

넷앱 랜섬웨어 복원력



실시간으로 랜섬웨어 공격을 탐지하고, 데이터 손실을 방지하고, 빠르게 복구하고, 비즈니스에 미치는 영향을 최소화하세요.

랜섬웨어 공격에 대응할 준비가 되어 있습니까?

랜섬웨어 공격에 대비하는 데 있어 중요한 측면은 스토리지 계층(최후의 방어선)에서 워크로드 데이터를 보호하는 것입니다. 랜섬웨어 공격이 점점 더 정교해지고 자동화되며 비용도 많이 들기 때문에 랜섬웨어 공격을 예방하는 것은 비현실적입니다. 공격자가 들어올 때를 대비해야 합니다.

백업만으로는 충분하지 않습니다. 중요한 워크로드 데이터에 대한 위험을 평가하고 위협을 감지하여 실시간으로 대응할 수 있어야 합니다. 또한 빠르고 쉽게 실행할 수 있는 복구 계획도 필요합니다. 그러나 랜섬웨어 공격에 대한 효과적인 회복력을 확보하는 것은 운영상의 부담이며, 오류가 발생하기 쉬운 수동 작업이 많고 필요한 전문 지식을 갖춘 직원이 너무 부족합니다.

적절한 프로그램이 없으면 워크로드에 대한 공격이 감지되지 않고 대응이 지연될 수 있습니다. 작업량 회복은 복잡할 것입니다. 평균 7일이 소요됩니다. 1 —그리고 데이터가 완전히 복구되지 않을 수도 있습니다. 너무 늦고, 효과적이지도 않습니다.

최종 방어선에서 포괄적인 보호 갖추기

NetApp® 랜섬웨어 복원력 서비스를 사용하면 예방부터 탐지, 대응, 복구까지 프로그램을 빠르고 쉽게 실행할 수 있습니다.

랜섬웨어 복원력은 워크로드 중심의 랜섬웨어 방어를 지능적으로 조율할 수 있는 단일 인터페이스를 제공합니다. 몇 번만 클릭하면 위험에 처한 중요 워크로드 데이터를 식별하고 보호할 수 있습니다. 또한 이 서비스는 잠재적인 공격을 정확하고 자동으로 감지하고 대응하며 그 영향을 제한합니다. 또한 몇 분 안에 악성 소프트웨어가 없는 상태로 워크로드를 복구하여 귀중한 데이터를 보호하고 손상과 비즈니스 중단 비용을 최소화할 수 있습니다.

랜섬웨어 복원력은 NetApp ONTAP® 소프트웨어의 강력한 기능과 NetApp 데이터 서비스를 통합하여 자동화된 워크플로를 통해 지능형 권장 사항과 지침을 추가하여 다음을 제공합니다.

- 식별.** NetApp 스토리지에서 워크로드(VM, 파일 공유, 인기 있는 데이터베이스)와 해당 데이터를 자동으로 식별하고, 데이터를 워크로드에 매핑하고, 데이터 민감도, 중요도, 위험을 파악합니다.
- 보호.** 워크로드 보호 정책에 대한 권장 사항을 받아 한 번의 클릭으로 적용하세요.
- 감지.** 잠재적인 데이터 유출 시도는 물론 파일 암호화 및 대량 삭제 시도를 나타낼 수 있는 의심스러운 파일 및 사용자 동작 활동을 실시간으로 감지합니다.
- 대응.** 잠재적인 공격이 의심될 경우 NetApp Snapshot™ 복사본을 자동으로 생성하고 사용자를 차단하여 작업 부하를 보호합니다. 이 서비스는 업계 최고의 보안 정보 및 이벤트 관리(SIEM) 솔루션과도 통합됩니다.
- 복구.** 간단하고 체계적인 복구 프로세스를 통해 작업 부하와 관련 데이터를 빠르게 복구합니다. 격리된 복구 환경을 사용하면 데이터를 깨끗하고 맬웨어 없이 복원할 수 있습니다.
- 통제.** 랜섬웨어 보호 전략과 정책을 구현하고 결과를 모니터링합니다.

공격에 대비: 시간을 절약하고 효율성을 높이세요

랜섬웨어 복원력은 NetApp 스토리지에 있는 데이터 유형을 자동으로 식별하고, 데이터를 특정 워크로드에 매핑하고, 데이터의 민감도와 중요도를 평가하고, 위험을 분석합니다. 이 프로세스를 통해 복잡한 수동 분석, 추가적인 타사 도구 및 전문 지식에 대한 의존도를 줄일 수 있습니다.

