제로 트러스트 모델을 사용합니다

ONTAP 9

NetApp
July 12, 2024

목차

제로 트러스트 모델을 사용합니다

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 지원 _ 의 내용이 ONTAP 제품 설명서의 나머지 부분과 통합되었습니다. 이 내용은 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 Research에서 처음 "존 킨더바그" 개발했습니다. 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 위해 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 활용해 보안을 구현하는 방법을 더 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.

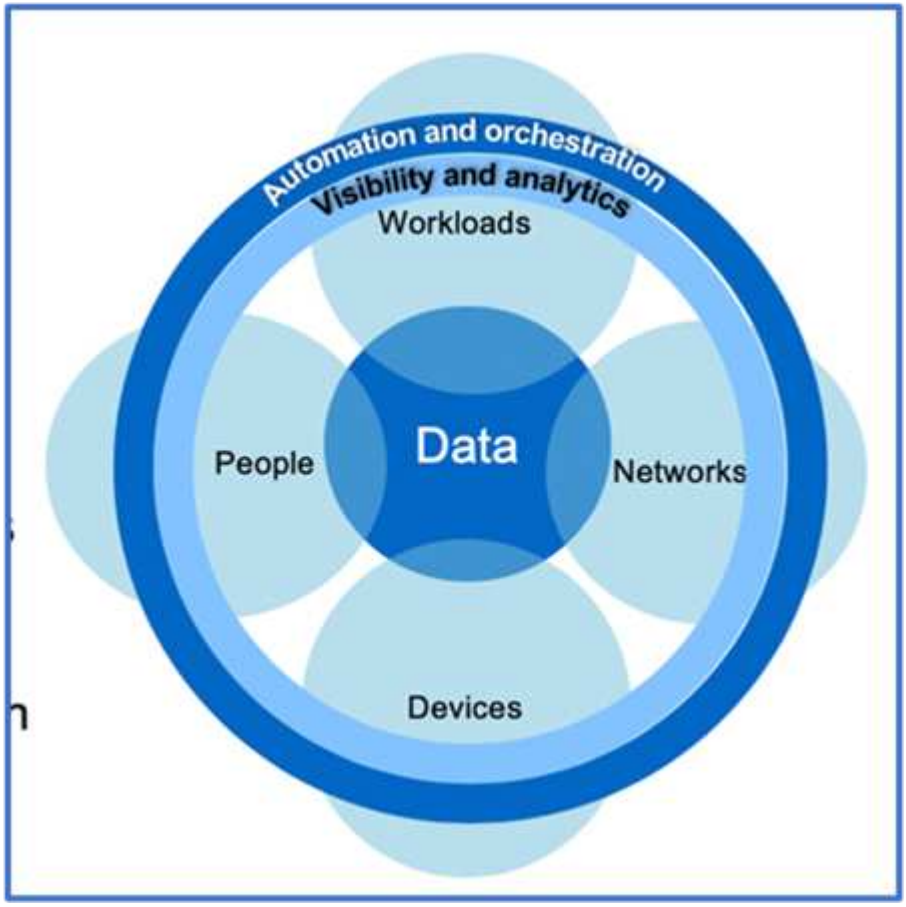
보안 리소스

취약성 및 사고 보고, NetApp 보안 응답 및 고객 기밀성에 대한 자세한 내용은 를 참조하십시오 "NetApp 보안 포털".

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 모델 용어에서 데이터 분류에는 독성 데이터의 식별이 포함됩니다. 독성 데이터는 조직 외부에 노출되지 않도록 설계된 중요 데이터입니다. 독성 데이터를 공개하면 규정 준수 위반을 초래하고 조직의 평판을 훼손할 수 있습니다. 규정 준수 측면에서 독성 데이터에는 에 대한 카드 소유자 데이터 "PCI-DSS(Payment Card Industry Data Security Standard)", EU의 개인 데이터 "일반 데이터 보호 규정(GDPR)"또는 에 대한 의료 데이터가 "HIPAA(Health Insurance Portability and Accountability Act)"포함됩니다. AI 기반 툴킷인 NetApp(이전의 Cloud Data Sense)를 사용하여 데이터를 자동으로 스캔, 분석, 범주화할 수 있습니다 "BlueXP 분류" .

