技术报告

NetApp 防勒索软件解决方案

NetApp 产品安全团队
2022年3月| TR-4572

摘要

本指南介绍了什么是勒索软件、它是如何演变的、以及如何使用NetApp® 解决方案 对勒索软件进行识别、早期检测、防止传播和尽快恢复。本文档中提供的指导和解决方案旨在帮助企业在实现信息系统机密性、完整性和可用性的规定安全目标的同时、提供具有网络弹性的解决方案。

目录

插图目录

勒索软件概述

每个人都知道、勒索软件攻击是企业可能面临的主要网络安全威胁之一。潜在的损害不仅在于直接相关的恢复成本(据Sophos称、2019年至2020年期间增加了241%)、还在于它对公司声誉和品牌的影响。

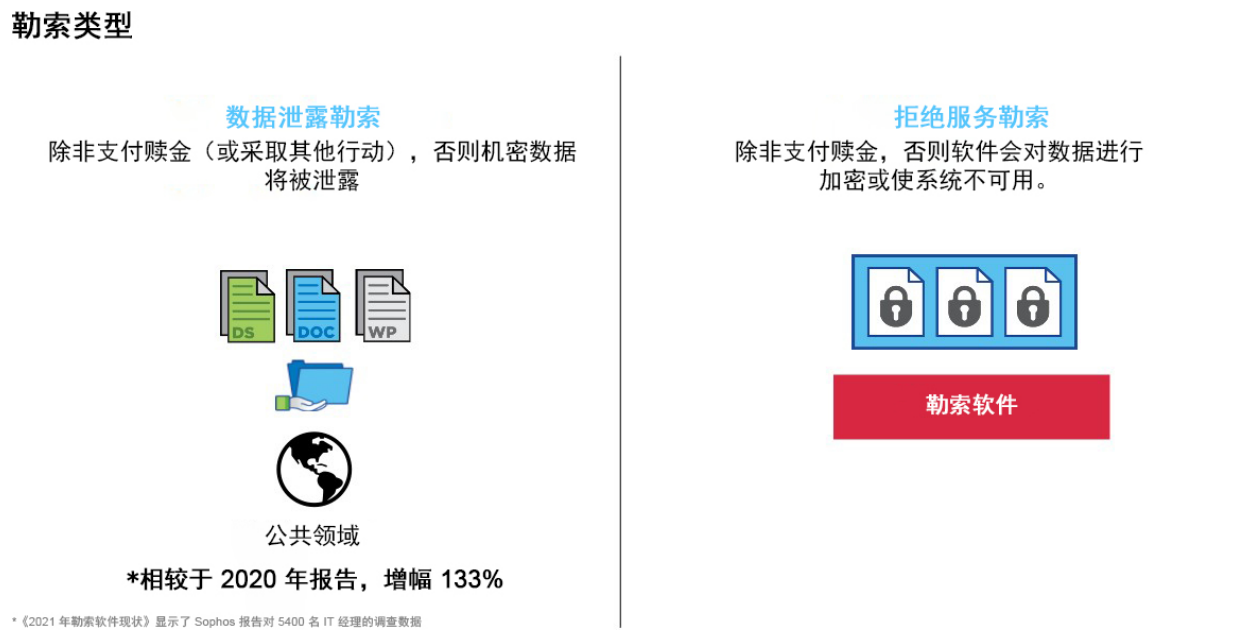
什么是勒索软件？

利用勒索软件的攻击者的目标只是尽可能廉价地赚钱。多年来、攻击者使用的策略不断发展。过去、攻击者通常使用分布式拒绝服务攻击、在这种攻击中、客户用来购买物品的公司网站将无法访问。拒绝服务一直存在、直到支付了一笔勒索。目前、这一策略的使用量并不多。另一种方法称为数据泄漏。通过此策略、攻击者可以访问公司的IT系统、将敏感数据移动到公司外部的未知位置、然后威胁公开发布该数据、除非支付了勒索。据Sophos称、数据泄漏再次呈上升趋势、与上一年相比、此领域的攻击增加了133%。

大多数人都熟悉的勒索软件的更常见版本称为拒绝服务勒索软件。在这种勒索软件策略中、攻击者会让您无意中下载加密程序(恶意软件)。安装后、该恶意软件会对公司网络上NFS或SMB共享上的所有本地客户端文件和每个文件进行加密。对文件进行加密后、原始文件将被删除、您将无法再访问这些文件中的数据。您仍然可以查看这些文件、因为它们仍位于您的网络上、但由于攻击者对它们进行了加密、您无法访问它们。

