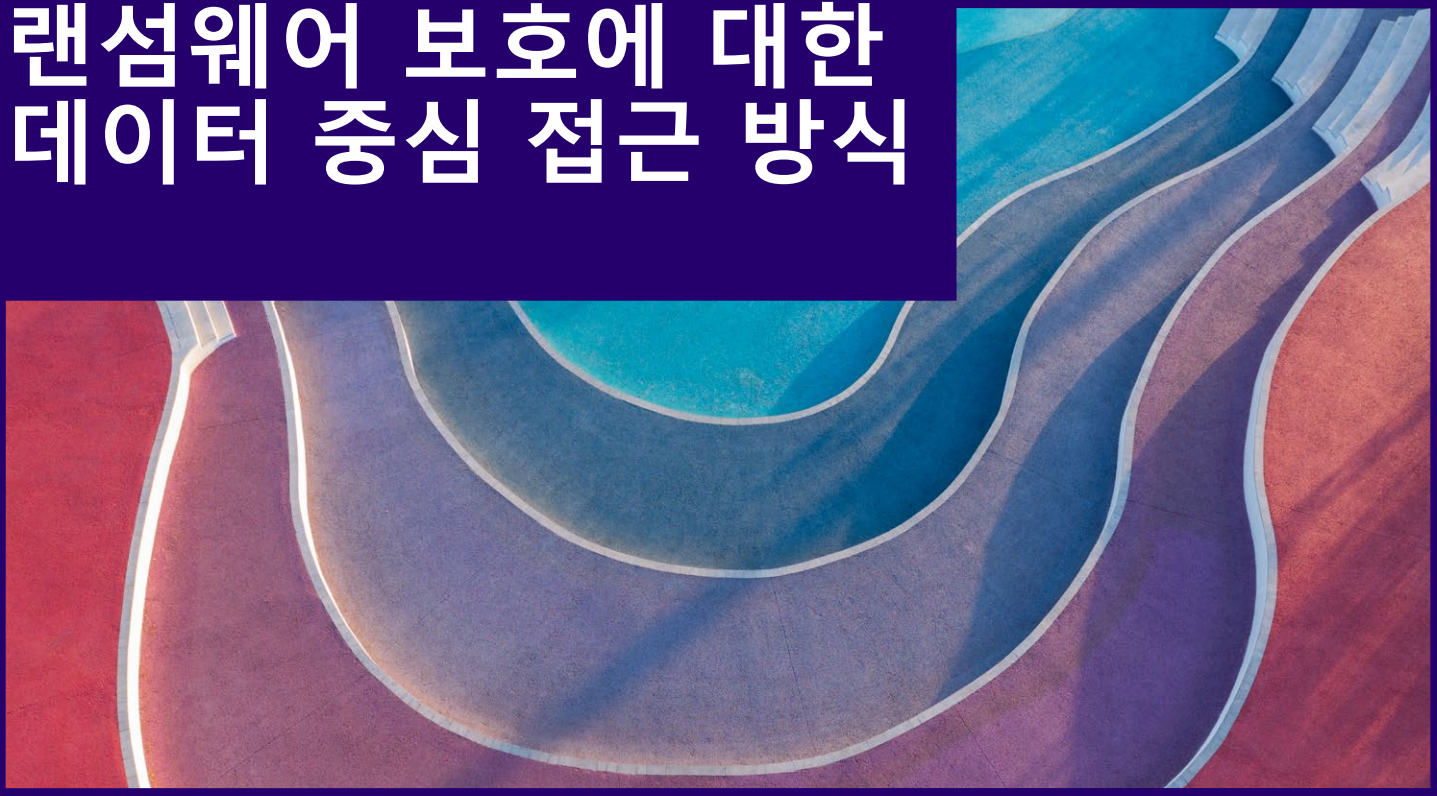
솔루션 개요

NetApp

보호. 감지. 복구.
랜섬웨어 보호에 대한 데이터 중심 접근 방식



보호: 환경을 보호합니다.
탐지: 위협을 예측합니다.
복구: 신속하게 복구합니다.

당면 과제
랜섬웨어 공격은 모든 규모의 조직에 점점 더 퍼지고 정교한 위협입니다. 이러한 악의적 공격은 귀중한 데이터를 암호화하고 출시에 대한 비용을 요구하며, 이로 인해 상당한 재정적 손실과 운영 중단이 발생할 수 있습니다.