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 매핑하고 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.

ONTAP를 사용하여 스냅샷 복사본을 보호하는 또 다른 "스냅샷 복사본 잠금"방법입니다. 스냅샷 복사본 잠금은 볼륨 스냅샷 복사본 정책에 대한 보존 기간을 두고 수동으로 또는 자동으로 스냅샷 복사본을 지울 수 없는 SnapLock 기능입니다. 스냅샷 복사본 잠금은 무단 조작 방지 스냅샷 복사본 잠금이라고도 합니다. 스냅샷 복사본 잠금의 목적은 악성 또는 신뢰할 수 없는 관리자가 1차 및 2차 ONTAP 시스템에서 스냅샷 복사본을 삭제하지 못하도록 방지하는 것입니다. 랜섬웨어에 의해 손상된 볼륨을 복원하기 위해 기본 시스템에서 잠겨 있는 Snapshot 복사본을 신속하게 복구할 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.

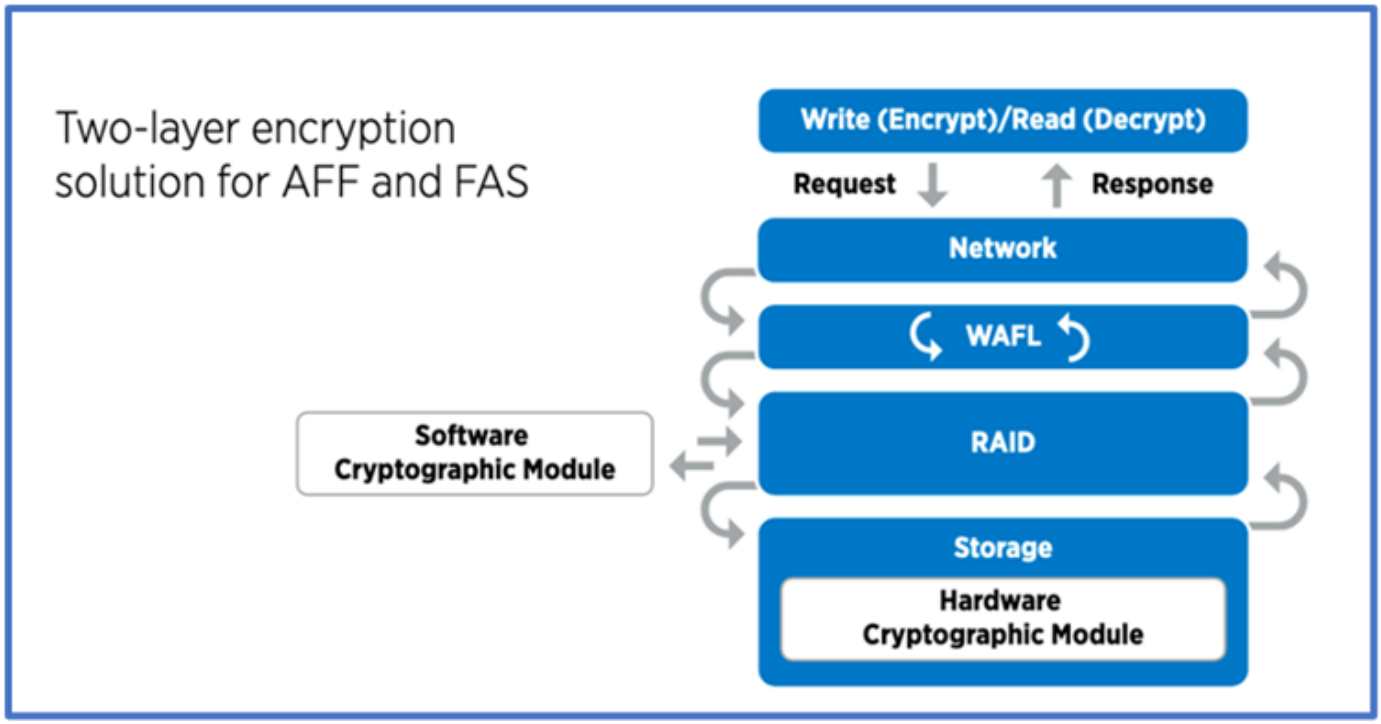
유휴 데이터와 사용 중인 데이터에 암호화 사용

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 ONTAP FIPS 140-2 level 2 검증된 자체 암호화 드라이브를 사용하는 유휴 데이터 솔루션입니다. "NVE와 NAE" 는 를 활용하는 ONTAP의 유휴 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.



