ESG SHOWCASE

选择 Veritas，增强网络安全韧性

日期： 2021 年 9 月 **作者：** 高级分析师 Christophe Bertrand；高级研究分析师 Monya Keane

摘要： 网络攻击日益猖獗，严重威胁着企业的运营。企业必须筑起集保护、检测及恢复为一体的强大防御体系，以应对严重事件的发生。Veritas 可助您一臂之力，其屡经验证的卓越技术可帮助 IT 专业人士对抗网络犯罪。

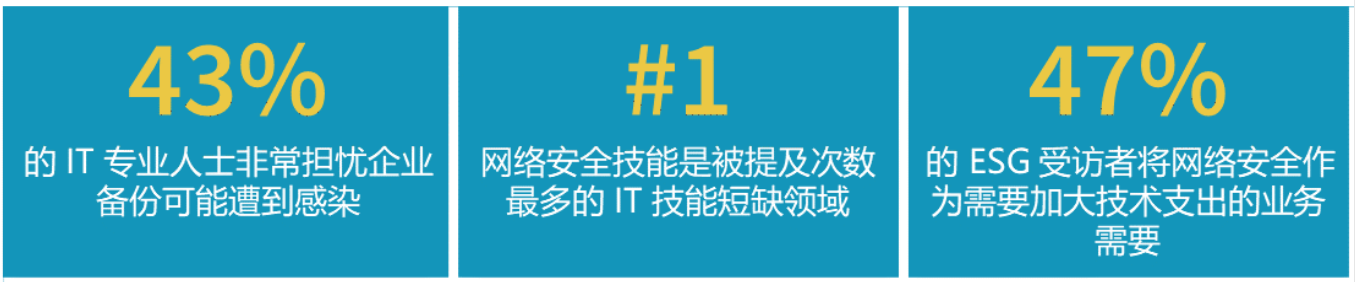
市场动态

ESG 研究证实了我们从各新闻渠道中获知的信息：勒索软件攻击频率居高不下。今年，24% 的企业称每周会受到攻击，18% 的企业称每天都会遭到攻击。[1] 这些攻击带来的直接影响就是停机。停机的代价巨大，它影响的不仅是 IT 部门，而是整个企业。ESG 研究指出，业务应用程序中关键任务应用程序平均占三分之一，其可容忍的平均停机时间预计为两个小时，但其中 15% 的关键任务应用程序非常重要，根本不能容忍停机时间。[2]

不仅是生产环境面临风险。事实上，参与 ESG 调查的受访者中，43% 的 IT 专业人员表示非常担心其企业备份可能被勒索软件攻击或毁坏（见图 1）。[3] 正是出于这种担忧，企业纷纷开始落实自己的措施：47% 的 ESG 受访者认为，保证网络安全是一项业务需求，因此要加大企业技术支出；25% 的受访者还特别投资于增强其业务连续性/灾难恢复能力的技术。[4]

一直以来严重困扰着 IT 行业的人员技能短缺现象加剧了这种情况。网络安全专业技能短缺位居榜首，48% 的受访者表示存在该技能短缺，24% 的受访者表示缺乏数据保护技能。[5]

图 1. 当下的网络威胁



资料来源：Enterprise Strategy Group

[1]资料来源：ESG 总体调查报告，《磁带在日益云化的 IT 环境中的地位》(Tape's Place in an Increasingly Cloud-based IT Landscape)，2021 年 1 月。

[2]资料来源：ESG 总体调查报告，《现实 SLA 和可用性的要求》(Real-world SLAs and Availability Requirements)，2020 年 8 月。

[3]资料来源：ESG 总体调查报告，《磁带在日益云化的 IT 环境中的地位》(Tape's Place in an Increasingly Cloud-based IT Landscape)，2021 年 1 月。

[4]资料来源：ESG 总体调查报告，《2021 年度 IT 支出意向调查》(2021 IT Spending Intentions Survey)，2020 年 12 月。

[5]出处同上。

本 ESG Showcase 受 Veritas 委托开展，由 ESG 授权许可发布。

选择 NIST 网络安全框架

美国国家标准与技术研究院 (NIST) 发布了 NIST 网络安全框架（见图 2），帮助企业评估其面临的网络风险。该框架指导企业内部和外部利益相关方管理并降低网络风险。

此框架划分为五大核心版块，每个版块又细分为 23 个类别。然后，按照网络安全和安全控制，在各类别下划分出子类别（共 108 个）。

图 2. NIST 框架

资料来源：NIST.gov

借助 Veritas 解决方案，轻松获得保护、检测和恢复能力

最近几个月，Veritas 一直在使用 NIST 框架寻找其解决方案与企业网络韧性战略的契合点。基于此，Veritas 确定了其解决方案的三大支柱功能：保护、检测和恢复。Veritas 相信，自己可以在这些方面助企业一臂之力。

