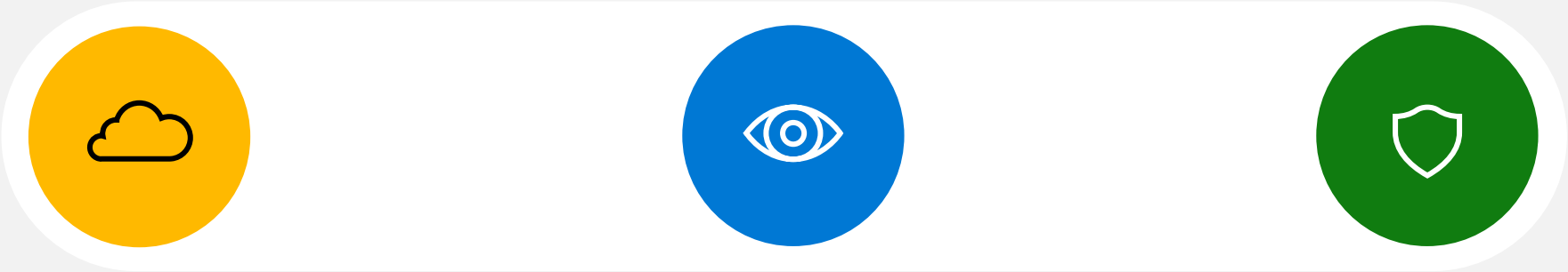
Microsoft Security

Microsoft Defender for Cloud

멀티 클라우드 및 하이브리드 환경 보호

이름 삽입

멀티 클라우드 환경 보안
최우선 순위



클라우드 내 안전한 앱 개발 및 운영

>54%

DevOps 파이프라인에 보안을 통합하지 않는 기업의 비율[1]

보안 및 규제 준수에 대한 가시성

86%

설문조사에 참여한 보안 의사결정 권자 중 자사의 사이버보안 전략이 멀티 클라우드 환경에 부합하지 않는다고 답한 비율[2]

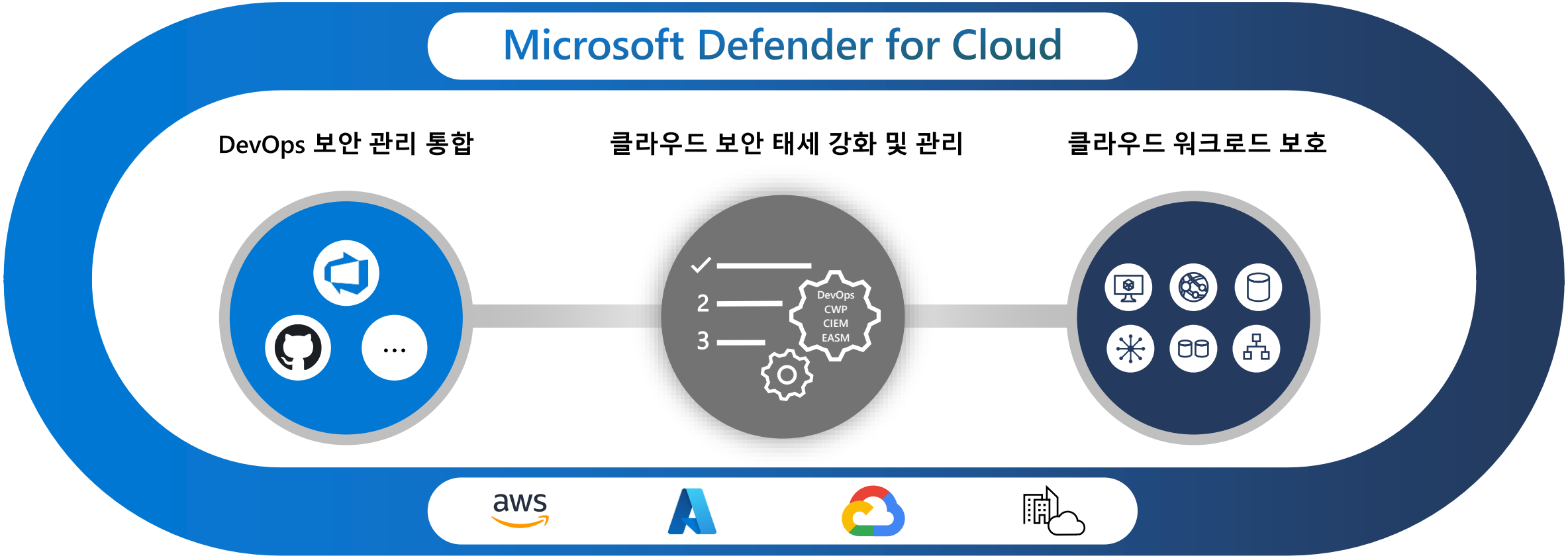
점점 늘어나는 정교한 공격으로부터 보호

$4.24M

침해로 인한 평균 비용, 2021[3]

1. Microsoft 엔터프라이즈 DevOps 보고서
2. Microsoft 클라우드 보안 우선순위 및 관행 연구
3. Ponemon Institute, 침해 비용 보고서

핵심 가치 제안


Microsoft Defender for Cloud
DevOps 보안 관리 통합
클라우드 보안 태세 강화 및 관리
클라우드 워크로드 보호
2
3
DevOps
CWP
CIEM
EASM
aws

Microsoft Defender for Cloud를 이용한 보안 태세 강화 및 관리

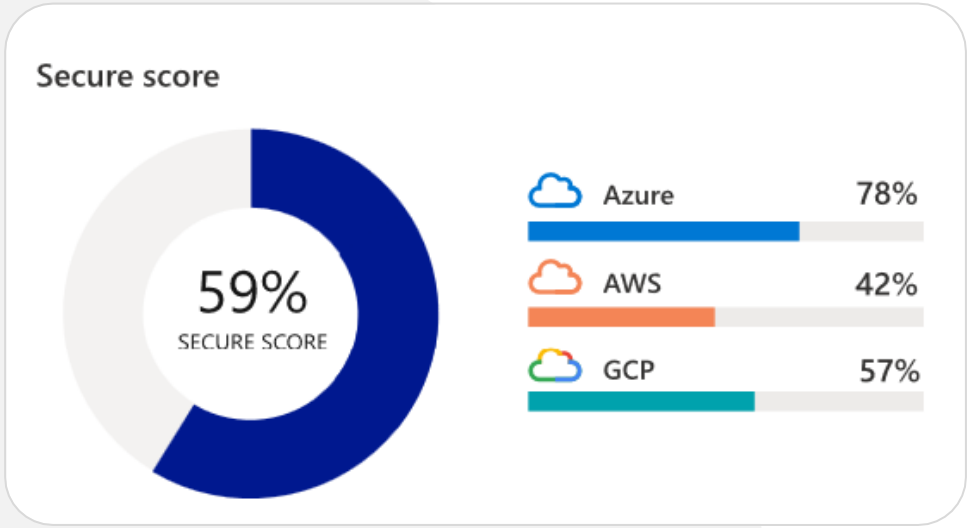
무료로 제공되는 기본 CSPM

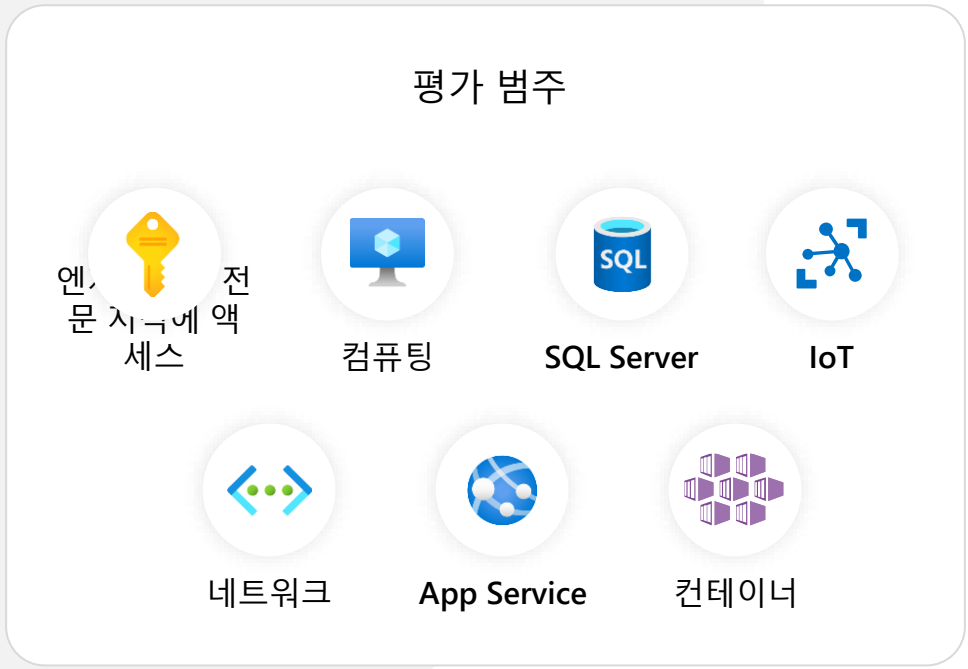
보안 점수

- 네트워크, 액세스, 컴퓨팅, 데이터베이스, 서비스 계층 등을 포함한 모든 핵심 클라우드 리소스의 보안 태세를 강화합니다.
- 바로 사용 가능한 450개 이상의 권장 사항
- 조직의 요건을 충족하는 맞춤형 권장 사항을 생성합니다.