与之前的方法不同、拒绝服务对攻击者的开销非常低、因为他们不必通过大量的机器人将公司网站脱机、也无需将数据复制到其他位置。攻击者要求您支付勒索费用以获取解密密钥、以便重新获得对数据的访问权限。勒索的规模通常足以使攻击者从攻击中获得相当大的利润、但并不大、组织支付的代价是不切实际的。

图1)目前对组织使用的两种主要勒索软件。

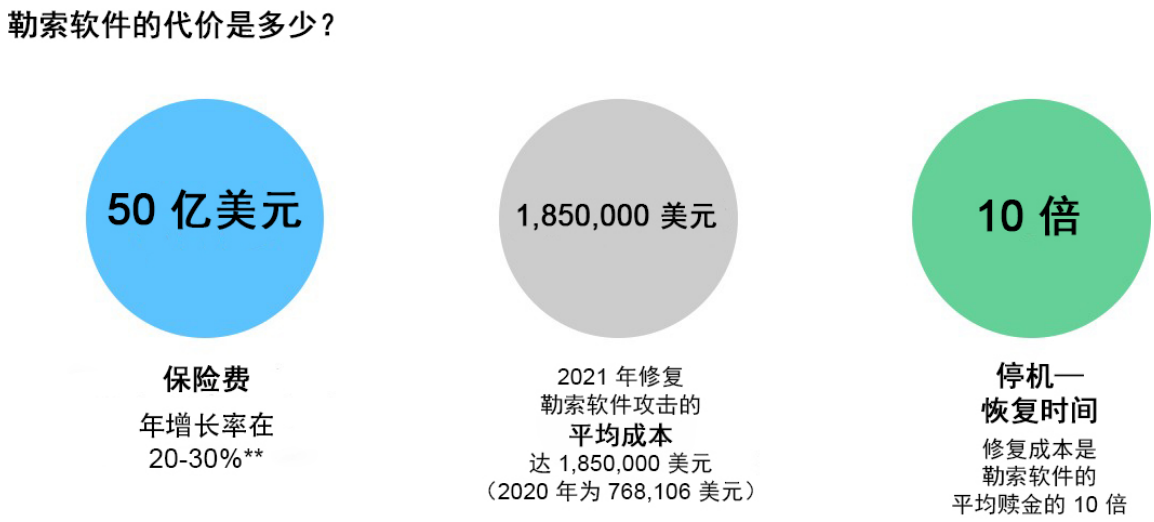


勒索软件的实际成本

您可能会认为、支付的勒索金额本身对企业的影响最大。但是、虽然付款并不微不足道(平均成本被认为每个意外事件高达154、108美元)、但与遭受勒索软件意外事件的实际成本(停机)相比、这笔金额微不足道。

当企业无法访问对业务至关重要的数据时、工作效率会受到严重影响。据乔维尔特2020年1 月的一项分析、勒索软件的平均停机时间超过16天、停机成本通常是实际勒索金额的10倍。美国的平均恢复成本为180万 美元。停机的影响和所产生的成本因业务类型而异。高度依赖IT可用性的企业(例如电子商务、股票交易和医疗保健)正在考虑10倍的成本因素。这意味着、如果实际停机时间不超过1、154、108美元、企业可能会面临的损失可能会高达1、154、108美元。请记住、此数量是按意外事件计算的；多个意外事件可能会增加成本。鉴于被保险公司遭受勒索软件攻击的真实可能性、网络保险成本也在持续上升。

图2)勒索软件的主要成本是企业在恢复期间面临的停机时间。



有关追加信息勒索软件的历史和实际成本、请参见《与勒索软件作斗争：第一部分—历史和成本》。

适用于勒索软件的NetApp解决方案

分层防御方法

必须尽早进行勒索软件检测、以防止其传播并避免代价高昂的停机。但是、有效的勒索软件检测策略应包括多个保护层。一个很好的比喻是在发生崩溃时保护车辆的安全功能。您不希望依靠安全带等单一功能在意外事件中为您提供保护。安全袋、防抱死制动器甚至是前向碰撞警告都是额外的安全功能、可以带来更好的结果。应以相同方式查看勒索软件保护。

