NetApp 랜섬웨어 방어 에 관해 알아보십시오

ONTAP 9

NetApp
August 31, 2024

목차

NetApp 랜섬웨어 방어 에 관해 알아보십시오

랜섬웨어 및 NetApp의 보호 포트폴리오

랜섬웨어는 2024년에 조직 중단을 초래하는 가장 중요한 위협 중 하나로 남아 있습니다. 에 따르면 "Sophos, 2024년 랜섬웨어 상태" 랜섬웨어 공격은 설문조사에 참여한 고객의 72%에 영향을 미친 것으로 나타났습니다. 랜섬웨어 공격은 그 영향과 수익을 극대화하기 위해 인공 지능과 같은 고급 기술을 사용하는 위협 공격자로 인해 더 정교하고 타겟이 되도록 진화하고 있습니다.

조직은 경계, 네트워크, ID, 애플리케이션, 데이터가 스토리지 수준에서 어디에 있는지, 그리고 이러한 계층을 안전하게 보호해야 합니다. 스토리지 계층에서 사이버 보호에 대한 데이터 중심의 접근 방식을 채택하는 것은 오늘날의 위협 환경에서 매우 중요합니다. 단일 솔루션으로 모든 공격을 차단할 수는 없지만, 파트너 관계 및 타사를 포함한 솔루션 포트폴리오를 사용하면 계층화된 방어 체계를 구축할 수 있습니다.

는 NetApp 제품 포트폴리오에 대해 자세히 살펴봅니다가시성, 감지, 해결을 위한 다양한 효과적인 툴을 제공하므로 랜섬웨어를 조기에 탐지하고 확산을 방지하고 필요한 경우 신속하게 복구하여 비용이 많이 드는 다운타임을 방지할 수 있습니다. 기존의 계층화된 방어 솔루션은 가시성과 감지를 위한 타사 및 파트너 솔루션처럼 널리 사용되고 있습니다. 효과적인 치료는 위협에 대한 대응의 중요한 부분입니다. 변경 불가능한 NetApp 스냅샷 기술 및 SnapLock 논리적 AIR GAP 솔루션을 활용하는 고유한 업계 접근법은 업계 차별화 요소이자 랜섬웨어 수정 기능에 대한 업계 모범 사례입니다.

2024년 7월부터 이전에 PDF로 게시되었던 NetApp 랜섬웨어 방지 기술 보고서_TR-4572: NetApp 랜섬웨어 방지 _ 의 내용이 다른 ONTAP 제품 설명서와 통합되었습니다.

데이터는 1차 타겟입니다

데이터를 직접 타겟으로 삼는 사이버 범죄자들이 점차 그 가치를 인식하게 되고 있습니다. 경계, 네트워크 및 애플리케이션 보안은 중요하지만 우회할 수 있습니다. 소스에서 데이터를 보호하는 데 중점을 둔 스토리지 계층은 중요한 최종 방어선을 제공합니다. 랜섬웨어 공격의 목표는 운영 데이터에 액세스하여 암호화하거나 액세스할 수 없도록 렌더링하는 것입니다. 이를 위해서는 공격자들이 경계에서 애플리케이션 보안에 이르기까지 오늘날 조직이 배포한 기존의 방어 체계를 이미 뚫어야만 합니다.

[경계에서 데이터 보안까지 레이어를 만듭니다]

안타깝게도 많은 기업들은 데이터 레이어에서 보안 기능을 활용하지 못하고 있습니다. 이것이 바로 NetApp 랜섬웨어 차단 포트폴리오가 제공하는 이유입니다.

랜섬웨어의 실제 비용

몸값 지급 자체는 기업에 미치는 가장 큰 금전적 효과가 아닙니다. 지불액은 중요하지 않지만 랜섬웨어 사고로 인해 발생하는 다운타임 비용과 비교해 볼 수 있습니다.

