

# WIZ | Cloocus

## Wiz Cloud



### Wiz – 클라우드 전환 속도에 부합하는 보안 체계 구축

클라우드에는 모든 조직을 더 빠르게 혁신하고 비즈니스를 확장할 수 있도록 만들어주었습니다. 그러나 이러한 혁신과 함께, 공격 표면도 더 많은 Abstraction Layer와 다양한 공격 경로로 확장되었고, 기존 클라우드 보안 솔루션은 이를 전체적으로 평가하고 관리하는 데 한계를 드러내고 있습니다.

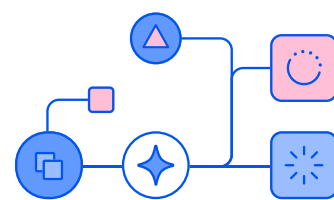
WizCloud는 Code-to-Cloud 전체 가시성과 위험 기반 위험 우선순위를 제공하여, 조직이 클라우드 환경 전반에 걸쳐 더욱 안전하게 운영 및 확장할 수 있도록 지원합니다. 클라우드 애플리케이션의 전체 수명 주기를 고려해 설계된 WizCloud는 잠재적 공격 경로와 연계된 리스크를 연관 지어 식별하고, 이를 수정하기 위한 클라우드 최적화 보안 기능들을 단일 플랫폼에 통합합니다. 여기에는 취약점 관리, 컨테이너 및 쿠버네티스 보안, AI 보안 태세 관리(AI-SPM), 인프라 권한 관리(CIEM), 데이터 보안 태세 관리(DSPM) 등이 포함됩니다.

기존의 클라우드 네이티브 애플리케이션 보호 플랫폼(CNAPP)이 보안 태세에 대한 단편적인 시각만을 제공했다면, WizCloud는 Wiz Security Graph를 기반으로 리스크와 공격 경로의 치명적인 보안 사고를 일으킬 수 있는 조합을 식별하여, 최적의 리스크 상관 관계 분석 결과를 제공합니다. WizCloud를 통해 단일 보안 기능들을 통합하여 클라우드 전환 속도를 더욱 빠르게 높일 수 있습니다.



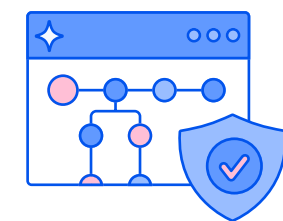
#### 쉽고 빠른 클라우드 전체 가시성 확보

Wiz Cloud는 API기반 통합 방식을 통해 몇 분 만에 전체 클라우드 환경에 연결되며, 별도의 유지 관리 없이도 전 스택에 대한 완전한 가시성을 제공합니다. 리소스나 워크로드 성능에 전혀 영향을 주지 않으면서, 어떤 클라우드 환경이든 수평 확장 가능한 구조로 설계되었습니다.



#### 심층 리스크 분석 기반의 안전한 기술 도입

Wiz는 가상 머신, 컨테이너, 서버리스 컴퓨팅 환경에 걸쳐 잘못된 설정, 취약점, 과도한 관리자 권한, 정책 위반, 노출된 시크릿 및 데이터 등 다양한 보안 리스크를 탐지합니다. 또한 IaC 및 코드 스캔을 통해 개발 파이프라인 초기 단계에서 위험 요소를 제거하는 시프트 레프트 (Shift Left) 전략을 지원합니다.



#### 보안 그래프 기반의 정교한 리스크 우선순위화

Wiz Security Graph와 Wiz Issues를 통해 반복적인 Alert Fatigue (경고 피로도)를 줄이고, 효과적으로 대응 우선순위를 설정할 수 있습니다. 이를 통해 다양한 팀, 위치, 역할에 걸쳐 클라우드 보안을 조직 전반으로 확장하고 협업을 강화할 수 있습니다.

### 글로벌 선도 기업들이 신뢰하는 보안 플랫폼, Wiz



Morgan Stanley



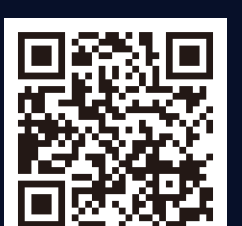
Wiz Cloud provides coverage for



Cloocus

솔루션에 대한 더 많은 정보가 필요하거나 제품 데모를 요청하시고 싶은 경우, AI 보안 전문가에게 최적의 서비스를 제안 받아보세요.

