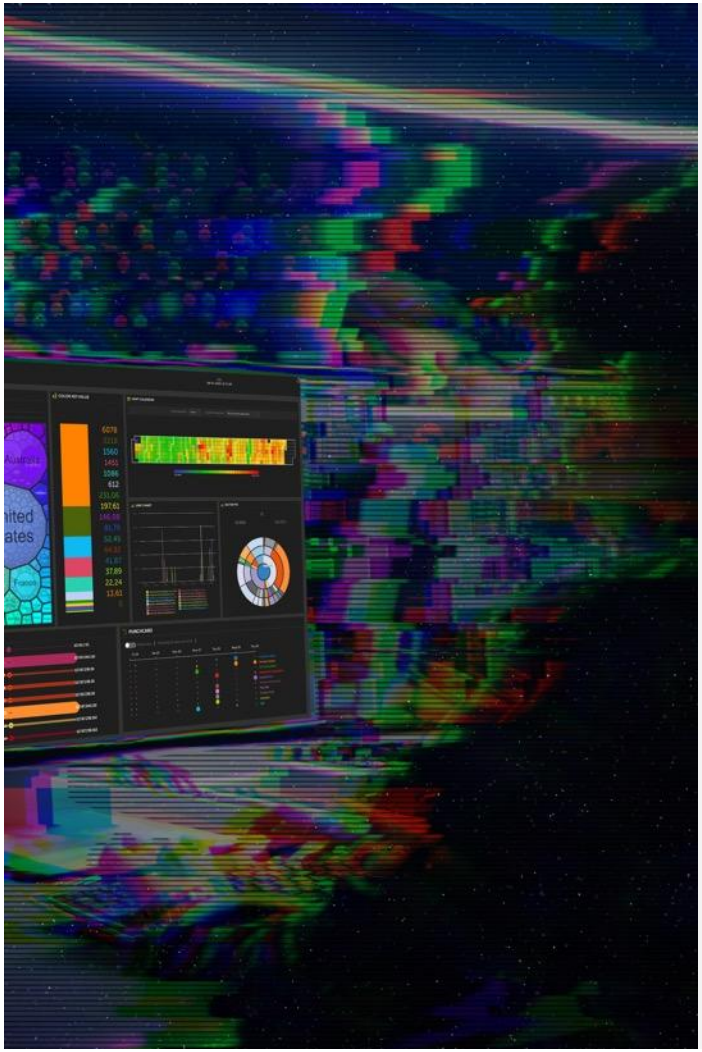


DEVO

WHY DEVO?

㈜한국밸런스

Devo 아키텍처 : 비타협 접근 방식 구조

No-Compromise 아키텍처

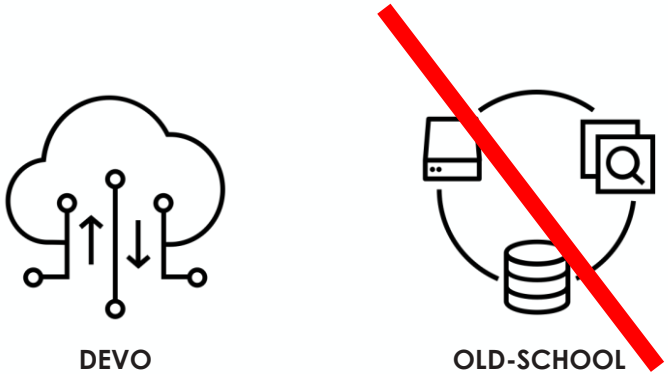
클라우드 기반의 기업을 위한 새로운 요구

100% 로그 데이터 통합	100% 충실도 달성	언제나 100% 핫 데이터	제로 레이턴시
일일 수십 TB 데 이터	10배 더 적은 저장 공간	하나의 데이터 세트, 다양한 용도	원하는 대로 새 데이터 소스 추가
클라우드 규모	데이터에 대한 대량 액세스	진정한 멀티 테넌시	미래의 워크로드 (인간과 알고리즘)