몸값 지불은 랜섬웨어 이벤트를 처리할 때 복구 비용의 한 요소에 불과합니다. 지불된 모든 랜스를 제외하고, 2024개 조직은 랜섬웨어 공격으로부터 복구하는 평균 비용이 27만 3천 달러로, 2023년 보고된 1.820만 달러에서 거의 100만 달러 "2024 Sophos 랜섬웨어 상태" 증가했습니다. 전자 상거래, 주식 거래, 의료 등 IT 가용성에 크게 의존하는 조직의 경우 비용이 10배 이상 높을 수 있습니다.

보험 비용은 보험 회사를 대상으로 랜섬웨어 공격이 발생할 가능성이 매우 높기 때문에 지속적으로 증가하고 있습니다.

데이터 계층에서 랜섬웨어 방어

NetApp은 스토리지 계층에서 데이터가 상주하는 위치까지 조직 전체에서 광범위하고 심층적인 보안 태세를 이해합니다. 보안 스택은 복잡하며 기술 스택의 모든 수준에서 보안을 제공해야 합니다.

데이터 레이어에서 실시간 보호가 훨씬 더 중요하고 고유한 요구 사항이 있습니다. 효율성을 높이려면 이 계층의 솔루션이 다음과 같은 중요한 속성을 제공해야 합니다.

- * 보안 설계 * 를 통해 공격 성공 가능성을 최소화합니다
- * 실시간 감지 및 응답 * 을 통해 공격이 성공할 경우 미치는 영향을 최소화합니다
- * Air-gapped WORM 보호 * 로 중요한 데이터 백업을 격리합니다
- * 포괄적인 랜섬웨어 방어를 위한 단일 제어 플레인 *

NetApp은 이러한 모든 것을 제공할 수 있습니다.

[주요 특성이 설명된 NetApp 랜섬웨어 차단 포트폴리오]

NetApp의 랜섬웨어 방어 포트폴리오

NetApp는 "랜섬웨어 방지 기능 내장"중요한 데이터를 실시간으로 강력한 다면적인 방어 기능을 제공합니다. 고급 AI 기반 감지 알고리즘은 데이터 패턴을 지속적으로 모니터링하여 99% 정확성으로 잠재적 랜섬웨어 위협을 신속하게 식별합니다. 공격에 신속하게 대응함으로써 신속하게 데이터를 스냅샷하고 복사본을 보호하여 신속한 복구를 보장합니다.

데이터를 더욱 강화하기 위해 NetApp의 "사이버 보관" 기능은 논리적 공극으로 데이터를 격리합니다. 중요한 데이터를 보호함으로써 신속한 비즈니스 연속성을 보장합니다.

NetApp는 "BlueXP 랜섬웨어 보호"단일 제어 플레인을 통해 운영 부담을 경감하여 엔드 투 엔드 워크로드 중심의 랜섬웨어 방어를 지능적으로 조정 및 실행하므로 클릭 한 번으로 중요 워크로드 데이터를 식별하고 보호하면서 잠재적 공격의 영향을 줄이고 며칠이 아닌 몇 분 내에 워크로드를 복구할 수 있으므로 중요한 워크로드 데이터를 보호하고 비용이 많이 드는 운영 중단을 최소화할 수 있습니다.

데이터에 대한 무단 액세스를 보호하기 위한 기본 내장 ONTAP 솔루션에는 "다중 관리자 인증(MAV)"볼륨 삭제, 추가 관리 사용자 생성 또는 스냅샷 복사본 삭제와 같은 작업을 적어도 두 번째 지정된 관리자로부터 승인을 받은 후에만 수행할 수 있는 강력한 기능이 포함되어 있습니다. 따라서 손상되거나 악의적이거나 경험이 부족한 관리자가 원치 않는 변경 또는 데이터 삭제를 방지할 수 있습니다. 지정된 관리자 승인자를 원하는 수만큼 구성하여 스냅샷 복사본을 삭제할 수 있습니다.