例如、NetApp FPolicy与NetApp Cloud Insights或我们合作伙伴提供的类似功能相结合、可以通过用户行为分析(UBA)出色地检测勒索软件。他们从个人用户行为的角度寻找潜在的勒索软件攻击。劫持一个用户帐户只是黑客在发起勒索软件攻击时可能采取的一种途径；恶意攻击者不断发展其攻击技术。

此外、NetApp Active IQ® 和NetApp Active IQ Unified Manager还为勒索软件提供了额外的检测层。Active IQ 会检查NetApp ONTAP® 系统是否符合NetApp配置最佳实践、例如启用FPolicy。Active IQ Unified Manager 会针对NetApp Snapshot®副本的异常增长或存储效率丢失生成警报、这可能表明存在潜在的勒索软件攻击。

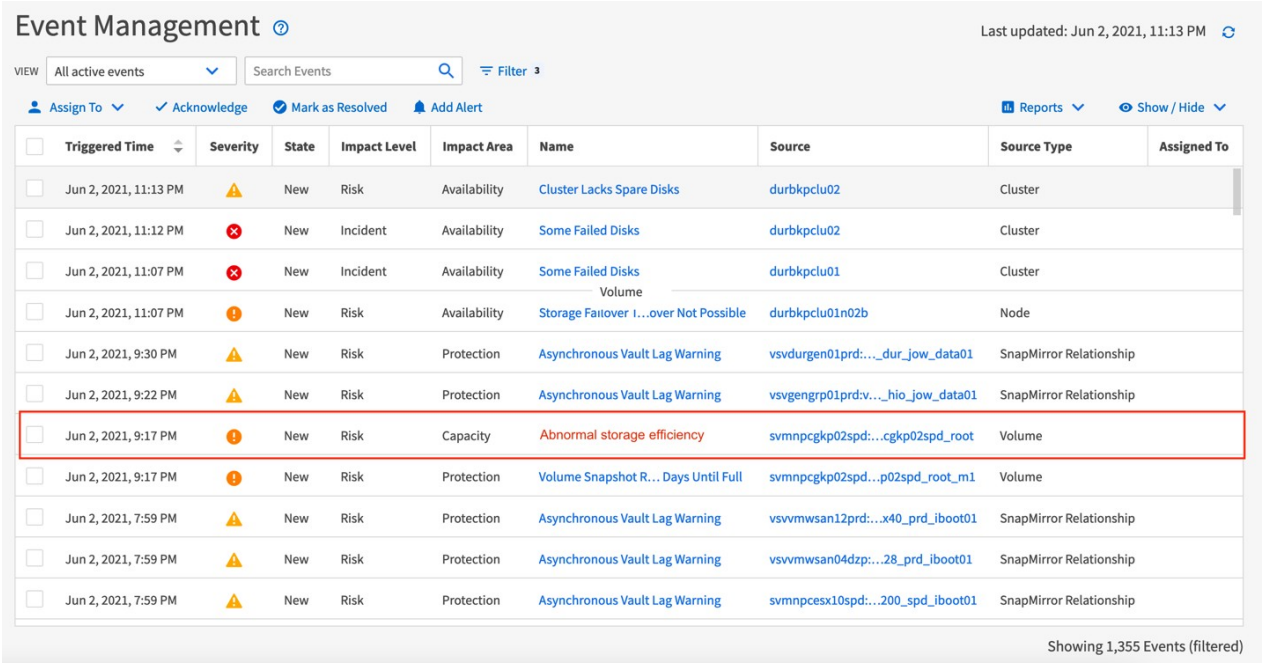
这就是ONTAP 9.10.1及更高版本中的反勒索软件功能发挥的作用。它利用内置的机载机器学习(ML)功能来查看卷工作负载活动以及数据资源、从而自动检测勒索软件。它可以监控与UBA不同的活动、以便检测UBA不支持的攻击。

对于追加信息、有关分层防御方法的信息、请参见博客《利用ONTAP 自动勒索软件保护防止勒索软件传播》。

NetApp原生 检测工具

NetApp提供了原生 或内置工具、可帮助您及早检测勒索软件。尤其是对于ONTAP、这些工具包括有关Snapshot副本和卷增长率异常以及存储效率下降的Active IQ Unified Manager 警报。

