用Cohesity对抗勒索软件攻击

主要优势

- 使用不可变快照保护备份
- 基于机器学习的异常检测
- 通过大规模快速恢复减少停机时间

数据是数字经济中的差异化因素。这就是为什么数据同时成为最有价值和最具针对性的业务资产的原因。据Cybersecurity Ventures报道，预计到2025年，全球网络犯罪成本每年将达到10.5万亿美元，到2021年，每11秒就有一家企业成为勒索软件攻击的受害者。人们对这种数字勒索计划的认识正在提高，但越来越多黑客采用更加复杂的手段，针对备份数据和基础设施的攻击，继续威胁着全球企业。对于确实受到损害的企业来说，巨大的财务损失通常会因客户的不信任而加剧，就医疗保健而言还会危及生命。

Cohesity有效地抵御勒索软件攻击并帮助您的企业避免支付赎金。Cohesity全面的端到端解决方案采用多层方法来保护备份数据免受勒索软件的侵害、检测并从攻击中快速恢复。Cohesity独特的不可变架构确保您的备份数据不会被加密、修改或删除。使用机器学习，它提供可视化并持续监察数据中的任何异常。如果发生最坏的情况，Cohesity有助于在您的全球足迹（包括公共云）中找到一份干净的数据副本，立即恢复并减少停机时间。

图 1：Cohesity 提供全面的功能来保护、检测和从勒索软件攻击中恢复数据

保护备份数据

Locky和Crypto等复杂的勒索软件已被用于破坏数据副本和恢复点数据，使企业备份基础设施成为主要的网络犯罪目标，而它应该是您企业防御中的重要部分。Cohesity防止您的备份成为攻击目标，不断阻止入侵者。

Cohesity及其全新的专用文件系统——Cohesity SpanFS™——独特地提供了多层防止勒索软件攻击。另外，Cohesity提供最高级别的对抗勒索软件攻击，因为从根本上说，它是一个具有只读状态快照的不可变文件系统。

- 不可变文件系统可以拍摄非常频繁的快照、这些无限制的只读状态快照占用存储空间极低。原始备份作业保持不可变状态，永远无法访问或由外部系统挂载。唯一方法是克隆该原始文件以读写模式挂载备份，这由系统自动完成。尽管勒索软件可能能够删除挂载后的读写备份，但它永不会影响到不可变快照。

- Cohesity SpanFS，文件系统允许您拥有非常大量的Views，并即时克隆这些Views，在存储利用率方面几乎为零成本。

防止未经授权访问敏感数据是Cohesity保护数据愿景的核心。这就是为什么Cohesity围绕勒索软件预防的创新不仅限于不可变文件系统，还包括：

- **DataLock** — 用于备份的WORM功能，它支持基于角色创建和应用Datalock策略以选定的备份快照。您企业中的安全官角色可以使用此功能将快照存储在WORM格式，即使管理员或安全人员也无法删除有时限设置的备份档案，为勒索软件攻击提供额外的保护。

- **Air-gap** — Cohesity提供多种基于策略的方法来隔离您的关键任务数据。根据您的企业独特的要求，您可以将数据复制或存档到外部基于云的目标，或以另一个物理位置或将以磁带存储到异地位置，例如Iron Mountain。基于政策的数据复制或存档提供更低的RTO和RPO，在向另一个位置数据传输的过程中仅保持灵活的网络连接便可。

- **因素身份验证 (MFA)** — 如果犯罪分子可以访问您的系统密码，该个人如果不通过MFA形式的额外安全层，将无法访问Cohesity备份或多步验证。Cohesity支持多种身份验证和授权功能，包括强大的Active Directory集成、MFA、访问控制列表、混合模式基于角色的访问控制 (RBAC)，以及全面的系统和产品级审计。

多云数据管理平台Cohesity Helios提供了不可变文件系统的独特组合具有DataLock功能，以及基于策略的Air-gap和MFA，以防止备份数据受到勒索软件攻击。

检测入侵者

随着网络犯罪分子不断加强和修改他们的方法，Cohesity使您的企业更容易使用基于 SaaS 的全球企业管理解决方案检测入侵。Cohesity 客户有单一仪表板可在全球范围内查看、管理其数据和应用程序并对其快速采取行动。在对抗勒索软件，Cohesity Helios 机器学习 (ML) 提供了人类可能会错过的资讯，因为它会自动和持续监察，并在检测到异常时通知您。

先进的ML算法会主动评估您的IT需求，并定期自动执行基础架构资源。如果贵企业的数据更改率（包括数据摄取）超出正常范围，基于逻辑数据、全局重复数据删除后的存储数据或历史数据摄取的每日更改率——Cohesity Helios的机器驱动异常检测会向您的IT管理员发送通知，IT 部门会立即被告知数据更改与正常模式不匹配。

