릴리스 정보

BlueXP ransomware protection

NetApp
December 20, 2024

This PDF was generated from https://docs.netapp.com/ko-kr/bluexp-ransomware-protection/whats-new.html on December 20, 2024. Always check docs.netapp.com for the latest.

목차

릴리스 정보

BlueXP 랜섬웨어 방어의 새로운 기능

BlueXP 랜섬웨어 보호의 새로운 기능에 대해 알아보십시오.

2024년 12월 16일

Data Infrastructure Insights 스토리지 워크로드 보안을 사용하여 비정상적인 사용자 행동을 감지합니다

이 릴리즈에서는 Data Infrastructure Insights 스토리지 워크로드 보안을 사용하여 스토리지 워크로드에서 비정상적인 사용자 행동을 감지할 수 있습니다. 이 기능을 사용하면 잠재적 보안 위협을 식별하고 악의적인 사용자를 차단하여 데이터를 보호할 수 있습니다.

자세한 내용은 을 "감지된 랜섬웨어 경고에 대응합니다"참조하십시오.

데이터 인프라 인사이트 스토리지 워크로드 보안을 사용하여 비정상적인 사용자 행동을 감지하기 전에 BlueXP 랜섬웨어 방지 * 설정 * 옵션을 사용하여 옵션을 구성해야 합니다.

을 "BlueXP 랜섬웨어 보호 설정을 구성합니다"참조하십시오.

검색하고 보호할 워크로드를 선택하십시오

이 릴리스에서는 이제 다음을 수행할 수 있습니다.

- 각 커넥터 내에서 워크로드를 검색할 작업 환경을 선택합니다. 사용자 환경에서 특정 워크로드를 보호하려는 경우 이 기능을 유용하게 사용할 수 있습니다.
- 워크로드 검색 중에 커넥터별 워크로드를 자동으로 검색할 수 있습니다. 이 기능을 통해 보호할 워크로드를 선택할 수 있습니다.
- 이전에 선택한 작업 환경에 대해 새로 생성된 워크로드를 검색합니다.

을 "워크로드 검색"참조하십시오.

2024년 11월 7일

데이터 분류 활성화 및 개인 식별 정보**(PII)** 검색

이번 릴리즈에서는 BlueXP 제품군의 핵심 구성 요소인 BlueXP 분류를 사용하여 파일 공유 작업 부하에서 데이터를 스캔하고 분류할 수 있습니다. 데이터를 분류하면 데이터에 개인 정보가 포함되어 있는지 아니면 개인 정보가 포함되어 있는지 식별하는 데 도움이 되므로 보안 위험이 증가할 수 있습니다. 또한 이 프로세스는 작업 부하의 중요도에 영향을 미치며 적절한 수준의 보호를 통해 워크로드를 보호합니다.

BlueXP 랜섬웨어 보호에서 PII 데이터를 검사하는 것은 일반적으로 BlueXP 분류를 구축한 고객에게 사용할 수 있습니다. BlueXP 분류는 BlueXP 플랫폼의 일부로 추가 비용 없이 사용할 수 있으며 사내 또는 고객 클라우드에 구축할 수 있습니다.

을 "BlueXP 랜섬웨어 보호 설정을 구성합니다"참조하십시오.

스캔을 시작하려면 보호 페이지에서 개인 정보 노출 열에 있는 * 노출 식별 * 을 클릭합니다.

"BlueXP 분류를 사용하여 개인 식별이 가능한 중요 데이터를 검색합니다"..

SIEM과 **Microsoft Sentinel** 통합

이제 Microsoft Sentinel을 사용하여 보안 및 이벤트 관리 시스템(SIEM)에 데이터를 전송하여 위협 분석 및 감지를 수행할 수 있습니다. 이전에는 AWS Security Hub 또는 Splunk Cloud를 SIEM으로 선택할 수 있었습니다.

"BlueXP 랜섬웨어 차단 설정 구성 에 대해 자세히 알아보십시오"..

30일 무료 평가판을 사용해 보십시오

이 릴리즈에서 새로운 BlueXP 랜섬웨어 방지 솔루션을 배포한 경우 30일 무료 평가판이 제공됩니다. 이전에는 BlueXP 랜섬웨어 방어 기능이 90일 무료 평가판으로 제공되었습니다. 이미 90일 무료 평가판을 사용 중인 경우 이 혜택은 90일 동안 계속됩니다.

Podman의 파일 레벨에서 애플리케이션 워크로드 복원

파일 수준에서 애플리케이션 워크로드를 복원하기 전에 공격의 영향을 받았을 수 있는 파일 목록을 보고 복원할 파일을 식별할 수 있습니다. 이전에는 조직의 BlueXP 커넥터(이전의 계정)가 Podman을 사용하고 있었다면 이 기능을 사용할 수 없었습니다. 이제 Podman에서 사용할 수 있습니다. BlueXP 랜섬웨어 방어 기능으로 복원할 파일을 선택하거나, 경고의 영향을 받은 모든 파일이 나열된 CSV 파일을 업로드하거나, 복원할 파일을 수동으로 식별할 수 있습니다.