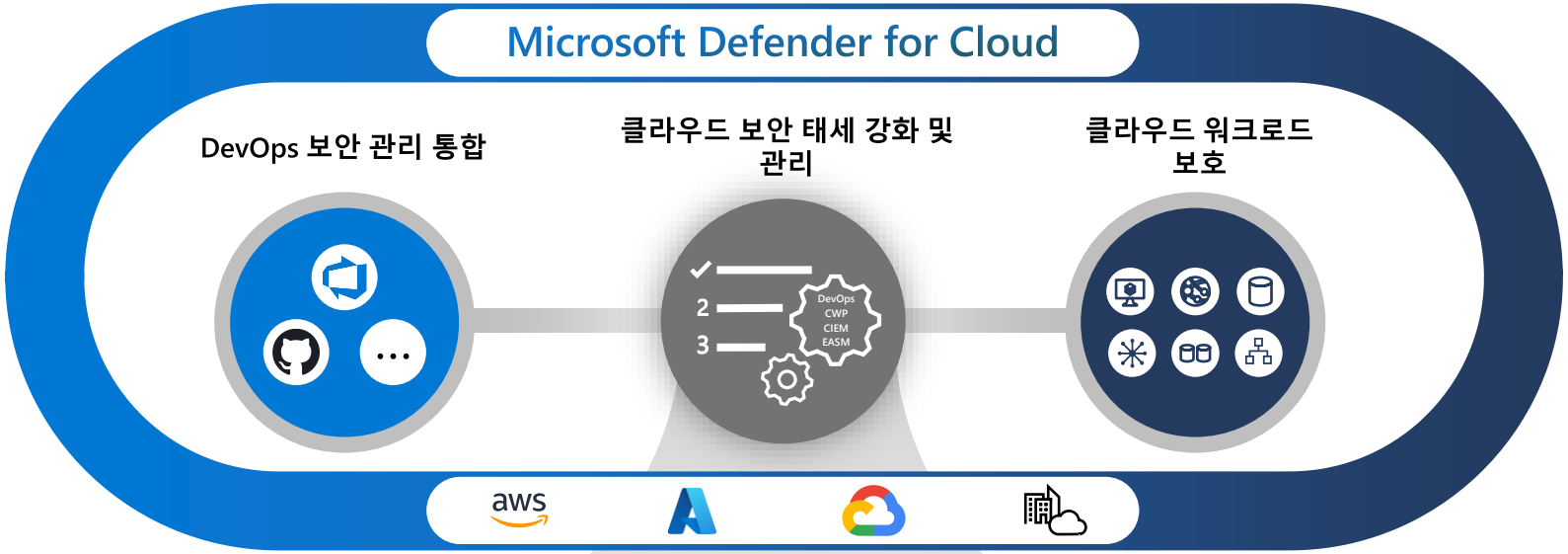
보안 규제 준수를 위한 멀티 클라우드 보안 벤치마크

- 단일 통합 대시보드에서 Amazon Web Services, Microsoft Azure 및 Google Cloud Platform 전반에 걸친 지속적인 클라우드 리소스 평가를 통해 클라우드 보안 규제 준수를 관리합니다.
- 업계 표준, 규제 준수 프레임워크 및 클라우드별 벤치마크를 활용해 모범 사례를 구현합니다 (CIS, PCI, NIST, SOC, ISO HIPAA 등).
- 조직의 고유한 요구 사항을 충족하는 맞춤형 권장 사항을 생성합니다.





Defender CSPM으로 가장 큰 위험에 집중하세요.



클라우드 워크로드 전반의 보안 태세에 대한 완전한 가시성

워크로드에 영향을 미치지 않는 에이전트리스 및 에이전트 기반 스캔 | 소프트웨어 및 CVE에 대한 가시성 | 디스크 스냅샷 | EDR

통합 데이터 및 인사이트

Defender for DevOps | Defender EASM | Entra Permissions Management | 하이브리드 및 멀티 클라우드 환경

상황에 기반한 위험 우선순위 지정

공격 경로 분석을 통한 위험 우선순위 결정 | 지능형 클라우드 보안 그래프 | 클라우드 보안 탐색기의 맞춤형 경로 쿼리

내장 워크플로 및 대규모 자동 시정 기능

규제 준수 | 마스터 그룹 관리 | 멀티 클라우드 Microsoft 클라우드 보안 벤치마크

DevOps
보안 관리 통합

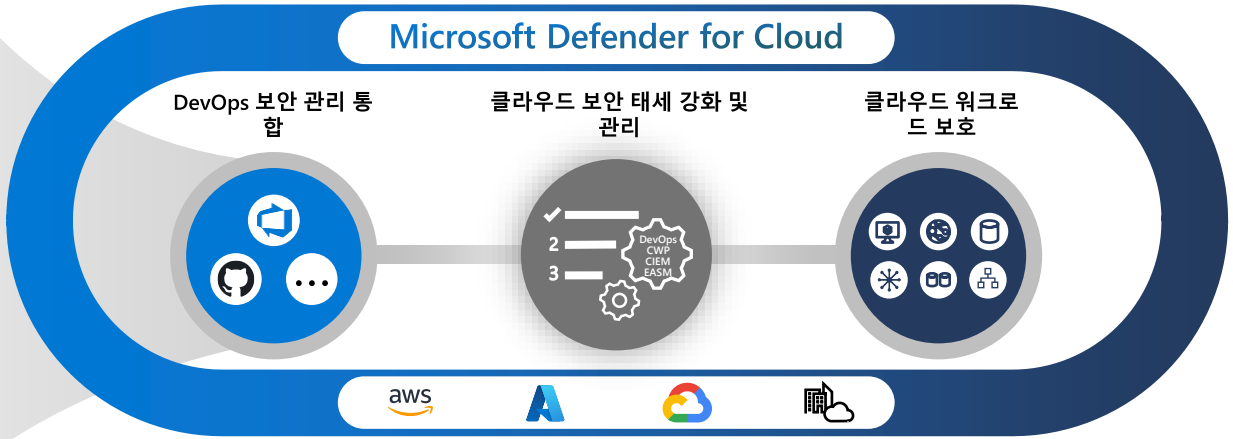
DevOps 보안 관리

DevOps 보안 태세에 대한 가시성
코드 | 종속성 | 비밀 | 컨테이너 이미지 | IaC(Infrastructure as Code) 보안 인사이트

IaC 보안
ARM | Bicep | Terraform | CloudFormation | 기타

코드-클라우드 맥락화
멀티 파이프라인 및 멀티 클라우드 환경 전반

통합 워크플로
끌어오기 요청 주석 | 개발자 소유권 할당



함께 사용하면 좋은 제품

GitHub Advanced Security
GitHub Advanced Security for Azure DevOps

개발자 우선. 커뮤니티 주도.

- 코드 보안
- 종속성 보안
- 내장 비밀 보호 기능
- 개발자 시정

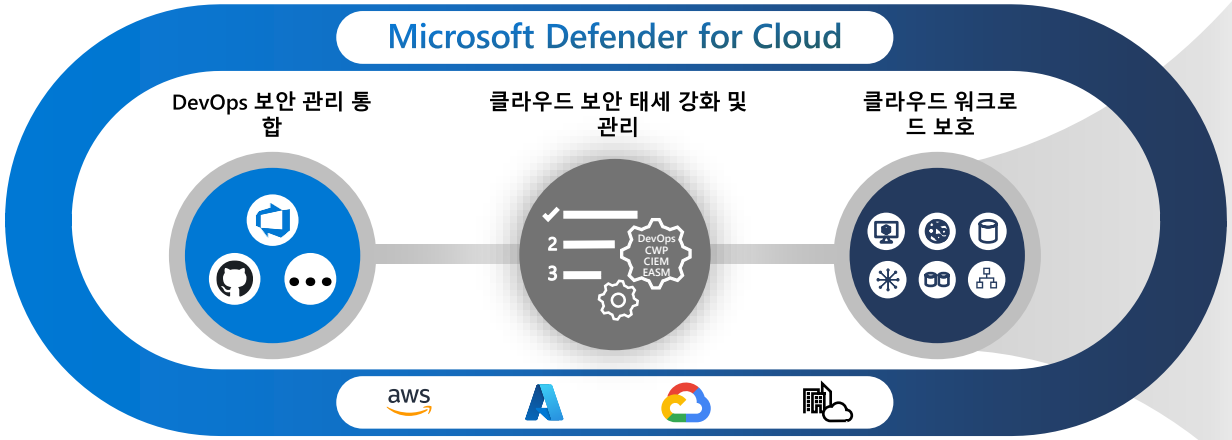
Defender for DevOps

멀티 파이프라인 DevOps 보안 통합

- 멀티 파이프라인 DevOps 보안 관리
- IaC 보안
- 코드-클라우드 맥락화
- 자동화된 워크플로

위협 감지
및
워크로드 보호

클라우드 워크로드 보호



컴퓨팅: 모든 서버 | Azure VMSS | Azure K8 | App Service | 비관리형 K8

서비스 계층: Azure DNS | Key Vault | Network Layer V1 | 리소스 관리

데이터베이스 및 스토리지: Blob 스토리지 | 파일 스토리지 | Maria DB | Cosmos DB | Azure SQL | MySQL | Postgres SQL | 비관리형 SQL

AWS 워크로드: Amazon EKS | Amazon EC2 | 비관리형 SQL | 비관리형 Kubernetes

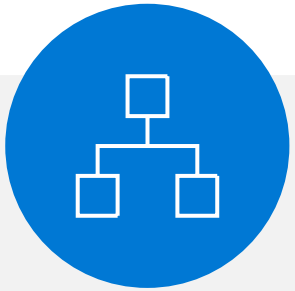
GCP 워크로드: GKE 클러스터 | Google Compute | 비관리형 SQL | 비관리형 Kubernetes

온프레미스 워크로드: Kubernetes | SQL Server | 서버

클라우드 및 온프레미스의 모든 계층에 대한 위협 차단

위협 감지

컴퓨팅, 데이터베이스, 클라우드 서비스 계층 전반의 알림 우선순위 지정



MITRE ATT&CK® 프레임워크 매핑

공격자의 공격 주기 전반에서의 영향 파악

선도적인 위협 인텔리전스

Microsoft의 글로벌 위협 인텔리전스에 기반한 매우 정교한 리소스별 알림 활용

에이전트리스 취약성 평가 & 관리

악용되기 전 선제적인 취약성 식별 및 시정

알림 상관관계 분석

인시던트별로 그룹화된 연결된 알림을 통한 보다 손쉬운 우선순위 지정

고객 이점

Rabobank 성공 사례

Rabobank는 Microsoft Defender for Cloud 롤아웃을 통해 하이브리드, 멀티 클라우드 워크로드를 모니터링하고 이를 Microsoft Sentinel 및 Microsoft Defender for Endpoint와 연결해 광범위한 가시성을 확보했습니다.

또한 비Microsoft 솔루션에 지불하던 €400,000(USD460,000)에 달하는 고가의 라이선스 비용을 없애 비용을 절감하고 벤더 수를 20개에서 4개로 줄일 수 있었습니다.

$460K
즉각적인 비용 절감

$3M
Azure Arc + Defender for Cloud를 통한 비용 절감 예상액

20개에서 4개
Microsoft 솔루션을 통한 벤더 수 감소

저렴한 비용으로 구현하는 향상된 클라우드 보안

Microsoft Defender for Cloud는 비용 절감 및 조직 내 위험 감소를 지원합니다.

219% ROI

3년간 달성한 ROI 증가율(회수 기간 6개월 미만)

연간 $200,000+

타사 보안 도구 및 서비스 비용 절감액

출처: Forrester TEI 연구

개발에서 런타임에 이르는 전반적인 멀티 클라우드 환경 보호

리소스

- ESG 기술 검증
- Microsoft Defender for Cloud 양방향 가이드
- Defender for Cloud 블로그
- Defender for Cloud 기술 커뮤니티
- Defender for Cloud 실제 활용 사례 비디오 시리
- 문서 및 빠른 시작

무료 체험판 시작하기 »

Microsoft Security

감사합니다.

