



NetApp와 제로 트러스트

ONTAP Technical Reports

NetApp
January 23, 2026

This PDF was generated from <https://docs.netapp.com/ko-kr/ontap-technical-reports/zero-trust/zero-trust-overview.html> on January 23, 2026. Always check docs.netapp.com for the latest.

목차

NetApp와 제로 트러스트	1
NetApp와 제로 트러스트	1
Zero Trust란 무엇입니까??	1
보안 리소스	2
ONTAP로 제로 트러스트에 대한 데이터 중심 접근 방식 설계	2
제로 트러스트 데이터 중심 MCAP 설계	2
ONTAP 외부 NetApp 보안 자동화 및 오케스트레이션 제어	6
제로 트러스트 및 하이브리드 클라우드 구축	7

NetApp와 제로 트러스트

NetApp와 제로 트러스트

제로 트러스트는 일반적으로 마이크로 코어 및 주변 장치(MCAP)를 설계하여 데이터, 서비스, 애플리케이션 또는 자산을 세그먼트 게이트웨이라고 하는 제어 기능으로 보호하는 네트워크 중심 접근 방식이었습니다. NetApp ONTAP는 제로 트러스트에 대한 데이터 중심 접근 방식을 취하고 있습니다. 제로 트러스트는 스토리지 관리 시스템이 세분화 게이트웨이가 되어 고객 데이터의 액세스 보호 및 모니터링을 수행합니다. 특히 FPolicy Zero Trust 엔진과 FPolicy 파트너 에코시스템은 정상 및 비정상적인 데이터 액세스 패턴을 세부적으로 이해하고 내부자 위협을 식별하기 위한 제어 센터가 됩니다.



2024년 7월부터 NetApp과 제로 트러스트: 데이터 중심의 제로 트러스트 모델 활성화 _ 의 내용이 docs.netapp.com에서 제공됩니다. 이 모델은 이전에 PDF로 게시되었습니다.

데이터는 조직의 가장 중요한 자산입니다. 2022년 기준 내부자 위협은 데이터 침해의 18%가 원인입니다. ["Verizon 데이터 침해 조사 보고서"](#) 조직은 NetApp ONTAP 데이터 관리 소프트웨어를 사용하여 데이터에 관한 업계 최고 수준의 제로 트러스트 제어를 구현하여 경계를 강화할 수 있습니다.

Zero Trust란 무엇입니까??

제로 트러스트 모델은 Forrester Research의 John Kindervag에 의해 처음 개발되었습니다. 네트워크 보안은 외부에서 들어오는 것이 아니라 내부 외부로부터의 네트워크 보안을 지향합니다. 인사이드아웃 제로 트러스트 방식에서는 마이크로코어 및 경계(MCAP)를 식별합니다. MCAP는 포괄적인 제어 집합으로 보호할 데이터, 서비스, 애플리케이션 및 자산의 내부 정의입니다. 안전한 외주개념은 더 이상 유효하지 않습니다. 신뢰할 수 있고 경계를 통해 성공적으로 인증할 수 있는 엔터티는 조직이 공격에 취약해질 수 있습니다. 내부자는 정의상 이미 보안 경계의 내부에 있습니다. 직원, 계약업체 및 파트너는 내부자이며 조직의 인프라 내에서 역할을 수행하기 위해서는 적절한 제어하에 작업을 수행할 수 있어야 합니다.

제로 트러스트는 2019년 9월 DoD에 약속을 제공하는 기술로 언급되었습니다. ["FY19-23 DoD 디지털 현대화 전략"](#) 제로 트러스트를 데이터 침해를 막기 위해 아키텍처 전체에 보안을 통합하는 사이버 보안 전략인 "로 정의합니다. 이 데이터 중심 보안 모델은 신뢰할 수 있거나 신뢰할 수 없는 네트워크, 장치, 사용자 또는 프로세스의 개념을 없애고, 최소 권한 액세스라는 개념 하에서 인증 및 권한 부여 정책을 가능하게 하는 다중 속성 기반 신뢰 수준으로 전환합니다. 제로 트러스트를 구현하려면 기존 인프라를 사용하여 보안을 구현하는 방법을 보다 간단하고 효율적인 방식으로 설계하고 방해받지 않는 운영을 가능하게 해야 합니다."

