Cohesity 的勒索软件检测与机器学习模型

为什么客户会使用 Cohesity 下一代数据管理平台?

因为它是防御勒索软件攻击的最后一道防线，快速保护、检测和恢复企业宝贵的数据。Cohesity 的技术能最大限度地减少攻击面，满足严格的备份服务级别协议（SLA），从而大大加快各种恢复操作的速度。Cohesity 在此基础上帮助客户更快地识别攻击并做出反应。并且，Cohesity 先进的低误报率威胁检测信号，能快速有效地接收、管理和处理警报，阻止攻击并加速清理。

阻止攻击者入侵

在备份过程中，备份数据发生异常变化，Cohesity 便收集数据变化情报，立即准确预警，不会产生大量误报。例如，新数据出现不易被压缩的情况，则可能存在加密攻击的危险，这有时会被称为“熵检测”，加密数据看起来非常随机，这就是它不压缩的原因。

为了检测实时攻击、避免误报，Cohesity 把多个指标输入到 Cohesity Helios 控制平台的机器学习算法中，包括但不限于:

- 每个备份的信息：写入的数据大小、读取的数据大小、合乎逻辑的数据大小。
- 每个备份的熵、压缩比。
- 更改每个备份的跟踪信息：添加的文件数、已删除的文件数、更新的文件数、未更改的文件数。
- 跨多个备份的汇总信息：最大数据写入字节数、最大源逻辑大小字节数、成功运行次数等。
- 表示由常用恶意软件生成的更改模式的训练集。

机器学习模型，不是传统意义上的“AI-washing”，而是多变量模型。Cohesity 至少需要 15 条有效历史记录才能触发检测，机器学习需要定义正常行为基线，建立指标基线后，Cohesity 的机器学习模型从积极学习阶段开始，过渡到稳定状态，然后不断优化精准度和召回率。

如果数据和替换文件可压缩，就不太可能会发生加密攻击。Cohesity 有人类编写的、基于规则的启发式模型，用于消除误报。通过组合多个模型，将人工智能和原始机器学习结合起来以获得最佳成果。

本着不断改进的精神，Cohesity 还测试了其他机器学习模型，对比了研究成果。如果改进模型里最新损害模式，Cohesity 就可以升级检测，而不会在检测范围内出现间隙。

Cohesity 勒索软件攻击检测功能

最具破坏性的恶意勒索软件攻击，是由黑客驱动的，不是由已入侵笔记本电脑、服务器的恶意软件自发感染的。但也有可能出现病毒破坏，这种普通的攻击不会速度缓慢、偷偷摸摸，其产生的破坏是显而易见的。

Cohesity 在独立于其他 Cohesity 云环境中，创建了损害模式样本，这些样本包含 Cerber、Cryptxxx、Cryptolocker、Locky 和 Wannacry，Cohesity 对它们进行了 100% 的检测。

Cohesity 的勒索软件攻击检测功能包含在 Cohesity Helios 平台中，基于软件即服务（SaaS）。客户无需支付额外费用即可享用，因此 Cohesity 积累了大量数据用于机器学习模型训练，这有助于机器学习模型适应黑客发起的真实攻击，即使黑客已经入侵到客户系统，Cohesity 也会即时恢复备份。

Cohesity 的勒索软件攻击检测功能与备份功能是集成在一起的，这可以提高工作效率、改进检测、更快响应、降低 “保险库重要数据”被攻击的风险。勒索数据的加密过程都有一个副作用，就是使数据看起来是随机的，或者用一个花哨的术语来形容——“高熵”，这种“熵”会导致数据压缩和删重变得无效。Cohesity 可以注意到增加的“熵”，无需执行大量额外工作，备份产品可进行数据压缩和删重。让一个单独产品读取所有数据来检查“熵”，是一种浪费。所以，当其他备份供应商推荐攻击监视类的单独产品时，要么不检查“熵”（这会降低检测性能），要么需要额外的高成本资源来检查熵。

为了解决部分“熵检测”资源问题，只有在备份完成并传输到单独的网络保险库后，才能运行单独的检测产品。如果保险库因基于时间的 air gap 而定期断开连接，则会进一步延迟警报。例如 U 盘受损，更新保险库的检测工具会增加保险库意外感染的风险，在保险库中进行更新的频率会降低，减慢训练或者算法更改的采用速度。