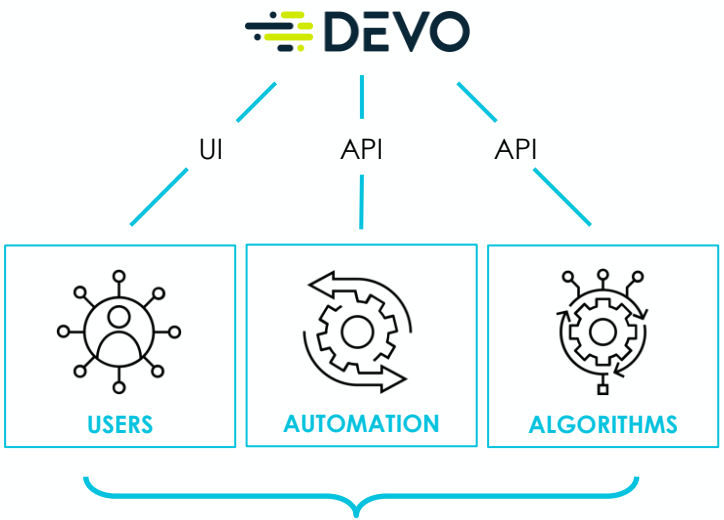
Devo 아키텍처가 제공하는 것

클라우드 네이티브 SaaS의 민첩성

- Devo는 처음부터 클라우드용으로 구축되었습니다.
- 더 이상 사용자가 스토리지 사용을 최적화하거나 인프라, 복제 요소 또는 구식 인덱스를 관리하는 데 시간을 할애할 필요가 없습니다.
- Devo는 사용자로부터 이 모든 것을 추상화하여 가장 중요한 로그 데이터에 대한 질문에 더 많은 시간을 할애할 수 있습니다.



Devo 아키텍처가 제공하는 것



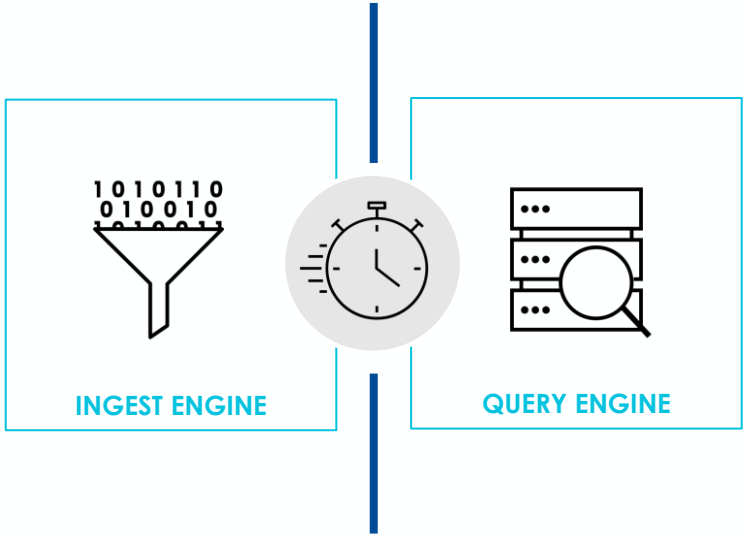
새로운 워크로드에 대한 분석

- Devo는 더 많은 데이터, 더 많은 사용자, 더 많은 알고리즘에 대한 엄청난 요구를 처리합니다.
- Devo 플랫폼은 대기 시간 없이 수천 개의 쿼리에 동시에 응답합니다.
- 모든 분석은 직관적인 웹 인터페이스와 API를 통해 제공되어 자동화 및 타사 도구를 지원합니다.

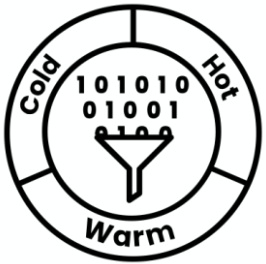
Devo 아키텍처가 제공하는 것

경합 없는 수집 및 쿼리

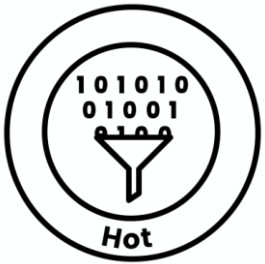
- 사용자는 수집 볼륨이 쿼리 성능을 저하시킬 것이라고 걱정할 필요가 없습니다.
- Devo 아키텍처에서 데이터 수집 및 쿼리 처리는 별도의 프로세스입니다. Devo의 쿼리 엔진은 집계 또는 원시 데이터를 지능적으로 쿼리하고 고도로 병렬화된 수평 확장 인덱스인 독점 마이크로 인덱스를 활용합니다.
- 결과: 수집을 차단하지 않는 수천 개의 동시 쿼리.



Devo 아키텍처가 제공하는 것



TRADITIONAL



DEVO

과거와 현재 보기

- Devo의 모든 데이터는 실시간 데이터 스트림과 수년간의 과거 데이터를 원활하게 분석하기 위한 최신 상태입니다.
- Devo 마이크로 인덱싱 기술 및 압축은 스토리지를 최소로 유지하면서 페타바이트의 데이터를 순식간에 쿼리할 수 있음을 의미합니다.