NetApp ONTAP는 "다중 요소 인증(MFA)" System Manager와 SSH CLI 인증의 웹 기반 요구사항을 해결합니다.

NetApp의 랜섬웨어 방지 기능은 끊임없이 변화하는 위협 환경에서 안심할 수 있도록 제공합니다. 이 포괄적인 접근 방식은 현재의 랜섬웨어 변종을 방어할 뿐만 아니라 새로운 위협에 대응하여 데이터 인프라에 장기적인 보안을 제공합니다.

다른 보호 옵션에 대해 알아봅니다

- "Active IQ 랜섬웨어 방어"
- "Cloud Insights 스토리지 워크로드 보안(CISWS)"
- "FPolicy를 참조하십시오"

- "SnapLock 및 변조 방지 스냅샷 복사본"

랜섬웨어 복구 보장

NetApp은 랜섬웨어 공격이 발생할 경우 스냅샷 데이터의 복원을 보장합니다. 보장: 스냅샷 데이터 복원을 지원할 수 없는 경우 NetApp이 바로잡을 것입니다. 이 보장은 AFF A-Series, AFF C-Series, ASA 및 FAS 시스템을 새로 구매할 때 사용할 수 있습니다.

자세한 정보

- "복구 보장 서비스 설명"
- "랜섬웨어 복구 보장 블로그"..

관련 정보

- NetApp 지원 사이트 리소스 페이지 http://mysupport.netapp.com/ontap/resources
- NetApp 제품 보안 https://security.netapp.com/resources/

랜섬웨어 방어를 위한 **SnapLock** 및 변조 방지 스냅샷 사본

NetApp의 Snap Arsenal에서 중요한 무기는 랜섬웨어 위협을 방어하는 데 매우 효과적인 것으로 입증된 SnapLock입니다. SnapLock는 무단 데이터 삭제를 방지함으로써 추가적인 보안 계층을 제공하여 악의적인 공격이 발생했을 때도 중요 데이터를 그대로 유지하고 액세스할 수 있도록 합니다.

SnapLock 규정 준수

SLC(SnapLock Compliance)는 데이터를 지워지지 않는 보호 기능을 제공합니다. SLC는 관리자가 스토리지를 다시 초기화하려고 시도해도 데이터가 삭제되는 것을 금지합니다. 다른 경쟁 제품과 달리 SnapLock Compliance는 해당 제품의 지원 팀을 통해 사회 공학 해킹에 취약하지 않습니다. SnapLock Compliance 볼륨으로 보호되는 데이터는 만료 날짜에 도달할 때까지 복구할 수 있습니다.

SnapLock를 활성화하려면 "ONTAP 1 을 참조하십시오"라이센스가 필요합니다.

자세한 정보

- "SnapLock 설명서"

스냅샷 복사본을 무단 복제했습니다

변조 방지 스냅샷(TPS) 복사본은 악의적인 공격으로부터 데이터를 보호하는 편리하고 빠른 방법을 제공합니다. SnapLock Compliance와 달리 TPS는 일반적으로 사용자가 정해진 시간 동안 데이터를 보호하고 빠른 복구를 위해 로컬에 남겨둘 수 있거나 운영 시스템에서 데이터를 복제할 필요가 없는 운영 시스템에서 사용됩니다. TPS는 SnapLock 기술을 사용하여 동일한 SnapLock 보존 만료 기간을 사용하는 ONTAP 관리자가 운영 스냅샷 복제본을 삭제하지 못하도록 방지합니다. 스냅샷과 SnapLock Compliance 볼륨의 삭제 불가능한 특성이 같지는 않지만, 볼륨이 SnapLock를 사용하도록 설정되어 있지 않더라도 스냅샷 복사본 삭제는 금지됩니다.

스냅샷 복사본을 무단 변경으로부터 보호하려면 "ONTAP 1 을 참조하십시오"라이센스가 필요합니다.

자세한 정보

- "랜섬웨어 공격으로부터 보호하기 위해 스냅샷 복사본을 잠급니다"..