✉ [marketing@cloocus.com](mailto:marketing@cloocus.com)  
🌐 [www.cloocus.com](http://www.cloocus.com)



## 위협 상관 관계 분석을 기반으로 리스크를 평가하고, 빠른 대응을 통해 피해를 최소화하는 통합 클라우드 보안 플랫폼

### 보안 상태 관리 및 위협 대응 자동화

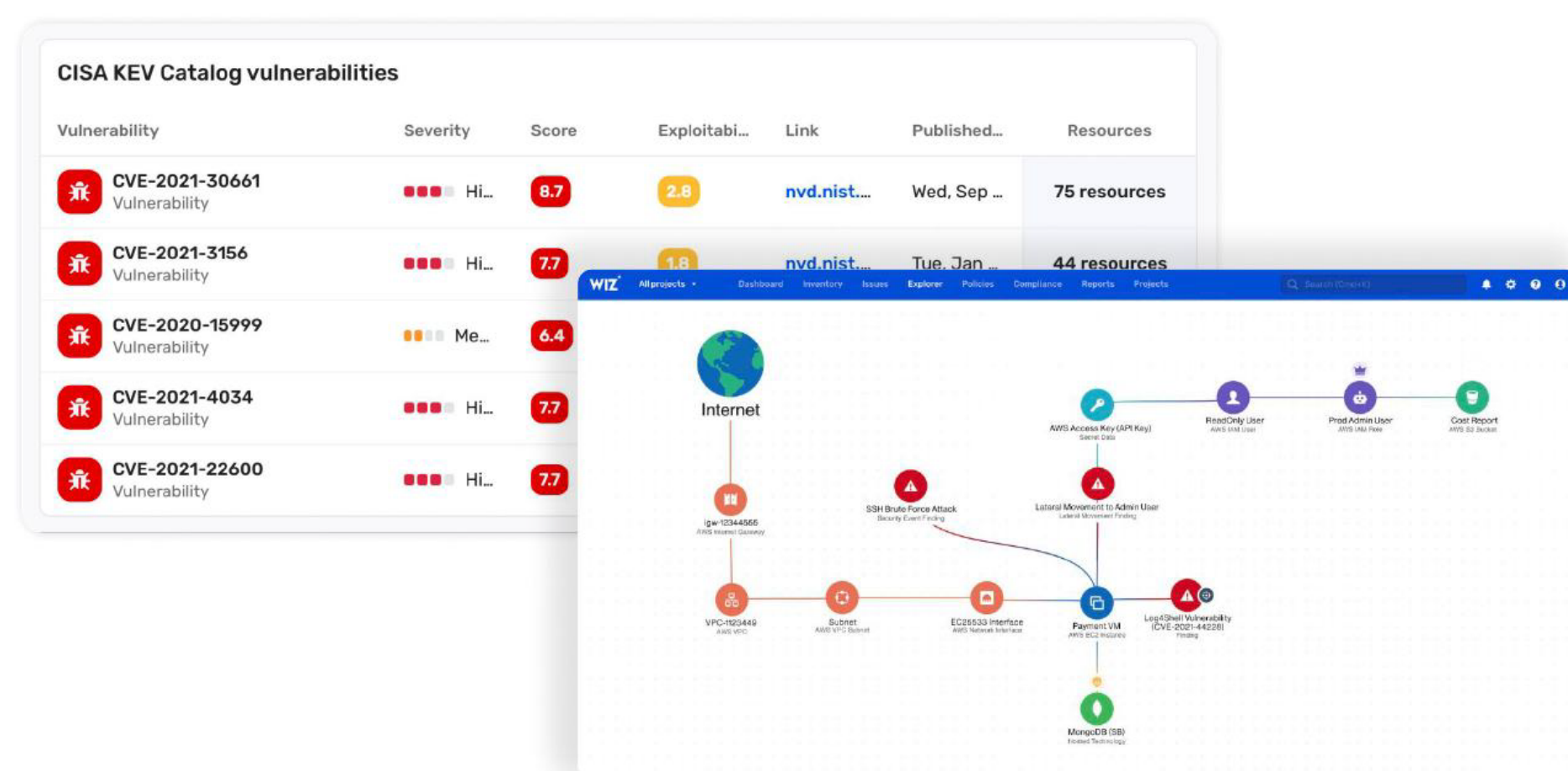
- **실시간 탐지 및 대응:** 잘못된 설정을 실시간으로 탐지하고, 원클릭 조치 및 자동화된 위협 조치 또는 자동 복구 프로세스를 통해 위협에 신속하게 대응합니다.
- **기본 제공되는 구성 평가 규칙 기반의 평가:** Azure, GCP, AWS, OCI, Alibaba 등 다양한 실행 환경과 Azure ARM Template, Terraform, CloudFormation 등의 IaC를 아우르는 2,300개 이상의 구성 규칙을 자동으로 평가하며, OPA (Open Policy Agent) 기반으로 커스터마이징할 수 있습니다.
- **지속적인 컴플라이언스 모니터링:** SOC2, NIST 800-53, PCI DSS 등 260개 이상의 사전 구축된 컴플라이언스 프레임워크를 기반으로 컴플라이언스 상태를 지속적으로 평가합니다.

