关于NetApp勒索软件保护

ONTAP 9

NetApp
August 31, 2024

目录

关于NetApp勒索软件保护

勒索软件和NetApp的保护产品组合

2024年、勒索软件仍然是导致企业业务中断的最严重威胁之一。根据 "《RSoos的Rans要索状态2024》"、勒索软件攻击影响了72%的受调查对象。勒索软件攻击已经变得更加复杂、更具针对性、威胁行为者采用人工智能等先进技术来最大限度地提高其影响和利润。

企业必须从外围、网络、身份、应用程序以及数据在存储级别的驻留位置全面审视其整个安全防护、并确保这些层的安全。在当今的威胁形势下、在存储层采用以数据为中心的网络保护方法至关重要。虽然没有一个解决方案可以抵御所有攻击、但使用合作伙伴和第三方等解决方案组合可提供分层防御。

NetApp产品组合提供了各种有效的可见性、检测和修复工具、可帮助您及早发现勒索软件、防止其蔓延、并在必要时快速恢复、以避免代价高昂的停机。传统的分层防御解决方案仍然很普遍、第三方和合作伙伴的可见性和检测解决方案也是如此。有效补救仍然是应对任何威胁的关键部分。利用不可固定的NetApp Snapshot技术和SnapLock逻辑空隙解决方案的独特行业方法是一项行业差异化优势、也是勒索软件修复功能的行业最佳实践。

> 从2024年7月开始、以前以PDF格式发布的技术报告_TR-4572：《NetApp防兰软件保护》中的内容已与ONTAP产品文档的其余部分集成在一起。

数据是主要目标

网络犯罪分子越来越多地直接将数据作为目标、认识到数据的价值。虽然外围、网络和应用程序安全非常重要、但可以绕过它们。专注于保护数据的源存储层、可提供关键的最后一道防线。勒索软件攻击的目标是访问生产数据并对其进行加密或使其无法访问。要达到这一目标、攻击者必须已经破破了当今组织部署的现有防御系统、从外围到应用程序安全。

[从外围到数据安全的安全层]

遗憾的是、许多企业无法利用数据层的安全功能。这就是NetApp勒索软件保护产品组合的出现之处、可在最后一道防线为您提供保护。

勒索软件的实际成本

赎金本身并不是对企业的最大货币影响。虽然支付的费用不是微不足道的、但与遭受勒索软件事件的停机成本相比、它微不足道。

在处理勒索软件事件时、赎金只是恢复成本的一个要素。如果不包括支付的任何赎金、2024年、各组织报告从勒索软件攻击中恢复的平均成本为27.3亿美元、比该 "2024年：《RSoos的Rans潘 莫斯状态》"报告所报告的2023年的18.2亿美元增加了近100万美元。对于严重依赖IT可用性(例如电子商务、股票交易和医疗保健)的企业来说、成本可能会高出10倍甚至更多。

鉴于勒索软件攻击被保险公司的真实可能性、网络保险成本也持续上升。

在数据层提供勒索软件保护

NetApp了解您的安全防护在整个组织中具有广泛而深入的作用、从外围到数据位于存储层的位置。您的安全堆栈非常复杂、应在技术堆栈的每个级别提供安全保护。

数据层的实时保护更加重要、并且具有独特的要求。为了有效、该层的解决方案必须提供以下关键属性：

- 设计安全，最大限度地减少攻击成功的可能性
- 实时检测和响应，最大限度地减少成功攻击的影响
- **Air-gapped WORM**保护，用于隔离关键数据备份
- *单一控制平台*实现全面的勒索软件防御

NetApp可以提供所有这些功能以及更多功能。

[NetApp勒索软件保护产品组合、包括所述的关键属性]

NetApp的勒索软件保护产品组合

NetApp"内置勒索软件保护"为您的关键数据提供实时、强大的多方面防御。其核心是由AI提供支持的高级检测算法、可持续监控数据模式、以99%的准确性快速识别潜在的勒索软件威胁。通过快速响应攻击、我们的存储可以快速创建数据快照并保护副本的安全、从而确保快速恢复。