부록

Microsoft Defender For Cloud

클라우드 및 온프레미스 환경 전반에 걸친 클라우드 네이티브 애플리케이션 보호

DevOps 보안 관리 통합

- 파이프라인 전반의 DevOps 보안 태세에 대한 가시성
- IaC 보안
- 코드-클라우드 맥락화
- 통합 워크로드 & 끌어오기 요청 주석

보안 태세 강화 및 관리

- 에이전트리스 및 에이전트 기반 스캔을 통한 완전한 가시성
- DevOps, EASM, CIEM 및 워크로드 전반의 통합 인사이트
- 공격 경로 기반 우선 순위 결정
- 대규모 거버넌스 & 자동 시정
- 보안 규제 준수 관리

위협 감지 및 워크로드 보호

- 풀스택 위협 차단
- 취약성 평가 & 관리

원하는 도구를 이용한 자동화

Amazon Web Services | Microsoft Azure | Google Cloud Platform | 온프레미스

새로운 혁신

Microsoft Defender CSPM(공개 프리뷰)

에이전트리스 스캔

워크로드에 대한 영향 또는 에이전트 유지가 필요 없이 모든 클라우드 리소스에 대한 완전한 가시성 및 지원 범위를 제공합니다.

공격 경로 분석 및 클라우드 보안 그래프

지능형 클라우드 보안 그래프를 기반으로 구축된 우선순위가 지정된 내부 이동 경로 및 상황별 보안 인사이트를 활용해 심각한 위험의 우선순위를 결정합니다.

통합 거버넌스 및 자동화된 시정 도구

구현된 모든 도구를 단일 뷰에서 관리하고 클라우드 전반에서 대규모 보안 규칙을 정의합니다.

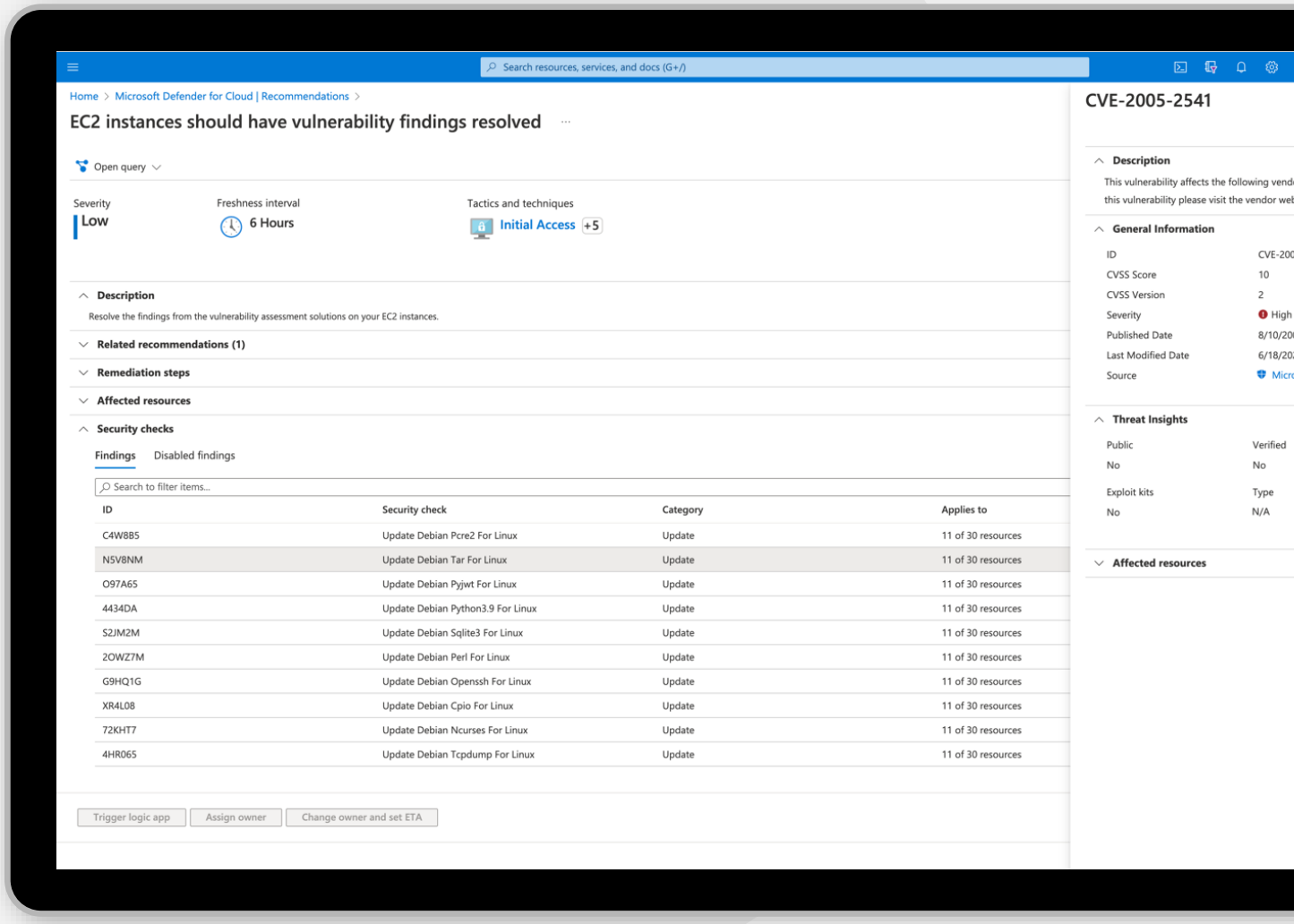
포괄적 보호

시장을 선도하는 엔드포인트 보호

- 심층적인 OS 가시성(프로세스, 커뮤니케이션 등)
- 실시간 모니터링 및 공격 탐지
- 정책 시행, 공격 차단, 대응 및 시정을 지원하는 능동적 기능

에이전트리스 취약성 스캔

- OS 보안 태세 관련 문제에 대한 즉각적인 대규모 가시성
- 워크로드 성능 영향 없음
- 워크로드 소유자에 의존하지 않는 보안팀



상황에 기반한 클라우드 보안을 통한 위험 우선순위 결정

» 새로운 지능형 클라우드 보안 그래프

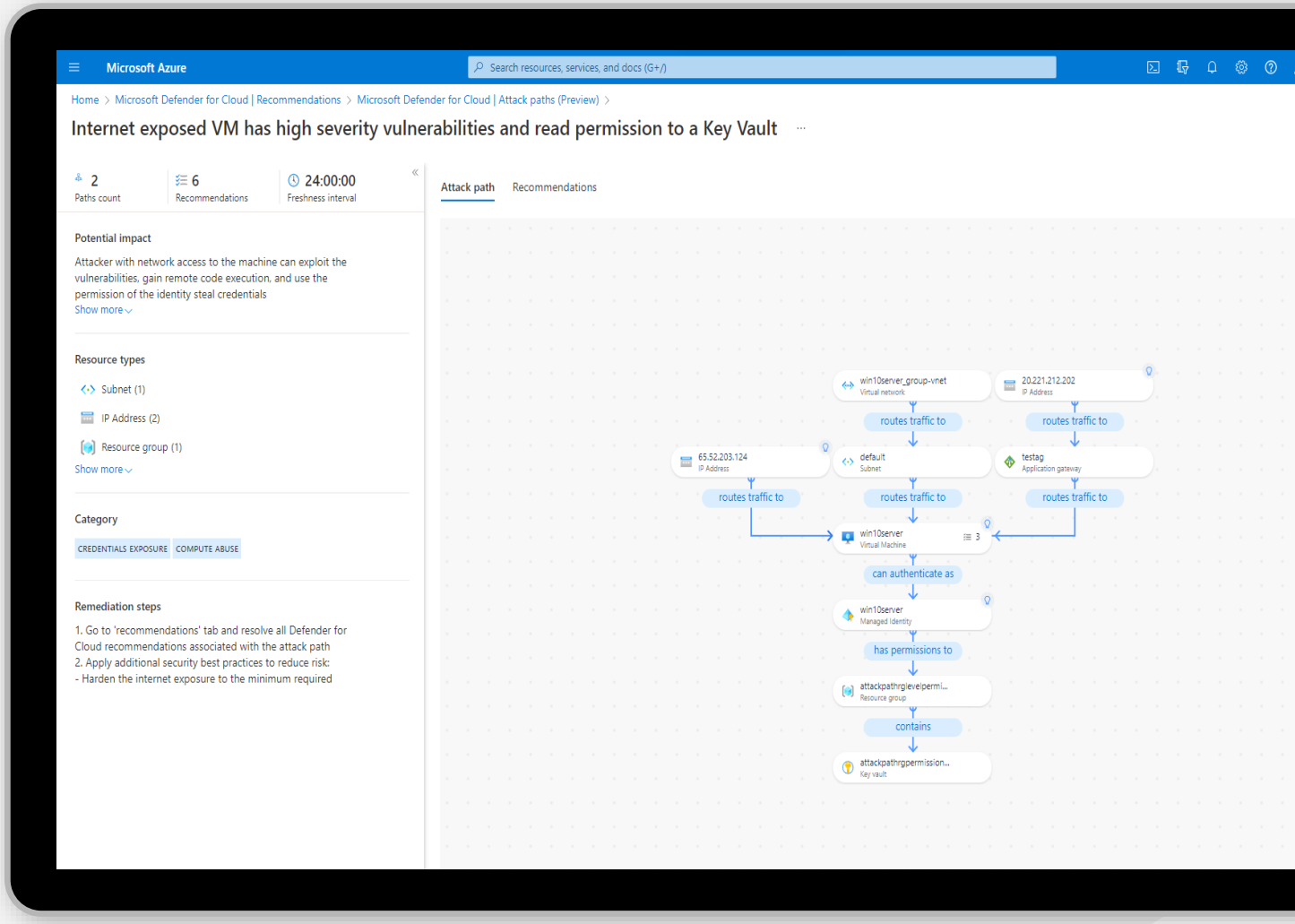
- 하이브리드 및 멀티 클라우드 환경 전반에 걸친 리소스 매핑
- 리소스와 관련 위험 및 비즈니스 컨텍스트 간 관계 파악 지원
- Defender for Cloud, DevOps 및 Defender External Attack Surface Management의 통합 인사이트

» 공격 경로 분석

- 잠재적으로 악용 가능한 내부 이동 경로를 따라 가장 취약한 리소스를 식별
- 관련 CVE 데이터 및 위험 컨텍스트를 확인해 시정에 집중

» 클라우드 보안 탐색기

- 사용자 지정이 가능한 쿼리를 이용한 선제적 클라우드 보안 그래프 검색을 통해 조직의 주요 우려 사항을 중심으로 환경 내 보안 위험을 탐색
- 특정 CVE, 인터넷 노출, 노출된 머신, 프로덕션 및 비즈니스 태그 등을 이용한 쿼리