图3) Active IQ Unified Manager 提供的存储效率异常警报。



您还可以使用ONTAP System Manager实时查看Snapshot百分比变化或存储效率节省情况。

要了解有关ONTAP 原生 检测工具的更多信息、请参见博客《与勒索软件作斗争：第二部分—用于检测勒索软件的ONTAP 原生 (也称为免费)工具》。

本机 FPolicy

NetApp FPolicy (名称文件策略的演变)是一个文件访问通知框架、用于通过NFS或SMB/CIFS协议监控和管理文件访问。它已成为ONTAP 的一部分超过十年、在帮助您检测勒索软件方面非常有用。此零信任引擎非常有用、因为您可以在访问控制列表(ACL)中获得超出权限范围的额外安全措施。

零信任背后的概念是从不信任、始终验证。您可以 在最近的另一篇NetApp博客文章中了解有关此问题的更多信息。但关键在于、仅仅因为用户(或管理员)有权访问文件或文件夹、他们就不一定能够更改其在该位置所需的任何内容。

FPolicy最初旨在帮助您阻止将不需要的文件存储在企业级存储设备上。(例如、许多用户在使用像SPOTIFY这样的音乐流服务之前将.mp3文件存储在其主文件夹中、从而使用户能够从其个人设备流式传输音乐。) 但是、FPolicy还为您提供了一种阻止已知勒索软件文件扩展名的方法。用户仍对其主文件夹具有完全访问权限、但FPolicy不允许他们存储您的管理员标记为已阻止的任何文件、无论这些文件是.mp3文件还是已知勒索软件文件扩展名。

要了解有关原生 FPolicy的更多信息、请阅读博客《与勒索软件作斗争：第三部分—ONTAP FPolicy》、这是另一款功能强大的原生 (也称为免费)工具。

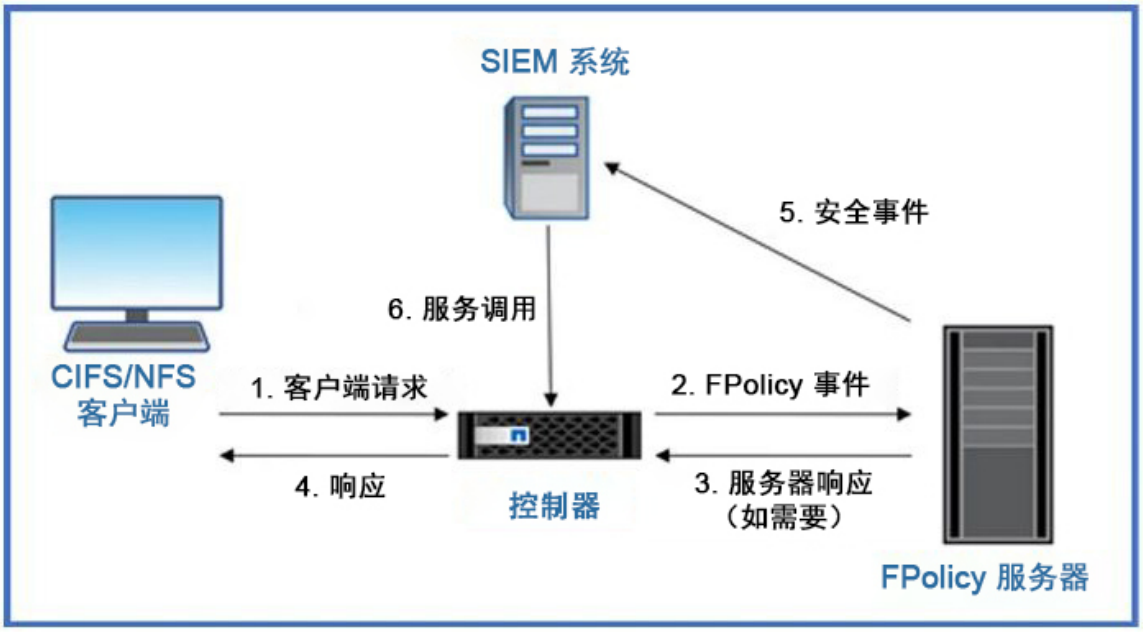
外部 FPolicy

ONTAP 中的FPolicy外部模式使用UBA (有时称为用户和实体行为分析或UEBA)作为停止零日勒索软件攻击的关键。要了解具体情况、您需要深入了解UBA。

人类是一种习惯。我们的习惯适用于许多方面、包括我们访问和处理数据的方式。用户和组经常访问特定数据集来执行其作业。UBA可跟踪这些行为、确定用户的典型访问模式、并可报告该用户的行为何时与模式不同。更进一步的是、如果用户在其常规模式之外执行操作、UBA也可以拒绝对文件数据的访问。FPolicy外部模式与使用UBA的外部服务器集成、用于确定用户何时执行他们通常不执行的操作。