"랜섬웨어 공격으로부터 복구하는 방법에 대해 자세히 알아보십시오"..

2024년 9월 30일

파일 공유 워크로드의 사용자 지정 그룹화

이 릴리스에서는 이제 파일 공유를 그룹으로 그룹화하여 데이터 자산을 보다 쉽게 보호할 수 있습니다. 이 서비스는 그룹의 모든 볼륨을 동시에 보호할 수 있습니다. 이전에는 각 볼륨을 별도로 보호해야 했습니다.

"랜섬웨어 방어 전략에서 파일 공유 워크로드를 그룹화하는 방법에 대해 자세히 알아보십시오"..

2024년 9월 2일

Digital Advisor의 보안 위험 평가

BlueXP 랜섬웨어 방어는 이제 NetApp Digital Advisor에서 클러스터와 관련된 높은 중요 보안 위험에 대한 정보를 수집합니다. 위험이 발견되면 BlueXP 랜섬웨어 방어는 대시보드의 * 권장 작업 * 창에서 "클러스터 <name>에서 알려진 보안 취약점을 해결합니다."라는 권장 사항을 제공합니다. 대시보드의 권장 사항에서 * 검토 및 수정 * 을 클릭하면 Digital Advisor 및 CVE(Common Vulnerability & Exposure) 문서를 검토하여 보안 위험을 해결할 수 있습니다. 여러 보안 위험이 있는 경우 Digital Advisor의 정보를 검토하십시오.

을 "Digital Advisor 설명서"참조하십시오.

Google Cloud Platform으로 백업하십시오

이 릴리즈에서는 백업 대상을 Google Cloud Platform 버킷으로 설정할 수 있습니다. 이전에는 백업 대상을 NetApp StorageGRID, Amazon Web Services, Microsoft Azure에만 추가할 수 있었습니다.

"BlueXP 랜섬웨어 차단 설정 구성 에 대해 자세히 알아보십시오"..

Google Cloud Platform 지원

이 서비스는 현재 스토리지 보호를 위해 Cloud Volumes ONTAP for Google Cloud Platform을 지원합니다. 이전에는 이 서비스는 Amazon Web Services 및 Microsoft Azure와 사내 NAS를 위한 Cloud Volumes ONTAP만 지원했습니다.

"BlueXP 랜섬웨어 차단 및 지원되는 데이터 소스, 백업 대상 및 작업 환경에 대해 알아보십시오"..

역할 기반 액세스 제어

이제 RBAC(역할 기반 액세스 제어)를 사용하여 특정 활동에 대한 액세스를 제한할 수 있습니다. BlueXP 랜섬웨어 방어는 BlueXP 의 두 가지 역할, 즉 BlueXP 계정 관리자 와 계정 관리자(뷰어)를 사용합니다.

각 역할이 수행할 수 있는 작업에 대한 자세한 내용은 을 참조하십시오 "역할 기반 액세스 제어 Privileges".

2024년 8월 5일

Splunk Cloud를 사용한 위협 감지

위협 분석 및 감지를 위해 SIEM(Security and Event Management System)으로 데이터를 자동으로 전송할 수 있습니다. 이전 릴리즈에서는 AWS Security Hub만 SIEM으로 선택할 수 있었습니다. 이 릴리즈에서는 AWS Security Hub 또는 Splunk Cloud를 SIEM으로 선택할 수 있습니다.

"BlueXP 랜섬웨어 차단 설정 구성 에 대해 자세히 알아보십시오"..

2024년 7월 1일

BYOL(Bring Your Own License)

이 릴리즈에는 NetApp 영업 담당자로부터 얻은 NLF(NetApp 라이센스 파일)인 BYOL 라이센스를 사용할 수 있습니다

"라이선스 설정에 대해 자세히 알아보세요".

파일 레벨에서 애플리케이션 워크로드 복원

파일 수준에서 애플리케이션 워크로드를 복원하기 전에 공격의 영향을 받았을 수 있는 파일 목록을 보고 복원할 파일을 식별할 수 있습니다. BlueXP 랜섬웨어 방어 기능으로 복원할 파일을 선택하거나, 경고의 영향을 받은 모든 파일이 나열된 CSV 파일을 업로드하거나, 복원할 파일을 수동으로 식별할 수 있습니다.

> ⓘ 이 릴리즈에서는 계정의 모든 BlueXP Connector가 Podman을 사용하지 않는 경우 단일 파일 복원 기능을 사용할 수 있습니다. 그렇지 않으면 해당 계정에 대해 비활성화됩니다.