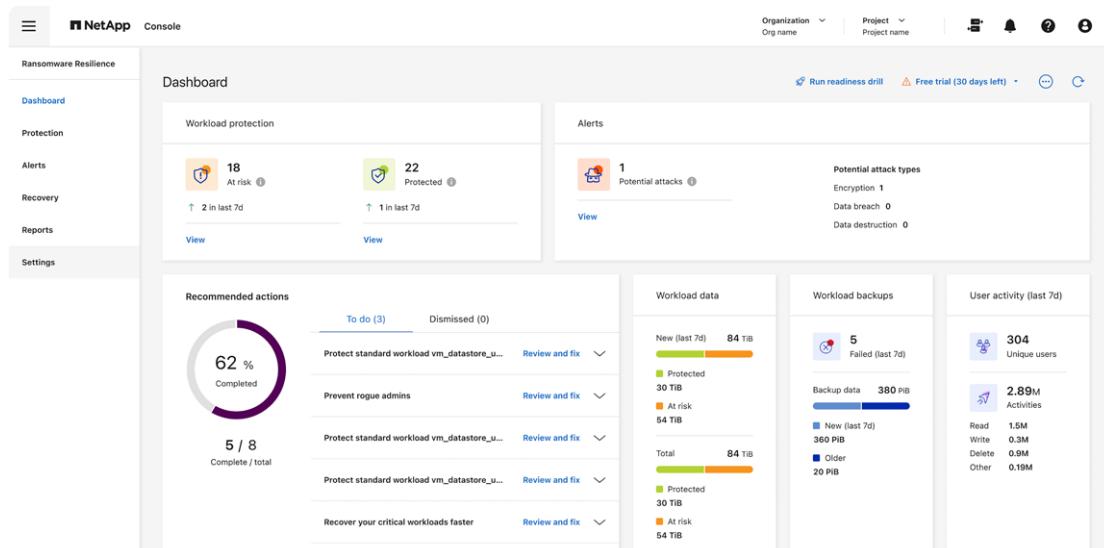


그림 1: NetApp 랜섬웨어 복원력 서비스는 단일 제어 평면을 통해 탐지부터 복구까지 포괄적이고 조율된 워크로드 중심 랜섬웨어 방어를 제공합니다.

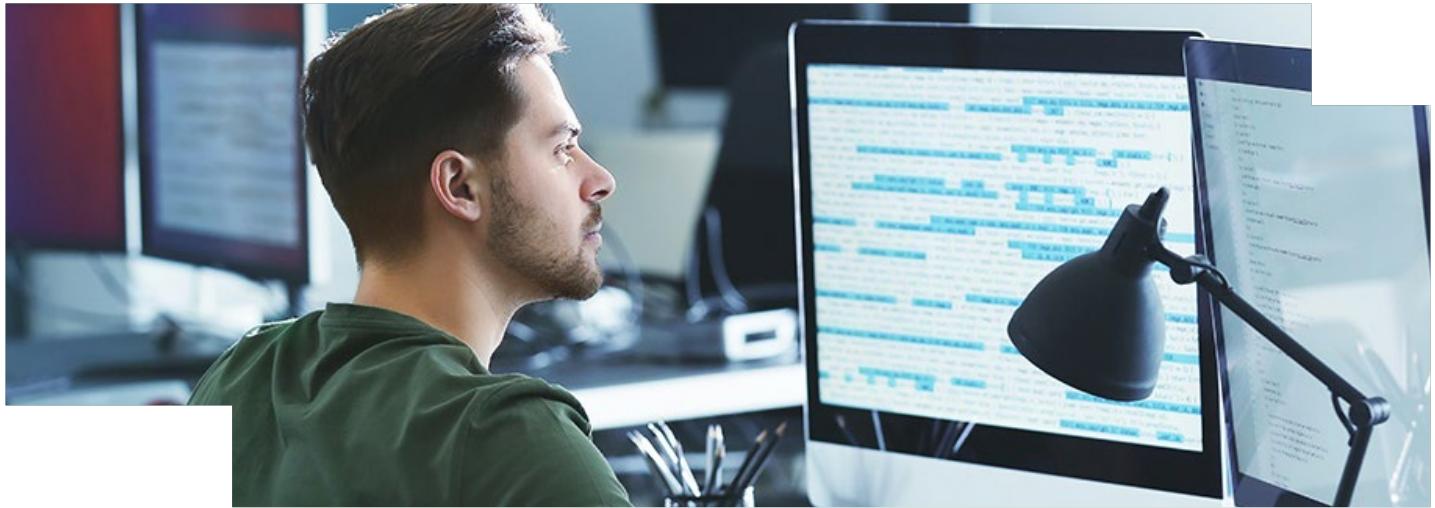
주요 이점

최후의 방어선에서 포괄적이고 조직적인 보호를 받을 수 있습니다

- 워크로드 보호 태세에 대한 완벽한 가시성 확보
- 공격을 조기에 감지하고 데이터 손실 방지
- 전체 워크로드를 맬웨어 없이 빠르게 복구하여 운영 중단, 비용, 매출 손실, 비즈니스 피해를 최소화
- 포렌식 분석에 필요한 데이터와 보안 태세를 개선하기 위한 권장 사항 확인

랜섬웨어 복원력은 NetApp 자율 랜섬웨어 보호(AI, ARP/AI) 이상 탐지, FPolicy 악성 확장 차단, 변조 방지 스냅샷 복사본 등 ONTAP 기능을 사용하여 지능형 보호 정책을 제안합니다. 랜섬웨어 복원력은 또한 데이터 자산의 민감성과 중요성에 맞춰 보호 권장 사항을 맞춤화합니다.