- 사이버 사고는 전 세계적으로 가장 큰 비즈니스 리스크입니다.
- 2031년이면 랜섬웨어는 2초마다 공격할 것으로 예상됩니다.
- 59%의 조직이 지난해 랜섬웨어의 영향을 받았습니다.
- 랜섬웨어 공격은 2022년에서 2023년까지 73% 증가했습니다.

많은 기업이 네트워크 및 엔드포인트 보안에 집중하지만, 데이터가 저장되는 스토리지 계층 보안의 중요성을 간과해서는 안 됩니다. 암호화, 액세스 제어 및 변경 불가능한 백업과 같은 스토리지 레벨에서 강력한 보안 조치를 구현하여 랜섬웨어에 대한 추가적인 방어선을 만들 수 있습니다.

이 접근 방식은 소스에서 데이터를 보호하므로 공격자가 중요한 정보를 암호화하거나 손상시키기가 더욱 어렵습니다. 보안 스토리지 솔루션은 공격이 성공할 경우 복구 시간을 단축하고 데이터 손실을 최소화할 수 있으므로 스토리지 인프라 강화를 포함한 포괄적인 보안 전략이 중요합니다.

NetApp 사이버 복원력: 랜섬웨어 방어에 대한 데이터 중심 접근 방식

사이버 사고에 대한 보호는 다계층 방어 체계를 포괄하여 광범위한 위협으로부터 보호합니다. 강력한 사이버 방어는 **ID 보안** 계층에서 시작되며 가장 바깥쪽 레이어인 **경계 보안은** 1차 방어선 역할을 합니다.

네트워크 보안은 이러한 기반을 바탕으로 구축되며 전송 중인 데이터를 보호하고 내부 네트워크 내에서 비정상적인 활동을 감지합니다. **엔드포인트** 보안은 네트워크에 연결된 개별 장치에 대한 방어 계층을 추가합니다. **애플리케이션 보안은** 소프트웨어 응용 프로그램을 취약성과 공격으로부터 보호하는 데 중점을 둡니다.

마지막으로 보안 상태의 핵심은 **데이터 보안입**니다. 데이터 보안은 조직의 가장 중요한 자산인 데이터와 가장 미션 크리티컬한 자산을 보호하는 것입니다. 이 계층에는 일반적으로 강력한 백업 및 복구 솔루션을 통한 데이터 보호가 포함됩니다.

이러한 상호 연결된 보안 계층을 통해 기업의 디지털 자산을 경계에서 데이터 센터까지 보호하여 IT 인프라의 모든 수준에서 위협을 해결할 수 있도록 설계된 포괄적인 방어 전략을 수립할 수 있습니다.

미션 크리티컬 자산에 대한 데이터 계층 보호는 훨씬 더 중요하고 고유한 요구 사항이 있습니다. 이 계층의 솔루션은 다음과 같은 4가지 주요 특성을 갖춰야 효율성을 높일 수 있습니다.

- 보안을 고려한 설계로 조직에 대한 공격이 성공할 가능성을 최소화합니다
- 실시간 감지 및 대응으로 공격에 따른 영향을 최소화합니다
- 에어 갭 WORM(Write Once, Read Many) 보호를 활용하여 중요한 데이터 백업을 격리합니다
- 포괄적인 랜섬웨어 보호와 빠른 복구를 위한 단순한 컨트롤 플레인을 제공합니다.

NetApp는 데이터 계층에서 감지, 보호 및 복구할 수 있습니다.

보안을 고려한 설계: 스토리지 내 ONTAP 내장 랜섬웨어 방지 기능

NetApp ONTAP 소프트웨어는 안전한 설계 접근 방식을 통해 강력한 랜섬웨어 보호를 제공합니다. 핵심 기능으로는 변경 및 삭제가 불가능한 스냅샷 복사본을 포함하므로 관라자도 데이터를 변경 또는 삭제할 수 없고 안정적으로 장애 지점을 만들어 복구할 수 있습니다. ONTAP FPolicy 기능은 악성 파일을 차단하여 시스템 내에서 위협 확산을 방지하여 보안을 강화합니다.