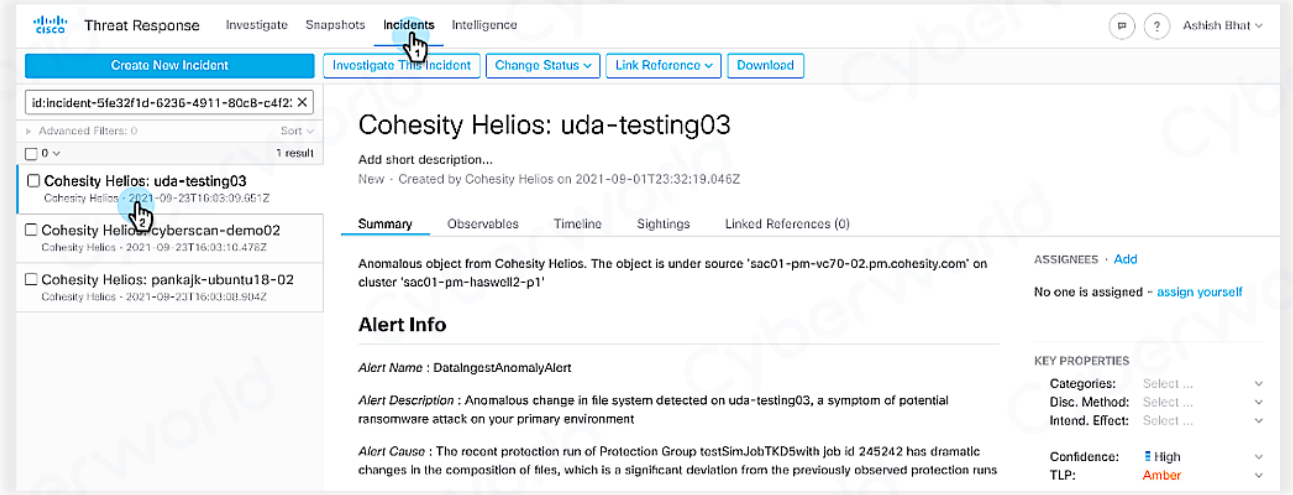
对于备份供应商而言，尝试区分检测功能是合理且明智的。有时 Cohesity 会被问到，是否在逐个文件的基础上开展“熵检测”（可压缩性）。据了解，在是否将备份标记为可疑分析这件事情上，从未有备份供应商执行过。如今，延迟警报和资源损失的情况已经越来越多。Cohesity 发现一个后处理步骤的说明，该步骤在备份时，被认为是可疑的后进行的文件级“熵分析”，这涉及到集群中与备份数据流不协同的附加处理，会延迟警报。Cohesity 工程师认为这种做法没有含金量。近来，虽然对备份工作替换的说明，没有提到逐个文件开展“熵检测”，但这种文件处理的主张却是说明的一部分，不再被视为“不可信赖”的情况。

迅速、确信、协调一致地响应

虽然 Cohesity 对以数据为中心的实时攻击视图很有信心，但 Cohesity 了解，实际上与其他信号关联，能进一步提高攻击响应的敏捷度。为了能快速响应事件，Cohesity 可以将警报发送到安全编排和自动化响应（SOAR）平台，SecOps 人员接收警报，确信地开展下一步调查。然而，精准警报有时会藏着不易被发现的失误，所以少量误报比精准警报更可取。为了在清理过时警报的同时，保持环境干净。Cohesity 提供与 Palo Alto XSOAR 和思科 SecureX 的闭环集成，允许从 SOAR 平台内部进行完整配置。通过利用自动化战术，用户无需重新登录备份界面，即可完成响应，减少了平均检测时间（MTTD）和平均响应时间（MTTR）。

