

개발에서 부터 배포까지 포괄하는 클라우드 인프라 보안

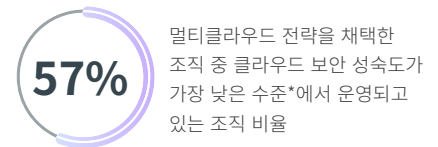
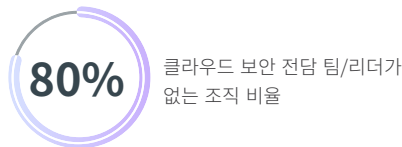
인프라, ID, 워크로드를 위한 종합적인 보호

AWS, Azure 및 GCP의 보안 취약점 파악, 우선 순위 지정 및 해결

전체 자산 검색 및 심층 위험 분석부터 런타임 위협 탐지 및 규정 준수에 이르기까지 Ermetic은 의미 있는 시각화와 단계별 지침을 통해 복잡한 클라우드 보안 운영을 자동화합니다. Ermetic은 ID (정체성) 우선 접근 방식을 사용하여 획기적으로 클라우드 공격 표면을 줄이고 고객의 규정에 따라 전체적으로 최소 권한을 적용합니다.

팀 전반의 조직 보안 작업 가속화

오늘날 대부분의 조직이 그렇듯이 귀사도 이미 비즈니스 애플리케이션을 클라우드로 마이그레이션하기 시작했거나 마무리 중일 것입니다. 최근 연구에 따르면, 클라우드 보안의 중요성은 분명해졌지만 많은 조직이 더 높은 수준의 클라우드 보안 성숙도를 달성하기 위해 우선순위를 정해야 할 사항을 결정하는 데 어려움을 겪고 있습니다..



내부 전문가 활용

- 우선순위가 지정된 보안 취약점을 찾아 즉시 해결합니다.
- 개발에서부터 배포까지 전체 라이프사이클을 보호합니다.
- 강력한 시각화 및 단계별 해결 방법을 활용합니다.
- 조직 보안 노력을 민주화하고 가속화합니다.

Ermetic은 멀티클라우드 환경 전반에서 정확한 위험 우선순위를 지정하고 문제를 해결할 수 있는 대단한 정확성으로 조직의 이해 관계자의 역량을 강화합니다. 몇 분 안에 배포하고 몇 시간 내에 실행 가능한 인사이트를 제공하는 에이전트 없는 솔루션으로 개발부터 운영까지 보안을 증강합니다.

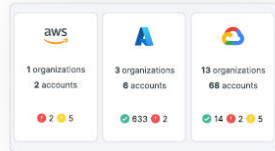
*오스터만 연구 보고서: 2022년 클라우드 보안 성숙도 현황

ID 우선 클라우드 네이티브 애플리케이션 보호

Ermetic 클라우드 네이티브 애플리케이션 보호 플랫폼(CNAPP)은 복잡한 클라우드 인프라 보안 운영을 자동화합니다. 전체 자산 검색, 심층 위험 분석, 런타임 위협 탐지 및 규정 준수 보고를 세분화된 시각화 및 단계별 지침과 결합하여 통합합니다. Ermetic은 ID (정체성) 우선 접근 방식을 사용하여 획기적으로 클라우드 공격 표면을 줄이고 고객의 규정에 따라 전체적으로 최소 권한을 적용합니다.

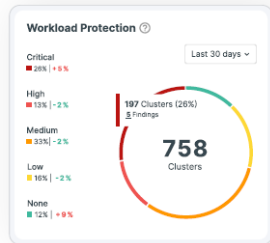
멀티클라우드 자산 관리 및 통합 가시성

클라우드 환경의 모든 ID, 데이터, 인프라, 워크로드에 대한 심층적이고 중앙 집중화된 가시성을 활용하세요.



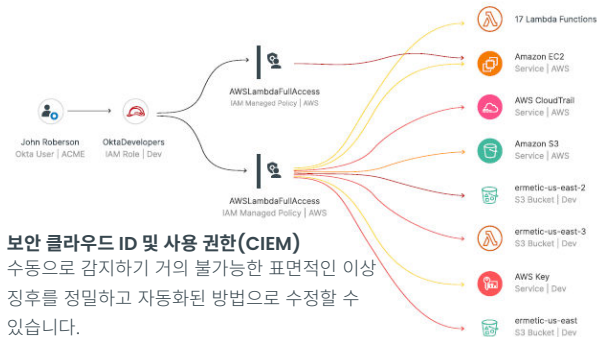
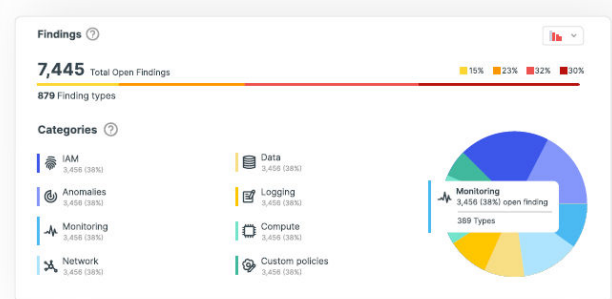
클라우드 워크로드 보호(CWP)

가상 머신, 컨테이너 및 서버리스 기능 전반에서 취약성, 노출된 기밀/민감 데이터, 악성 프로그램 및 잘못된 구성을 식별하는 중대한 위험을 스캔하고 탐지합니다.



플 스택 위험 분석 및 우선순위 지정

전체 스택 분석을 활용하여 민감한 데이터를 노출시킬 수 있는 유해한 시나리오를 포함한 위험을 파악하고 실행 가능한 인사이트를 제공합니다.



보안 클라우드 ID 및 사용 권한(CIEM)

수동으로 감지하기 거의 불가능한 표면적인 이상 징후를 정밀하고 자동화된 방법으로 수정할 수 있습니다.

거버넌스 및 컴플라이언스 (CSPM)

클라우드 전반의 구성과 리소스를 지속적으로 스캔하고, 위반 사항을 식별하고, 문제 해결을 자동화하는 단일 플랫폼으로 클라우드 컴플라이언스를 간소화합니다.



셀프 서비스 저스트 인 타임 (JIT) 액세스

필요에 따라 액세스를 신속하게 승인하여 클라우드 공격 표면을 최소화하고 오랫동안 취소되지 않은 권한으로 인한 위험을 방지합니다.

Kubernetes 형상 관리(KSPM)

Kubernetes Cluster가 기본적으로 안전하지 확인하고, 잘못된 구성이 감지되는 경우 관련 이해관계자가 신속하게 문제를 완화할 수 있도록 사전에 문제를 경고합니다.

자동화된 보안 치유 / 문제 해결

자동화된 대응 조치를 실행하여 문제를 해결함으로써 클라우드 인프라 위험의 해결 속도를 높입니다.



시프트 레프트를 향한 IaC 보안

CI/CD 파이프라인의 일부로 클라우드 인프라 환경을 강화하기 위해 코드형 인프라(IaC)에서 잘못된 구성 및 기타 위험을 발견합니다.

클라우드 감지 및 대응

지속적인 행동 분석 및 이상 징후 탐지를 적용하여 클라우드 위험을 신속하게 식별하고 조사합니다.

