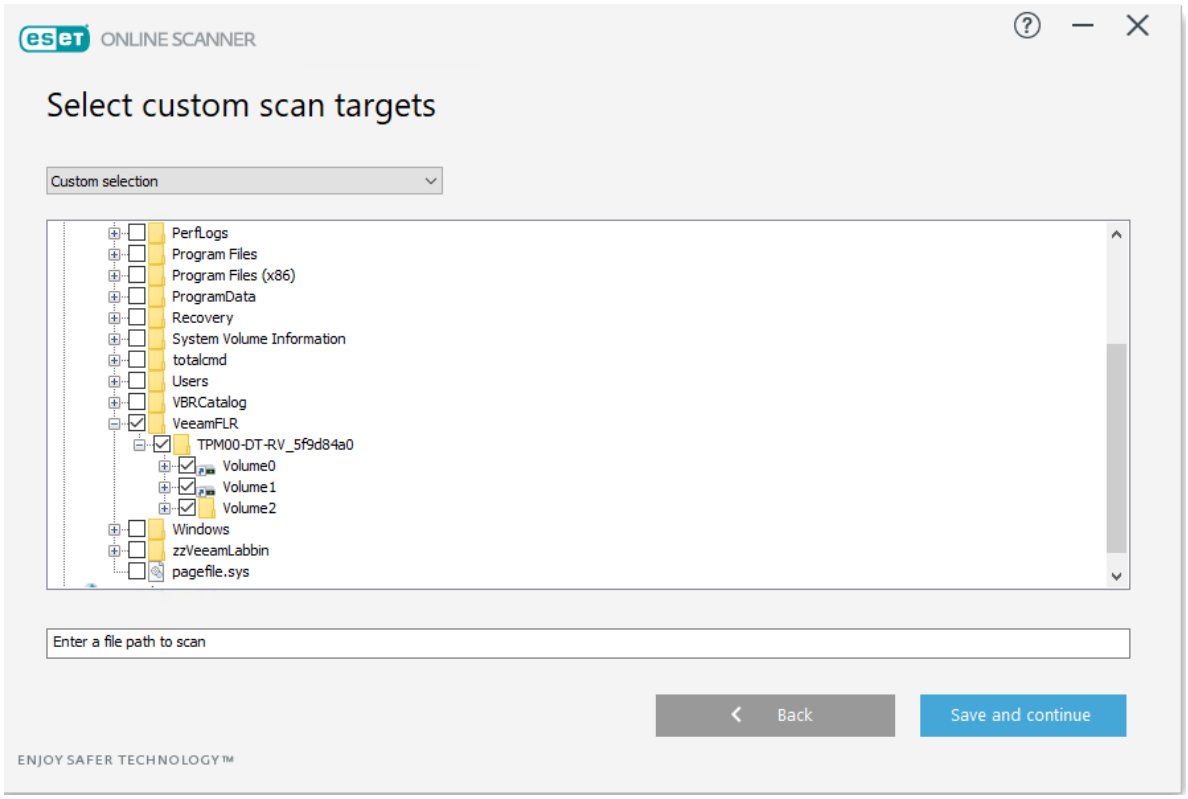


一旦像上图一样运行，备份驱动器的内容就会像 Veeam Backup & Replication 服务器上的本地文件夹一样公开：

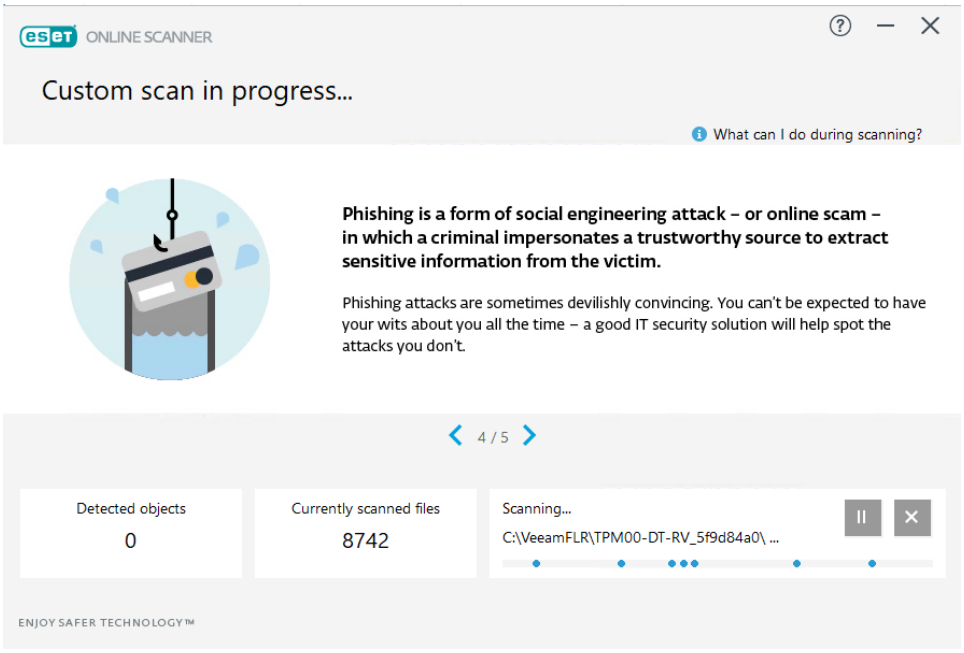


此时备份基础架构便可彰显用武之地了。然后，使用 Veeam 备份的系统会接受一些高级扫描。接下来我将总结有助于检测的两个特定示例，它们分别使用了 ESET 扫描工具和 Total Commander。

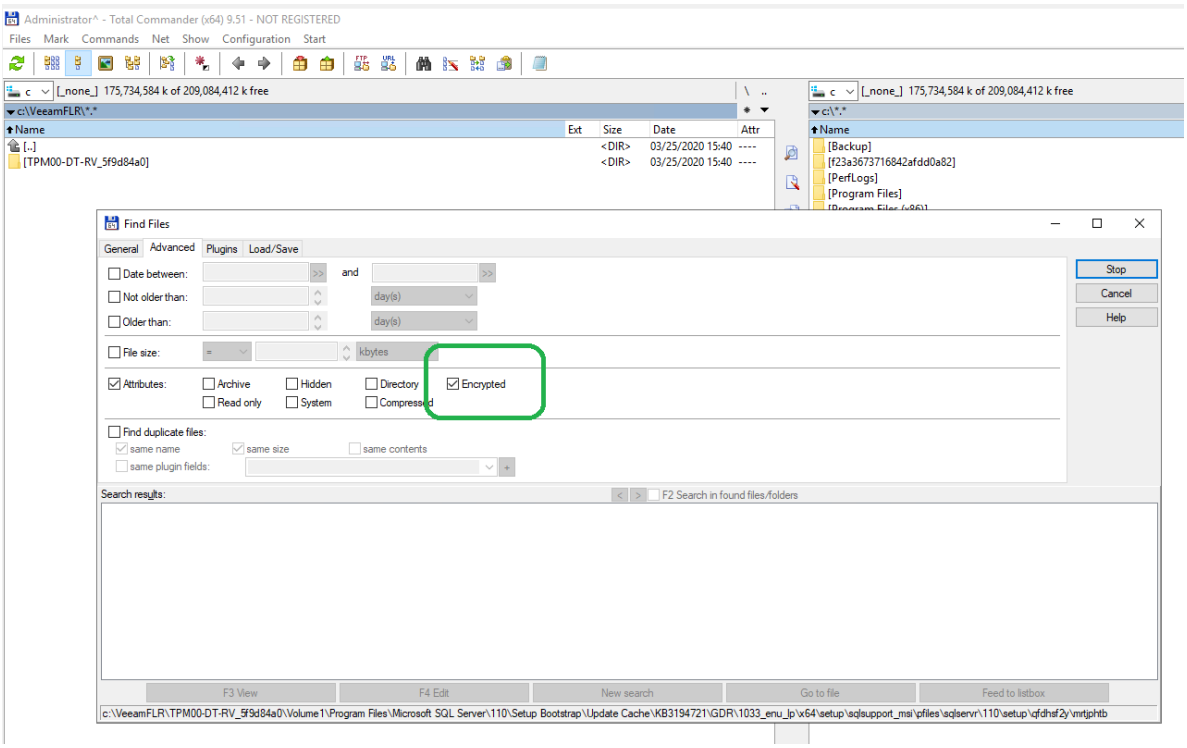
在第一个示例中，ESET 可用于仅扫描包含已发布备份的 VeeamFLR 路径。



使用 ESET 工具选择 VeeamFLR 路径后，即可执行自定义扫描。然后，ESET 工具将在扫描之前下载最新威胁定义文件，以获取要扫描的最新信息。扫描进度如下所示：



使用数据集成 API 时还有一种工具可以检测潜在的威胁：Total Commander。这是许多使用高级存储功能的 IT 管理员的必备工具。Total Commander 还有一个比较有趣的功能，即穿过 VeeamFLR 路径搜索已加密的文件，如下所示：



由于勒索软件威胁自身就有碎片化的特点，加密搜索可能无法显示被勒索软件加密的文件。Veeam 数据集成 API 可以与每个 IT 部门专业领域中的部分首选工具包搭配使用，从而在威胁大规模爆发之前就提前发现。在规模较大的自动化场景中，Veeam 数据集成 API 也有机会发挥作用。无论是执行备份、执行 SureBackup 作业，还是自动使用数据集成 API 执行备份后可能无法在生产工作负载上执行的更密集的扫描任务，都有可能压缩从威胁侵入到发起攻击之间的时间。

