

## NetApp 랜섬웨어 차단 및 복구 서비스



데이터의 보안, 가용성, 안정성 및 복구 가능성을  
보장하는 랜섬웨어 대비 하이브리드 클라우드 데이터  
인프라를 계획, 배포 및 관리

랜섬웨어 공격이 증가하고 있으며 공격과 관련된 비용과  
데이터 손실을 보상하려면 사이버 보안 보험보다 더 많은  
것이 필요합니다. 최선의 방어가 훌륭한 공격입니다. 즉,  
발생하기 전에 적절한 보안 및 데이터 보호 기능을 모두  
갖추고 있는지 확인해야 합니다. 하지만 랜섬웨어 복원력을  
갖춘 데이터 환경을 구축하기 위한 올바른 단계를 파악하는  
것은 쉽지 않습니다.

어떤 데이터가 위험에 노출되어 있는지, 그리고 이러한 위험을 해결하기 위해 무엇을 해야 하는지 명확하게 파악해야 합니다. 특정 비즈니스 요구사항을 충족하는 모범 사례와 툴을 결정하고 구현할 수 있어야 합니다. 그리고 공격이 발생할 경우 공격 대상 및 중요 데이터 손실을 방지하기 위해 신속하게 복구할 수 있는 방법을 즉시 파악할 수 있는 리소스와 전문 지식이 필요합니다.

### NetApp 랜섬웨어 차단 및 복구 서비스

NetApp® 프로페셔널 서비스 전문가의 도움을 받아 랜섬웨어로부터의 복원력과 생존 능력을 높이십시오. NetApp 랜섬웨어 차단 및 복구 서비스는 비즈니스 크리티컬 데이터의 보안, 가용성, 안정성 및 복구 가능성을 보장하는 랜섬웨어 대비 하이브리드 클라우드 데이터 인프라를 계획, 구축 및 관리하는 데 필요한 전문 지식을 제공합니다.

NetApp의 포괄적인 접근 방식은 랜섬웨어 복원력을 갖춘 스토리지 환경을 구축하고 랜섬웨어 공격이 발생할 경우 초래되는 다운타임, 비용 및 잠재적인 데이터 손실을 최소화할 수 있도록 설계되었습니다. NetApp 프로페셔널 서비스 전문가는 비즈니스를 적절하게 보호할 수 있도록 다음과 같은 3가지 단계로 서비스를 제공합니다.

- 탐색:** 현재 환경을 평가하고, 보안 공백을 식별하고, 데이터 복구 계획(사용 가능한 경우)을 평가하고, NetApp 랜섬웨어 방지 소프트웨어 제품군을 완벽하게 사용하기 위한 권장안을 제공합니다.
- 구축:** NetApp의 전문가들이 고객의 하이브리드 클라우드 환경에 NetApp 보안 툴을 구축하고 적절하게 구성합니다.
- 관리:** 구독 기반 관리 서비스 기능을 통해 NetApp 전문가가 환경을 24/7/365 상시 모니터링하고 관리합니다.

### 공격이 발생하기 전에 대비

랜섬웨어에 대한 대비는 잠재적인 위험 및 보안 공백을 파악하고 적절한 조치를 결정하는 것에서 시작됩니다. NetApp의 전문가는 고객의 현재 NetApp 데이터 환경을 완벽하게 평가하여 비즈니스 연속성 위험을 식별하고, NetApp 기본 소프트웨어 솔루션의 보안 공백을

### 주요 이점

랜섬웨어 공격이 발생하기 전에 보안 위험을 감지하고 치료

구독 기반의 하이터치 프로페셔널 서비스를 통해 랜섬웨어 대비 상태를 개선하고 데이터를 보호:

- 업계 최고 수준의 NetApp 랜섬웨어 방지 툴 구현 및 구성
- 24/7/365 연중무휴 경고 모니터링, 문제 해결 및 소프트웨어 관리 제공랜섬웨어 공격이 발생했을 때 데이터 백업을 신속하게 복원할 수 있도록 하여 데이터를 신속하게 복구

확인하고, 데이터 보호가 없는 중요한 스토리지 볼륨을 감지하고, 랜섬웨어로부터 복구할 수 있는 고객의 역량을 평가합니다. 이러한 인사이트를 바탕으로 랜섬웨어 공격이 발생하기 전에 보안 문제와 위험을 신속하게 해결할 수 있는 실용적인 권장안을 제공합니다. 또한 NetApp의 전문가들이 기존 데이터 보호 및 보존 정책의 격차를 파악하고 해결하여 복구하는 동안 정의된 RTO 및 RPO를 충족할 수 있도록 지원합니다.

