NetApp

NETAPP BLUEXP 랜섬웨어 방어

워크로드 데이터 손실을 최소화하고 신속하게 복구하는 데 필요한 인텔리전스 및 지원

랜섬웨어 공격에 대응할 준비가 되어 있습니까?
랜섬웨어에 대한 대응 능력과 복원력은 더 이상 선택이 아니라 필수입니다. 공격은 점점 더 정교해지고 자동화되고 있으며, 복구 비용은 점점 늘어나고 있습니다. 제로데이 취약성과 자격 증명 도용을 완전히 예방하는 것은 불가능하므로, 공격자가 침입하는 경우에 항상 대비해야만 합니다.

대비한다는 것은 최종 방어선인 스토리지 계층에서 워크로드 데이터를 보호한다는 의미입니다. 하지만 백업만으로는 부족합니다. 주요 워크로드 데이터에 대한 위험을 인식하고, 신속한 위협 탐지 및 대응을 갖추고, 공격이 시작되면 신속하고 간단하게 실행할 수 있는 복구 계획도 수립해야 합니다. 그러나 수동적인 단계가 너무 많아 오류 발생 가능성이 높고 운용할 수 있는 직원이 적어 막대한 운영 부담이 들 수밖에 없습니다.

이러한 요구사항을 충족하지 않으면 워크로드에 대한 공격을 탐지할 수 없고, 대응이 지연되며, 워크로드 복구가 복잡해져 평균 7일의 복구 시간이 필요하고[1] 모든 데이터를 복구할 수도 없습니다. 너무 늦고, 효과적이지도 않습니다.

최종 방어선에서 포괄적인 보호 갖추기
NetApp은 NetApp® BlueXP™ 랜섬웨어 보호를 통해 워크로드 중심의 종합적인 랜섬웨어 방어를 지능적으로 조정하고 실행하기 위한 단일 컨트롤 플레인을 제공하는 유일한 스토리지 공급업체입니다. 클릭 몇 번으로 위험에 처한 주요 워크로드 데이터를 식별하고 보호할 수 있습니다. 잠재적인 공격을 자동으로 정확하게 탐지하고 대응하여 공격의 영향을 제한할 수 있습니다. 또한, 몇 분 이내에 워크로드를 복구해 귀중한 워크로드 데이터를 보호하고 운영 중단 비용을 최소화할 수 있습니다.

BlueXP 랜섬웨어 방어는 NetApp ONTAP® 소프트웨어의 강력한 기능에 BlueXP 데이터 서비스를 결합하여 지능적인 권장사항과 안내, 자동화된 워크플로를 통해 다음과 같은 기능을 제공합니다.

- **식별**: 워크로드(VM, 파일 공유, 주요 데이터베이스)와 NetApp 스토리지 내 워크로드 데이터를 자동으로 식별하고, 데이터를 워크로드에 매핑하며, 워크로드 데이터 민감도, 중요도, 위험을 판정합니다.
- **보호**: 워크로드 보호 정책을 추천하며 클릭 한 번으로 적용할 수 있습니다.
- **탐지**: 파일 이상 징후와 악성 행위자를 모두 실시간 탐지하는 AI 기반 파일 활동과 사용자 및 엔터티 행동 분석(UEBA)으로 잠재적 워크로드 데이터 공격을 탐지합니다.
- **대응**: 자동 스냅샷 사본을 활용하고 잠재적 공격이 의심될 때 사용자를 수동 또는 자동으로 차단하여 워크로드를 보호합니다. 가장 많이 사용되는 SIEM 솔루션과 통합됩니다.
- **복구**: 간소화되고 오케스트레이션된 애플리케이션 일관성 복구를 통해 워크로드 및 관련 데이터를 빠르게 복구합니다.
- **통제**: 랜섬웨어 방어 전략과 정책을 개선하고 결과를 모니터링합니다.