FPolicy 파일 차단

FPolicy는 원치 않는 파일이 엔터프라이즈급 스토리지 어플라이언스에 저장되지 않도록 차단합니다. 또한 FPolicy는 알려진 랜섬웨어 파일 확장자를 차단하는 방법을 제공합니다. 사용자는 여전히 홈 폴더에 대한 모든 액세스 권한을 가지고 있지만 FPolicy는 관리자가 차단으로 표시한 파일을 사용자가 저장할 수 없도록 합니다. 해당 파일이 MP3 파일 또는 알려진 랜섬웨어 파일 확장자인지 여부는 중요하지 않습니다.

FPolicy 기본 모드로 악성 파일 차단

NetApp FPolicy 기본 모드(파일 정책 이라는 이름의 진화)는 파일 확장 차단 프레임워크로, 원치 않는 파일 확장명이 사용자 환경에 유입되는 것을 차단할 수 있습니다. 10년 이상 ONTAP의 일부였으며 랜섬웨어로부터 보호하는 데 매우 유용합니다. 이 제로 트러스트 엔진은 액세스 제어 목록(ACL) 권한을 넘어서는 추가 보안 조치를 취하기 때문에 유용합니다.

ONTAP 시스템 관리자 및 BlueXP 에서는 3000개 이상의 파일 확장자 목록을 참조할 수 있습니다.

일부 확장은 사용자의 환경에서 합법적일 수 있으며 이러한 확장을 차단하면 예기치 않은 문제가 발생할 수 있습니다. 기본 FPolicy를 구성하기 전에 환경에 적합한 목록을 생성하십시오.

FPolicy 기본 모드는 모든 ONTAP 라이센스에 포함되어 있습니다.

자세한 정보

- "블로그: 랜섬웨어에 대항하기: 3부 - 강력한 기본(무료) 툴인 ONTAP FPolicy"

FPolicy 외부 모드로 사용자 및 엔터티 행동 분석(UEBA)을 설정합니다

FPolicy 외부 모드는 파일 활동 알림 및 제어 프레임워크로, 파일 및 사용자 활동에 대한 가시성을 제공합니다. 이러한 알림은 외부 솔루션에서 AI 기반 분석을 수행하여 악의적인 행동을 감지하는 데 사용할 수 있습니다.

특정 작업이 수행되도록 허용하기 전에 FPolicy 서버의 승인을 기다리도록 FPolicy 외부 모드도 구성할 수 있습니다. 이와 같은 여러 정책을 클러스터에서 구성할 수 있으므로 유연성이 크게 향상됩니다.

FPolicy 서버는 승인을 제공하도록 구성된 경우 FPolicy 요청에 응답해야 합니다. 그렇지 않으면 스토리지 시스템 성능이 저하될 수 있습니다.

FPolicy 외부 모드가 에 포함되어 "모든 ONTAP 라이센스"있습니다.

자세한 정보

- "블로그: 랜섬웨어에 대항하기: 4부 - FPolicy 외부 모드를 사용하는 UBA 및 ONTAP"

Cloud Insights 스토리지 워크로드 보안(CISWS)

SWS(스토리지 워크로드 보안)는 NetApp Cloud Insights ONTAP 환경의 보안 태세, 복구 기능 및 책임 능력을 대폭 향상하는 기능입니다. SWS는 사용자 중심 접근 방식을 통해 환경에 있는 인증된 모든 사용자의 모든 파일 활동을 추적합니다. 고급 분석을 사용하여 모든 사용자에 대한 일반 및 기간별 액세스 패턴을 설정합니다. 이러한 패턴은 랜섬웨어 서명 없이 의심스러운 행동을

신속하게 식별하는 데 사용됩니다.

SWS가 잠재적 랜섬웨어, 데이터 삭제 또는 유출 공격을 감지하면 다음과 같은 자동 조치를 취할 수 있습니다.