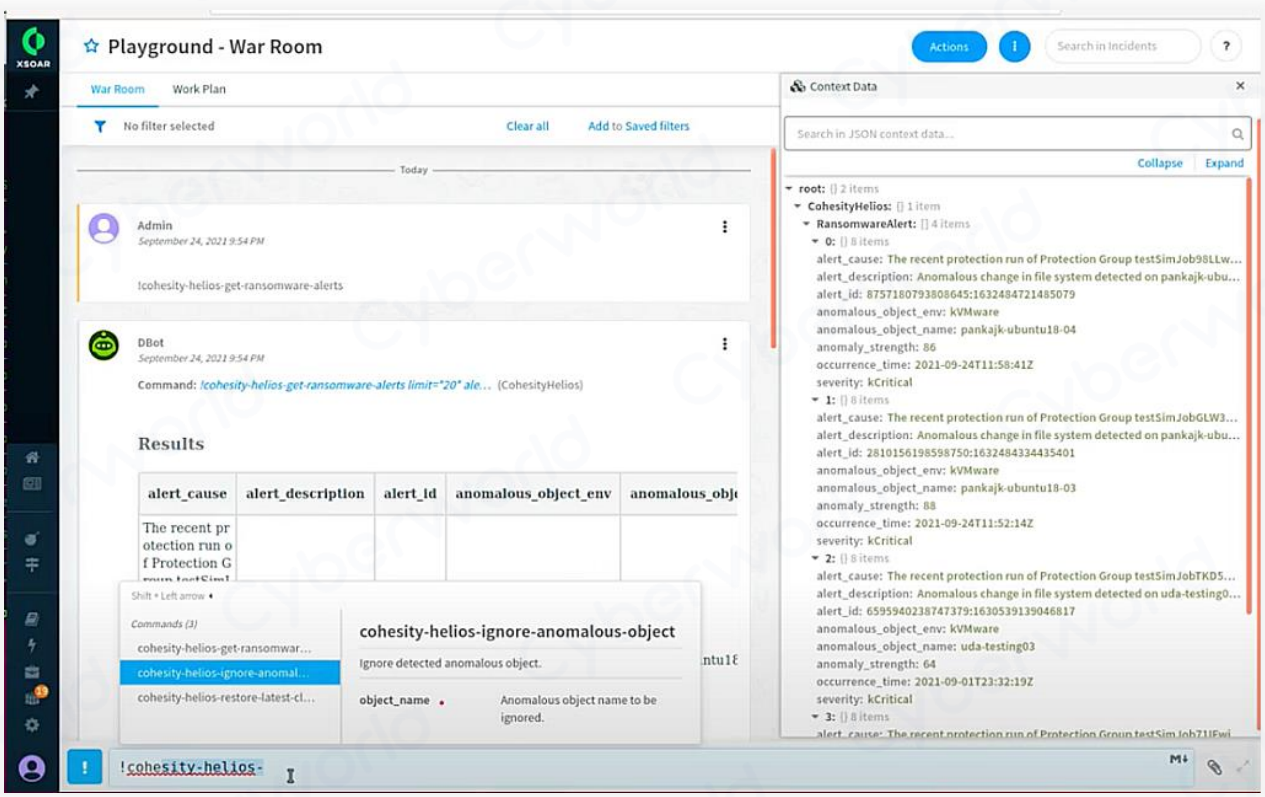
范例如下：

思科 SecureX：要使用 Cohesity 的集成查看思科 SecureX 中的警报，对其采取行动，点击”Incident”，选择 Cohesity Helios 异常对象事件。



在可观察的条件下，单击主机名的下拉列表，然后选择 Cohesity 还原异常对象。

Palo Alto XSOAR：首先研究 XSOAR 上忽略异常中的异常，然后确定需要采取的行动。在这种情况下，Cohesity 发现一个错误的地方，选择“Ignore”来确认如下所示的警报。



在检测到攻击后，用手机通知管理员，并与事件响应集成。企业可以快速反应，阻止任何攻击。

快速恢复功能

攻击停止后，检测输出能否帮助客户更快地恢复？当然能！

其他备份供应商，只会把受攻击的文件恢复到受攻击的服务器上。专业安全团队和网络保险公司表示，恢复到受感染的环境中是不可取的。Cohesity 会生成一个疑似受到攻击的文件列表，用不同的解决方法帮助客户从攻击中恢复文件。

实际上最佳的做法是，将已经隔离处理的所有数据恢复到全新构建的服务器或 VM 中，最好是已扫描最新已知漏洞，并没有任何高风险问题的服务器或 VM，而不是恢复到原始的服务器或 VM 中。