> 深入了解 Veeam 数据集成 API
>
> 如欲了解有关 Veeam 数据集成 API 和相关 Cmdlet 的更多信息，请访问： http://vee.am/vdapi

Veeam DataLabs：Veeam DataLabs 可通过检测和恢复技术帮助您弹性抵御勒索软件。SureBackup 作业将运行 Veeam DataLab，以执行多项任务：

- 确保备份系统的可恢复性
- 在系统上执行更新和应用程序更改等测试。
- 分阶段恢复和安全恢复技术

从勒索软件检测的角度来看，如果威胁在系统下次启动时暴露，则 SureBackup 作业可以识别导致系统无法启动或应用程序无法按预期启动的问题。SureBackup 作业可确保应用程序按预期从备份（或 Vmware 环境中的副本）中启动，并提供表明还原点确实能够被还原的报告。

SureBackup 作业具有多种功能，其中一项便是能够在启动后让作业继续运行。默认情况下，SureBackup 作业将运行并执行配置的检查。如果作业设置为继续运行，则可以从备份还原点对系统执行其他检查。这可能包括手动检查是否仍然存在勒索软件威胁，检查特定文件是否存在、是否已被加密或是否可能在提取选定的数据。

Veeam 备份数据加密

在勒索软件防卫战中，建议加密 Veeam 备份似乎有点不合常理。但是这种加密的出发点是好的，目的是为了增强抵御勒索软件和内部威胁的能力。

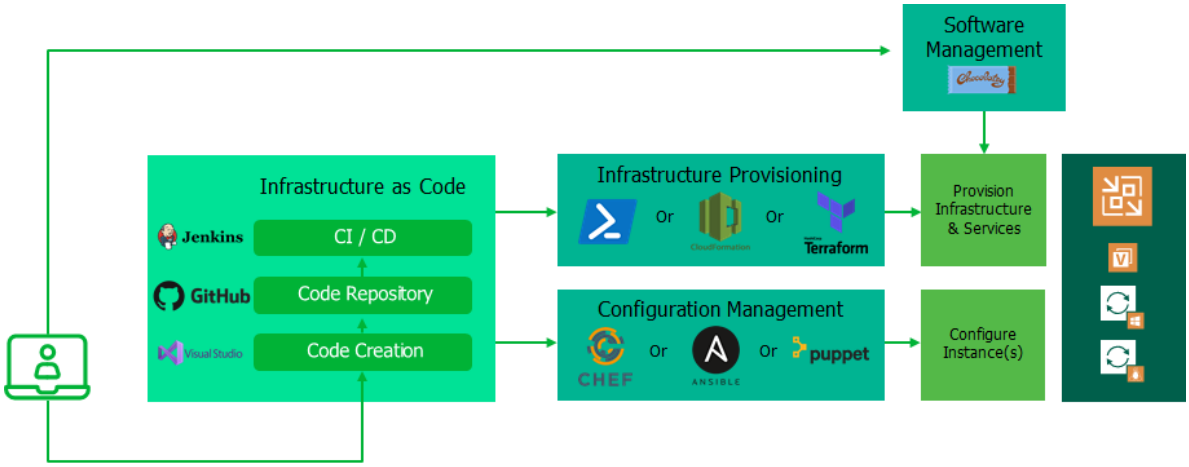
此处我们建议您尽可能对备份使用 Veeam 加密，包括第一次备份。首次备份通常在靠近源数据的同一站点上进行，并且通常是在内部备份存储库中。Veeam 备份数据的其他实例也应进行加密，例如通过备份复制作业获得的备份或处理到 Veeam Cloud Tier 的备份。

通过对第一次备份和所有后续备份数据副本进行加密，Veeam 备份文件可以免受新型勒索软件的侵害。如果您需要解密数据和防止数据泄露，黑客往往会要求您支付赎金。这些赎金实际上就是为了“赎回”已泄露的数据。毕竟，谁都不希望指向机密数据的备份文件的公共链接被拍卖。除了防止上文提到的防止这种情况外，Veeam 加密可以也是一层额外的保护措施，它支持备份作业、备份复制作业、备份至磁带作业、VeeamZIP 和磁带加密。

自动化投资

此外，我们建议您实施自动化，以进一步增强勒索软件弹性防御策略。由于原始基础架构可能并不可靠，这一措施特别适用于潜在的修复情况。Veeam、Microsoft、VMware 和相关技术厂商均提供“基础架构即代码”技术。