为了进一步增强数据的安全、NetApp的"网络保险"功能可以隔离具有逻辑空隙的数据。通过保护关键数据、我们可以确保快速的业务连续性。

NetApp"BlueXP勒索软件保护"通过一个控制平台智能地协调和执行以工作负载为中心的端到端勒索软件防御、减轻运营负担、因此您只需单击一下即可识别和保护存在风险的关键工作负载数据、准确、自动地检测和响应以限制潜在攻击的影响、并在几分钟内恢复工作负载、而不是几天内恢复工作负载、从而保护您宝贵的工作负载数据并最大限度地减少代价高昂的中断。

作为一款内置的本机ONTAP解决方案、"多管理员验证(MAV)"可保护对数据的未经授权访问、它具有一组强大的功能、可确保删除卷、创建额外的管理用户或删除Snapshot副本等操作只能在至少另一位指定管理员批准后才能执行。这样可以防止受到影响的管理员、恶意管理员或经验不足的管理员进行不希望的更改或删除数据。在删除Snapshot副本之前、您可以根据需要配置任意数量的指定管理员批准者。

NetApp ONTAP满足了 "多因素身份验证(MFA)"System Manager中基于Web的身份验证和SSH命令行界面身份验证的要求。

NetApp的勒索软件保护功能可以让您在不断演变的威胁环境中高枕无忧。其全面的方法不仅可以抵御当前的勒索软件变体、还可以适应新出现的威胁、为您的数据基础架构提供长期的安全性。

了解其他保护选项

- "Active IQ勒索软件防护"
- "Cloud Insights存储工作负载安全性(CWSs)"
- "fpolicy"
- "SnapLock和防篡改Snapshot副本"

勒索软件恢复担保

NetApp保证在发生勒索软件攻击时还原Snapshot数据。我们的保证：如果我们无法帮助您还原快照数据、我们会帮您解决问题。此担保适用于新购买的AFF A系列、AFF C系列、ASA和FAS系统。

了解更多信息。

- "恢复保证服务说明"
- "勒索软件恢复担保博客"(英文)

相关信息

- NetApp支持站点资源页面 http://mysupport.netapp.com/ontap/resources
- NetApp产品安全性 https://security.netapp.com/resources/

SnapLock和防篡改Snapshot副本、用于勒索软件保护

SnapLock是NetApp Snap Arvanson中的一项重要武器、经验证、它在防范勒索软件威胁方面非常有效。通过防止未经授权的数据删除、SnapLock提供了额外的安全保护层、确保即使发生恶意攻击、关键数据也能保持完好并可访问。

SnapLock 合规性

SnapLock Compliance (SLC)可为您的数据提供不可替代的保护。即使管理员尝试重新初始化阵列、SLC也禁止删除数据。与其他竞争产品不同、SnapLock Compliance不容易通过这些产品的支持团队遭受社会工程黑客攻击。受SnapLock Compliance卷保护的数据在达到其到期日期之前是可恢复的。

要启用SnapLock、"ONTAP One"需要许可证。

了解更多信息。

- "SnapLock文档"

防篡改Snapshot副本

防篡改Snapshot (TPS)副本提供了一种便捷快速的方法来保护数据免受恶意行为的影响。与SnapLock Compliance不同、TPS通常在主系统上使用、在主系统中、用户可以在确定的时间内保护数据、并将数据留在本地进行快速恢复、或者无需将数据复制出主系统。TPS使用SnapLock技术来防止主Snapshot副本被使用相同SnapLock保留期限的ONTAP管理员删除。即使卷未启用SnapLock、也会阻止删除Snapshot副本、尽管快照与SnapLock Compliance卷的不可删除性质不同。

要使Snapshot副本不经过篡改、"ONTAP One"需要许可证。

了解更多信息。

- "锁定Snapshot副本、防止勒索软件攻击"(英文)