주요 이점

- **보안을 고려한 설계** 스토리지 계층에서 데이터 보호 기능 내장
- **실시간 탐지 및 대응** AI 기반 랜섬웨어 방어
- **사이버 저장소** 변경 및 삭제가 불가능한 백업
- **통합 컨트롤 플레인** 감지에서 복구까지 지능적인 오케스트레이션
- **복구 보장** NetApp Snapshot 복사본으로 데이터 손실 방지

액세스 제어를 강화하려면 다중 관리자 검증에서 여러 관리자가 중요한 작업을 승인해야 하므로 내부자 위협 또는 자격 증명이 손상될 위험이 줄어듭니다. 또한 다단계 인증을 통해 보안이 강화되므로 권한이 있는 직원만이 기밀 데이터와 시스템에 액세스할 수 있습니다.

실시간 탐지 및 대응

NetApp의 강력한 랜섬웨어 보호 기능 외에도 NetApp 은 99% 정확성과 거의 즉각적인 대응 기능을 갖춘 실시간 감지를 제공하며 ONTAP에 직접 내장된 AI 기반 자율 기술을 활용합니다. 이 고급 감지 기능은 의심스러운 활동과 이상 징후를 지속적으로 모니터링하여 잠재적인 랜섬웨어 공격이 파일, 블록 및 Amazon FSx for ONTAP의 기본 클라우드에서 전개될 때 이를 신속하게 식별합니다. 위협이 감지되면 시스템이 영향을 받는 데이터를 자동으로 격리하고 추가 확산을 방지하여 잠재적인 손상을 최소화할 수 있습니다.

NetApp DII(데이터 인프라 인사이트)는 내부자 위협에 대한 추가적인 방어 계층을 제공합니다. 잠재적인 비정상적인 사용자 동작을 감지하고 스토리지 시스템에 대한 사용자 액세스를 차단하고 스냅샷을 생성하는 등의 즉각적인 조치를 취합니다. 또한 DII는 포렌식 분석 및 감사를 위한 상세 분석 기능을 제공합니다. 이 포괄적인 접근 방식은 사전 예방 위협 감지, 신속한 대응 메커니즘, 상세한 사용자 활동 모니터링을 결합하여 외부 랜섬웨어 공격과 내부 위협 모두를 완벽하게 차단합니다.

그림 1: NetApp은 엔드투엔드 암호화, 다단계 인증, 역할 기반 액세스를 통한 데이터 액세스 등 데이터를 지능적이고 효율적으로 보호하는 다계층 방어 기능을 갖춘 지구상에서 가장 안전한 데이터 스토리지를 제공합니다.

사이버 보관을 위해 격리된 백업

SnapLock® 규정 준수 소프트웨어 기반의 NetApp Cybervaulting은 가장 중요한 데이터 자산을 보호할 수 있는 포괄적이고 유연한 솔루션을 제공합니다. ONTAP을 위한 강력한 강화 방법론이 적용된 논리적 에어 갭을 통해 진화하는 사이버 위협에 탄력적으로 대응하는 안전하고 격리된 스토리지 환경을 구축할 수 있습니다. NetApp을 사용하면 스토리지 인프라의 민첩성과 효율성을 유지하면서 데이터의 기밀성, 무결성, 가용성을 안심하고 유지할 수 있습니다.

보안을 강화하기 위해 NetApp을 사용하면 추가적인 데이터 보호 계층을 만들 수 있습니다.

- 안전하고 격리된 스토리지 인프라(예: 에어갭 스토리지 시스템)
- 변경 및 삭제가 불가능한 데이터 백업 복사본
- 엄격한 액세스 제어 및 다단계 인증
- 빠른 데이터 복원 기능
- SnapLock은 WORM 기술을 적용하여 데이터 암호화 및 삭제를 방지하고 파괴할 수 없는 효율적인 데이터 복사본을 제공합니다.

단순하고 견고한 컨트롤 플레인

NetApp은 엔드 투 엔드 워크로드 중심 랜섬웨어 방어 기술을 지능적으로 조정하고 실행하기 위해 NetApp BlueXP™ 를 갖춘 단일 제어 플레인을 제공하는 유일한 스토리지 공급업체입니다. 이러한 기술을 사용하면 클릭 한 번으로 위험한 중요 워크로드 데이터를 **식별하고 보호할** 수 있으며, 잠재적 공격의 영향을 정확하고 자동으로 **감지하여 대응하며**, 며칠 또는 몇 달이 아닌 몇 분 내에 워크로드를 **복구할** 수 있으므로 중요한 워크로드 데이터를 보호하고 비즈니스 중단 비용을 최소화할 수 있습니다.