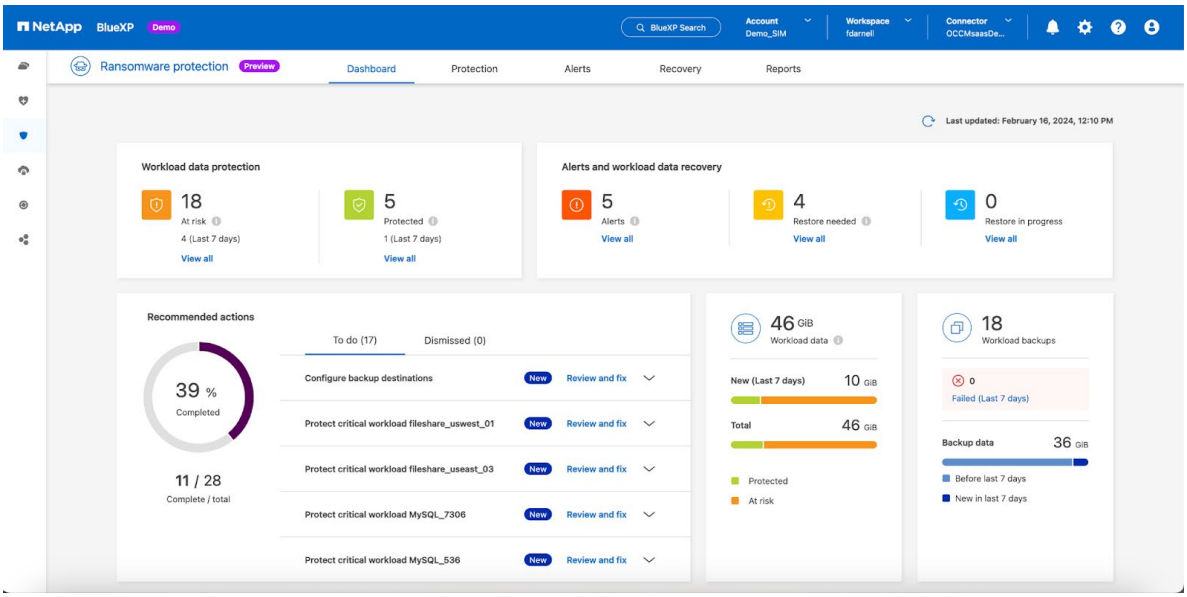
랜섬웨어 대비 태세 지원을 통해 시간 절약 및 효과 향상
BlueXP 랜섬웨어 방어는 NetApp 스토리지에 있는 데이터의 유형을 자동으로 식별하고, 데이터를 워크로드에 매핑하며, 워크로드 데이터 민감도 및 중요도를 판정하고, 워크로드 위험을 분석합니다. 이러한 기능 덕분에 조직은 복잡한 수동 분석 절차, 전문적인 기술, 여러 타사 툴에 대한 의존도를 낮출 수 있습니다.

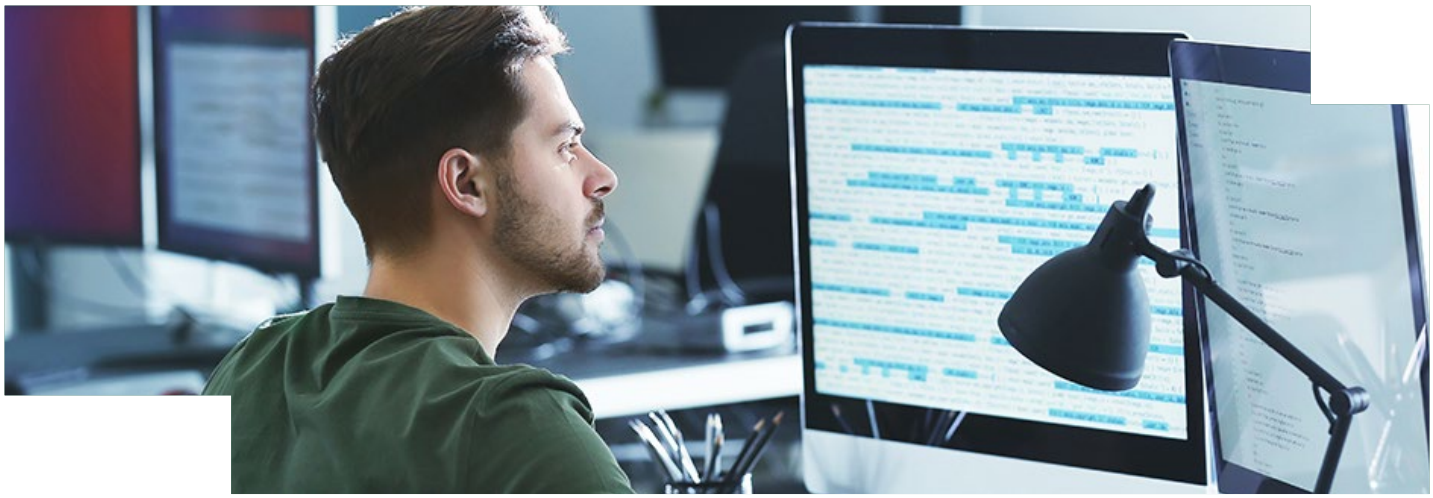
주요 이점

- 방어 최종선에서 포괄적인 보호 제공: 백업을 넘어 미국 국립표준기술연구소(NIST) 사이버 보안 프레임워크의 6가지 영역에 모두 대응
- 워크로드 중심의 애플리케이션 정합성을 보장하는 솔루션
- 우선순위가 지정된 지능형 추천
- 자동화된 조치 안내
- 위협을 조기에 탐지
- 전체 워크로드를 빠르게 복구할 수 있으며, 볼륨 또는 파일 단위로 세분화된 복원 옵션 제공