"랜섬웨어 공격으로부터 복구하는 방법에 대해 자세히 알아보십시오"..

영향을 받는 파일 목록을 다운로드합니다

파일 레벨에서 애플리케이션 워크로드를 복원하기 전에 알림 페이지에 액세스하여 CSV 파일에서 영향을 받은 파일 목록을 다운로드한 다음 복구 페이지를 사용하여 CSV 파일을 업로드할 수 있습니다.

"응용 프로그램을 복원하기 전에 영향을 받는 파일을 다운로드하는 방법에 대해 자세히 알아봅니다"..

보호 계획을 삭제합니다

이 릴리스에서는 랜섬웨어 방지 전략을 삭제할 수 있습니다.

"워크로드 보호 및 랜섬웨어 보호 전략 관리에 대해 자세히 알아보십시오"..

2024년 6월 10일

운영 스토리지의 스냅샷 복사본 잠금

랜섬웨어 공격이 백업 스토리지 대상으로 관리하는 경우에도 일정 기간 동안 스냅샷 복사본을 수정하거나 삭제할 수 없도록 이 기능을 활성화하십시오.

"랜섬웨어 보호 전략에서 워크로드를 보호하고 백업 잠금을 지원하는 방법에 대해 자세히 알아보십시오".

Cloud Volumes ONTAP for Microsoft Azure 지원

이 릴리즈에서는 Cloud Volumes ONTAP for AWS 및 사내 ONTAP NAS 외에도 작업 환경으로서 Microsoft Azure용 Cloud Volumes ONTAP를 지원합니다.

"Azure에서 Cloud Volumes ONTAP를 빠르게 시작합니다"

"BlueXP 랜섬웨어 보호에 대해 알아보십시오".

Microsoft Azure가 백업 대상으로 추가되었습니다

이제 Microsoft Azure를 AWS 및 NetApp StorageGRID와 함께 백업 대상으로 추가할 수 있습니다.

"보호 설정을 구성하는 방법에 대해 자세히 알아보십시오".

2024년 5월 14일

라이선스 업데이트

90일 무료 평가판에 등록할 수 있습니다. 곧 Amazon Web Services Marketplace에서 용량제 구독을 구매하거나 자체 NetApp 라이센스를 사용할 수 있습니다.

"라이선스 설정에 대해 자세히 알아보세요".

CIFS 프로토콜

이제 AWS 작업 환경에서 NFS 및 CIFS 프로토콜을 모두 사용하는 온프레미스 ONTAP 및 Cloud Volumes ONTAP를 지원합니다. 이전 릴리즈에서는 NFS 프로토콜만 지원했습니다.

워크로드 세부 정보

이번 릴리즈에서는 향상된 워크로드 보호 평가를 위한 보호 및 기타 페이지의 워크로드 정보에 대해 자세히 설명합니다. 워크로드 세부 정보에서 현재 할당된 정책을 검토하고 구성된 백업 대상을 검토할 수 있습니다.

"보호 페이지에서 작업 부하 세부 정보를 보는 방법에 대해 자세히 알아보십시오".

애플리케이션 정합성 보장 및 **VM** 정합성 보장 보호 및 복구

이제 NetApp SnapCenter 소프트웨어 및 VMware vSphere용 SnapCenter 플러그인을 사용하여 VM 일관성 있는 보호를 통해 애플리케이션 정합성이 보장되는 보호를 수행할 수 있으므로, 복구가 필요한 경우 나중에 잠재적인 데이터 손실을 방지하기 위해 대기 상태의 일관된 상태를 유지할 수 있습니다. 복구가 필요한 경우 애플리케이션이나 VM을 이전에 사용 가능한 상태로 복구할 수 있습니다.

"워크로드 보호에 대해 자세히 알아보십시오".

랜섬웨어 방어 전략

워크로드에 스냅샷 또는 백업 정책이 없으면 이 서비스에서 생성하는 다음 정책이 포함된 랜섬웨어 보호 전략을 생성할 수 있습니다.

- 스냅샷 정책
- 백업 정책
- 감지 정책

"워크로드 보호에 대해 자세히 알아보십시오".

위협 탐지

이제 타사 SIEM(Security and Event Management) 시스템을 통해 위협 감지 기능을 사용할 수 있습니다. 이제 대시보드에 설정 페이지에서 구성할 수 있는 "위협 감지 사용"에 대한 새로운 권장 사항이 표시됩니다.

"설정 옵션 구성에 대해 자세히 알아봅니다".

거짓 긍정 경고를 해제합니다

이제 Alerts(경고) 탭에서 오탐을 해제하거나 데이터를 즉시 복구할 수 있습니다.

"랜섬웨어 알림에 대응하는 방법을 자세히 알아보십시오"..