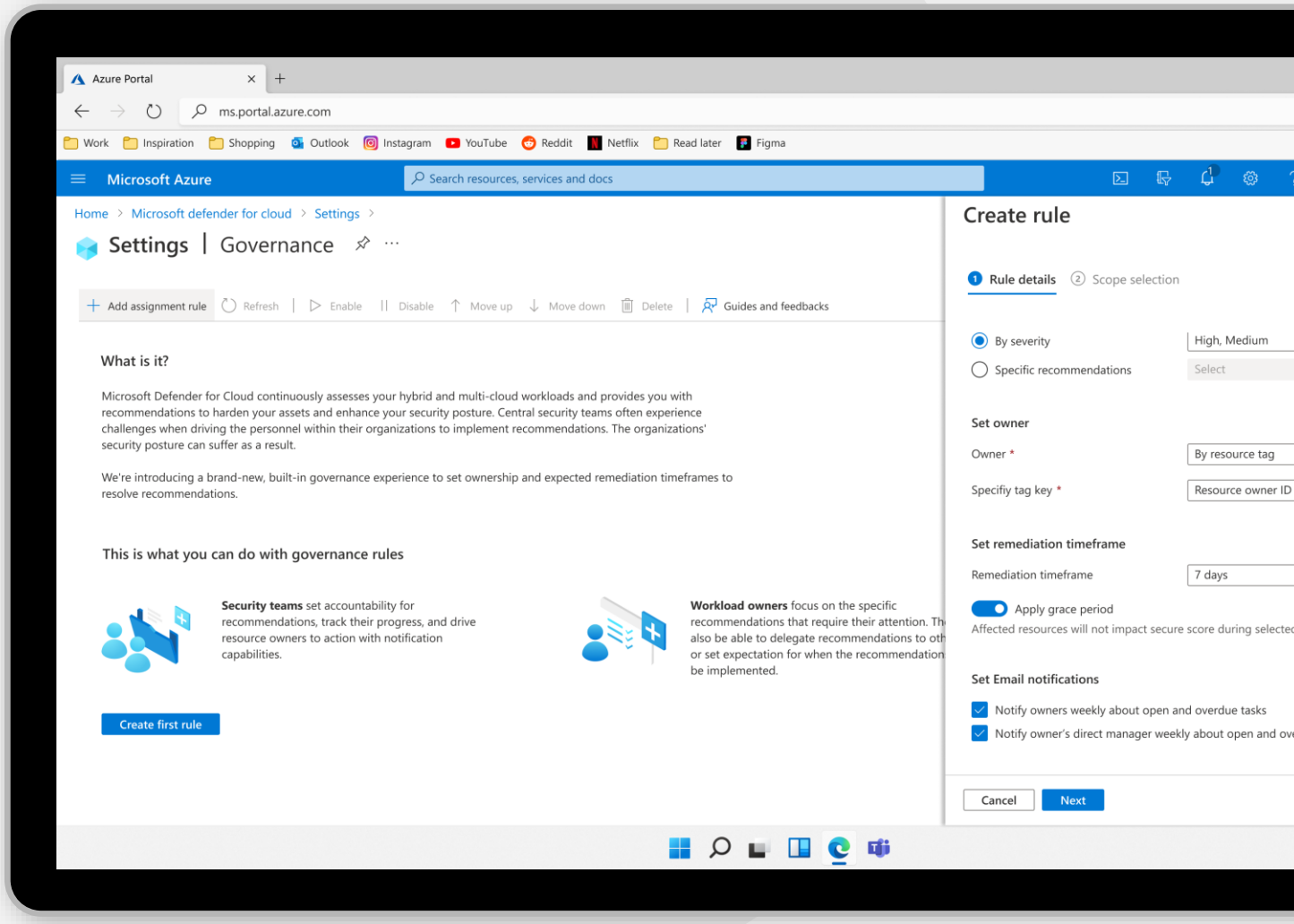
대규모 관리 및 시정 자동화

조직 전반에 걸친 대규모 거버넌스 구현

- 소유자 할당 및 시정 기한 설정
- 전체 조직에 적용되는 대규모 거버넌스 규칙 구성
- 소유자 및 관리자 보고 관련 자동 이메일 리마인더

자동 시정

- 지속적 평가
- ServiceNow 및 Azure Logic Apps와의 통합

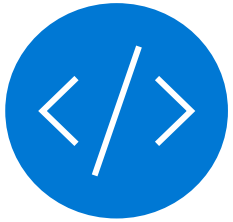


새로운 혁신

Microsoft Defender for DevOps(공개 프리뷰)

DevOps 보안 태세에 대한 가시성 통합

보안 관리자에게 단일 뷰에서 이용 가능한 멀티 파이프라인
DevOps 환경 전반에 대한 완전한 가시성 및 관리 기능을 제공합니다.



코드 관련 클라우드 리소스 구성 강화

IaC 템플릿 및 컨테이너 이미지의 보안을 활성화해
프로덕션 환경에 도달하는 클라우드 구성 오류를 최소화합니다.

통합 보안 인텔리전스를 통한 자동화

중요 코드 수정을 위한 개발자의 우선순위 결정을 돕는 코드-클라우드 컨텍스트 인사이트를 제공합니다.

DevOps 보안 태세에 대한 가시성 통합

» 발견 자동화

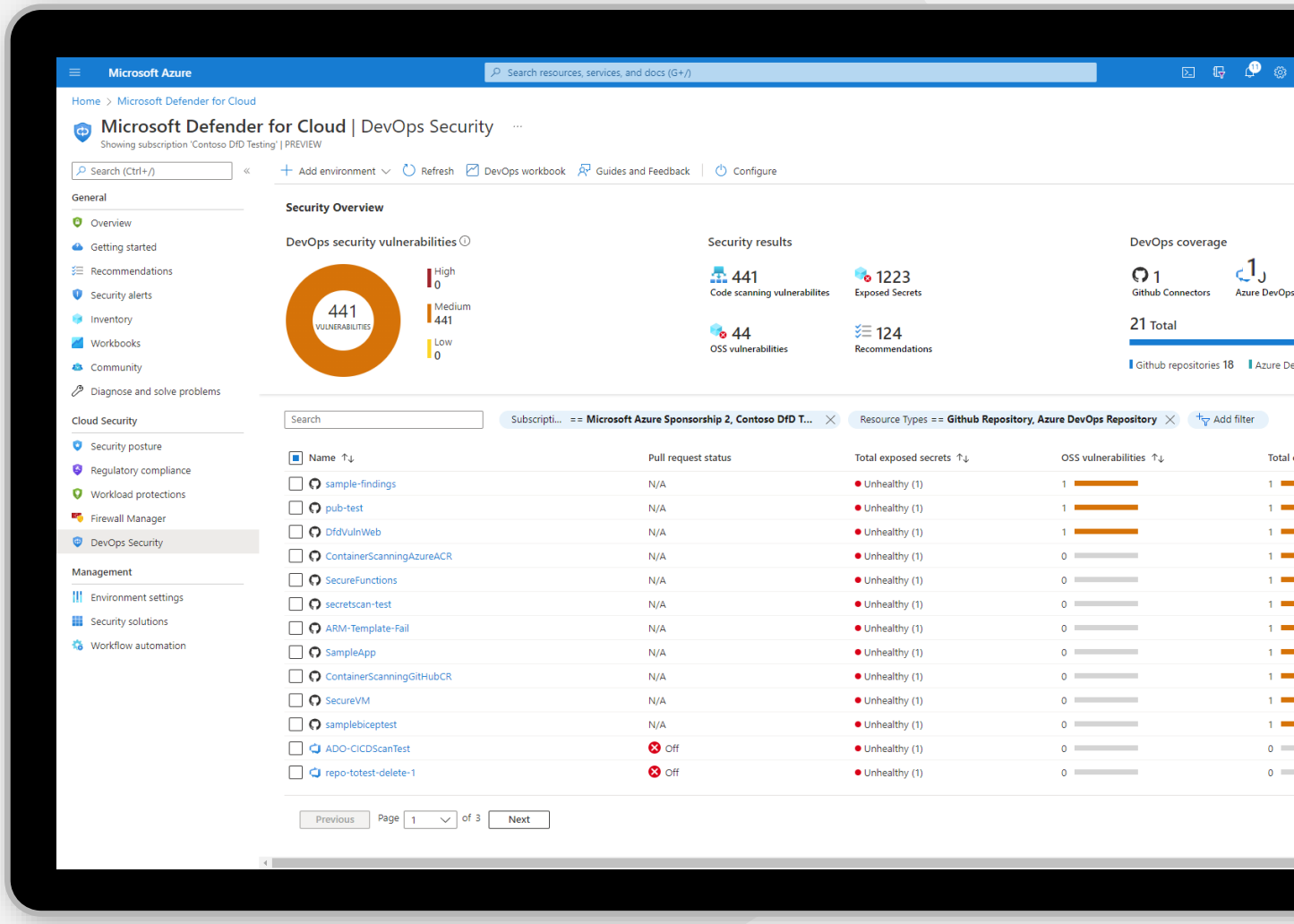
- 전체 DevOps 인벤토리
- 멀티 파이프라인(GitHub, Azure DevOps)