保护

企业亟需一款全方位的保护软件。如果环境的任何部分有可能暴露勒索软件攻击之下，从根本上来说，这表示您的整体环境保护还不完善。恢复也因此变得艰难，甚至根本无法恢复。值得注意的是，当今许多攻击者不仅盯着您的数据，还有基础架构本身，例如摧毁企业的虚拟机环境或攻击网络的特定组件。

防篡改性

这种趋势之下，防篡改能力变得至关重要。数据一经存储，勒索软件就无法再更改或破坏存储中的数据。这相当于一个强大的保护层。Veritas 的 Flex 一体机内置本地防篡改功能，而且不止于此。Flex 一体机还设有独立的防篡改时钟，可防止攻击者人为地加速映像生命周期（众所周知，这是勒索软件盗取数据采用的无耻伎俩）。

Veritas 与 Dell Data Domain、NEC HYDRAstor 等第三方硬件提供商合作，在解决方案中采用 OST 插件技术，通过 API 与接收数据的硬件通信，告知其数据保持不变的时间。Veritas 创建了两种部署模式。分别是：

- **合规模式**：这是一个锁定模式。无论您拥有什么凭据，在维持数据不可篡改的预定义时间内，数据都将保持不变且不可擦除。换句话说，没人可以执行数据删除或加密操作。
- **企业模式**：在该模式下，如果出现有关存储容量的管理问题（这是防篡改数据面临的挑战），IT 管理员可以使映像过期。与核启动钥匙的“双人规则”保护机制类似，企业模式也要求至少输入两个管理员凭据，以提高安全性。

请注意，两个部署模式仅针对 Veritas Flex Appliance 一体机的防篡改存储功能，而非 OST 功能。

气隙隔离备份

从广义上讲，气隙隔离是指创建一个与外部网络不存在任何有线或无线连接的系统、数据或网络。多年来，Veritas 一直采用数据保管库和可弹出的盒式介质支持磁带气隙隔离备份。长期以来，这种方法行之有效。但是如今许多企业希望以数字形式（可以看作“电子气隙隔离备份”）构建类似的韧性。Veritas 另辟蹊径，通过自动映像复制功能模拟传统磁带气隙隔离备份的诸多优势。

具体来说，主 NetBackup 备份服务器将数据单向写入 NetBackup 辅助服务器。在辅助的备份服务器中，保留去重且加密的数据。提供出站服务的网络与单向主服务器完全隔离，从而相当于复制了气隙隔离功能。

重要的是，服务器的凭据可能也不相同。因此，即使是整个主生产环境遭到感染，也不意味会感染辅助环境。

而且，数据以 NetBackup 映像数据格式写入。这意味着数据是"惰性"的。如果您的备份映像不慎被勒索软件加密，它们不会感染系统的其余部分。它们将作为惰性映像保留并及时冻结，而无法传染环境的其他部分。所有映像彼此隔离，进一步增强了这种方法的安全强度。

云和 S3

NetBackup 可部署在云环境中。NetBackup v9.1 可使用 S3 作为存储目标，并非“转储”数据，而是可真正感知数据并与目标通信，定义保留映像的时间。这种方法无需还原去重的数据，也不依赖第三方提供商。数据直接进入 S3 对象存储桶，在这里保留去重的数据。这是利用云防篡改存储抵御勒索软件的有效方法。

检测

Veritas 可帮助企业实现对整体环境的完全可视化。如上所述，如果 IT 部门对环境中的任何部分（例如工作负载或硬件）不了解，都将存在风险。缺少环境的完整视图犹如盲人摸象。

Veritas NetBackup IT Analytics

Veritas NetBackup IT Analytics 可报告环境中的所有计算要素、存储、物理服务器、虚拟机和云服务器。除 Veritas 外，它还可以报告受其他备份供应商（例如 Dell EMC、Rubrik、Cohesity、Veeam、Commvault 等）产品保护的部分环境。

Veritas NetBackup IT Analytics 可以执行异常检测，检测范围十分广泛。它预置勒索软件异常检测模板，为并不精通网络安全领域的管理员带来自动化和易用性两大优势。尤其当虚拟机达到成百上千台时，这样的解决方案非常有用。