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

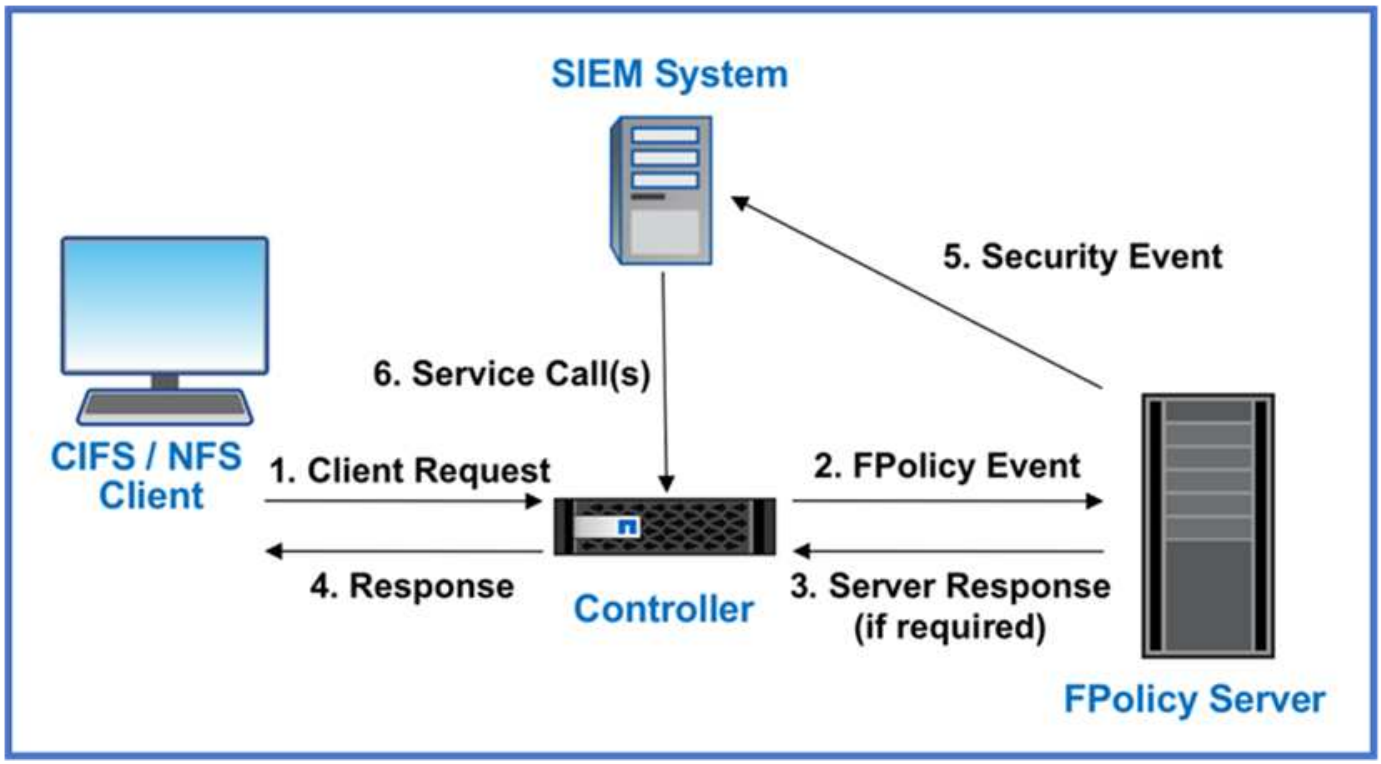
전송 중인 데이터 암호화

ONTAP의 전송 중인 데이터 암호화는 사용자 데이터 액세스 및 제어 플레인 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 플레인 액세스는 TLS(Transport Layer Security)로 암호화됩니다. ONTAP는 제어 플레인 액세스를 위한 규정 준수 모드를 제공하여 "FIPS 를 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 스토리지 워크로드 보안(이전 명칭 "Cloud Secure")은 클라우드와 온프레미스 ONTAP 스토리지 시스템 모두에서 FPolicy 인터페이스와 사용자 행동 분석을 사용하여 악의적인 사용자 행동에 대한 실시간 경고를 제공합니다. 스토리지 워크로드 보안은 악의적인 사용자 또는 보안을 침해하는 사용자가 조직 데이터를 악용하지 못하도록 고급 머신 러닝 및 이상 징후 탐지를 통해 보호합니다. 스토리지 워크로드 보안은 랜섬웨어 공격 또는 기타 악의적인 행동을 식별하고 스냅샷 복사본을 호출하고 악의적인 사용자를 격리할 수 있습니다. 스토리지 워크로드 보안에는 사용자 및 엔터티 활동을 자세히 볼 수 있는 포렌식 기능도 있습니다. 스토리지 워크로드 보안은 NetApp Cloud Insights의 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 스냅샷 복사본을 호출하여 관리자에게 경고를 보냅니다. 스토리지 워크로드 보안은 ONTAP와 통합되어 ARP 이벤트를 수신하고 추가적인 분석 및 자동 응답 계층을 제공합니다.