- 영향을 받는 볼륨의 스냅샷을 생성합니다.
- 악의적인 활동으로 의심되는 사용자 계정 및 IP 주소를 차단합니다.
- 관리자에게 알림을 보냅니다.

내부자 위협을 빠르게 차단하고 모든 파일 활동을 추적하기 위해 자동화된 조치를 취할 수 있기 때문에 SWS를 사용하면 랜섬웨어 이벤트에서 훨씬 더 쉽고 빠르게 복구할 수 있습니다. 사용자는 고급 감사 및 포렌식 도구가 내장되어 있어 공격의 영향을 받은 볼륨 및 파일, 공격이 발생한 사용자 계정 및 수행된 악의적인 작업을 즉시 확인할 수 있습니다. 자동 스냅샷은 손상을 완화하고 파일 복원을 가속화합니다.

[Cloud Insights 스토리지 워크로드 보안 공격 결과]

ONTAP의 ARP(자율적 랜섬웨어 방어)의 경고도 SWS에서 볼 수 있으므로 ARP와 SWS를 모두 사용하여 랜섬웨어 공격으로부터 보호할 수 있는 단일 인터페이스를 제공합니다.

자세한 정보

- "NetApp Cloud Insights를 참조하십시오"

NetApp ONTAP 내장형 AI 기반 감지 및 응답 기능

랜섬웨어 위협이 점점 더 정교해짐에 따라 방어 메커니즘도 갖춰져야 합니다. NetApp의 ARP(자율 랜섬웨어 방어)는 ONTAP에 내장된 지능형 이상 징후 감지 기능을 갖춘 AI를 기반으로 합니다. 이를 통해 사이버 레질리언스에 또 다른 방어 계층을 추가합니다.

ARP 및 ARP/AI는 ONTAP 내장 관리 인터페이스인 System Manager를 통해 구성할 수 있으며 볼륨별로 활성화됩니다.

자율 랜섬웨어 보호(ARP)

9.10.1 이후 내장된 또 다른 네이티브 ONTAP 솔루션인 ARP(자율 랜섬웨어 방어)는 NAS 스토리지 볼륨 워크로드 파일 활동 및 데이터 엔트로피를 연구하여 잠재적 랜섬웨어를 자동으로 감지합니다. ARP는 관리자에게 전례 없는 온박스(on-box) 잠재적인 랜섬웨어 감지를 위한 실시간 감지, 인사이트 및 데이터 복구 지점을 제공합니다.

ARP를 지원하는 ONTAP 9.15.1 및 이전 버전의 경우 ARP는 일반적인 작업 부하 데이터 활동을 학습하기 위해 학습 모드에서 시작됩니다. 대부분의 환경에서 이 작업에는 7일이 걸릴 수 있습니다. 학습 모드가 완료되면 ARP가 자동으로 활성 모드로 전환되어 랜섬웨어가 될 수 있는 비정상적인 워크로드 활동을 찾기 시작합니다.

비정상적인 활동이 감지되면 스냅샷 자동 복사본이 즉시 생성되므로 감염된 데이터를 최소화하면서 공격 시간에 최대한 가까운 복원 지점을 제공합니다. 이와 동시에 관리자가 비정상적인 파일 활동을 확인할 수 있도록 자동 경고(구성 가능)가 생성되므로 해당 활동이 실제로 악의적인지 확인하고 적절한 조치를 취할 수 있습니다.

작업이 예상 작업량인 경우 관리자는 이를 가양성 작업으로 쉽게 표시할 수 있습니다. ARP는 이 변경 사항을 정상적인 워크로드 활동으로 인식하여 앞으로 발생할 수 있는 공격 대상으로 더 이상 플래그를 지정하지 않습니다.

ARP를 활성화하려면 "ONTAP 1 을 참조하십시오"라이센스가 필요합니다.