在备份过程中，Veritas NetBackup 会执行异常检测，例如操作时间是否过长、备份是否过大，以及重复数据删除率是否与预期不符等。这些异常可能是感染的迹象，将会立即触发报告，有助于管理员视需要评估和修复问题。随着时间的推移，Veritas NetBackup 会通过人工智能技术不断学习，不断优化异常检测功能，减少误报率。

与降低网络钓鱼风险相关的其他 NetBackup 功能还有：基于角色的访问控制、环境分段和多因素身份验证，以避免其给您造成严重威胁。Veritas 支持用于多重身份验证的安全断言标记语言（SAML），因此可在 NetBackup 环境中有效实施多重身份验证。

Veritas 还确保网络钓鱼不会攻击通信，具体做法是要求客户端和备份服务器之间进行证书授权。在最终用户方面，NetBackup 提供基于角色的细粒度级别访问控制。

数据的静态和动态加密可有效防止勒索软件对备份数据的攻击，防止数据泄露。NetBackup 支持多种加密服务。

Veritas Data Insight

对于文件系统，Veritas Data Insight 解决方案提供现成可用的内置模板，用于查找已知的勒索软件文件扩展名。它还对用户活动进行细粒度监控（据悉，勒索软件入侵企业的最常见手段是网络钓鱼）。Veritas Data Insight 可按照用户和群组的方式跟踪文件的使用情况。它可识别：

- 异常读取操作（发生渗透攻击时，系统通常会出现异常读取活动。）
- 异常写入操作，这可能是加密攻击的一种信号。
- 用户访问文件过程中的任何异常活动。

在识别过程中，它会将异常活动标记为潜在的预备攻击。然后，您可以通过 Veritas Data Insight 提供的细粒度用户活动视图，将攻击扼杀在萌芽状态。

恢复

对于恢复，您应有“选择的余地”。被勒索软件加密的可能是正在运行数据库的服务器，可能是特定的文件系统，也可能是一组文件。或许您的环境中还有其他运行工作负载的服务器位于不同的虚拟机群，或在 AWS 和 Azure 上。

粒度恢复

Veritas 可快速进行粒度恢复，例如物理服务器的裸机还原，虚拟机、云虚拟机和 Kubernetes 容器的就地还原等。

这种恢复不仅可以在单独的目标系统中实现，例如，如果服务器被加密，NetBackup 可对整个服务器执行完整的裸机还原。它还可以执行快速批量恢复。另外，Veritas 旗舰软件 NetBackup 最新版本中包含的 Instant Rollback 功能， 将连续数据保护与回滚结合起来，在执行恢复时可以无需选择完整还原。这样只发送较少的数据，就可以让虚拟机快速完全恢复运行。

云

如上所述，Veritas 的种种卓越功能可将去重数据高效地写入和存储到 S3 防篡改存储。利用这些数据，Veritas 可在云中按需建立数据中心 — 这些曾经的二级或三级数据副本，现在成为数据中心的核心。

该功能可节省正常运行期间的成本：您只需按需启动并运行数据中心。在万不得已时，它还提供最终选项：替换整个数据中心。IT 部门可以通过去重数据在云端创建 EC2 环境，以作备用。结果就是企业多了一个功能齐全的独立数据中心，而不会产生永远在线的计算费用。

编排和测试

只需轻点鼠标，一切都在精心编排下完成。几十台服务器和堆栈的不同部分可以按特定顺序有条不紊的恢复。您只需单击一下，就可以执行韧性恢复计划。

您还可以测试该计划，而不影响系统运行。计划的效果取决于最终测试。但是，如果测试会关停您的生产环境，您恐怕就不会进行该测试。Veritas 希望您可以轻松地定期测试勒索软件恢复功能。

更多的事实

勒索软件和网络风险不仅不会消失，而且还会愈演愈烈。构建一个能积极主动对抗风险的韧性基础架构是赢得这场战斗的关键。Veritas 利用 NIST 框架寻找解决问题的良策。

Veritas 拥有卓越不凡的解决方案，例如支持自动映像复制的强大电子气隙隔离备份，将本地去重数据直接发送到 S3 对象的功能，NetBackup AI/ML 引擎，全面的报告、分析和警报功能，粒度恢复选项以及高级编排，所有这些均证明 Veritas 帮助客户和潜在客户远离威胁的决心。

Veritas 打造集保护、检测和恢复能力于一体的解决方案，为客户创造价值。总的来说，这些都是屡经检验的技术，适用于各种规模的环境。

Enterprise Strategy Group 是一家 IT 分析、研究、鉴定和战略公司，为全球 IT 团体提供市场情报和可行性见解。

www.esg-global.com contact@esg-global.com 508.482.0188