Hewlett Packard Enterprise 慧与 | VEEAM

保护您的数据免于恶意勒索软件的威胁

该数据可用性最佳实践旨在确保所有企业做好充分准备，防范勒索软件攻击及其可能造成的数据丢失和停机。借助 HPE 和 Veeam® 软件并遵循行业最佳实践，IT 经理可打造轻松应付日常运营的可靠数据可用性解决方案，避免支付赎金。

“没有哪个方法或工具可帮助您或您的企业完全杜绝勒索软件攻击。应急和补救计划对于业务恢复和连续性至关重要，且这些计划应进行定期测试”。

— FBI 前网络部门助理总监 James Trainor。

这段话可帮助用户了解勒索软件只是其所面临的网络威胁之一。最佳解决方案是保护攻击目标 — 数据。fbi.gov/news/stories/incidents-of-ransomware-on-the-rise

勒索软件攻击日益增多

勒索软件通过利用监管与合规需求、薄弱的网络和低效的备份最佳实践，继续将攻击目标扩展至多个垂直领域。随着威胁的升级，越来越多的垂直领域和各类公司正成为攻击目标。即使在强大网络安全解决方案和实践的保护下，网络入侵还是不时发生。Institute for Critical Infrastructure Technology (ICIT) 认为，勒索软件预计在 2016 年和 2017 年对目标公司造成严重破坏。勒索软件威胁不断加剧，“近 40% 的企业遭受攻击”。[1]

勒索软件的业务和 IT 风险

勒索软件攻击不仅会造成安全风险。遭遇勒索软件攻击的企业面临财务和技术问题，而且其品牌信誉可能受到不可挽回的损害。

重大经济损失

巨额赎金、IT 时间浪费及关键任务应用程序停机会对企业造成永久损害。

IT 障碍

黑客会保留对受害者网络的控制和访问能力，以便在未来发起攻击和勒索赎金。IT 经理面临恶性威胁循环，需要投入更多资源防范勒索软件，挤占实施对业务至关重要的 IT 实践的时间。

品牌信誉受损

许多企业未能及时发布受到勒索软件攻击的信息，导致商业信誉受损、客户流失和市场份额下降。支付赎金或没有备份数据的企业最终可能遭遇更严重的攻击，导致其在市场中的品牌形象和信誉受到重创。

[1] “勒索软件威胁不断加剧，‘近 40% 的企业受到攻击’”《卫报》，2016 年 8 月。

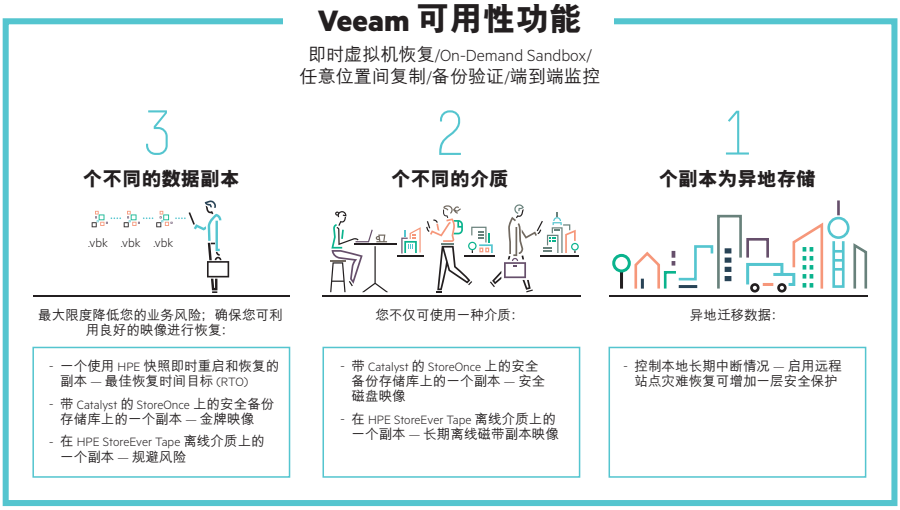
Veeam 和 HPE 解决方案概述

Veeam 和 HPE 联手推出的行业领先解决方案具备全面功能，可帮助大小企业抵抗恶意攻击和保护数据。

- **快速数据还原和恢复**
  HPE Storage Snapshots 支持快速虚拟机 (VM) 和颗粒恢复，可帮助破解加密的勒索软件数据库、应用程序、文件和操作系统 (OS)。与 HPE 3PAR StoreServ、Store Virtual、StoreOnce 和 StoreOnce Catalyst 业经验证的集成有助于快速恢复和避免应用程序停机。
- **基础架构锁定**
  勒索软件无法感染看不见的内容。HPE 通过集成 StoreOnce Catalyst 实现了这一目标，该功能使得勒索软件无法看见备份映像，从而支持恢复。离线磁带和异步远程复制副本增加了一个保护层。
- **测试环境**
  借助 Veeam On-Demand Sandbox™ 和 Veeam SureBackup，在将虚拟机恢复至生产前快速测试和删除勒索软件项目。
- **内置易用性**
  通过内置备份评估确保 Veeam ONE™ 监控、报告和容量规划工具可帮助保护关键虚拟机。

这些功能是 Veeam Availability Suite™ 和 HPE 存储集成的标准功能。该解决方案不需要任何特殊脚本，采用了 Veeam 和 HPE 的标准产品。

现在立即注册，以便获得最新资讯



案例研究 — 采用 Veeam 产品成功防范勒索软件

英国 Bedford School 曾受到勒索软件的恶意攻击，CryptoLocker 病毒感染了一位教职工的电脑并加密了所有文件。该校支付不起巨额赎金，也无法承受网络的额外停机。

Bedford IT 团队通过实施 3-2-1 备份规则避免了支付任何赎金或丧失网络功能。Veeam 帮助他们快速恢复每个加密文件。

Veeam 和 HPE 联手推出勒索软件解决方案

Veeam 和 HPE 联手推出的数据可用性解决方案旨在抵御黑客发起的任何勒索软件攻击。采用 Veeam 的 3-2-1 备份最佳实践，企业可确保数据的完整性和可用性。上图描述了 3-2-1 规则和行业领先的建议。

采用 3-2-1 备份规则遏制勒索软件

3-2-1 规则的目标是为客户提供有效的数据保护解决方案，以最大限度延长应用程序正常运行时间和提升数据可用性。通过妥当实施 3-2-1 备份最佳实践和遵从我们的 3-2-1 指南，IT 经理可有效保护他们的数据：

- 保持三 (3) 个数据副本 — 原始数据和两个副本，避免因备份错误丢失数据。
- 将备份副本存储在两 (2) 类介质上，如磁带、磁盘、二级存储或云。
- 将一 (1) 个副本异地存储在磁带或云中，以防范本地危害或网络中的勒索软件感染。

概要

数据可用性解决方案是采用了现有技术的全面集成解决方案，不仅可帮助企业从勒索软件攻击中快速恢复，而且可为企业的日常运营提供强大保障。这一最佳实践解决方案既灵活又经济，可由 Veeam 认证合作伙伴快速实施。

阅读 Veeam Backup & Replication™ 博文，详细了解如何实施 3-2-1 规则。

Hewlett Packard Enterprise 慧与 | VEEAM

a00000445chp，2017 年 1 月