» 지속적 평가

- DevOps 환경 강화
- 개발자와 SecOps 간 연속성 구축
- DevOps 규제 준수

» 보안 인사이트

- DevOps 보안 관리를 위한 단일 콘솔
- 맞춤형 워크북



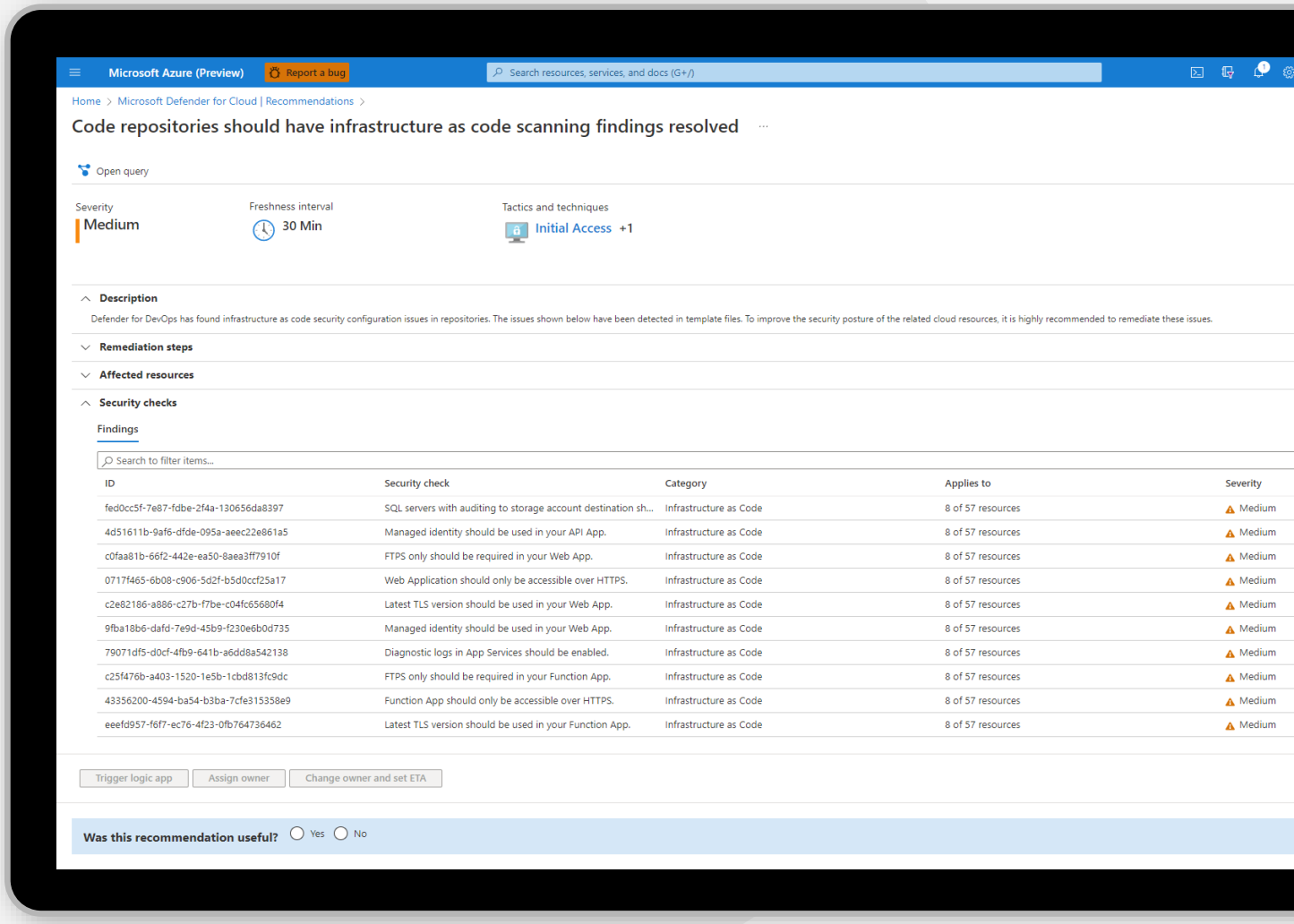
코드 관련 클라우드 리소스 구성 강화

IaC 구성 오류 발견

- IaC 템플릿에 Microsoft Cloud 보안 벤치마크 검사 적용
- 코드 라인 관련 보안 문제 식별을 통한 빠른 수정
- 명확한 시정 지침을 통한 개발자 역량 강화

멀티 클라우드 지원

- ARM, Bicep, Helm, CloudFormation 및 Terraform 템플릿 지원



통합 보안 인텔리전스를 통한 자동화

코드-클라우드 맥락화

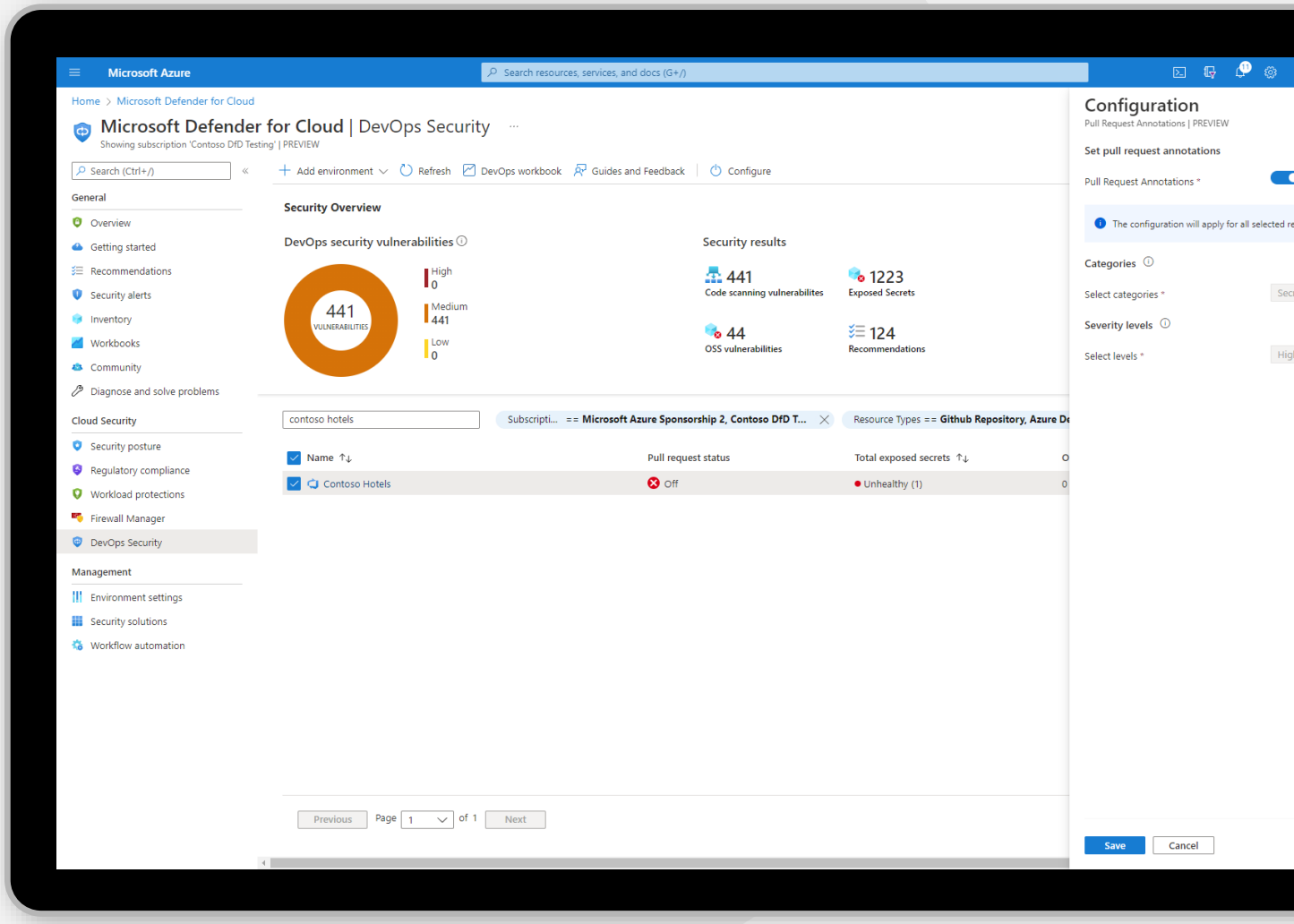
- 애플리케이션 코드 인사이트를 통한 클라우드 보안 그래프 강화

코드 관련 핵심 보안 문제의 우선순위 결정

- OSS 취약성
- 노출된 자격 증명

코드 시정 촉진

- 개발자 소유권 할당을 위한 맞춤형 워크플로
- SecOps에 의해 개시되는 끌어오기 요청 주석



전용 감지 기능을 제공하는 풀스택 지원 범위

컴퓨팅

- 모든 서버
- 비관리형 K8
- App Service
- Azure VMSS
- Azure K8

서비스 계층

- Resource Manager
- Key Vault
- Network Layer V1
- Azure DNS

데이터베이스 및 스토리지

- Blob 스토리지
- 파일 스토리지
- Maria DB
- Azure Cosmos DB
- Azure SQL
- MySQL
- Postgres SQL
- 비관리형 SQL