2020년 8월 NIST 발표 ["SPECIAL Pub 800-207 제로 트러스트 아키텍처"](#) (ZTA), ZTA는 네트워크 위치가 더 이상 리소스의 보안 태세의 주요 구성 요소로 간주되지 않기 때문에 네트워크 세그먼트가 아닌 리소스 보호에 중점을 둡니다. 리소스는 데이터와 컴퓨팅입니다. ZTA 전략은 엔터프라이즈 네트워크 설계자를 위한 것입니다. ZTA는 원래 Forrester 개념에서 몇 가지 새로운 용어를 소개합니다. PDP(Policy Decision Point)와 PEP(Policy Enforcement Point)라는 보호 메커니즘은 Forrester 세그멘테이션 게이트웨이와 유사합니다. ZTA는 네 가지 배포 모델을 도입합니다.

- 장치 에이전트 또는 게이트웨이 기반 배포
- 독립 기반 구축(Forrester MCAP와 다소 유사함)
- 리소스 포털 기반 배포
- 장치 응용 프로그램 샌드박싱

이 설명서의 목적상 당사는 NIST ZTA 대신 Forrester Research의 개념과 용어를 사용합니다.

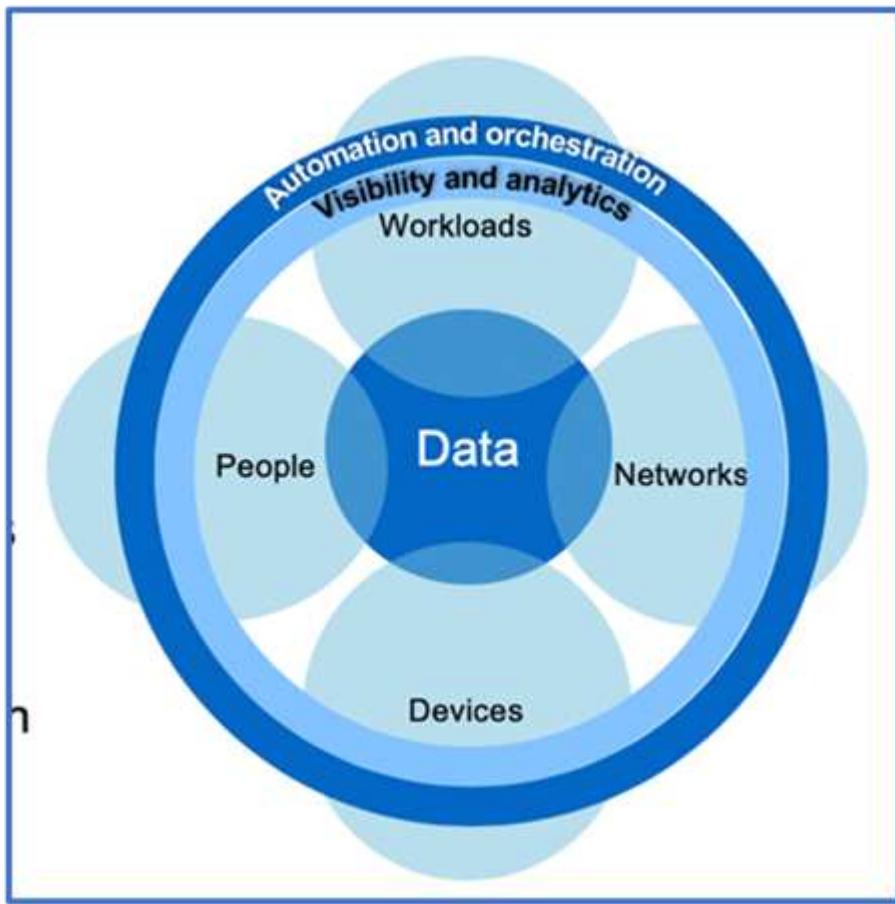
보안 리소스

취약성 및 사고 보고, NetApp 보안 응답 및 고객 기밀성에 대한 자세한 내용은 ["NetApp 보안 포털"](#)을 참조하십시오.

ONTAP로 제로 트러스트에 대한 데이터 중심 접근 방식 설계

제로 트러스트 네트워크는 데이터 중심 접근 방식으로 정의되며, 보안 제어는 데이터와 최대한 가까운 위치에 있어야 합니다. ONTAP의 기능을 NetApp FPolicy 파트너 에코시스템과 결합하여 데이터 중심 제로 트러스트 모델에 필요한 제어 기능을 제공할 수 있습니다.