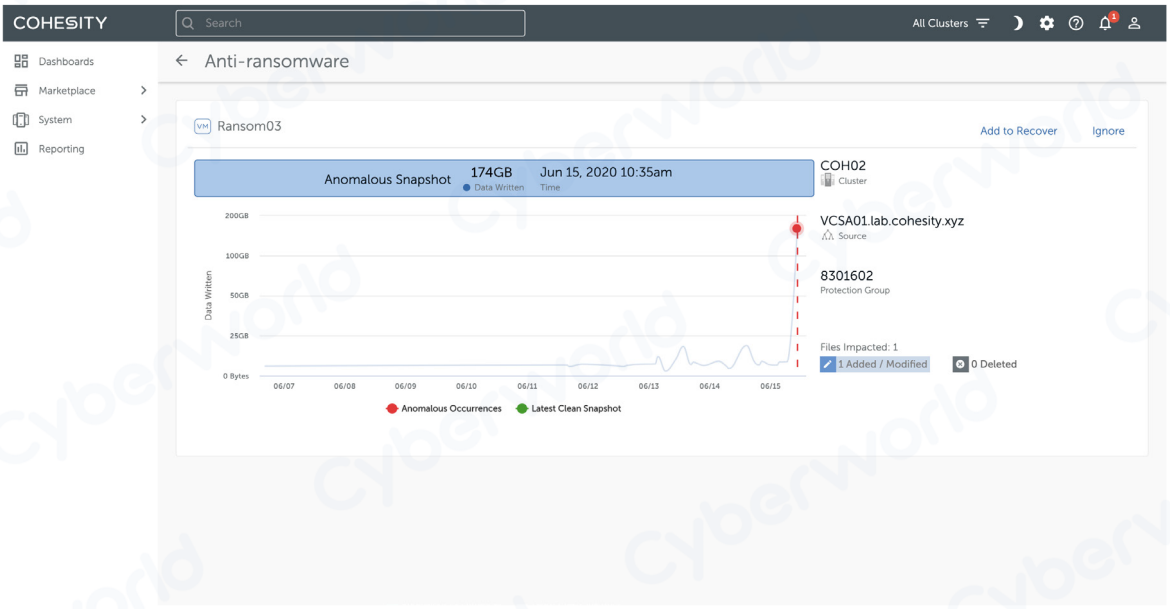

图 2：企业使用 Cohesity Helios 检测勒索软件入侵

因为Helios用机器驱动学习建立模式并自动扫描数据摄取或更改率异常，它会标示潜在的勒索软件攻击。如果检测到异常，平台会同时发出警报并通知您的企业IT团队和Cohesity的支持团队加快修复。

除了监察备份数据更改率以检测潜在的勒索软件攻击外，Cohesity还非常独特地检测到并针对非结构化文件和对象数据中的文件级异常发出警报。 这包括分析频率访问的文件数量、特定用户或应用程序修改、添加或删除的文件数量等确保快速检测到勒索软件攻击。

快速恢复

攻击确实会发生，而且速度很快。这就是为什么恢复必须是可预测和快速的。Cohesity加速了大规模恢复被勒索企业的数据和应用程序的时间。Cohesity Helios的机器驱动辅助会建议IT使用干净的数据副本执行还原。或者，您可以利用该平台的类似Google的全球跨环境快速定位和访问数据的搜索功能以找到你想还原的数据。

确保干净还原并避免将网络威胁或软件漏洞重新注入您的生产环境环境中，Cohesity的CyberScan可以深入了解受保护的健康和可恢复状态快照。CyberScan显示每个快照的漏洞索引和可行的建议，以解决任何问题软件漏洞。这可以帮助您从勒索软件攻击中干净且可预测地恢复。

Cohesity平台完美整合快照与Cohesity专有的SnapTree的 B+Tree架构、MegaFile和即时挂载功能，您可以即时恢复数百个虚拟机 (VM)、文件、对象和大型数据库。

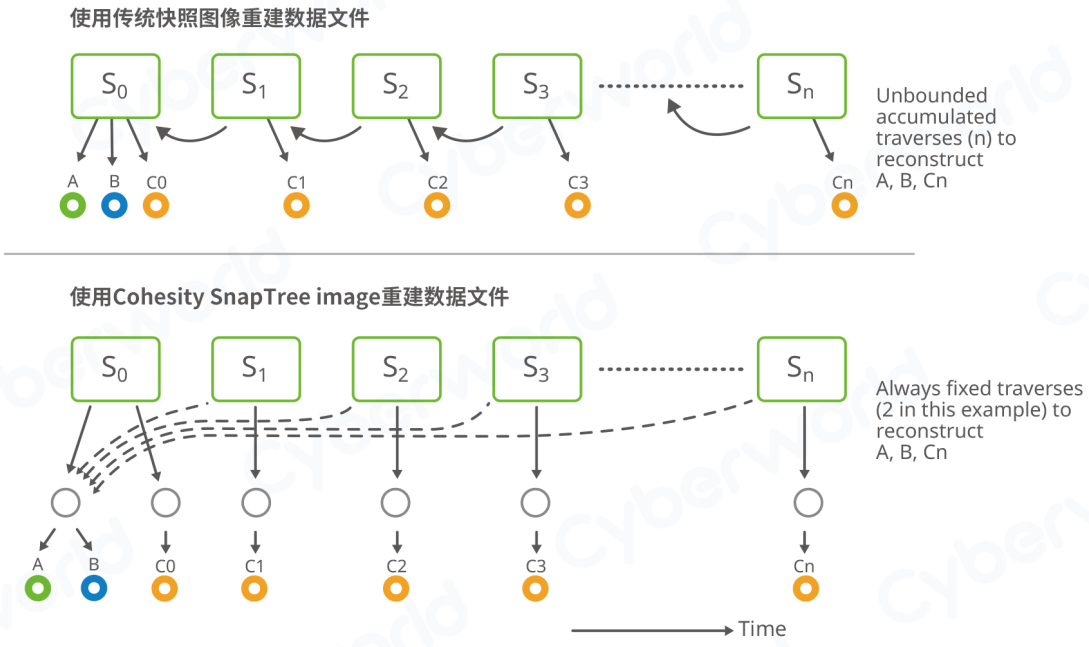

图 3：Cohesity获得专利的SnapTree技术可提供无限的快照，无需大量存储空间，支持大规模即时恢复

用 Cohesity 对抗勒索软件攻击

备份是您抵御复杂且严重的勒索软件攻击的最后一道防线。Cohesity全面的反勒索软件解决方案可保护、隔离、检测，最重要的是快速恢复以减少停机时间并确保业务连续性。

了解更多信息，请访问 www.cohesity.com/solutions/ransomware

COHESITY