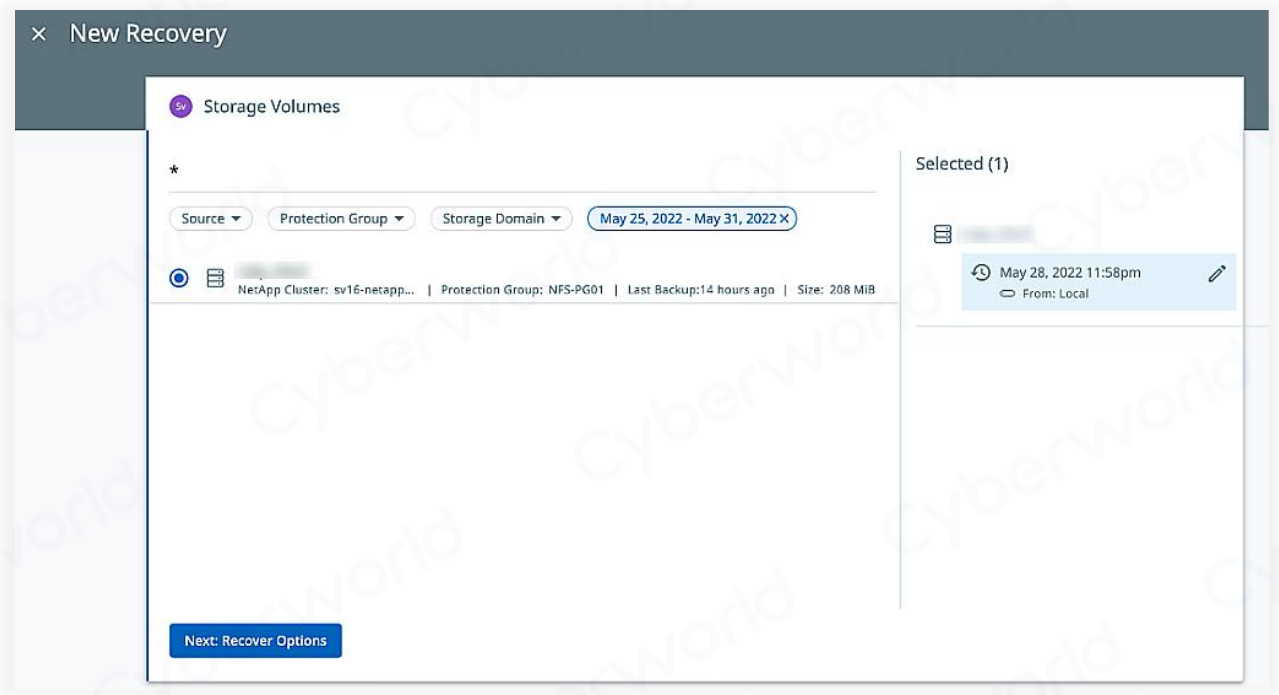
当发生攻击时， Cohesity 的客户都需要在沙箱中对整个数据集进行隔离处理，而不是覆盖文件。为了检查整个数据集，Cohesity 具有独特的可扩展的快速批量恢复、即时网络附属存储（NAS）备份访问权限。这些是由

Cohesity 独特的快照元数据、强大的文件系统技术所驱动。该技术能快速恢复企业的文件和对象，检查异常状况，通过 Cohesity Smartfiles 视图 或 NAS 快速实现数据干净状态。