ONTAP는 NetApp의 보안이 풍부한 데이터 관리 소프트웨어이며, FPolicy 제로 트러스트 엔진은 세부적인 파일 기반 이벤트 알림 인터페이스를 제공하는 업계 최고의 ONTAP 기능입니다. NetApp FPolicy 파트너는 이 인터페이스를 사용하여 ONTAP 내의 데이터 액세스를 더욱 잘 파악할 수 있습니다.



제로 트러스트 데이터 중심 MCAP 설계

데이터 중심의 제로 트러스트 MCAP를 설계하려면 다음 단계를 따르십시오.

1. 모든 조직 데이터의 위치를 식별합니다.
2. 데이터를 분류합니다.
3. 더 이상 필요하지 않은 데이터는 안전하게 폐기합니다.

4. 데이터 분류에 액세스해야 하는 역할을 이해합니다.
5. 최소 권한 원칙을 적용하여 액세스 제어를 적용합니다.
6. 관리 액세스 및 데이터 액세스에 다단계 인증을 사용하십시오.
7. 유휴 데이터와 사용 중인 데이터에 암호화 사용
8. 모든 액세스를 모니터링하고 기록합니다.
9. 의심스러운 액세스 또는 행동을 경고합니다.

모든 조직 데이터의 위치를 식별합니다

ONTAP의 FPolicy 기능과 FPolicy 파트너의 NetApp 제휴 파트너 에코시스템과 결합하여 조직의 데이터가 어디에 있고 누가 액세스하는지를 파악할 수 있습니다. 이 작업은 데이터 액세스 패턴의 유효성 여부를 식별하는 사용자 행동 분석을 통해 수행됩니다. 사용자 행동 분석에 대한 자세한 내용은 모든 액세스 모니터링 및 로그에서 설명합니다. 데이터가 어디에 있고 누가 데이터에 액세스할 수 있는지 모르는 경우 사용자 행동 분석을 통해 경험적 관찰을 통해 분류 및 정책을 수립할 수 있습니다.

데이터를 분류합니다

Zero Trust 모델의 용어로, 데이터 분류에는 유해 데이터를 식별하는 것이 포함됩니다. 유해 데이터는 조직 외부에 노출될 의도가 없는 민감한 데이터입니다. 유해 데이터가 공개되면 규정 준수에 문제가 생기고 조직의 평판이 손상될 수 있습니다. 규정 준수 측면에서 독성 데이터에는 카드 소지자 데이터가 포함됩니다. "[PCI-DSS\(Payment Card Industry Data Security Standard\)](#)" , EU의 개인 데이터 "[일반 데이터 보호 규정\(GDPR\)](#)" 또는 의료 데이터 "[HIPAA\(Health Insurance Portability and Accountability Act\)](#)" . NetApp 사용할 수 있습니다 "[NetApp Data Classification](#)" (이전 명칭: Cloud Data Sense)는 데이터를 자동으로 스캔, 분석, 분류하는 AI 기반 툴킷입니다.

더 이상 필요하지 않은 데이터는 안전하게 폐기합니다

조직의 데이터를 분류한 후 일부 데이터가 더 이상 필요하지 않거나 조직의 기능과 관련이 없다는 것을 알게 될 수 있습니다. 불필요한 데이터의 보유는 책임이며, 그러한 데이터는 삭제되어야 한다. 데이터를 암호화하여 삭제하는 고급 메커니즘은 저장된 데이터 암호화의 보안 삭제 설명을 참조하십시오.

데이터 분류에 액세스해야 하는 역할을 이해하고 액세스 제어를 적용하기 위해 최소 권한 원칙을 적용합니다

중요한 데이터에 대한 액세스를 매팅하고 최소 권한 원칙을 적용하면 조직 내 사용자가 작업을 수행하는 데 필요한 데이터만 액세스할 수 있습니다. 이 프로세스에는 역할 기반 액세스 제어가 포함되는데, 이 제어는 ("[RBAC](#)" 데이터 액세스 및 관리 액세스에 적용됩니다.