BlueXP 랜섬웨어 방어는 조작 방지된 스냅샷 복사본, FPolicy 악성 확장 프로그램 차단, 자율적 랜섬웨어 방어 이상 징후 탐지 등 업계 최고 수준의 ONTAP 기능을 활용하는, 즉시 사용 가능한 지능형 보호 정책을 제공합니다. 또한, 투자 수익률의 최적화를 위해 BlueXP 랜섬웨어 방어는 데이터 민감도 및 중요도에 맞춘 보호 권장사항도 제공합니다.

클릭 한 번으로 보호 정책을 워크로드 데이터에 원활하고 일관되게 적용할 수 있습니다. BlueXP 랜섬웨어 방어는 백그라운드에서 작동하며 ONTAP 및 BlueXP 기능을 구성하고, 할당된 각 볼륨에서 보호 워크플로를 조정하므로, 반복적인 수동 작업의 필요성이 줄어듭니다.





파일 및 사용자 행동 이상 징후에 대해 AI 기반 탐지를 배포하여 실시간 위험 포착 및 대응
BlueXP 랜섬웨어 방어는 수상한 파일 및 사용자 행동 이상 징후를 지속해서로 모니터링하고 공격의 추가 영향을 자동으로 차단합니다. 공격이 의심되면 스냅샷 사본을 생성하고 사용자를 차단하여 피해를 최소화합니다.

또한, BlueXP 랜섬웨어 방어는 고급 AI 기반 랜섬웨어 탐지를 운영 스토리지에 적용하여 운영 데이터에 대한 잠재적인 공격을 조기에 탐지하여 즉시 대응할 수 있다는 점에서 혁신적입니다.

뿐만 아니라 데이터와 함께 인시던트 보고서를 제공하여 공격 포렌식을 지원하고 가장 많이 사용되는 SIEM 솔루션과 통합하여 위험 대응을 간소화 및 가속합니다.

애플리케이션 정합성을 보장하는 복구 안내를 통해 워크로드를 몇 분 이내에 복구
BlueXP 랜섬웨어 방어는 선택한 복구 옵션에 따라 최적의 복구 시점(RPA)을 제공하는 스냅샷 복사본 또는 백업을 알려주고, 워크로드 레벨이나 볼륨 또는 파일 단위로 세부적으로 복원할 수 있는 기능을 제공합니다.

또한, 관련된 모든 워크로드 데이터의 애플리케이션 정합성 복구에 대한 워크플로를 조정하며, 실시간 복구 상태에 대한 가시성을 제공하여 복구를 신속히 진행하고 성공을 촉진합니다.

비즈니스 중단 최소화
BlueXP 랜섬웨어 방어는 랜섬웨어 관련 다운타임 및 데이터 손실로부터 워크로드를 보호해야 하는 부담과 불안을 줄여줍니다. 랜섬웨어 대비 태세를 개선하고, 공격에 대응하고, 복구 과정을 안내하는 종합적인 솔루션입니다. 공격이 발생하면 즉시 알림을 받고, 귀중한 워크로드 데이터를 보호하고, 신속하고 간단하게 복구하며, 비즈니스 중단을 최소화할 수 있는 기업은 NetApp뿐입니다.

지금 바로 BlueXP 랜섬웨어 보호를 설치하십시오.

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

문의하기

NetApp 정보
NetApp은 유니파이드 데이터 스토리지, 통합된 데이터 서비스, CloudOps 솔루션을 결합하여 파괴적 혁신 속에서 모든 고객에게 기회를 제공하는 지능적인 데이터 인프라 회사입니다. NetApp은 사일로가 없는 인프라를 만들고, 관측 가능성과 AI를 활용하여 최선의 데이터 관리를 지원합니다. 세계 최대의 클라우드에 네이티브로 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/ko에서 자세히 알아보시거나 Twitter, LinkedIn, Facebook, Instagram에서 팔로우해 주십시오.

NetApp