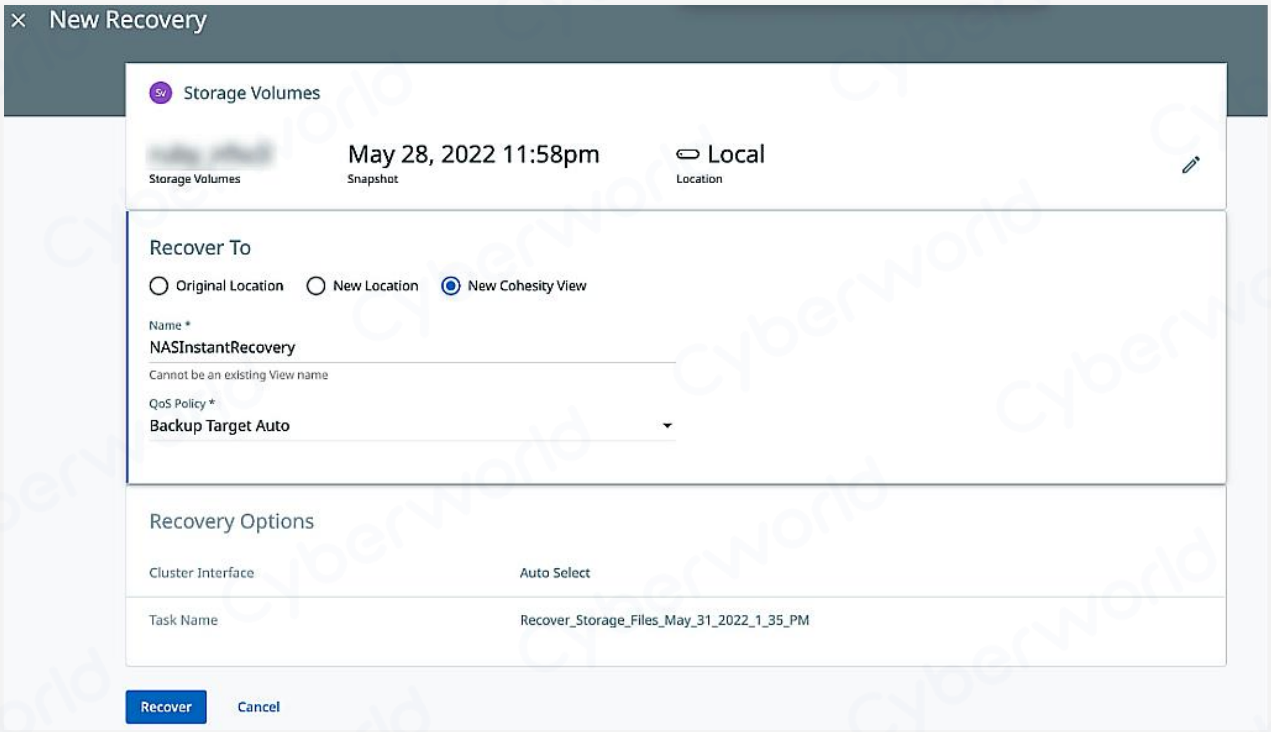
如何立即将 NAS 恢复到 Cohesity 视图

- 用 Cohesity 备份 NAS。
- 转到 Cohesity 范围选择器，选择集群。
- 选择恢复 > NAS > 存储容量。
- 单击 NAS，选择准确的数据进行恢复。