ONTAP를 사용하면 스토리지 가상 머신(SVM)을 ONTAP 클러스터 내의 테넌트가 조직 데이터 액세스를 분할하는 데 사용할 수 있습니다. RBAC는 데이터 액세스뿐만 아니라 SVM에 대한 관리 액세스에도 적용할 수 있습니다. RBAC는 클러스터 관리 레벨에서 적용할 수도 있습니다.

RBAC와 더불어 MAV(ONTAP)를 사용하면 한 명 이상의 관리자가 또는 같은 명령을 승인하도록 할 수 있습니다 "[다중 관리자 인증](#)" volume delete volume snapshot delete. MAV가 활성화되면 MAV를 수정하거나 사용하지 않도록 하려면 MAV 관리자의 승인이 필요합니다.

스냅샷을 보호하는 또 다른 방법은 ONTAP를 "[스냅샷 잠금](#)" 사용하는 것입니다. 스냅샷 잠금은 볼륨 스냅샷 정책에 대한 보존 기간에 수동 또는 자동으로 스냅샷을 지울 수 없는 SnapLock 기능입니다. 스냅샷 잠금은 무단 변경 방지 스냅샷 잠금이라고도 합니다. 스냅샷 잠금의 목적은 악의적인 관리자 또는 신뢰할 수 없는 관리자가 운영 및 보조 ONTAP 시스템에서 스냅샷을 삭제하지 못하도록 하는 것입니다. 랜섬웨어에 의해 손상된 볼륨을 복원하기 위해 기본 시스템에서 잠긴 스냅샷의 신속한 복구를 수행할 수 있습니다.

관리 액세스 및 데이터 액세스에 다단계 인증을 사용하십시오

클러스터 관리 RBAC 외에도 "[다단계 인증\(MFA\)](#)" ONTAP 웹 관리 액세스 및 SSH(Secure Shell) 명령줄 액세스용으로 구축할 수 있습니다. 관리 액세스를 위한 MFA는 미국 공공 부문 조직 또는 PCI-DSS를 준수해야 하는 조직의 요구 사항입니다. MFA를 사용하면 공격자가 사용자 이름과 암호만 사용하여 계정을 손상시킬 수 없습니다. MFA를 인증하려면 두 개 이상의 독립적인 요소가 필요합니다. 2단계 인증의 예로는 개인 키와 같이 사용자가 소유한 것과 암호 등 사용자가 알고 있는 것을 들 수 있습니다. ONTAP System Manager 또는 ActiveIQ Unified Manager에 대한 관리 웹 액세스는 SAML(Security Assertion Markup Language) 2.0을 통해 활성화됩니다. SSH 명령줄 액세스는 공개 키 및 암호와 함께 연결된 2단계 인증을 사용합니다.

ONTAP의 ID 및 액세스 관리 기능을 사용하여 API를 통해 사용자 및 시스템 액세스를 제어할 수 있습니다.

- 사용자:
 - 인증 및 권한 부여 SMB 및 NFS용 NAS 프로토콜 기능을 사용합니다.
 - * 감사 * 액세스 및 이벤트의 syslog. 인증 및 권한 부여 정책을 테스트하기 위한 CIFS 프로토콜에 대한 자세한 감사 로깅 파일 수준에서 세부적인 NAS 액세스에 대한 FPolicy 감사
- 장치:
 - * 인증. * API 액세스를 위한 인증서 기반 인증.
 - * 승인. * 기본 또는 맞춤형 역할 기반 액세스 제어(RBAC)
 - * 감사 * 수행한 모든 작업의 syslog.