### 클라우드 전반의 취약점 진단 통합 관리

- **멀티 클라우드 취약점 스캔:** 클라우드 네이티브 보안 API 커넥터를 통해 모든 주요 클라우드 환경을 단일 인터페이스에서 스캔하며, CVE 기반 12만 개 이상을 지속적으로 커버합니다.
- **다양한 기술 스택 지원:** 가상 머신, 에페메럴(ephemeral) 리소스, 컨테이너 및 레지스트리, 서버리스 기능, 가상 어플라이언스, 매니지드 컴퓨트 환경 전반을 아우르는 정밀한 취약점 분석을 제공합니다.
- **Wiz 위협 센터 통합:** Wiz Research의 최신 취약점 정보와 외부 위협 인텔리전스를 통합해, 워크로드의 실시간 취약 노출 상태를 식별할 수 있습니다.

### 기존 보안 툴을 넘어서는 진보된 보안 기능

- **컨텍스트 기반 리스크 우선순위화:** Wiz Security Graph를 기반으로 외부 노출, 클라우드 권한, 노출된 인증 정보 (Secrets), 민감 데이터, 멀웨어(Malware) 등 리스크 요소를 Wiz Security Graph를 통해 상관 관계 분석을 실시하여 경고 피로도도를 줄이고, 실제 공격 경로에 기반한 우선순위를 설정합니다.
- **데이터 보안 관리(DSPM):** 민감 데이터의 저장 위치, 접근 주체, 클라우드 환경 내 이동 경로를 파악하여 데이터가 클라우드 환경 내에서 어떻게 이동하는지를 파악하고 노출 경로를 분석하여 주요 자산을 보호합니다.
- **AI 보안 태세 관리(AI-SPM):** AI 파이프라인 전반에 대한 가시성을 확보하고, AI 환경의 보안 구성 오류를 탐지하며, AI 서비스로의 공격 경로를 분석하여 안전한 AI 혁신을 가속화합니다.
- **에이전트리스 호스트 설정 분석:** CIS 벤치마크(CIS Ubuntu, Red Hat, Windows 등)에 따라 운영 체제 및 애플리케이션 설정을 지속적으로 모니터링하며, 별도의 에이전트나 외부 스캔 없이 수행됩니다.
- **코드 스캐닝 및 IaC 분석:** 개발 파이프라인 내 코드와 IaC(인프라 코드)의 보안 결함 및 설정 오류를 개발 단계에서 탐지하여 운영 환경 반영 전에 차단합니다.



Wiz Cloud는 Fortune 100 기업 중 45%를 포함한 글로벌 고객에게 새로운 클라우드 보안 운영 모델을 제공하며, 복잡한 클라우드 환경의 보안 관리를 효율화 합니다. Wiz의 CNAPP 접근 방식은 코드부터 클라우드까지의 전 과정에 걸친 실행 가능한 가시성을 바탕으로, 보안팀과 개발팀이 민첩하고 안전하게 서비스를 설계하고 운영할 수 있도록 지원합니다.



Wiz는 취약점 관리에 필요한 모든 Telemetry, 모니터링, 가시성을 완전하게 통합 제공함으로써 보안 운영의 신뢰성을 높여줍니다.

Adam Schoeman  
Interim CISO, Copper



Wiz Cloud는 손쉬운 사용성과 강력한 기능을 동시에 제공하며, 우리 조직의 핵심 보안 도구로 자리 잡았습니다. Wiz를 통해 수집되는 방대한 인사이트는 향후 보안 전략 수립에 있어 중요한 방향성을 제시해 줍니다.

Brad Abe  
Enterprise and Security Architect, ASOS



Wiz Cloud를 통해 자사 클라우드 환경의 구성 및 자산 현황을 명확히 파악할 수 있게 되었으며, 이를 기반으로 보안 활동의 목적과 효과를 경영진에게 명확히 보고할 수 있게 되었습니다. 이전에는 가장 이해하기 어려웠던 클라우드가, 이제는 가장 투명하게 관리되는 영역이 되었고, 이는 전적으로 Wiz의 도움 덕분입니다.

Greg Poniatowski  
Head of Threat and Vulnerability Management, Mars



현재 클라우드 환경에서 서비스를 운영 중이며 해결해야 할 보안 과제가 있다면, 지금 바로 Wiz와 상담해 보시길 권장합니다.

Igor Tsyganskiy  
CTO, Bridgewater Associates