AWS 워크로드

- Amazon EKS
- Amazon EC2
- 비관리형 Kubernetes
- 비관리형 SQL

GCP 워크로드

- GKE 클러스터
- Google Compute
- 비관리형 Kubernetes
- 비관리형 SQL

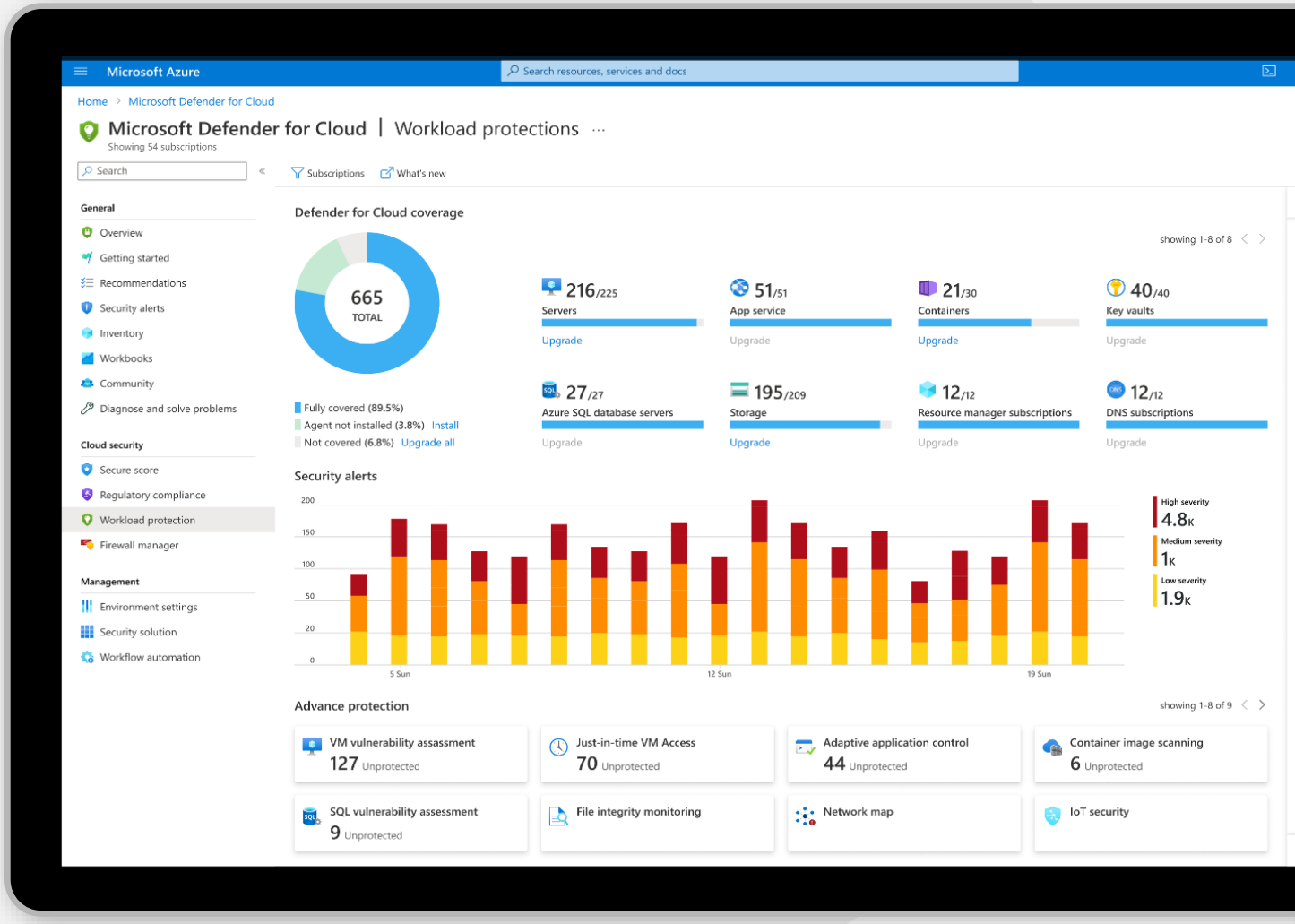
온프레미스 워크로드

- Kubernetes
- SQL Server
- 서버

Azure aws 온프레미스

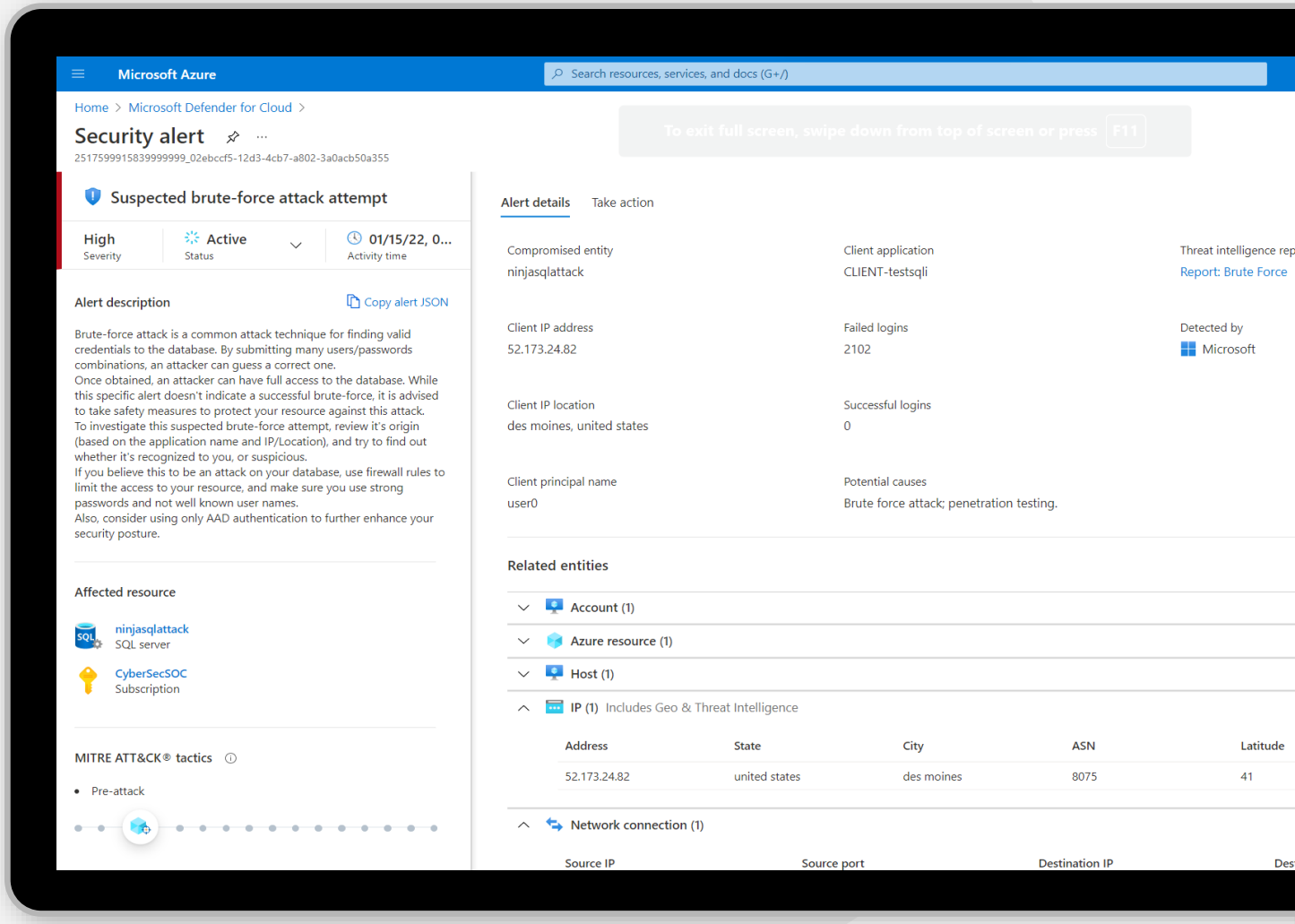
클라우드 및 온프레미스 워크로드 보호

- Microsoft 위협 인텔리전스의 강력한 인사이트를 기반으로 구축되어 각 리소스 유형의 고유한 공격 벡터를 대상으로 하는 감지 기능을 사용합니다.
- 지속적인 워크로드 스캔을 통한 취약성 식별 및 관리로 공격 표면을 줄입니다.
- 새로운 워크로드가 배포되는 즉시 자동으로 보호합니다.
- SIEM과의 통합을 통해 손쉬운 인시던트 관리를 지원합니다.



보안 알림 및 인시던트

- 리소스에서 위협이 감지되면 우선순위가 지정된 알림을 사용합니다.
- 여러 알림과 저충실도 신호를 보안 사고와 결합하는 스마트한 알림 상관관계 분석을 통해 효과적인 조사를 실시합니다.
- 공격 캠페인 및 관련 알림을 보여주는 중앙 뷰로 인시던트를 관리합니다.



Defender for Cloud 운영

멀티 클라우드 및 하이브리드 보호

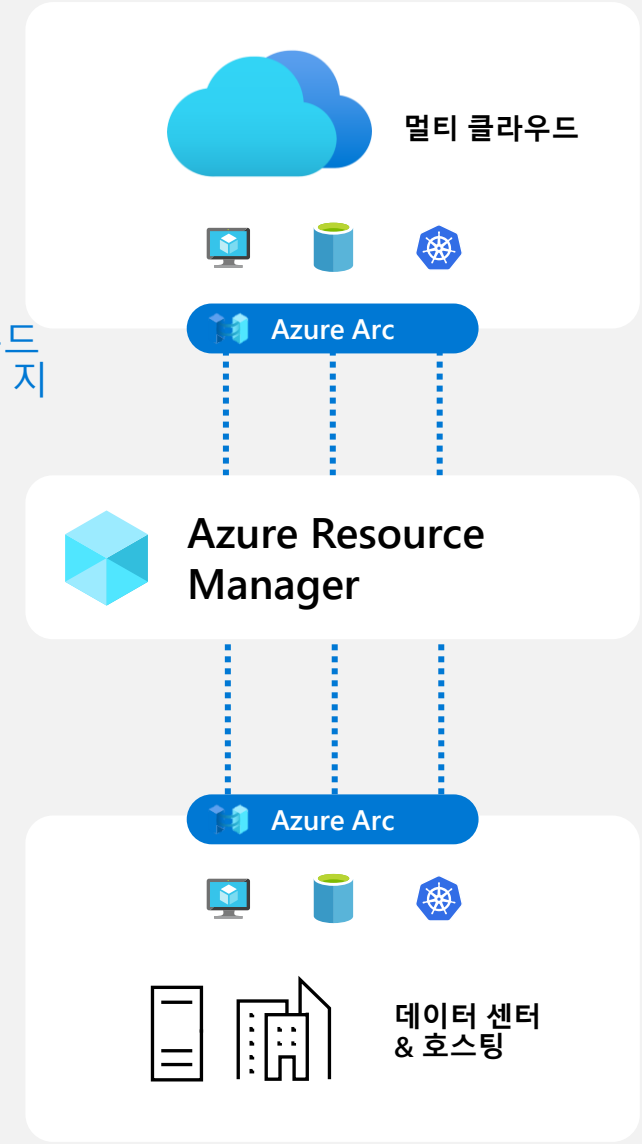
- Azure 구독 자동 온보딩
- API 커넥터를 이용한 AWS 및 GCP 계정 온보딩으로 보안 태세 관리 기능 강화
- Azure Arc 에이전트를 이용한 Azure 외부 워크로드 온보딩 및 위협 차단

Azure Arc로 어디서나 워크로드에 Microsoft Defender for Cloud를 배포해 위협 보호를 구현하세요.

- 확장 프로그램 설치(예: Log Analytics 에이전트)
- 규제 준수 시행 및 감사 보고 간소화
- Azure Portal 내 통합 뷰를 제공하는 자산 조직 및 인벤토리 — Azure 태그
- 규제 준수 충족을 위한 확인 및 시정이 가능한 서버 소유자 — Azure RBAC

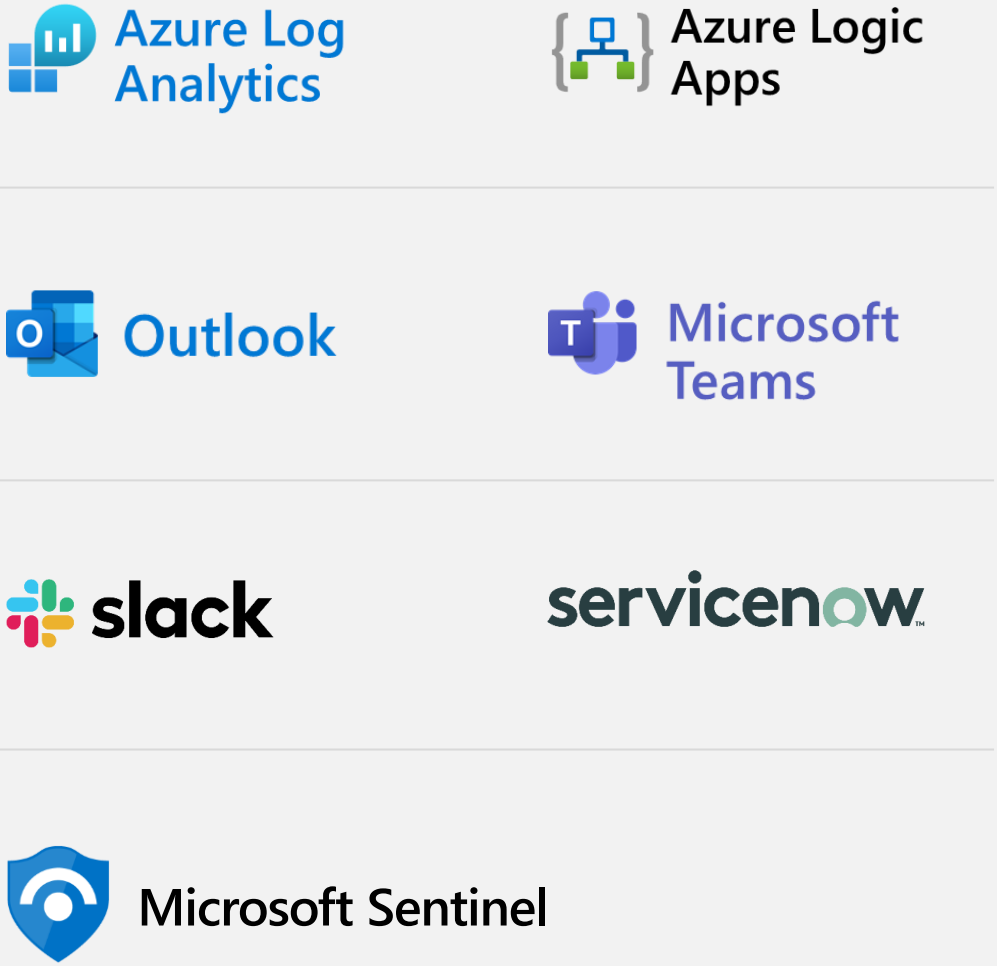
Azure Arc는 클라우드 관리 및 보안 보호를 지원합니다.