유휴 데이터와 사용 중인 데이터에 암호화 사용

유휴 데이터의 암호화

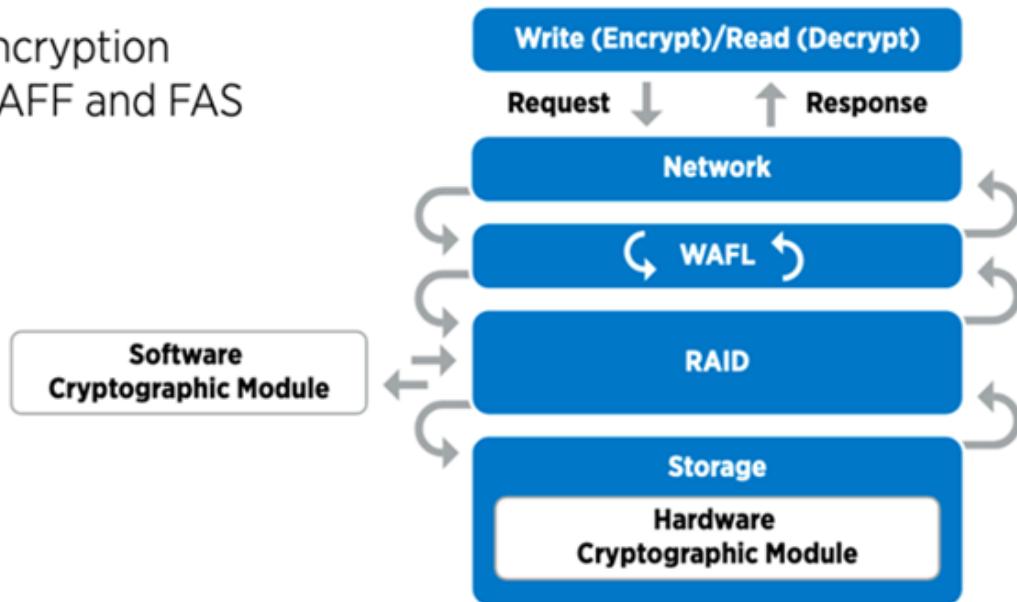
조직에서 드라이브의 용도를 변경하거나 결함 있는 드라이브를 반환하거나 판매 또는 거래하여 대용량 드라이브로 업그레이드하는 경우, 스토리지 시스템의 위험과 인프라 격차를 줄이기 위한 새로운 요구사항이 있습니다. 스토리지 엔지니어는 데이터의 관리자이자 운영자로서 라이프사이클 전반에서 데이터를 안전하게 관리하고 유지해야 합니다.

["NetApp 스토리지 암호화\(NSE\) 및 AMP, #44, NetApp 볼륨 암호화\(NVE\) 및 AMP, #44, NetApp 애그리게이트 암호화"](#) 독성 여부와 관계없이 일상 작업에 영향을 주지 않고 유휴 데이터를 항상 암호화할 수 있도록 지원합니다. "NSE를 선택합니다"는 FIPS 140-2 레벨 2 검증된 자체 암호화 드라이브를 사용하는 ONTAP 하드웨어 ["사용되지 않는 데이터"](#) 솔루션입니다. "NVE와 NAE"는 를 사용하는 ONTAP 소프트웨어 ["사용되지 않는 데이터"](#) ["FIPS 140-2 Level 1 검증 NetApp 암호화 모듈"](#) 솔루션입니다. NVE와 NAE에서는 하드 드라이브 또는 Solid State Drive를 유휴 데이터 암호화에 사용할 수 있습니다. 또한 NSE 드라이브를 사용하여 암호화 이중화와 추가 보안을 제공하는 네이티브 계층화된 암호화 솔루션을 제공할 수 있습니다. 한 계층이 침해되더라도 두 번째 계층은 여전히 데이터를 보호합니다. 이러한 기능을 통해 ONTAP은 [에 대한 유리한 위치를 점할 수 "양자 지원 암호화"](#) 있습니다.

NVE는 기밀 파일이 기밀이 아닌 볼륨에 작성될 때 데이터 유출로부터 독성 데이터를 암호화 방식으로 제거하는 기능을 ["안전한 제거"](#) 제공합니다.

ONTAP에 내장된 키 관리자인 [를 "온보드 키 관리자\(OKM\)"](#) 사용하거나 ["승인됨"](#) , NSE 및 NVE와 함께 타사 ["외부 키 관리자"](#) 를 사용하여 키 자료를 안전하게 저장할 수 있습니다.

Two-layer encryption solution for AFF and FAS



위의 그림에서 볼 수 있듯이 하드웨어 및 소프트웨어 기반 암호화를 결합할 수 있습니다. 이 기능으로 인해는 "기밀 프로그램을 위한 NSA의 상용 솔루션에 대한 ONTAP 검증" 최고 비밀 데이터를 저장할 수 있게 되었습니다.