클릭 한 번으로 보호 정책을 워크로드 데이터에 원활하고 일관되게 적용할 수 있습니다. 랜섬웨어 복원력은 백그라운드에서 ONTAP 및 NetApp 데이터 서비스 기능을 구성하고 각 데이터 볼륨에서 보호 워크플로를 조율하여 반복적인 수동 작업의 필요성을 줄여줍니다.



실시간으로 위협 탐지 및 대응

랜섬웨어 복원력은 의심스러운 파일과 사용자 행동 이상을 지속적으로 모니터링합니다. 이 솔루션은 잠재적인 데이터 유출 시도를 나타낼 수 있는 사용자 행동을 조기에 식별하고 파일 암호화 및 대량 삭제 시도를 감지하여 데이터 침해를 감지할 수 있습니다. 공격이 의심되면 랜섬웨어 복원력은 데이터 손실을 방지하기 위해 스냅샷 사본을 생성하고, 공격을 가하는 사용자를 차단하여 공격을 중단시키고 추가 공격을 방지합니다.

이 서비스는 기본 스토리지에서 혁신적이고 고급 AI 기반 랜섬웨어 감지 기능을 사용합니다. 이러한 접근 방식을 사용하면 잠재적인 공격을 신속하게 찾아내고 즉시 완화할 수 있습니다.

랜섬웨어 복원력은 포렌식을 지원하기 위한 사고 보고서를 제공하며 업계 최고의 SIEM 솔루션과 통합됩니다.

몇 분 안에 간편하게 워크로드 복구

랜섬웨어 복원력은 관련된 모든 워크로드 데이터의 애플리케이션 일관성 복구를 위한 워크플로를 조율하고 프로세스와 상태에 대한 실시간 가시성을 제공합니다. 스냅샷 사본은 작업 부하 수준에서 복원할 수도 있고, 볼륨이나 파일 수준에서 더 세부적으로 복원할 수도 있습니다.

랜섬웨어 복원력은 복구 프로세스의 일환으로 감염된

워크로드를 격리하고, 맬웨어를 제거하고, 복구 지점을 권장하고, 사용자에게 직관적인 복구 프로세스를 안내하는 격리된 복구 환경을 제공합니다. 이 방법을 사용하면 악성 소프트웨어가 없는 깨끗한 복구가 가능하며 데이터 재감염을 방지할 수 있습니다.

비즈니스 중단 최소화

랜섬웨어 복원력은 랜섬웨어 관련 가동 중지 및 데이터 손실로부터 워크로드를 보호하는 데 따르는 부담과 불안을 제거합니다. 이 서비스는 귀하의 준비 상태를 개선하고, 공격에 대응하고, 복구 과정을 안내하는 포괄적인 서비스를 제공합니다. NetApp 사용하면 공격이 발생할 때 즉시 알림을 받고 귀중한 워크로드 데이터가 보호되며 빠르고 쉽게 복구할 수 있으므로 비즈니스 중단을 최소화할 수 있으므로 마음의 평화를 누릴 수 있습니다.

지금 NetApp 랜섬웨어 복원력을 확보하십시오.

¹ ESG, 2023 Ransomware Preparedness: Lighting the Way to Readiness and Mitigation, 2023년 11월.

이 문서는 기계 번역을 통해 생성된 참고 번역입니다. 영어 버전과 내용에 모순되거나 일치하지 않는 부분이 있을 경우, 영어 버전의 내용이 우선 적용됩니다.



문의하기

NetApp 정보

NetApp 통합 데이터 스토리지, 통합 데이터, 운영 및 워크로드 서비스를 결합하여 혼란스러운 세상을 모든 고객에게 기회로 전환하는 지능형 데이터 인프라 회사입니다. NetApp은 사일로 없는 인프라를 구축하고 통합 가시성과 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. 당사의 운영 및 워크로드 서비스는 관찰 가능성과 AI를 통해 인프라와 워크로드의 성능과 효율성을 지속적으로 최적화합니다. NetApp과 함께라면 데이터 유형, 워크로드, 환경과 관계없이 데이터 인프라를 혁신하여 비즈니스의 가능성을 실현할 수 있습니다. 자세한 내용은 www.netapp.com에서 확인하거나 NetApp을 팔로우하십시오. X, [LinkedIn](#), [Facebook](#) 및 [Instagram](#).



© 2025 NetApp, Inc. All Rights Reserved. NETAPP.NETAPP 로고 및 <http://www.netapp.com/TM>에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다. SB-4278-0925-koKR