자세한 정보

- "자율 랜섬웨어 보호"

자율 랜섬웨어 방어/AI(ARP/AI)

ONTAP 9.15.1에서 기술 미리보기로 소개된 ARP/AI는 NAS 스토리지 시스템을 온박스 실시간 감지를 한 차원 높여줍니다. 새로운 AI 기반 감지 기술은 100만 개 이상의 파일과 알려진 다양한 랜섬웨어 공격에 대해 훈련됩니다. ARP에서 사용되는 신호 외에 ARP/AI는 헤더 암호화도 감지합니다. AI 출력 및 추가 신호를 통해 ARP/AI는 99% 이상의 검출 정확도를 제공할 수 있습니다. 이는 ARP/AI가 AAA 등급에서 가장 높은 등급을 받은 독립 테스트 연구소인 SE Labs에 의해 검증되었습니다.

모델을 지속적으로 클라우드에서 훈련하기 때문에 ARP/AI는 학습 모드가 필요하지 않습니다. 이 기능은 켜지는 순간 활성화됩니다. 또한 지속적인 훈련은 새로운 랜섬웨어 공격이 발생했을 때 ARP/AI가 항상 검증된다는 것을 의미합니다. ARP/AI에는 모든 고객에게 새로운 매개 변수를 제공하여 랜섬웨어 탐지를 최신 상태로 유지하는 자동 업데이트 기능도 제공됩니다. ARP의 다른 모든 탐지, 인사이트 및 데이터 복구 지점 기능은 ARP/AI에 대해 유지됩니다.

ARP/AI를 활성화하려면 "ONTAP 1 을 참조하십시오"라이센스가 필요합니다.

자세한 정보

- "블로그:NetApp의 AI 기반 실시간 랜섬웨어 감지 솔루션은 AAA 등급을 획득했습니다"

사이버 보관을 통한 폭발적 WORM 보호

NetApp의 사이버 소산 접근 방식은 논리적으로 에어갭 사이버 틈새를 위해 특별 제작된 참조 아키텍처입니다. 이 접근 방식은 보안 강화 및 SnapLock 같은 규정 준수 기술을 활용하여 변경 불가능하며 지워지지 않는 스냅샷을 허용합니다.

SnapLock Compliance과 논리적 격차가 있는 사이버 소산

공격자가 백업 사본을 폐기하고 경우에 따라 암호화하는 경향이 증가하고 있습니다. 따라서 사이버 보안 업계의 많은 기업들이 전반적인 사이버 복원력 전략의 일환으로 에어 갭 백업을 사용하도록 권장합니다.

문제는 기존 공기 격차(테이프 및 오프라인 미디어)가 복원 시간을 크게 증가시켜 가동 중지 시간과 전반적인 관련 비용을 증가시킬 수 있다는 것입니다. 에어 갭 솔루션에 대한 보다 현대적인 접근 방식도 문제가 될 수 있습니다. 예를 들어, 새 백업 복사본을 받기 위해 백업 볼트가 일시적으로 열렸다가 기본 데이터에 대한 네트워크 연결을 끊고 다시 한 번 "공기 차단"하는 경우 공격자는 임시 열기의 이점을 활용할 수 있습니다. 연결이 온라인 상태일 때 공격자는 데이터를 손상시키거나 파괴할 수 있습니다. 이러한 유형의 구성은 일반적으로 원치 않는 복잡성을 가중시킵니다. 논리적 공기 격차는 백업을 온라인 상태로 유지하면서 동일한 보안 보호 원칙을 가지고 있기 때문에 전통적인 또는 현대적인 공기 격차의 훌륭한 대안이 됩니다. NetApp를 사용하면 변경 불가능한 스냅샷 복사본과 NetApp SnapLock Compliance를 통해 논리적 공기 가핑을 사용하여 테이프나 디스크 기핑의 복잡성을 해결할 수 있습니다.