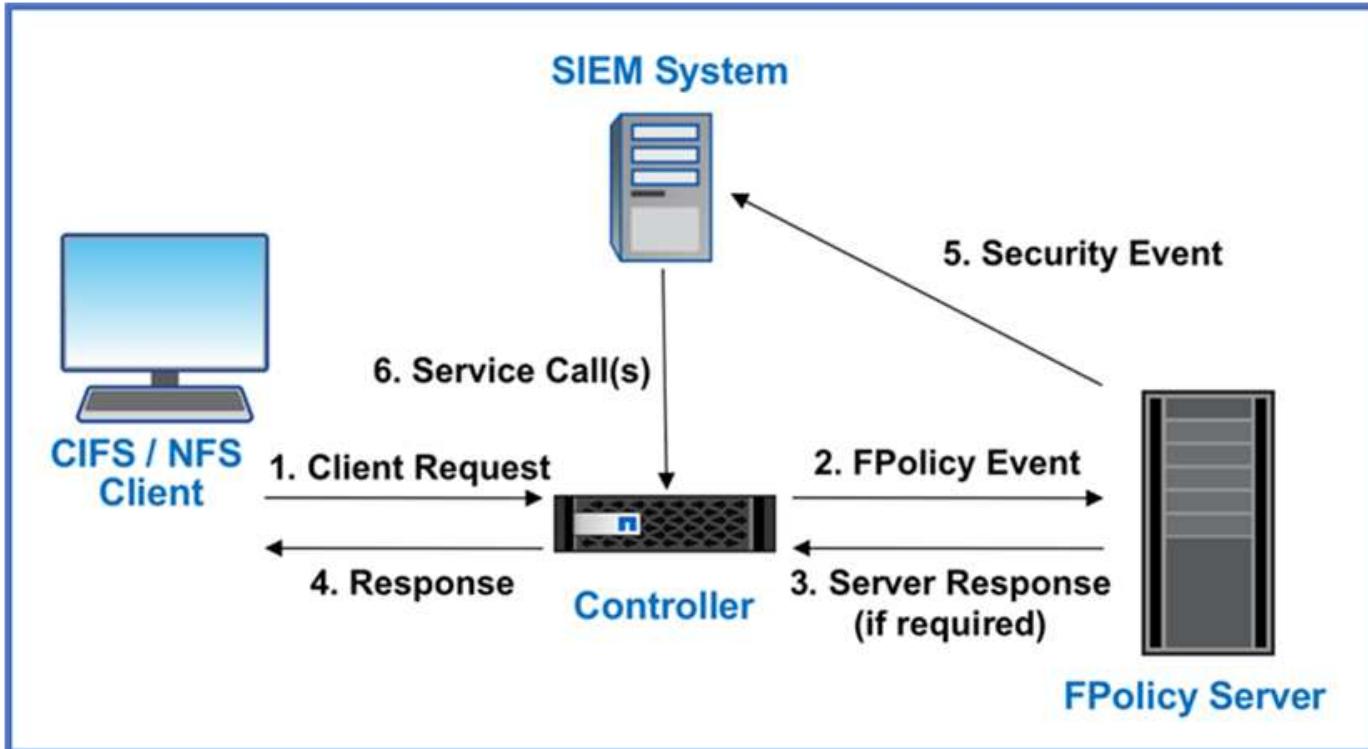
전송 중인 데이터 암호화

ONTAP의 전송 중인 데이터 암호화는 사용자 데이터 액세스 및 제어 플레이 액세스를 보호합니다. 사용자 데이터 액세스는 Microsoft CIFS 공유 액세스의 경우 SMB 3.0 암호화 또는 NFS Kerberos 5의 경우 krb5P로 암호화될 수 있습니다. CIFS, NFS 및 iSCSI에 대해 사용자 데이터 액세스를 암호화할 수도 "[IPsec을 선택합니다](#)" 있습니다. 컨트롤 플레이 액세스는 TLS(Transport Layer Security)로 암호화됩니다. ONTAP는 제어 플레이 액세스를 위한 규정 준수 모드를 제공하여 "[FIPS를 참조하십시오](#)" FIPS 승인 알고리즘을 활성화하고 FIPS가 승인되지 않은 알고리즘을 비활성화합니다. 데이터 복제는 로 암호화됩니다. "[클러스터 피어 암호화](#)" ONTAP SnapVault 및 SnapMirror 기술에 대한 암호화를 제공합니다.