您可以使用现有的各种工具处理基础架构、配置和关键服务。



创建一个自动化还原的全新平台是潜在恢复场景中的关键环节。这样的平台支持您将数据还原到一个新的“平台”，同时保留安全的 Veeam 备份数据。当需要完整恢复时，这些工具包可帮助您实现快速部署。如欲了解这些技术，请参考以下相关主要内容：

Veeam VMworld 2018 大会：
https://videos.vmworld.com/global/2018/videoplayer/26243

Chef 中的 Veeam 部署（第 1 部分）：
https://vzilla.co.uk/vzilla-blog/cooking-up-some-veeam-deployment-with-chef-automation-part-1

Chef 中的 Veeam 部署（第 2 部分）：
https://vzilla.co.uk/vzilla-blog/cooking-up-some-veeam-deployment-with-chef-automation-part-2

基础架构即代码工具示例：
https://vzilla.co.uk/vzilla-blog/summerproject-infrastructure-as-code-example-tools

Windows 操作以及使用 Chocolatey 与 Veeam Agent 进行 Windows 软件包管理：
https://vzilla.co.uk/vzilla-blog/windowsoperationsusingchocolateyforveeamdeployment

修复

尽管为抵御勒索软件采取了各种培训措施和实施技术，但组织还应做好威胁入侵后的善后准备。Veeam 建议您采用以下方法修复勒索软件造成的损害：

- 不要支付赎金
- 唯一的选择是还原数据

如前文所述，组织应建立抵御勒索软件攻击的多层弹性。很多组织可能都没有考虑过发现威胁后该怎么做。

一旦发生勒索软件事件，建议您采取如下补救措施：

Veeam 支持：Veeam 支持部门设有一支专业团队，他们有特定的工作流程，可以指导客户在勒索软件事件中完成数据还原。不要将您的备份置于风险之中，它们对您的恢复能力至关重要。

沟通至上：在任何类型的灾难中，沟通都是首要的挑战之一。制定与合适人员进行线下沟通的计划，包括通过群组文本列表、电话号码或其他已扩展到整个 IT 运营组的随叫随到的机制。

专家：提供一份负责安全、事件响应和身份管理的专家清单，以便在需要时与他们联系。他们可以是组织内部专家，也可以是外部专家。如果使用了 Veeam 服务提供商，则可以考虑在其基础产品上增加附加值（例如 Veeam Cloud Connect 内部保护）。

决策链：灾难恢复中最困难的一个环节就是确定决策权限。谁下令进行还原和故障切换等措施？请事先进行商务讨论。

准备还原：如果具备适当的还原条件，则请先执行额外的安全检查，然后再将系统重新连接到网络。除了上文提到的部分技巧外，您还可以在禁用网络访问的情况下进行还原并进行最终检查。

还原选项：虚拟机整机恢复可能是最好的选择，但应视情况而定，文件级恢复可能也很有效。请务必提前熟悉各个恢复选项。

安全恢复：如上文所述，Veeam 安全恢复将在完成还原之前触发映像的防病毒扫描。请使用最新防病毒和恶意软件定义，并且如果有可能，请使用其他工具来确保威胁不会二次侵入。

强制密码重置：虽然用户不喜欢这种方法，但是会全面强制更改密码，从而减少威胁的传播面。

结语此时不准备，更待何时！

威胁是真实存在的，我们必须要居安思危，未雨绸缪。抵御勒索软件需要采取哪些措施？本文简要介绍了在培训、实施和修复方面的一些技巧。通过妥善的准备，本文提到的措施可以增强您抵御勒索软件攻击的能力，从而避免数据丢失、财务损失和商誉受损等。

如欲详细了解 Veeam 如何助您弹性抵御勒索软件，请访问：
http://vee.am/ransomwareseriespapers

关于作者

Rick Vanover（Cisco Champion，vExpert）现任 Veeam Software 产品战略高级总监。Rick 在 IT 行业拥有丰富的从业经验，负责过系统管理和 IT 管理，最近专注于开展虚拟化业务。您可以在 Twitter 上关注 Rick：@RickVanover 或 @Veeam。

关于 Veeam Software

Veeam在提供云数据管理备份解决方案方面位居全球前列，为备份现代化、加速混合云和保护数据安全提供了单一平台。我们在全球拥有超过37. 5万多家客户，其中包括82%的财富500强企业和67%的全球2, 000强企业。我们拥有业界最高的客户满意度评分，是行业平均水平的3. 5倍。我们的100%渠道生态系统包括全球合作伙伴，以及独家经销商慧与（HPE）、NetApp、思科和联想。Veeam在30多个国家设有办事处。要了解更多信息，请访问 http: //www. veeam. com/cn/。

VEEAM

Cloud Data

Backup for what's next

5 Stages of Cloud Data Management — start your journey today!

Learn more: veeam.com