FPolicy文件阻止

FPolicy可阻止不需要的文件存储在企业级存储设备上。FPolicy还提供了一种阻止已知勒索软件文件扩展名的方法。用户仍对主文件夹拥有完全访问权限、但FPolicy不允许用户存储管理员标记为已阻止的文件。无论这些文件是MP3文件还是已知的勒索软件文件扩展名、都无关紧要。

使用FPolicy本机模式阻止恶意文件

NetApp FPolicy本机模式(名称"文件策略"的演变)是一个文件扩展名阻止框架、可用于阻止不需要的文件扩展名进入环境。它已成为ONTAP的一部分超过十年、在帮助您防范勒索软件方面非常有用。此零信任引擎非常有用、因为您可以获得超出访问控制列表(ACL)权限的额外安全措施。

在ONTAP系统管理器和BlueXP 中、提供了3000多个文件扩展名列表供参考。

某些扩展在您的环境中可能是合法的、阻止它们可能会导致意外问题。在配置本机FPolicy之前、创建适合您环境的列表。

所有ONTAP许可证均包含FPolicy本机模式。

了解更多信息。

- "博客：应对网络软件：第三部分—ONTAP FPolicy、另一个功能强大的本机(也称为免费)工具"

在FPolicy外部模式下启用用户和实体行为分析(UEA)

FPolicy外部模式是一种文件活动通知和控制框架、可提供文件和用户活动的可见性。外部解决方案可以使用这些通知执行基于AI的分析以检测恶意行为。

也可以将FPolicy外部模式配置为等待FPolicy服务器批准、然后再允许执行特定活动。可以在一个集群上配置多个类似这样的策略、从而为您提供极大的灵活性。

如果FPolicy服务器配置为提供批准、则必须对FPolicy请求做出响应；否则、存储系统性能可能会受到负面影响。

FPolicy外部模式包括在中"所有ONTAP许可证"。

了解更多信息。

- "博客：应对异常：第四部分—采用FPolicy外部模式的UBA和ONTAP。"

Cloud Insights存储工作负载安全性(CWSs)

存储工作负载安全性(Storage Workload Security、SWS)是NetApp Cloud Insights的一项功能、可显著增强ONTAP环境的安全防护、可恢复性和可问责性。SWS采用以用户为中心的方法、跟踪环境中每个经过身份验证的用户的所有文件活动。它使用高级分析为每个用户建立正常和季节性访问模式。这些模式用于快速识别可疑行为、而无需勒索软件签名。

当SWS检测到潜在的勒索软件、数据删除或渗漏攻击时、它可以自动执行以下操作：

- 为受影响的卷创建快照。
- 阻止涉嫌恶意活动的用户帐户和IP地址。
- 向管理员发送警报。

由于SWS可以采取自动化操作来快速阻止内部威胁并跟踪每个文件活动、因此可以更轻松、更快速地从勒索软件事件中恢复。借助内置的高级审核和取证工具、用户可以立即查看受攻击影响的卷和文件、攻击来自哪个用户帐户以及执行了哪些恶意操作。自动快照可减少损坏并加快文件还原速度。

[Cloud Insights存储工作负载安全攻击结果]

ONTAP的自动勒索软件保护(Autonomous Ransomware Protection、ARP)发出的警报也会显示在SWS中、从而为同时使用ARP和SWS的客户提供一个界面来防止勒索软件攻击。

了解更多信息。

- "NetApp Cloud Insights"

NetApp ONTAP内置基于AI的内置检测和响应功能

随着勒索软件威胁变得越来越复杂、您的防御机制也会越来越复杂。NetApp的自主勒索软件保护(ARP)由AI提供支持、ONTAP内置智能异常检测功能。启用它可为您的网络故障恢复能力增加另一层防御。

ARP和ARP/AI可通过ONTAP内置管理界面System Manager进行配置、并按卷启用。

自主勒索软件保护(ARP)

自主勒索软件保护(ARP)是自9.10.1以来另一种内置的本机ONTAP解决方案、它关注NAS存储卷工作负载文件活动和数据熵、以自动检测潜在的勒索软件。ARP为管理员提供实时检测、洞察力和数据恢复点、实现前所未有的机载潜在勒索软件检测。