在以下安全信息和事件管理(Security Information and Event Management、SIEM)系统示例中、每个CIFS或NFS客户端请求都会发送到FPolicy服务器、从而判断是否允许访问。

图4)外部模式下的FPolicy使用FPolicy专用API与外部服务器集成。



即使用户对尝试操作的文件数据具有文件权限、也会进行这种额外级别的分析。由于权限很难始终正确使用、因此、使用FPolicy的UBA可以更好地衡量用户是否尝试执行恶意操作。有关UBA的详细信息、请参见NetApp技术报告 TR-4829：NetApp和Zero Trust。

UBA功能强大、但它不是应对零日勒索软件攻击的最终目标。许多NetApp合作伙伴和供应商已开始将 人工智能 (AI)和ML整合到其外部FPolicy服务器中。由于每个供应商都会加入ONTAP 中内置的FPolicy功能、因此您可以立即利用这些AI/ML增强功能。

要了解用户行为分析和FPolicy外部模式、请阅读博客《与勒索软件作斗争：第四部分—采用FPolicy外部模式的UBA和ONTAP》

Cloud Insights

如前所述、UBA需要外部模式FPolicy服务器。尽管NetApp拥有提供此服务的合作伙伴、但我们也拥有自己的外部模式FPolicy服务器：采用Cloud Secure 的Cloud Insights。

Cloud Insights 是一款SaaS基础架构和服务监控解决方案、适用于内部环境、私有云和公有 云环境、包括AWS、Azure和Google Cloud。Cloud Secure 是 NetApp Cloud Insights 的一项功能，用于分析数据访问模式，以识别遭受勒索软件攻击的风险。

图5) Cloud Secure 通过三种主要方式帮助防止勒索软件。

要了解有关使用Cloud Secure 的Cloud Insights 的详细信息、请参见 cloud.netapp.com。

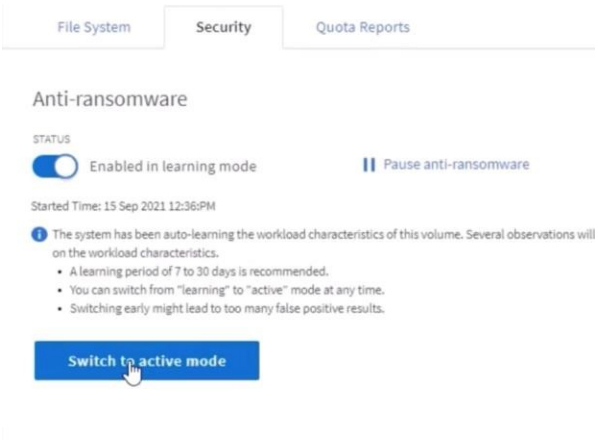
即装即用的反勒索软件

ONTAP 9.10.1及更高版本在其反勒索软件功能中引入了一种全新形式的勒索软件检测和预防。它利用内置的机内ML来查看卷工作负载活动以及数据数据资源、从而自动检测勒索软件。此外、它还会监控与UBA不同的活动、以便检测UBA未检测到的攻击。

安装了多租户加密密钥管理(MT_EK_Mgmt)许可证后、9.10.1中将启用ONTAP 反勒索软件保护。它可通过ONTAP 内置管理界面System Manager进行配置、并按卷启用。

反勒索软件功能从学习模式开始。NetApp建议至少使用30天的时间、以便ML有机会了解NAS卷上的典型工作负载。当反勒索软件进入活动模式时、它会开始查找可能是勒索软件的异常卷活动。

图6)在设置为活动模式之前、在建议的30天内启用学习模式下的反勒索软件。



如果检测到异常活动、则会立即自动创建Snapshot副本、从而尽可能接近文件感染提供一个恢复点。同时、系统会生成一个自动警报、使管理员可以查看异常文件活动、以便确定此活动是否确实是恶意的并采取适当措施。或者、如果活动是预期工作负载、他们可以轻松地将其标记为误报；反勒索软件ML会记录工作负载的变化、不再将其标记为潜在攻击。此外、此功能不会以任何方式中断I/O。而是为管理员提供原生分析、洞察力和数据恢复功能、以实现前所未有的机载勒索软件检测。通过反勒索软件功能、您可以比以往更轻松地在ONTAP 中为NAS工作负载启用自动勒索软件检测。