모든 액세스를 모니터링하고 기록합니다

RBAC 정책을 적용한 후에는 활성 모니터링, 감사 및 알림을 배포해야 합니다. NetApp ONTAP의 FPolicy 제로 트러스트 엔진을 과 결합하여 "[NetApp FPolicy 파트너 에코시스템](#)" 데이터 중심 제로 트러스트 모델에 필요한 제어 기능을 제공합니다. NetApp ONTAP는 보안이 풍부한 데이터 관리 소프트웨어이며 "[FPolicy를 참조하십시오](#)" , 세부적인 파일 기반 이벤트 알림 인터페이스를 제공하는 업계 최고의 ONTAP 기능입니다. NetApp FPolicy 파트너는 이 인터페이스를 사용하여 ONTAP 내의 데이터 액세스를 더욱 잘 파악할 수 있습니다. ONTAP의 FPolicy 기능과 FPolicy 파트너의 NetApp 제휴 파트너 에코시스템과 결합하여 조직의 데이터가 어디에 있고 누가 액세스하는지를 파악할 수 있습니다. 이 작업은 데이터 액세스 패턴의 유효성 여부를 식별하는 사용자 행동 분석을 통해 수행됩니다. 사용자 행동 분석을 사용하여 정상적인 패턴에서 벗어난 의심스럽거나 잘못된 데이터 액세스를 경고하고 필요한 경우 액세스를 거부하기 위한 조치를 취할 수 있습니다.

FPolicy 파트너는 사용자 행동 분석을 넘어 머신 러닝(ML) 및 인공 지능(AI)으로 이동하여 이벤트 충실도를 높이고 오탐률을 줄이고 있습니다. 모든 이벤트는 syslog 서버 또는 ML 및 AI를 활용할 수 있는 SIEM(Security Information and Event Management) 시스템에 로깅해야 합니다.



NetApp의 ["DII 스토리지 워크로드 보안"](#) 클라우드와 온프레미스 ONTAP 스토리지 시스템 모두에서 FPolicy 인터페이스와 사용자 행동 분석을 활용하여 악의적인 사용자 행동에 대한 실시간 알림을 제공합니다. 스토리지 워크로드 보안은 고급 머신 러닝과 이상 감지를 통해 악의적이거나 손상된 사용자가 조직 데이터를 오용하는 것을 방지합니다. 스토리지 워크로드 보안은 랜섬웨어 공격이나 기타 악의적인 행위를 식별하고 스냅샷을 호출하고 악의적인 사용자를 격리할 수 있습니다. 스토리지 워크로드 보안에는 사용자 및 엔터티 활동을 매우 자세히 볼 수 있는 포렌식 기능도 있습니다. 스토리지 워크로드 보안은 NetApp Data Infrastructure Insights 의 일부입니다.

ONTAP에는 스토리지 워크로드 보안뿐만 아니라 (ARP)라고 하는 온보드 랜섬웨어 감지 기능이 ["자율 랜섬웨어 보호"](#) 있습니다. ARP는 머신 러닝을 사용하여 비정상적인 파일 활동이 랜섬웨어 공격이 진행 중임을 나타내고 스냅샷을 호출하고 관리자에게 경고를 보냅니다. 스토리지 워크로드 보안은 ONTAP와 통합되어 ARP 이벤트를 수신하고 추가적인 분석 및 자동 응답 계층을 제공합니다.

이 절차에서 설명하는 명령에 대한 자세한 내용은 ["ONTAP 명령 참조입니다"](#) 참조하십시오.

ONTAP 외부 NetApp 보안 자동화 및 오케스트레이션 제어

자동화를 통해 최소한의 인적 지원만으로 프로세스 또는 절차를 수행할 수 있습니다. 조직은 자동화를 통해 제로 트러스트 구축을 수동 절차를 훨씬 넘어 확장할 수 있으므로 자동화되는 악의적인 활동을 방지할 수 있습니다.