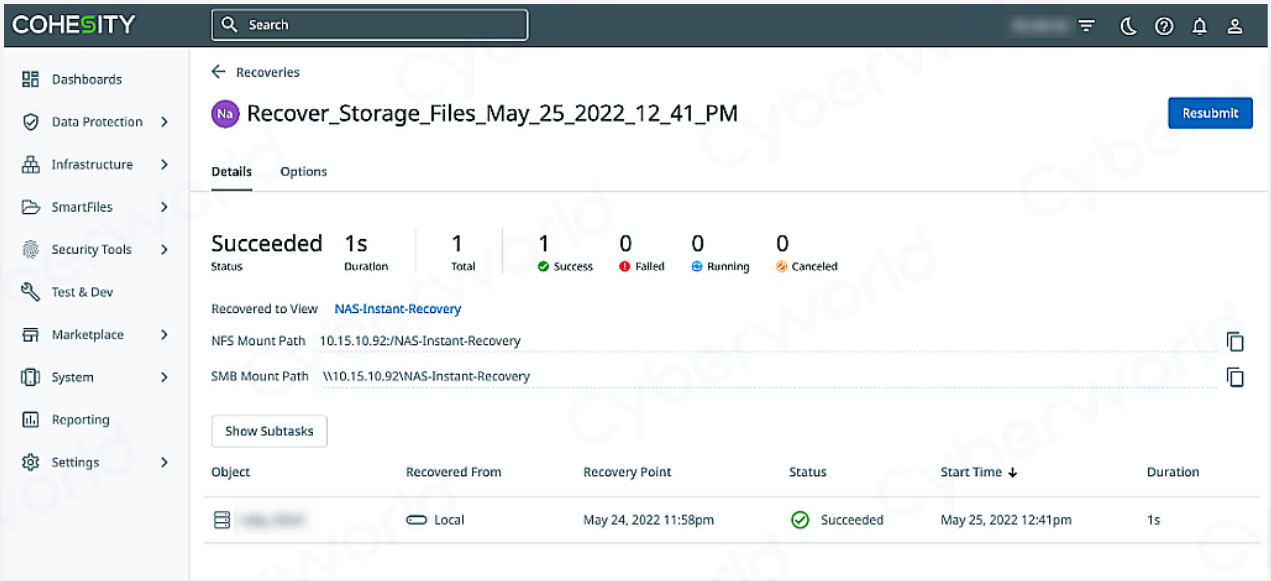
立即将数据恢复到新的 Cohesity 视图，以获得即时 NAS 访问权限



- 单击“Next：Recover Options ”按钮。
- 选择下图中显示的设置，恢复到新的 Cohesity 视图，然后单击 “Recover”。



· 确认恢复已完成，开始在 Cohesity 视图中使用文件和对象数据集。



即时 NAS 访问权限是一项关键技术，能在攻击后加快净化进程。但是，有些从业者认为它是一个必备的功能。

以下 2 个论据可以让大家了解真相：

不可变文件系统和 NAS

不可变文件系统提供了一种创建数据快照的方法，快照创建后便无法修改，文件系统本身也不能修改。文件系统中的 SmartFiles 视图具有任何文件服务器必备的添加、修改或删除文件的命令。Cohesity 的备份软件无需使用视图，即可连接到内部文件系统。一旦通过 Cohesity 的备份软件或 Smartfiles 在 Cohesity 内部文件系统中创建快照，就没有任何命令（甚至内部也没有）用于添加、修改或删除文件，或以任何其他方式更改快照内容。

Cohesity 还具备整个快照的不可删除性。除了不可变快照之外，Cohesity 的数据锁功能，可以在快照上设置一个附加的时间限制。在锁定的天数内，超级管理员和 Cohesity Support 都不能删除快照。

在即时访问期间，不可变快照保持隐藏状态。公开的是零成本克隆，而不是备份本身。使用不可变快照，即使在节点运行进程上试图更改文件出现错误，结果也会创建一个新的克隆，其中包含新内容，而不是修改的备份数据，这被称为“不可变文件系统”。

Cohesity 的深度融合解决方案可以减少攻击面。拥有 NAS 服务并希望进入备份行列的供应商，可能会创建一个在内部挂载 NAS 视图的备份应用程序。Cohesity 的解决方案正好与它们相反。Cohesity DataProtect 早于 SmartFiles 面市。DataProtect 使用安全的 API 和 RPC，而不是开放的 NAS 或对象协议。只能通过 Cohesity 的 API 和 RPC 枚举或连接备份数据，DataProtect 将备份服务器连接到集群，并在集群内的节点之间建立连接。在某些情况下，本机应用程序将数据转储到一个共享，然后对该共享创建不可更改的快照并将其脱机。为了保护这些工作流程，Cohesity 支持 NFSv4.1 访问控制列表（ACL），防止网络上不良行为者连接到临时挂载，试图窃取数据。

可扩展且可靠的实时访问备份

当警报提示 VM 出现问题时，请务必加快沙箱操作进程。消除遍历链，会使得 Cohesity 快速批量恢复更具可扩展性。使用重复数据删除闪存，可进一步加速即时批量恢复。

大部分备份系统，都不打算用于防止硬件故障而进行的更新数据。Cohesity 的文件系统是生产级的：在保护新数据免受节点故障或重启之前，没有 IO 被认为是完整的。使用 Cohesity 真正横向扩展的文件系统，节点故障

时不会导致文件句柄丢失，也不会根据可用数据而导致 VM 或应用程序崩溃。

Cohesity 如何帮助

Cohesity 的功能包括不变性，保护备份数据。它提供了独特的技术，使企业能够加速清理和大规模恢复正常操作。此外，Cohesity 的勒索软件检测与机器学习模型，满足了当今网络世界的关键要求，使客户能够在攻击后，更快地做出反应并加速全面恢复——特别是在与领先的第三方网络安全解决方案集成时。总之，Cohesity 具有保护企业备份数据、检测威胁和大规模快速恢复数据的能力，把勒索软件攻击和其他网络威胁的影响降至最低。