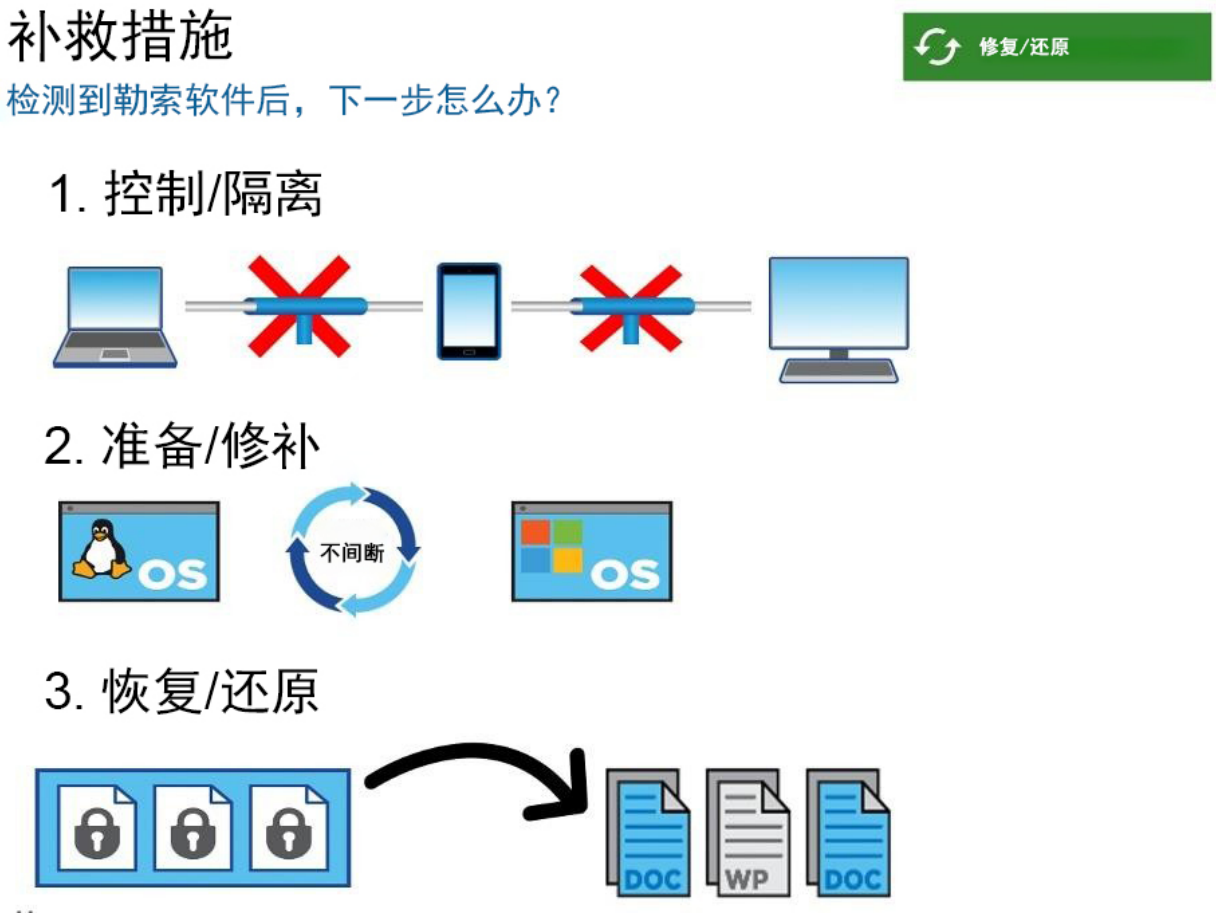
要了解有关反勒索软件功能的详细信息、请参见反勒索软件ONTAP 9文档。

从勒索软件攻击中恢复的建议

勒索软件攻击后、您的第一个直觉可能是即时恢复数据。您当然可以这样做、但如果您不采取其他措施来确保勒索软件不会再次出现、您可能最终会被重新感染、并且这项工作将浪费宝贵的时间。