감지 상태

워크로드에 적용된 랜섬웨어 감지 상태를 보여주는 새로운 감지 상태가 보호 페이지에 표시됩니다.

"작업 부하 보호 및 보호 상태 보기에 대해 자세히 알아보십시오".

CSV 파일을 다운로드합니다

보호, 경고 및 복구 페이지에서 CSV 파일 * 을 다운로드할 수 있습니다.

"대시보드 및 기타 페이지에서 CSV 파일을 다운로드하는 방법에 대해 자세히 알아봅니다".

설명서 링크

이제 UI에 설명서 보기 링크가 포함되어 있습니다. 대시보드 수직 * 작업 * 옵션에서 이 설명서에 액세스할 수 있습니다. BlueXP 랜섬웨어 보호 문서 홈 페이지를 보려면 * 새로운 기능 * 을 선택하여 릴리즈 노트 또는 * 설명서 * 에서 자세한 내용을 확인하십시오.

BlueXP 백업 및 복구

이제 작업 환경에서 BlueXP 백업 및 복구 서비스를 이미 활성화할 필요가 없습니다. 을 "필수 구성 요소"참조하십시오. BlueXP 랜섬웨어 보호 서비스는 설정 옵션을 통해 백업 대상을 구성하는 데 도움이 됩니다. 을 "설정을 구성합니다 "참조하십시오.

설정 옵션

이제 BlueXP 랜섬웨어 보호 설정 에서 백업 대상을 설정할 수 있습니다.

"설정 옵션 구성에 대해 자세히 알아봅니다".

2024년 3월 5일

보호 정책 관리

미리 정의된 정책을 사용하는 것 외에도 이제 정책을 생성할 수 있습니다. "정책 관리에 대해 자세히 알아보십시오"..

2차 스토리지의 불변성**(DataLock)**

이제 오브젝트 저장소에서 NetApp DataLock 기술을 사용하여 보조 스토리지에서 백업을 변경할 수 없게 만들 수 있습니다. "보호 정책 만들기에 대해 자세히 알아보십시오"..

NetApp StorageGRID에 자동 백업

AWS를 사용하는 것 외에도, 이제 StorageGRID를 백업 대상으로 선택할 수 있습니다. "백업 대상 구성에 대해 자세히 알아보십시오"..

잠재적 공격을 조사하기 위한 추가 기능

이제 더 많은 포렌식 세부 정보를 보고 감지된 잠재적 공격을 조사할 수 있습니다. "감지된 랜섬웨어 경고에 대응하는 방법에 대해 자세히 알아보십시오"..

복구 프로세스

복구 프로세스가 개선되었습니다. 이제 볼륨별 또는 워크로드의 모든 볼륨을 복구할 수 있습니다. "랜섬웨어 공격에서 복구하는 방법에 대해 자세히 알아보십시오(인시던트가 중립화된 후)."..

"BlueXP 랜섬웨어 보호에 대해 알아보십시오".

2023년 10월 6일

BlueXP 랜섬웨어 방어 서비스는 데이터를 보호하고, 잠재적 공격을 감지하며, 랜섬웨어 공격으로부터 데이터를 복구하는 SaaS 솔루션입니다.

미리 보기 버전의 경우 이 서비스는 온프레미스 NAS 스토리지의 Oracle, MySQL, VM 데이터 저장소, 파일 공유와 BlueXP 조직 전체에서 AWS 기반 Cloud Volumes ONTAP(NFS 프로토콜 사용)의 애플리케이션 기반 워크로드를 보호하고 데이터를 Amazon Web Services 클라우드 스토리지에 백업합니다.

BlueXP 랜섬웨어 보호 서비스는 여러 NetApp 기술을 최대한 활용할 수 있으므로 데이터 보안 관리자 또는 보안 운영 엔지니어가 다음 목표를 달성할 수 있습니다.

- 모든 워크로드에서 랜섬웨어 방지 기능을 한눈에 확인하십시오.
- 랜섬웨어 방지 권장 사항에 대한 인사이트를 얻을 수 있습니다
- BlueXP 랜섬웨어 방어 권장 사항에 따라 보호 태세를 개선하십시오.
- 랜섬웨어 방지 정책을 할당하여 랜섬웨어 공격으로부터 상위 워크로드와 높은 위험의 데이터를 보호합니다.
- 데이터 변칙을 찾는 랜섬웨어 공격으로부터 워크로드의 상태를 모니터링합니다.
- 랜섬웨어 사고가 워크로드에 미치는 영향을 빠르게 평가합니다.
- 데이터를 복원하고 저장된 데이터로부터 재감염이 발생하지 않도록 하여 랜섬웨어 인시던트에서 지능적으로 복구합니다.

"BlueXP 랜섬웨어 보호에 대해 알아보십시오".

저작권 정보

Copyright © 2024 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 그래픽, 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/TM에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.