BlueXP 랜섬웨어 차단 오케스트레이터는 NetApp ONTAP 의 강력한 기능을 BlueXP 데이터 서비스와 병합하여, 인공 지능 및 머신 러닝 기반 권장 사항, 지침을 자동 워크플로우와 추가함으로써 다음과 같은 이점을 제공합니다.

- **식별:** 워크로드(VM, 파일 공유, DB)와 NetApp 스토리지 내 워크로드 데이터를 자동으로 식별하고, 데이터를 워크로드에 매핑하며, 워크로드의 중요도를 판단하고, 워크로드 위험을 분석합니다.
- **보호:** 워크로드 보호 정책을 추천하며 한 번의 클릭으로 추천된 정책을 적용할 수 있습니다.

- **탐지:** 업계 최고 수준의 ML 기반 탐지 기능으로 워크로드 데이터에 대한 잠재적 공격을 거의 실시간으로 탐지합니다.
- **대응:** 잠재적 공격이 의심되면 변경하거나 삭제할 수 없는 스냅샷 복사본을 만들어 거의 실시간으로 자동으로 대응합니다.
- **복구:** 복구: 백업의 무결성을 검증하고 최적의 복구 시점을 식별하며, 간소화된 오케스트레이션 복구 기능으로 애플리케이션 정합성을 보장하며 워크로드 및 관련된 데이터를 신속하게 복원합니다.

"최근에 랜섬웨어 사고가 있었는데 Cloud Insights 랜섬웨어 탐지 기능의 효과를 직접 보고 완전히 반했습니다."

한 운송업체의 IT 담당 이사

BlueXP 랜섬웨어 차단 오케스트레이터는 랜섬웨어 대비 상태를 지원하고, 공격에 대응하고, 복구 과정을 안내하는 포괄적인 솔루션을 제공하여 랜섬웨어 관련 다운타임 및 데이터 손실로부터 워크로드를 방어하는 데 따르는 부담과 불안감을 제거합니다. NetApp만이 공격이 발생할 경우 즉시 이를 파악하고, 중요 워크로드 데이터를 보호하며, 복구를 쉽고 빠르게 진행하여 비즈니스 운영 중단을 최소화할 수 있습니다.

NetApp의 랜섬웨어 방지 기능을 사용하면 저장된 데이터를 식별하고 보호하고, 정확하고 자동으로 감지해 잠재적 공격의 영향을 최소화하고, 며칠 또는 몇 달이 아닌 몇 분 안에 데이터를 복구할 수 있습니다. 이 기능은 소중한 데이터를 보존하고 사이버 복원력을 위해 비용이 많이 드는 중단을 최소화하는 데 도움이 됩니다.

랜섬웨어는 IT를 진지하게 고려하지 않는 기업을 약화시킬 수 있습니다. NetApp의 데이터 중심 사이버 복원력 접근 방식만이 복구를 보장하면서 운영 및 2차 데이터에 대해 포괄적인 통합 보안 및 보호 기능을 제공합니다.

NetApp 랜섬웨어 솔루션에 관해 자세히 알아보기

문의하기

NetApp 정보

NetApp은 유니파이드 데이터 스토리지, 통합된 데이터 서비스, CloudOps 솔루션을 결합하여 격변하는 세상에서 모든 고객에게 기회를 제공하는 지능형 데이터 인프라 회사입니다. NetApp은 사일로가 없는 인프라를 만들고, 관찰 가능성과 AI를 활용하여 업계 최고 수준의 데이터 관리를 지원합니다. 세계 최대 규모의 클라우드에 기본적으로 내장된 유일한 엔터프라이즈급 스토리지 서비스인 NetApp의 데이터 스토리지는 원활한 유연성을 제공합니다. 또한, NetApp의 데이터 서비스는 우수한 사이버 복원력, 거버넌스, 애플리케이션 민첩성을 통해 데이터 우위를 만듭니다. NetApp의 CloudOps 솔루션은 관찰 가능성과 AI를 통해 성능과 효율성의 지속적인 최적화를 제공합니다. NetApp과 함께라면 데이터 유형, 워크로드, 환경과 관계없이 데이터 인프라를 혁신하여 비즈니스의 가능성을 실현할 수 있습니다.

www.netapp.com/ko

NetApp