要正确且全面地修复您的环境、使其免受勒索软件感染、需要执行三个关键步骤。下图显示了这些步骤、这些步骤最好按所列顺序完成(尽管不是必需的)。

图7)从攻击中恢复的建议步骤。



这种方法最有效地确保了在还原数据时、数据不会再被感染。

要了解有关勒索软件恢复最佳实践的更多信息、请参见博客《与勒索软件作斗争：第五部分—通过智能恢复避免重新感染》。

ONTAP 恢复功能

每个人都知道、从勒索软件攻击中恢复的最快方法是从备份中恢复。听起来很简单、但实际还原过程可能很复杂、更不用说速度较慢了。

- 备份数据是否也已加密？
- 我需要的备份是否仍然存在？
- 还原加密数据需要多长时间？
- 恢复数据是否会影响我的生产工作负载？

请务必对所有这些问题进行问题解答、以避免 在还原期间出现长时间停机(勒索软件的实际成本)。

ONTAP Snapshot技术是回答所有这些问题、提供快速恢复(以数秒为单位、以TB为单位)、保护您的备份免受勒索软件加密的影响以及防止删除有价值的备份数据的关键。您可以在整个生态系统中利用Snapshot副本的强大功能来实现灾难恢复、数据归档和数据分层等功能。

要了解有关ONTAP 恢复功能的更多信息、包括如何强化Snapshot副本以防止删除以及实现完全备份不可移动性、请参见博客文章《与勒索软件作斗争：第六部分—使用ONTAP Snapshot副本快速恢复数据》。

SnapLock、一种逻辑气隙

越来越多的趋势是、攻击者会销毁备份副本、在某些情况下甚至会对其进行加密。因此、网络安全行业中的许多企业都建议在整体网络故障恢复策略中使用空隙备份。

问题在于、传统的空隙可能会显著增加恢复时间、从而增加停机时间和整体相关成本。它通常还会增加复杂性。逻辑空位是传统空位的最佳替代方案、因为它在保持备份联机的同时具有相同的安全保护原则。借助NetApp、您可以通过逻辑间隙来解决磁带或磁盘间隙的复杂性、这一点可通过不可变的Snapshot副 本和NetApp SnapLock®合规性来实现。

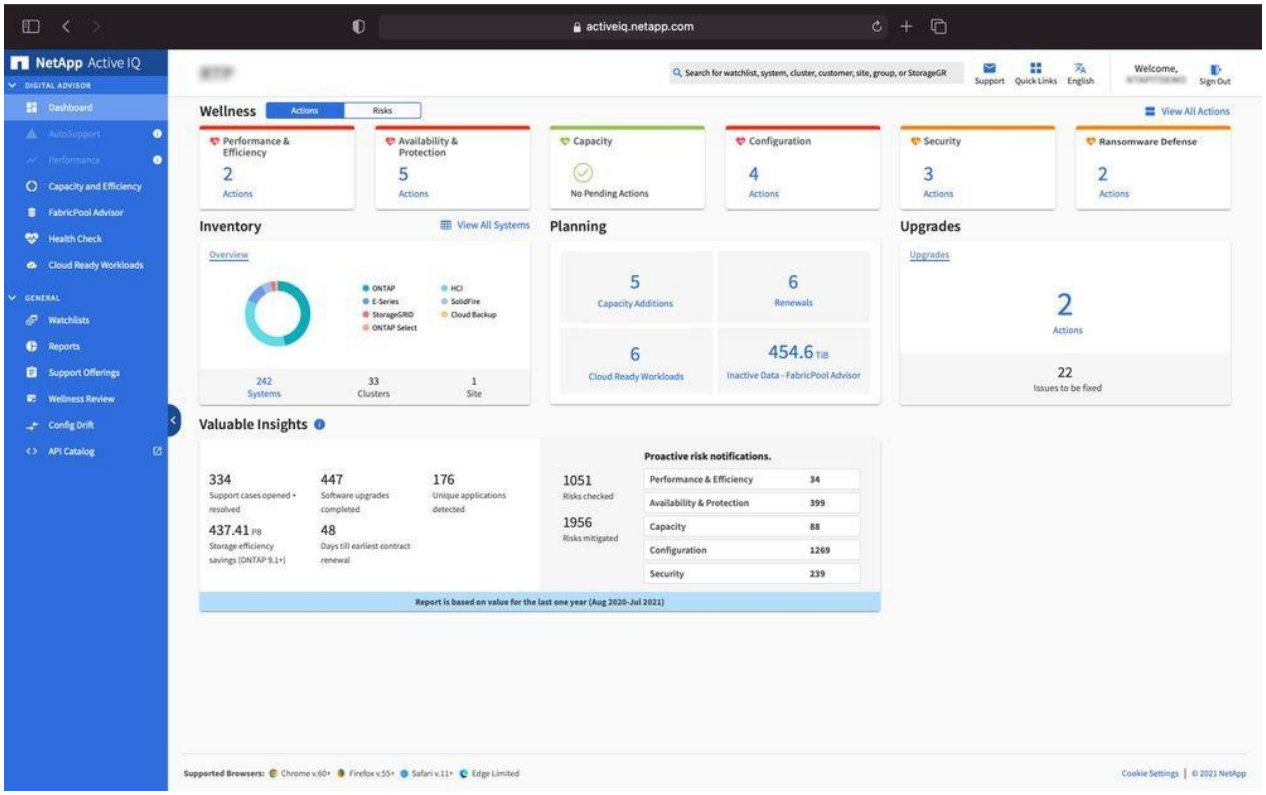
10多年前、NetApp发布了SnapLock 功能、以满足数据合规性的要求、例如健康保险携带和责任法案(HIPAA)、萨班斯-奥克斯利法案以及其他法规数据规则。您还可以将主Snapshot副本存储到SnapLock 卷、以便将这些副本提交到WORM、从而防止删除。SnapLock 许可证版本有两个：SnapLock Compliance和SnapLock Enterprise。对于勒索软件保护、NetApp建议遵循SnapLock 合规性、因为您可以设置一个特定的保留期限、在该期限内、即使ONTAP 管理员或NetApp支持人员也无法删除Snapshot副本。