[NetApp 사이버 저장소와의 논리적 항공 격차]

NetApp은 10년 이상 SnapLock 기능을 발표하여 HIPAA(Health Insurance Portability and Accountability Act), 사베인즈 옥슬리(Sarbanes-Oxley) 및 기타 규정 데이터 규정 준수 요구 사항을 해결했습니다. 또한 기본 스냅샷 복사본을 SnapLock 볼륨에 저장하여 복사본을 WORM으로 커밋할 수 있으므로 삭제를 방지할 수 있습니다. SnapLock 라이센스 버전은 SnapLock Compliance 및 SnapLock Enterprise의 두 가지입니다. 랜섬웨어 보호를 위해 NetApp은 ONTAP 관리자 또는 NetApp 지원팀에서도 스냅샷 복사본이 잠겨 있고 삭제할 수 없는 특정 보존 기간을 설정할 수 있으므로 SnapLock Compliance을 권장합니다.

자세한 정보

- "블로그: NetApp의 Cyber Vault 솔루션을 이용한 계층화된 랜섬웨어 방어"

변조 방지 스냅샷 복사본

SnapLock Compliance를 논리적 AIR Gap으로 활용하면 공격자가 백업 복사본을 삭제하지 못하도록 궁극의 보호 기능을 제공할 수 있지만, SnapVault을 사용하여 스냅샷 복사본을 2차 SnapLock 지원 볼륨으로 이동해야 합니다. 결과적으로 많은 고객이 네트워크를 통한 보조 스토리지에 이 구성을 구현합니다. 따라서 기본 스토리지에서 기본 볼륨 스냅샷 복사본을 복원하는 것보다 복원 시간이 더 길 수 있습니다.

ONTAP 9.12.1부터 무단 변경 방지 스냅샷 복사본은 기본 스토리지 및 기본 볼륨의 스냅샷 복사본에 대해 SnapLock Compliance 수준에 가까운 보호 기능을 제공합니다. SnapVault를 사용하여 스냅샷 복사본을 보조 SnapLocked 볼륨에 저장할 필요가 없습니다. 변조 방지 스냅샷 복사본은 SnapLock 기술을 사용하여 동일한 SnapLock 보존 만료 기간을 사용하는 전체 ONTAP 관리자가 기본 스냅샷 복사본을 삭제하지 못하도록 방지합니다. 따라서 복원 시간이 빨라지고 무단 변경 방지 및 보호된 스냅샷 복사본으로 FlexClone 볼륨을 백업할 수 있습니다. 기존의 SnapLock Compliance 저장 스냅샷 복사본으로는 할 수 없는 작업입니다.

SnapLock Compliance와 변조 방지 스냅샷 복사본의 중요한 차이점은 만료 날짜에 도달하지 않은 SnapLock Compliance 볼륨에 저장된 Snapshot 복사본이 있다면 SnapLock Compliance에서는 ONTAP 어레이를 초기화하고 초기화할 수 없다는 점입니다. 스냅샷 복사본을 위조 방지가 되도록 하려면 SnapLock Compliance 라이센스가 필요합니다.

자세한 정보

- "랜섬웨어 공격으로부터 보호하기 위해 스냅샷 복사본을 잠급니다"

Active IQ 랜섬웨어 방어

NetApp Active IQ는 최적의 데이터 관리를 위해 실행 가능한 인텔리전스를 통해 NetApp 스토리지의 선제적 관리 및 최적화를 간소하게 진행하는 디지털 자문업체입니다. NetApp의 매우 다양한 설치 기반에서 얻은 원격 분석 데이터와 고급 AI 및 ML 기술을 사용하여 스토리지 환경의 위험을 줄이고 성능 및 효율성을 개선할 기회를 찾아줍니다.

이 "NetApp Active IQ를 참조하십시오" 방법은 도움이 될 뿐만 "보안 취약점을 제거합니다" 아니라 랜섬웨어로부터 보호하는 것과 관련된 통찰력과 지침도 제공합니다. 전용 웰니스 카드는 필요한 조치와 해결된 위험을 보여줍니다. 따라서 시스템이 이러한 모범 사례 권장 사항을 충족하는지 확인할 수 있습니다.