어디서나 모든 리소스를 지원하는 단일 제어 평면



대응 및 자동화

- 권장 사항을 가장 빠르게 구현할 수 있는 "빠른 수정" 기능 활용
- Azure Logic Apps를 통한 위협 알림 대응 자동화 및 원하는 앱을 이용한 지능형 워크플로 생성
- Microsoft Sentinel 연결을 통한 인시던트 및 조사 및 관리 시 포털 간 손쉬운 이동



Microsoft Azure

[조치 필요] **Microsoft Defender for Cloud**에서 귀하에게 할당된 활성 권장 사항을 구현하세요.

귀하는 '데모 구독'에서 여러 활성 Microsoft Defender for Cloud 보안 권장 사항의 소유자로 지정되었습니다.

이러한 권장 사항을 구현해 워크로드의 보안 태세를 강화하세요.

주의가 필요한 Microsoft Defender for Cloud 권장 사항 목록은 다음과 같습니다.

권장 사항	영향을 받은 리소스 수
구독에 대한 소유자 권한이 있는 계정에서 MFA를 활성화해야 합니다.	**10**(기한 만료: **6**)
가상 머신 내 취약성을 시정해야 합니다.	**8**(기한 만료: **8**)
네트워크 액세스 제어를 적시에 실시해 가상 머신의 관리 포트를 보호해야 합니다.	**6**

필요 조치

식별된 보안 구성 오류 및 약점을 기반으로 워크로드를 강화하려면 **권장 사항 검토**를 선택해 Microsoft Defender for Cloud에서 보안 권장 사항을 구현하세요.

권장 사항 검토 >

Defender for Cloud 보안 대시보드

» 중앙집중식 보안 태세 뷰

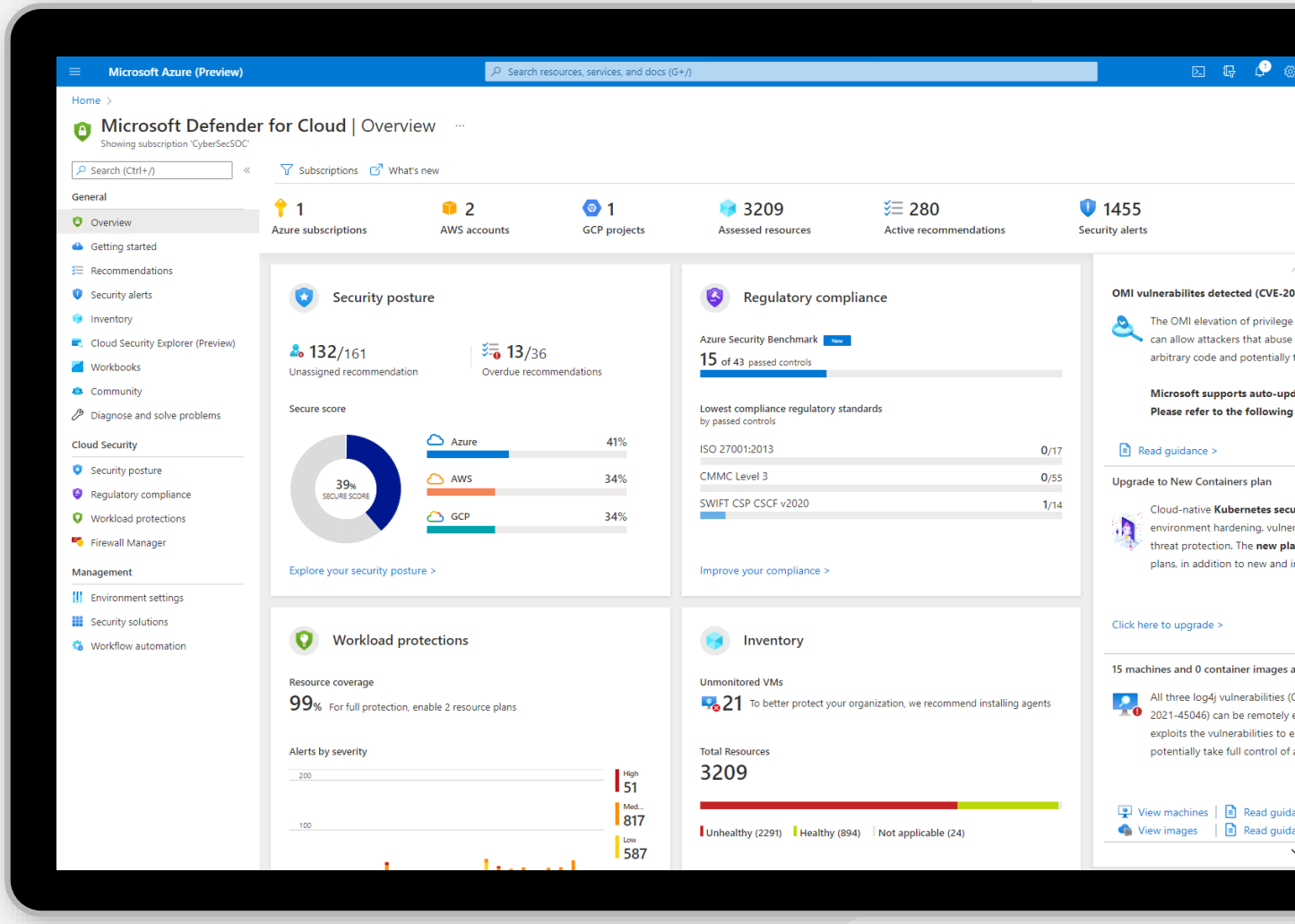
- 한 곳에서 확인 가능한
  Azure, AWS 및 GCP 전반의 보안 태세
- 하이브리드 및 멀티 클라우드 환경 전반의 자산 인벤토리

» 집중 뷰

- 손쉽게 액세스 가능한
  보안 태세, 리소스 인벤토리, 워크로드 보호 등에 대한 심층 분석 뷰

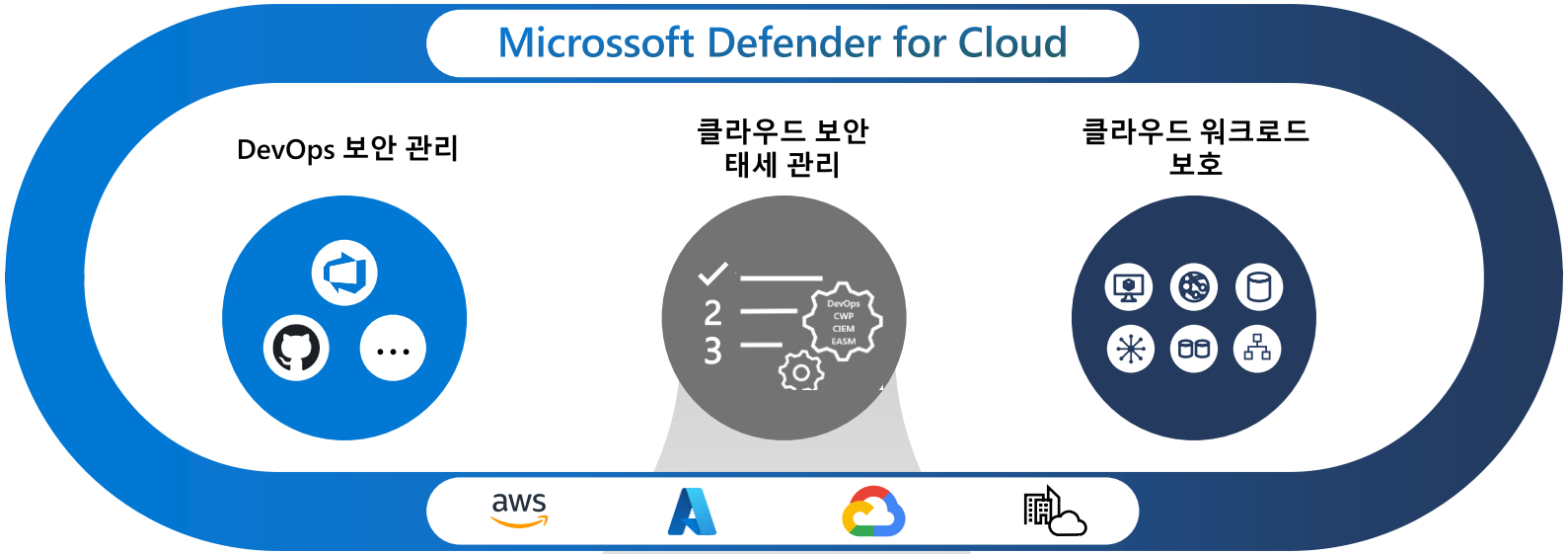
» 최고의 인사이트

- 우선순위를 부여할 권장 사항 파악
- 가장 많은 공격을 받는 리소스 확인
  및 조치 시행



Defender Cloud Security Posture Management (CSPM)

(공개 프리뷰)



에이전트리스 및 에이전트 기반 취약성 스캔

소프트웨어 및 CVE에 대한 가시성 | 디스크 스냅샷 | EDR

통합 데이터 및 인사이트

Defender for DevOps | Defender EASM | Entra Permissions Management | 하이브리드 및 멀티 클라우드 환경