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 구성을 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 허용 을 수행할 수 있습니다. NetApp은 그 이상을 개발했으며 "ONTAP 소프트웨어용 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.

Cloud Insights는 전체 인프라에 대한 가시성을 제공하는 인프라 모니터링 툴입니다. Cloud Insights를 사용하면 퍼블릭 클라우드 인스턴스 및 프라이빗 데이터 센터를 비롯한 모든 리소스에 대한 모니터링, 문제 해결 및 최적화 작업을 수행할 수 있습니다. Cloud Insights는 평균 해결 시간을 90% 단축하고 최종 사용자에게 영향을 미치는 클라우드 문제를 80% 예방합니다. 또한, 실행 가능한 인텔리전스로 데이터를 보호하여 클라우드 인프라 비용을 평균 33% 절감하고 내부자 위협에 대한 노출을 줄일 수 있습니다. Cloud Insights의 스토리지 워크로드 보안 기능을 사용하면 내부자 위협으로 인해 비정상적인 사용자 행동이 발생할 경우 AI 및 ML을 통한 사용자 행동 분석을 수행할 수 있습니다. ONTAP의 경우 스토리지 워크로드 보안은 제로 트러스트 FPolicy 엔진을 사용합니다.

제로 트러스트 및 하이브리드 클라우드 구축

NetApp은 하이브리드 클라우드 환경에서 데이터 관련 최고의 권위자입니다. NetApp은 AWS(Amazon Web Services), Microsoft Azure, GCP(Google Cloud Platform) 및 기타 주요 클라우드 제공업체를 통해 온프레미스 데이터 관리 시스템을 하이브리드 클라우드로 확장할 수 있는 다양한 옵션을 제공합니다. NetApp 하이브리드 클라우드 솔루션은 사내 ONTAP 시스템 및 ONTAP Select 소프트웨어 정의 스토리지에서 사용할 수 있는 동일한 제로 트러스트 보안 제어를 지원합니다.