### 랜섬웨어 복원력을 갖춘 환경 구축

사이버 복원력이 뛰어난 데이터 환경을 구축하려면 일련의 보안 툴을 구매하는 것만으로는 충분하지 않습니다. NetApp의 프로페셔널 서비스 전문가가 이러한 구독 기반의 하이터치 서비스를 통해 데이터 스토리지 시스템을 보호하기 위한 검증된 모범 사례를 구현합니다. 랜섬웨어 복원력을 향상시킬 수 있는 올바른 NetApp 소프트웨어 및 툴을 구현 및 구성하는 동시에 데이터 취약점을 줄이는 데 도움이 됩니다.

NetApp의 전문가들은 고급 데이터 암호화를 구현하고 데이터 복구 테스트 및 검증을 수행하여 랜섬웨어 공격으로부터 복구할 수 있도록 지원하는 서비스 수준 목표를 준수합니다. 또한, 이 서비스를 이용하면 사이버 보안 보험 설문조사에 대한 응답과 보험 자격 점수에 도움이 될 수 있습니다.

그런 다음 NetApp 전문가가 NetApp 랜섬웨어 솔루션 (NetApp Cloud Secure, FPolicy, SnapLock®, SnapCenter® 및 SnapMirror® 소프트웨어)을 관리하고 24/7/365 연중무휴 경고를 모니터링하고 치료 및 관리합니다. 이 서비스에는 보고 및 지속적인 컨설팅이 포함되어 있어 보안 요구사항을 지속적으로 충족할 수 있으므로 IT 팀은 데이터가 안전하고 복구 가능하다는 확신을 갖고 다른 작업에 몰두할 수 있습니다.

#### 랜섬웨어 공격이 발생할 경우 신속하게 복구

공격이 발생할 경우 비즈니스 연속성 및 데이터 무결성을 유지하면서 데이터를 신속하게 복구할 수 있어야 합니다. NetApp 프로페셔널 서비스 전문가가 있으면 랜섬웨어 공격으로부터 신속하게 복구하고 중요 데이터 손실을 방지하는 데 필요한 전문 지식을 얻을 수 있습니다. NetApp 서비스 팀은 SnapCenter 기반 복구를 사용하여 변경 불가능한 데이터 보관소로부터 비즈니스 크리티컬 데이터를 감염되지 않은 상태로 완벽하게 복구하고 랜섬웨어 확산을 막습니다.

#### 권장되는 추가 프로페셔널 서비스

- **Flex 관리 서비스:** Flex 관리 서비스는 필요한 서비스 모듈만 사용하여 하이브리드 클라우드 NetApp ONTAP® 환경을 유지 관리할 수 있는 유연성을 제공합니다.
- **다단계 인증(MFA):** 추가적인 보호를 위해 NetApp 전문가는 운영, 보조 및 SnapLock 시스템에 MFA를 구현합니다.

#### 지금 시작하십시오

NetApp 랜섬웨어 차단 및 복구 서비스에 대해 자세히 알아보려면 해당 지역의 NetApp 세일즈 담당자에게 문의하거나 [www.netapp.com](http://www.netapp.com)을 방문하십시오.

#### NetApp Services 정보

투자에서 더 큰 비즈니스 가치 실현 차세대 데이터 센터를 계획하고 있거나, 주요 스토리지 배포에 대한 전문 지식을 원하거나, 기존 인프라의 운영 효율성을 최적화하기를 원하는 경우처럼, NetApp 서비스는 어떠한 요건이라도 도움을 드릴 수 있습니다.

#### NetApp 정보

평범함으로 가득한 세상에서 NetApp은 특별함을 선사합니다. NetApp은 귀사가 데이터를 최대한 활용할 수 있도록 돋는다는 한 가지 목표에 주력하고 있습니다. NetApp은 귀사에서 사용 중인 엔터프라이즈급 데이터 서비스를 클라우드로 전환하고, 클라우드의 유연성을 데이터 센터에 제공합니다. 업계 최고 수준의 NetApp 솔루션은 다양한 고객 환경과 세계 최대의 퍼블릭 클라우드에서 작동합니다.

클라우드 주도형 데이터 중심 소프트웨어 회사인 NetApp만이 고유한 Data Fabric을 구축하고, 클라우드를 단순화하고 연결하며, 언제 어디서나 원하는 사람에게 원하는 데이터와 서비스, 애플리케이션을 안전하게 제공하도록 지원할 수 있습니다.