상황 기반 클라우드 보안 및 위험 우선순위 결정

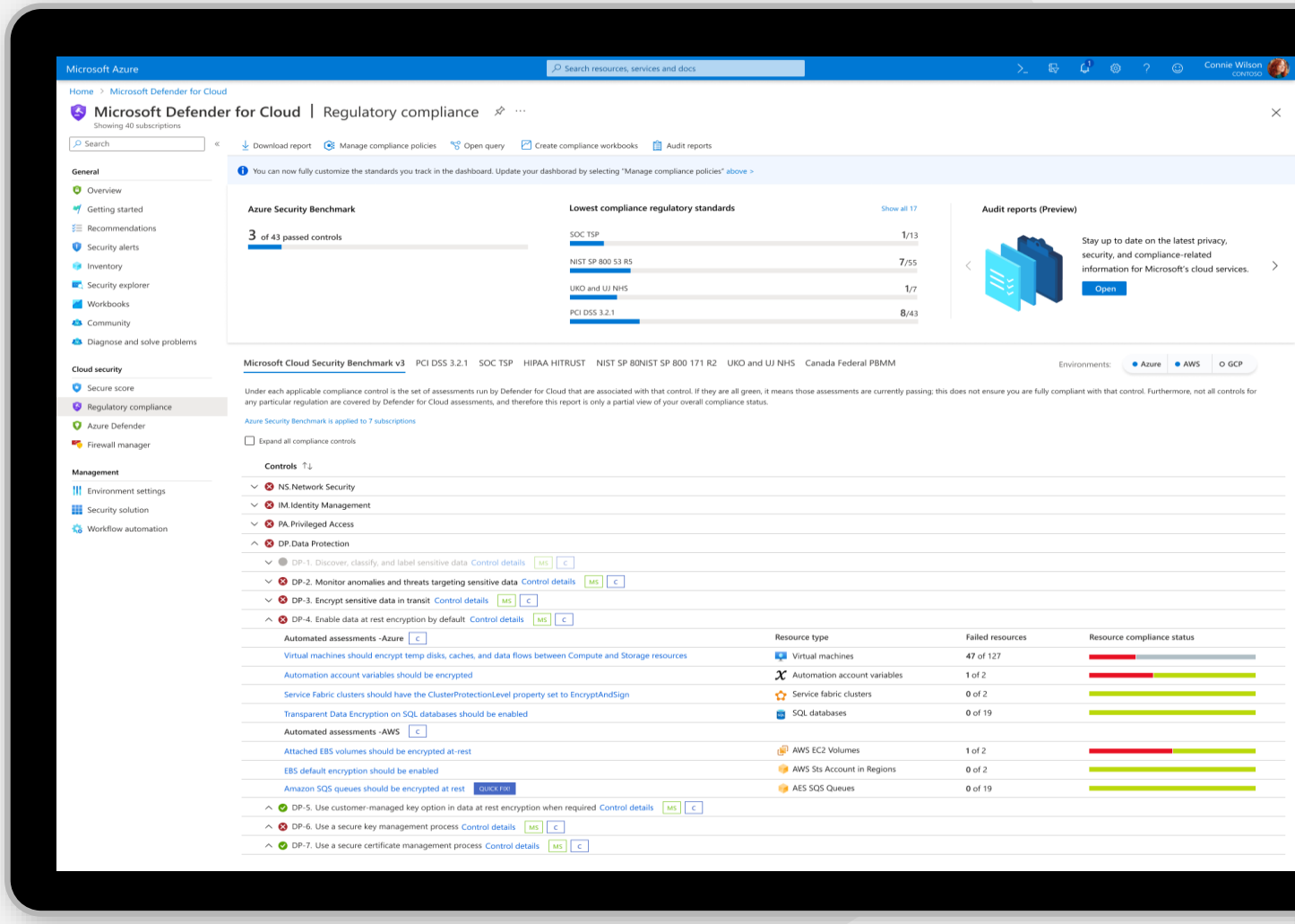
공격 경로 분석을 통한 위험 우선순위 결정 | 지능형 클라우드 보안 그래프 | 클라우드 보안 탐색기의 맞춤형 경로 쿼리

통합 워크플로 및 자동 시정 기능

규제 준수 | 마스터 그룹 관리 | 멀티 클라우드 Microsoft 클라우드 보안 벤치마크

규제 준수 평가 및 관리를 위한 멀티 클라우드 보안 벤치마크

- 단일 통합 대시보드에서 AWS, Azure 및 GCP 전반의 클라우드 리소스를 지속적으로 평가해 규제 준수 상태를 평가 및 관리합니다.
- 업계 표준, 규제 준수 프레임워크 및 벤더가 제공한 클라우드별 벤치마크를 사용해 보안 및 규제 준수 모범 사례를 구현합니다.
- 조직의 고유한 요구 사항을 충족하는 맞춤형 권장 사항을 생성합니다.



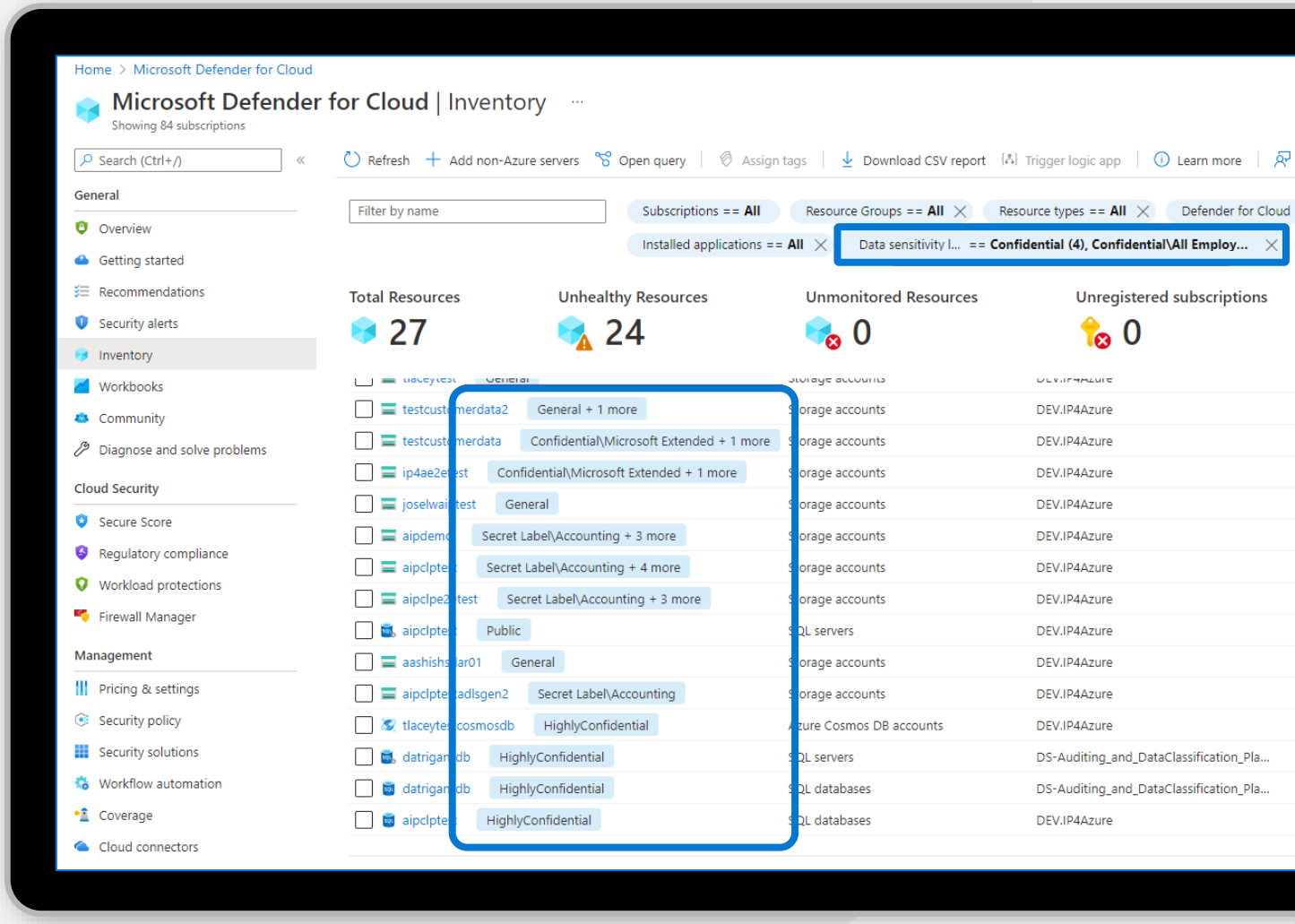
지원:

- ✓ CIS
- ✓ PCI
- ✓ NIST
- ✓ SOC
- ✓ ISO
- ✓ HIPAA
- ✓ 지역/국가 규제 준수 표준
- ✓ Azure Security Benchmark
- ✓ AWS Foundational Security 모범 사례

클라우드 리소스 내 민감 데이터 식별

Microsoft Purview와의 통합

- 클라우드 인프라 리소스에서 데이터 계층으로
  가시성을 확장합니다.
- 완전히 새로운 방식을 활용해 보안 정책 및 알림 조사의 우선순위를 결정합니다.
- 데이터 민감도별로 권장 사항 및 리소스를 필터링합니다.
- 전체 환경에서 민감 정보를 포함한 자산의 수를 손쉽게 확인합니다.



Microsoft Defender for Cloud 활용 사례

최고정보보안책임자 (CISO)

책임

사이버 공격에 대한 회복탄력성을 구축하고 시간 경과에 따라 성능을 추적하는 전반적인 보안 전략을 수립합니다.

제품 활용 사례

- 멀티 클라우드 보안 상태에 대한 최상위 수준 뷰
- 시간 경과에 따른 진행 상황을 시각화하는 대시보드 생성

보안 관리자

책임

조직의 클라우드 환경 공격 표면 축소

제품 활용 사례

- 권장 사항에 기반한 클라우드 환경 강화
- 환경 관련 보안 정책 설정, 구현 모니터링, 취약성 추적
- 멀티 클라우드 자산 인벤토리 관리

보안 운영

책임

24시간 위협 헌팅, 침해 조사, 인시던트 완화

제품 활용 사례

- 워크로드별 위협 탐지 및 대응 메커니즘을 활용해 공격을 식별하고 알림 및 인시던트를 조사하며 위협을 신속하게 완화

Microsoft의 차별점

멀티 클라우드 및 하이브리드 지원

- 신규 리소스에 대한 자동 프로비저닝 간소화
- 규제 준수 평가 및 관리를 위한
- 멀티 클라우드 에이전트리스 취약성 스캔
- 배포가 필요 없이 광범위한 보호 범위를 제공하는 Azure 내장 기능

상황 기반 코드-클라우드 보안

- 보안 태세 관리, 위험 평가 및 필요 조치 시행을 지원하는 클라우드 전반에 대한 통합 뷰
- 공격 경로에 기반해 우선 순위가 결정된 권장 사항으로 노이즈 최대 99% 감소
- 시간 경과에 따른 보안 태세 상태 추적 및 관리

전체 수명 주기 보호

- 단일 플랫폼을 이용한 클라우드 네이티브 애플리케이션 보안 관리
- 코드 스캐닝 및 IaC 스캔을 통한 프로덕션 단계의 취약성 최소화
- 개발자 환경에 통합된 워크플로를 통한 시정 시간 단축

고급 위협 차단

- 워크로드별 신호 및 위협 알림
- Azure 스토리지 및 데이터베이스를 위한 전용 워크로드 보호 기능을 제공하는 CWPP
- 결정론적, AI 및 이상 기반 감지 메커니즘
- 매일 43조 개의 신호를 처리하는 Microsoft 위협 인텔리전스 활용