Ansible은 오픈 소스 소프트웨어 프로비저닝, 구성 관리 및 애플리케이션 배포 툴입니다. 많은 유닉스와 유사한 시스템에서 실행되며, 유닉스와 유사한 시스템과 Microsoft Windows를 모두 구성할 수 있습니다. 시스템 구성 설명하는 고유한 선언적 언어가 포함되어 있습니다. Ansible은 Michael DeHaan이 작성했으며 2015년에 Red Hat에 인수되었습니다. Ansible은 에이전트가 없습니다. SSH 또는 Windows 원격 관리를 통해 일시적으로 원격으로 연결하여 원격 PowerShell 실행 허용을 수행할 수 있습니다. NetApp은 그 이상을 개발했으며 ["ONTAP 소프트웨어 Ansible 모듈 150개"](#) Ansible 자동화 프레임워크와 추가적인 통합을 가능하게 했습니다. NetApp용 Ansible 모듈은 원하는 상태를 정의하고 타겟 NetApp 환경에 전달하는 방법에 관한 일련의 지침을 제공합니다. 이들 모듈은 라이센스 설정, 애그리게이트 및 스토리지 가상 머신 생성, 볼륨 생성, 스냅샷 복원 등의 작업을 지원할 목적으로 개발되었습니다. Ansible 역할은 NetApp DoD UC(Unified Capabilities ["GitHub에 게시되었습니다"](#)) 배포 가이드에 따라 다릅니다.

사용자는 사용 가능한 모듈 라이브러리를 통해 쉽게 Ansible 플레이북을 개발하고 고유한 애플리케이션 및 비즈니스 요구사항에 맞게 맞춤화하여 일상적인 작업을 자동화할 수 있습니다. 플레이북을 작성한 후 특정 작업을 수행하도록 실행하면 시간이 절약되고 생산성이 향상됩니다. NetApp은 직접 사용하거나 필요에 맞게 맞춤화할 수 있는 샘플 플레이북을 마련하여 공유했습니다.

Data Infrastructure Insights 는 전체 인프라에 대한 가시성을 제공하는 인프라 모니터링 도구입니다. Data Infrastructure Insights 사용하면 퍼블릭 클라우드 인스턴스와 프라이빗 데이터 센터를 포함한 모든 리소스를 모니터링하고, 문제를 해결하고, 최적화할 수 있습니다. Data Infrastructure Insights 해결에 걸리는 평균 시간을 90%까지 단축하고 클라우드 문제의 80%가 최종 사용자에게 영향을 미치지 않도록 예방할 수 있습니다. 또한 실행 가능한 인텔리전스로 데이터를 보호함으로써 클라우드 인프라 비용을 평균 33% 절감하고 내부 위협에 대한 노출도 줄일 수 있습니다. Data Infrastructure Insights 의 스토리지 워크로드 보안 기능을 사용하면 AI와 ML을 활용한 사용자 행동 분석을 통해 내부 위협으로 인해 비정상적인 사용자 행동이 발생할 때 경고를 받을 수 있습니다. ONTAP 의 경우, 스토리지 워크로드 보안은 Zero Trust FPolicy 엔진을 활용합니다.

제로 트러스트 및 하이브리드 클라우드 구축

NetApp 은 하이브리드 클라우드의 데이터 권위자입니다. NetApp Amazon Web Services(AWS), Microsoft Azure, Google Cloud 및 기타 주요 클라우드 공급업체와 협력하여 온프레미스 데이터 관리 시스템을 하이브리드 클라우드로 확장하기 위한 다양한 옵션을 제공합니다. NetApp 하이브리드 클라우드 솔루션은 온프레미스 ONTAP 시스템 및 ONTAP Select 소프트웨어 정의 스토리지에서 사용할 수 있는 것과 동일한 Zero Trust 보안 제어를 지원합니다.

AWS(FSxN), Google Cloud(GCNV), Microsoft Azure용 Azure NetApp Files 등 엔터프라이즈급 클라우드 기반 파일 서비스를 사용하면 일반적인 CAPEX 제약 없이 퍼블릭 클라우드에서 용량을 쉽게 확장할 수 있습니다. 분석 및 DevOps와 같은 데이터 집약적 워크로드에 적합한 이러한 클라우드 데이터 서비스는 NetApp 의 탄력적인 온디맨드 스토리지 서비스와 ONTAP 데이터 관리를 완벽하게 관리되는 제품으로 결합합니다.

ONTAP NetApp SnapMirror 데이터 복제 소프트웨어를 통해 온프레미스 ONTAP 시스템과 AWS, Google Cloud 또는 Azure 스토리지 환경 간에 데이터를 이동할 수 있도록 합니다.

저작권 정보

Copyright © 2026 NetApp, Inc. All Rights Reserved. 미국에서 인쇄됨 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그레픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이센스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 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 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이센스도 제공하지 않습니다.

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

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이센스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이센스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

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.