要了解有关SnapLock 及其逻辑空中摆动功能的更多信息、请参见博客文章《利用 SnapLock 逻辑空中漏洞增强勒索软件保护》和技术报告 TR-4526：使用NetApp SnapLock 的合规WORM存储。

Active IQ —勒索软件保护最佳实践

在勒索软件保护以及确保您的NetApp系统遵循最佳实践来打击勒索软件方面、NetApp Active IQ也起着重要作用。Active IQ 不仅可以帮助消除安全漏洞、还可以提供针对防范勒索软件的见解和指导。专用的健康卡可显示所需的操作和已解决的风险、因此您可以确保系统符合这些最佳实践建议。

图8) NetApp Active IQ 信息板上的健康监控器。



在勒索软件防护健康页面上跟踪的风险和操作包括以下(以及更多内容)：

- 卷Snapshot副本数较低、降低了潜在的勒索软件保护。
- 未为配置了NAS协议的所有Storage Virtual Machine (SVM)启用FPolicy。要查看Active IQ 的

勒索软件防护措施的实际应用、请参见 NetApp Active IQ。

结论

显而易见、勒索软件与许多其他恶意软件威胁一样、仍在不断演变。正如防御方法得到改进一样、攻击方法和向量也会得到改进。虽然没有任何一个解决方案 可以阻止所有攻击、但使用包括合作伙伴和第三方在内的一系列解决方案可提供分层防护。

NetApp解决方案 提供了各种有效的工具来实现可见性、检测和补救、可帮助您尽早发现勒索软件、防止此类传播、并在必要时快速恢复、以避免代价高昂的停机。传统分层防御解决方案以及第三方和合作伙伴的可见性和检测解决方案仍然普遍存在。有效的补救仍然是应对任何威胁的关键部分。利用不可变的NetApp Snapshot技术和SnapLock Logical Air Gap解决方案 的独特行业方法是勒索软件补救功能的行业差异化优势和行业最佳实践。

从何处查找其他信息

如需详细了解本文档所述的信息，请参见以下文档和/或网站：

- NetApp ONTAP 文档中心
  http://docs.netapp.com/ontap-9/index.jsp
- NetApp勒索软件博客系列
  https://www.netapp.com/blog/prevent-ransomware/
- NetApp支持站点资源页面
  https://mysupport.netapp.com/ontap/resources
- NetApp产品安全性
  https://security.netapp.com/resources/
- NetApp Snapshot 技术
  http://www.netapp.com/us/media/ds-2477.pdf
- 所有 NetApp 产品文档
  https://docs.netapp.com

要验证您的特定环境是否支持本文档所述的确切产品和功能版本，请参见 NetApp 支持站点上的互操作性表工具 (IMT)。NetApp IMT 中定义的产品组件和版本可用于构建 NetApp 所支持的配置。具体的配置结果取决于每个客户如何依照所发布规格进行安装。

版权信息

商标信息

TR-4582-0322-CN

NetApp