AWS 및 GCP용 최초의 엔터프라이즈급 클라우드 네이티브 파일 서비스인 NetApp Cloud Volumes Service 및 Microsoft Azure용 Azure NetApp Files를 사용하여 일반적인 설비 투자의 제한 없이 퍼블릭 클라우드의 용량을 쉽게 확장할 수 있습니다. 이러한 클라우드 데이터 서비스는 분석 및 DevOps와 같은 데이터 집약적인 워크로드에 이상적이며, NetApp의 탄력적인 온 디맨드 서비스형 스토리지와 ONTAP 데이터 관리를 결합하여 완벽하게 관리됩니다.

AWS EBS, S3 또는 Azure 스토리지와 같은 클라우드 블록 또는 오브젝트 스토리지 서비스를 위한 고급 데이터 서비스를 원하는 고객을 위해 Cloud Volumes ONTAP은 사내 환경과 퍼블릭 클라우드 간의 데이터 관리를 단일 공통 뷰로 제공합니다. 온디맨드 인스턴스로 AWS 또는 Azure에서 실행되는 Cloud Volumes ONTAP은 ONTAP 소프트웨어의 스토리지 효율성, 가용성 및 확장성을 제공합니다. ONTAP은 NetApp SnapMirror 데이터 복제 소프트웨어를 통해 사내 ONTAP 시스템과 AWS 또는 Azure 스토리지 환경 간에 데이터를 이동할 수 있도록 지원합니다.

ONTAP 제로 트러스트 콘텐츠에 대해 자세히 알아보십시오

ONTAP 제로 트러스트 콘텐츠에 설명된 정보에 대한 자세한 내용은 다음 문서 및/또는 웹 사이트를 참조하십시오.

- "Verizon 데이터 침해 조사 보고서"
- "DoD 디지털 현대화 전략"
- "NIST SP 800-207 제로 트러스트 아키텍처"
- "NetApp Partner Connect: 보안 제휴 파트너"
- "SVM에서 파일 모니터링 및 관리에 FPolicy 사용"
- "PCI-DSS 3.2 ONTAP 9"
- "일반 데이터 보호 규정(GDPR)"

- "HIPPA 개인 정보 보호 규칙 요약"
- "NetApp BlueXP 분류"
- "다중 관리 검증"
- "스냅샷 복사본의 무단 잠금 방지"
- "ONTAP 9의 다단계 인증"
- "NetApp 스토리지 암호화, NVMe 자체 암호화 드라이브, NetApp 볼륨 암호화 및 NetApp 애그리게이트 암호화"
- "NetApp 스토리지 암호화"
- "NetApp 볼륨 암호화 및 NetApp 애그리게이트 암호화"
- "NetApp 암호화 모듈 FIPS-140-2 인증서"
- "NetApp의 Quantum Ready 유휴 데이터 암호화"
- "보안을 통한 혁신: NetApp과 Ontrack이 Flash Memory Summit Award를 수상했습니다"
- "온보드 키 관리 활성화"
- "NetApp 상호 운용성 매트릭스 툴"
- "외부 키 관리를 구성하는 중입니다"
- "분류용 상업 솔루션"
- "ONTAP IPsec입니다"
- "FIPS 모드를 사용하도록 보안 구성을 수정합니다"
- "기존 피어 관계에서 클러스터 피어링 암호화 활성화"
- "스토리지 워크로드 보안(Cloud Secure)"
- "NetApp 및 Ansible로 개발 작업 흐름 자동화를 시작하십시오"
- "NetApp DoD UC(Unified Capabilities) 배포 가이드 전용 Ansible 모듈입니다"
- "관리자 인증 및 RBAC"
- "ONTAP 유휴 데이터 암호화"
- "TR-4569 NetApp ONTAP 9 보안 강화 가이드"