对于支持ONTAP 9的ARP.151及更早版本、ARP将从学习模式开始学习典型的工作负载数据活动。对于大多数环境、此操作可能需要七天时间。学习模式完成后、ARP将自动切换到活动模式、并开始查找可能是勒索软件的异常工作负载活动。

如果检测到异常活动、则会立即自动创建Snapshot副本、这将提供一个尽可能接近攻击时间的恢复点、并且受感染数据最少。同时、系统会生成一个自动警报(可配置)、允许管理员查看异常文件活动、以便确定该活动是否确实是恶意活动并采取适当措施。

如果活动是预期工作负载、管理员可以轻松地将其标记为误报。ARP将此变化视为正常工作负载活动、不再将其标记为未来的潜在攻击。

要启用ARP、"ONTAP One"需要许可证。

了解更多信息。

- "自主勒索软件保护"

自主防兰森保护/AI (ARP/AI)

ARP/AI作为技术预览在ONTAP 9 15.1中推出、将NAS存储系统机载实时检测提升到一个新的水平。由AI提供支持的全新检测技术针对超过100万个文件和各种已知勒索软件攻击进行了训练。除了ARP中使用的信号之外、ARP/AI还会检测报头加密。AI的功率和附加信号使ARP/AI的检测精度超过99%。这已经过SE Labs的验证、SE Labs是一家独立的测试实验室、为ARP/AI提供了最高的AAA评级。

由于训练模型会在云中持续进行、因此ARP/AI不需要学习模式。它在打开时即处于活动状态。持续培训还意味着ARP/AI始终可以在新出现的勒索软件攻击类型中进行验证。ARP/AI还附带自动更新功能、可为所有客户提供新参数、以使勒索软件检测保持最新。ARP的所有其他检测、洞察和数据恢复点功能均为ARP/AI保留。

要启用ARP/AI、"ONTAP One"需要许可证。

了解更多信息。

- "博客：NetApp基于AI的实时勒索软件检测解决方案达到AAA评级"

通过网络数据保护实现无线WORM保护

NetApp的网络存储方法是一种专用参考架构、用于逻辑上隔离的网络存储。这种方法利用SnapLock等安全强化和合规性技术实现了不可变和不可删除的快照。

利用SnapLock Compliance进行网络存储、并形成合理的空隙

攻击者破坏备份副本的趋势越来越明显、在某些情况下甚至会对其进行加密。因此、网络安全行业的许多企业都建议将空隙备份作为整体网络弹性策略的一部分。

问题在于、传统的空隙(磁带和脱机介质)可以显著增加恢复时间、从而增加停机时间和整体相关成本。即使采用更现代化的方法来解决空隙问题也会有问题。例如、如果临时打开备份存储以接收新的备份副本、然后断开并关闭其与主数据的网络连接、以便再次"无线连接"、则攻击者可以利用临时打开的空间。在连接联机期间、攻击者可能会攻击以破坏或销毁数据。此类配置通常还会增加不必要的复杂性。逻辑空隙非常适合替代传统或现代空隙、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、您可以通过逻辑气隙来解决磁带或磁盘气隙的复杂性、而逻辑气隙可以通过不可固定的Snapshot副本和NetApp SnapLock Compliance来实现。

[与NetApp网络存储的逻辑空隙]

NetApp在10多年前发布了SnapLock功能、旨在满足数据合规性要求、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许可证有两个版本：SnapLock Compliance和SnapLock Enterprise。对于勒索软件防护、NetApp建议使用SnapLock Compliance、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支持人员也可以锁定Snapshot副本、并且无法将其删除。

了解更多信息。

- "博客：利用NetApp网络存储解决方案提供分层勒索软件保护"

防篡改Snapshot副本

虽然利用SnapLock Compliance作为逻辑空隙可提供防止攻击者删除备份副本的终极保护、但它确实要求您使用SnapVault将Snapshot副本移动到启用了SnapLock的二级卷。因此、许多客户都会在网络中的二级存储上部署此配置。与在主存储上还原主卷Snapshot副本相比、这可能会导致还原时间更长。