[NetApp Active IQ 대시보드의 웰니스 모니터]

랜섬웨어 방어 웰빙 페이지에서 추적된 위험 및 작업은 다음과 같습니다.

- 볼륨 스냅샷 복사본 수가 적기 때문에 잠재적인 랜섬웨어 방어가 줄어듭니다.
- NAS 프로토콜용으로 구성된 모든 SVM(스토리지 가상 머신)에 FPolicy가 사용되지 않는다.

Active IQ 랜섬웨어 방어의 실제 작동 모습을 보려면 를 참조하십시오."NetApp Active IQ를 참조하십시오"

BlueXP 랜섬웨어 보호를 통한 포괄적인 복원력

확산을 방지하고 비용이 많이 드는 다운타임을 방지하려면 랜섬웨어 탐지를 가능한 한 빨리 수행하는 것이 중요합니다. 하지만 효과적인 랜섬웨어 감지 전략에는 단일 계층 이상의 보호를 포함해야 합니다. NetApp의 랜섬웨어 방어는 BlueXP 과 사이버 보관을 위한 격리된 계층적

솔루션을 사용하여 데이터 서비스로 확장되는 실시간 온박스 기능을 포함하는 종합적인 접근 방식을 취합니다.

BlueXP 랜섬웨어 보호

BlueXP 는 워크로드 중심의 포괄적인 랜섬웨어 방어를 지능적으로 오케스트레이션하는 단일 제어 플레인입니다. BlueXP 랜섬웨어 방어 기능은 ARP, FPolicy, 무단 변경 방지 스냅샷 등 ONTAP의 강력한 사이버 레질리언스 기능과 BlueXP 백업 및 복구와 같은 BlueXP 데이터 서비스를 통합합니다. 또한 자동화된 워크플로에 권장 사항과 지침을 추가하여 단일 UI를 통해 완벽한 방어 기능을 제공합니다. 워크로드 수준에서 작동하므로 비즈니스를 실행하는 애플리케이션을 보호하고 공격 발생 시 가능한 한 신속하게 복구할 수 있습니다.

[BlueXP 랜섬웨어 방어는 워크로드 데이터 손실을 최소화하고 신속하게 정상화하는 데 필요한 AI 기반의 인텔리전스 및 서비스입니다. 이 이미지는 BlueXP UI를 보여 줍니다.]

고객 이점:

- 랜섬웨어 대비 지원을 통해 운영 오버헤드를 줄이고 효율성을 높일 수 있습니다
- AI/ML을 통한 이상 징후 탐지는 정확성을 높이고 위험을 억제하기 위한 더 빠른 응답을 제공합니다
- 안내된 애플리케이션 정합성이 보장된 복원을 통해 몇 분 내에 워크로드를 더 쉽게 복구할 수 있습니다

"BlueXP 랜섬웨어 보호" 다음과 같은 NIST 함수를 보다 쉽게 구현할 수 있습니다.

- NetApp 스토리지의 데이터를 자동으로 검색 * 하고 우선 순위를 정할 수 있습니다 *.
- * 상위 워크로드 데이터 백업, 변경 불가, 보안 구성, 악성 파일 차단 및 다양한 보안 도메인에 대한 원 클릭 보호 *.
- * 차세대 AI 기반 이상 징후 감지 * 를 사용하여 * 랜섬웨어를 최대한 빠르게 * 감지합니다 *
- 응답 및 워크플로우 자동화, 최고의 * SIEM 및 XDR 솔루션 * 과의 통합
- 간소화된 * 오케스트레이션 * 을 통해 데이터를 빠르게 복원하여 애플리케이션 가동 시간을 단축합니다.
- 랜섬웨어 보호 * 전략 * 및 * 정책 * 을 구현하고 * 결과를 모니터링 * 하십시오.

저작권 정보

상표 정보