



# 시작하십시오

## Ransomware Protection

NetApp  
July 19, 2022

# 목차

시작하십시오 .....	1
랜섬웨어 차단 에 대해 알아보십시오 .....	1

# 시작하십시오

## 랜섬웨어 차단 에 대해 알아보십시오

랜섬웨어 공격은 비즈니스 시간, 리소스 및 평판에 악영향을 줄 수 있습니다. 랜섬웨어 보호 서비스를 통해 사이버 보안에 대한 관련 정보를 보고 사이버 공격에 대한 조직의 복원력을 평가할 수 있습니다. 또한 알림 목록과 데이터 보안 개선을 위한 해결 방법도 제공합니다.

"랜섬웨어 차단 의 사용 사례에 대해 알아보십시오".



랜섬웨어 보호 서비스는 현재 베타 버전입니다.

### 피처

랜섬웨어 차단 기능은 단일 가시성 및 제어 지점을 제공하여 다양한 작업 환경과 인프라 계층에서 데이터 보안을 관리 및 세분화하여 위협이 발생했을 때 보다 효과적으로 대응할 수 있도록 지원합니다. 현재 사이버 스토리지 보호 작업에 도움이 되는 여러 기능을 제공하고 있습니다. 향후 추가 기능이 추가될 예정입니다. 현재 기능은 다음과 같은 경우에 식별합니다.

- 작업 환경의 볼륨은 정기적인 Snapshot 복사본을 만들어 보호되지 않습니다.
- 를 사용하여 클라우드에 백업을 생성하면 작업 환경의 볼륨이 보호되지 않습니다 "[클라우드 백업](#)".
- 작업 환경 및 데이터 소스의 데이터는 를 사용하여 스캔되지 않습니다 "[클라우드 데이터 감지](#)" 규정 준수 및 개인 정보 보호에 대한 우려 사항을 파악하고 최적화 기회를 찾습니다.

이 기능은 랜섬웨어 보호 관점에서도 중요합니다. 중요한(비즈니스에 중요한) 데이터의 위치를 더 잘 이해하여 보호에 집중할 수 있기 때문입니다.

- 랜섬웨어 공격으로 인해 복구해야 할 경우 가장 중요한 범주의 데이터가 백업되지 않습니다.
- 작업 환경 또는 데이터 소스에서 암호화된 파일의 비율이 비정상적으로 증가했습니다.

이는 네트워크에서 랜섬웨어 공격이 시작했다는 것을 나타내는 지표가 될 수 있습니다.

- 파일에서 중요한 데이터가 검색되고 작업 환경 또는 데이터 소스에서 액세스 권한 수준이 너무 높습니다.
- 사용자가 Active Directory 도메인 관리자 그룹에 추가되었습니다.
- 클러스터의 ONTAP 소프트웨어 버전은 오래되었으며 최상의 보호 및 보안 기능을 제공하도록 업데이트해야 합니다.
- ONTAP 시스템에서 NAS 파일 시스템 감사가 설정되지 않았습니다.

CIFS 감사를 설정하면 시스템 관리자가 폴더 권한 변경, 파일 읽기 또는 쓰기 실패, 파일 생성, 수정 또는 삭제 시기 등의 정보를 추적하는 감사 이벤트가 생성됩니다.

- 온박스 안티 랜섬웨어 기능은 ONTAP 시스템에서 지원되지 않습니다.

ONTAP의 랜섬웨어 방지 기능은 랜섬웨어 공격을 나타낼 수 있는 비정상적인 활동을 사전에 감지하여 경고합니다.

"랜섬웨어 보호 대시보드에서 이러한 잠재적인 문제를 확인하는 방법을 알아보십시오."

Cloud Volumes ONTAP 시스템을 사용할 경우 작업 환경에서 직접 배포할 수 있는 몇 가지 추가적인 랜섬웨어 보호 기능이 있습니다. ["랜섬웨어에 대한 보호를 강화하는 방법을 알아보십시오"](#).

## 지원되는 작업 환경 및 데이터 소스

"클라우드 데이터 감지" 랜섬웨어 보호 서비스를 이용하려면 사전 요구사항이 있어야 합니다. Data Sense를 설치 및 활성화한 후 랜섬웨어 Protection을 사용하여 다음 유형의 작업 환경 및 데이터 소스에 대한 사이버 공격에 데이터가 얼마나 복원되는지 확인할 수 있습니다.

- 작업 환경: \*
  - Cloud Volumes ONTAP(AWS, Azure 또는 GCP에 구축)
  - 온프레미스 ONTAP 클러스터
  - Azure NetApp Files
  - ONTAP용 Amazon FSx
  - Amazon S3
- 데이터 소스: \*
  - 비 NetApp 파일 공유
  - 오브젝트 스토리지(S3 프로토콜 사용)
  - 데이터베이스(Amazon RDS, MongoDB, MySQL, Oracle, PostgreSQL, SAP HANA, SQL Server)
  - OneDrive 계정
  - SharePoint 계정
  - Google Drive 계정

또한 랜섬웨어 차단 기능은 글로벌 Active Directory 구성이 있는 경우 모니터링하기도 합니다 ["클라우드 데이터 센스에서 구성했습니다"](#).

## 랜섬웨어 차단 작동 방식

고수준에서 랜섬웨어 차단은 다음과 같이 작동합니다.

1. 랜섬웨어 방지 기능은 스토리지 시스템, Cloud Data Sense, Cloud Backup 및 기타 Cloud Manager 리소스에서 정보를 수집하여 랜섬웨어 보호 대시보드를 채웁니다.
2. 랜섬웨어 보호 대시보드를 사용하여 시스템의 보호 기능을 대략적으로 파악할 수 있습니다.
3. 제공된 보고 툴을 사용하여 사이버 스토리지 보호 노력을 지원할 수 있습니다.

## 비용

Beta 기간 중에는 랜섬웨어 보호 서비스에 별도의 비용이 들지 않습니다.

## 저작권 정보

Copyright © 2022 NetApp, Inc. All rights reserved. 미국에서 인쇄된 본 문서의 어떤 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 그래픽, 전자적 또는 기계적 수단(사진 복사, 레코딩 등)으로도 저작권 소유자의 사전 서면 승인 없이 전자 검색 시스템에 저장 또는 저장.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지 사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 "있는 그대로" 제공되며 상품성 및 특정 목적에 대한 적합성에 대한 명시적 또는 묵시적 보증을 포함하여 이에 제한되지 않고, 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 또는 파생적 손해(소계 물품 또는 서비스의 조달, 사용 손실, 데이터 또는 수익 손실, 계약, 엄격한 책임 또는 불법 행위(과실 또는 그렇지 않은 경우)에 관계없이 어떠한 책임도 지지 않으며, 이는 이러한 손해의 가능성을 사전에 알고 있던 경우에도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구입의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허 또는 해외 특허, 해외 특허, 해외 특허, 해외 특허, 해외 특허, 해외 특허, 해외 특허, 해외 특허, 미국 출원 중인 특허로 보호됩니다.

권리 제한 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.277-7103(1988년 10월) 및 FAR 52-227-19(1987년 6월)의 기술 데이터 및 컴퓨터 소프트웨어의 권리(Rights in Technical Data and Computer Software) 조항의 하위 조항 (c)(1)(ii)에 설명된 제한사항이 적용됩니다.

## 상표 정보

NETAPP, NETAPP 로고 및 에 나열된 마크는 NetApp에 있습니다 <http://www.netapp.com/TM> 는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.