从ONTAP 9．12.1开始，防篡改快照副本可以为主存储和主卷上的快照副本提供接近SnapLock Compliance级别的保护。无需使用SnapVault将Snapshot副本存储到二级SnapLocked卷。防篡改Snapshot副本使用SnapLock技术来防止主Snapshot副本被删除、即使是使用相同SnapLock保留期限的完整ONTAP管理员也是如此。这样可以缩短还原时间、并可通过防篡改的受保护Snapshot副本备份FlexClone卷、而传统的SnapLock Compliance存储Snapshot副本则无法做到这一点。

SnapLock Compliance与防篡改Snapshot副本之间的主要区别在于、如果SnapLock Compliance卷中存储的Snapshot副本尚未达到到期日期、则SnapLock Compliance不允许对ONTAP阵列进行初始化和擦除。要使Snapshot副本不经过篡改、需要SnapLock Compliance许可证。

了解更多信息。

- "锁定Snapshot副本、防止勒索软件攻击"

Active IQ勒索软件防护

NetApp Active IQ是一家数字顾问、可利用可指导行动的智能信息来优化数据管理、从而简化NetApp存储的主动维护和优化。借助我们高度多样化的客户群提供的遥测数据、它可以利用高级AI和ML技术发现降低风险并提高存储环境的性能和效率的机会。

```
https://www.netapp.com/services/support/active-iq/["NetApp Active IQ"^]
https://www.netapp.com/blog/fix-security-vulnerabilities-with-active-
iq/["消除安全漏洞"^]它不仅可以提供帮助，还提供针对勒索软件的防护的见解和指导。一张专用健康卡可显示所需的操作和已解决的风险、因此您可以确保您的系统符合这些最佳实践建议。
```

[NetApp Active IQ信息板上的健康监控器]

在"防兰索防健康"页面上跟踪的风险和操作包括以下(以及更多)：

- 卷Snapshot副本数较低、从而降低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。

要了解Active IQ勒索软件保护的实际操作，请参见"NetApp Active IQ"。

通过BlueXP 勒索软件保护实现全面的故障恢复能力

尽早进行勒索软件检测非常重要、这样您才能防止病毒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不止一层保护。NetApp的勒索软件保护采用全面的方法、包括实时机载功能、可通过BlueXP 扩展到数据服务、以及一个用于网络存储的隔离分层解决方案。

BlueXP勒索软件保护

BlueXP 是一个单一控制平台、可智能地编排以工作负载为中心的全面勒索软件防御。BlueXP 勒索软件保护将ONTAP强大的网络弹性功能(如ARP、FPolicy和防篡改快照)以及BlueXP 数据服务(如BlueXP 备份和恢复)集于一体。此外、它还为自动化工作流添加了建议和指导、以便通过单一UI提供端到端防护。它可以在工作负载级别运行、以确保运行业务的应用程序受到保护、并在发生攻击时尽快恢复。

[BlueXP 防间谍软件是一种基于AI的智能和协助、可最大限度地减少工作负载数据丢失并快速恢复。此图显示了BlueXP UI。]

客户获益：

- 辅助防勒索软件可降低运营开销并提高效率
- 采用AI/ML技术的异常检测可提供更高的准确性和更快的响应来控制风险
- 借助应用程序一致的引导式还原、您可以在几分钟内更轻松地恢复工作负载

"BlueXP勒索软件保护"使这些NIST功能更易于实现：

- 自动*发现* NetApp存储中的数据并确定数据优先级*，重点关注基于应用程序的顶级工作负载*。

- *一键保护*顶级工作负载数据备份、不可变、安全配置、恶意文件阻止和不同的安全域。
- 使用*基于**AI**的下一代异常检测、尽可能*快速*准确检测*勒索软件
- 自动响应和工作流、并与顶级*暹粒和XDR解决方案集成。*
- 通过简化的*协调恢复*快速恢复数据，加快应用程序正常运行时间。
- 实施勒索软件保护*策略*和*策略*，并*监控结果*。