Devo 아키텍처가 제공하는 것

자신감이 필요한 콘텐츠

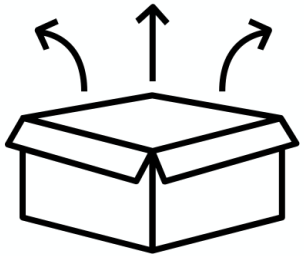
- Devo Content Stream은 Devo Platform 사용자가 위협에 보조를 맞출 수 있도록 고가치 콘텐츠를 원활하게 제공합니다.
- 조직을 보호하기 위해 몇 초 만에 운영할 수 있는 사전 구축된 경보 및 위협 인텔리전스에 즉각적이고 지속적인 액세스를 제공하여 Devo가 귀하의 동맹이 되도록 하십시오.

DEVO CONTENT STREAM

Devo 아키텍처가 제공하는 것

실행 가능한 머신 러닝

- 팀은 즉시 사용 가능한 ML을 원하고 데이터 과학자는 사용자 지정 기능을 원합니다. Devo는 둘 다 제공합니다.
- Devo 시계열 이상 탐지는 수천 개의 메트릭을 모니터링합니다. 사용자 지정 모델을 배포하시겠습니까? Devo ML Workbench는 사용자 지정 모델을 사용하여 방대한 양의 스트리밍 및 기록 데이터에 대해 작업합니다.
- 보안 중심 ML 모델은 숨겨진 위협을 효율적으로 식별합니다.

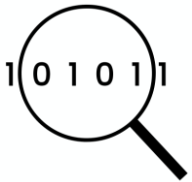


OUT-OF-THE-BOX ML & CUSTOMIZE

Devo 아키텍처가 제공하는 것

DEEPER CONTEXT IN ONE VIEW

AGGREGATED & ENRICHED



UNIFIED RAW DATA

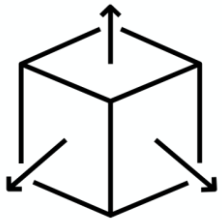
로그 데이터 그 너머로

- 격리된 보기를 넘어 더 깊은 컨텍스트를 위해 로그 데이터를 100% 강화하고 결합합니다.
- Devo는 기존 인덱스를 제거하고 모든 데이터를 원시 형식으로 함께 저장하므로 새로운 소스를 쉽게 추가하고 모든 데이터 유형을 결합하고 강화할 수 있습니다. 이 모든 것이 실시간으로 이루어집니다.

Devo 아키텍처가 제공하는 것

재설계가 필요 없는 확장성

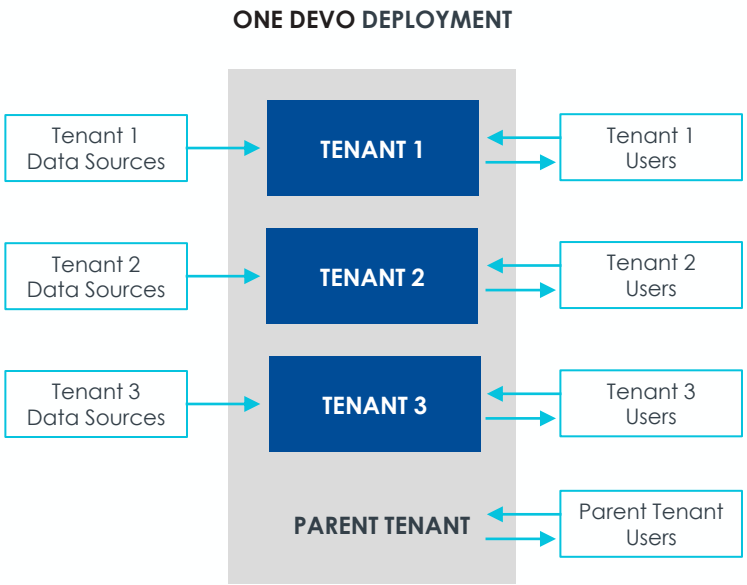
- 플랫폼의 클라우드 규모 아키텍처는 요구 사항이 GB에서 TB, PB로 변화함에 따라 확장됩니다.
- Devo는 모든 데이터 볼륨을 수집할 수 있고 10배의 수집 버스트를 처리할 수 있으며 동시에 수천 개의 동시 쿼리를 처리할 수 있습니다.
- Devo는 조직에 맞게 원활하게 확장됩니다.



10x
INGEST BURSTS HANDLING

100+TB
DAILY INGESTING

Devo 아키텍처가 제공하는 것



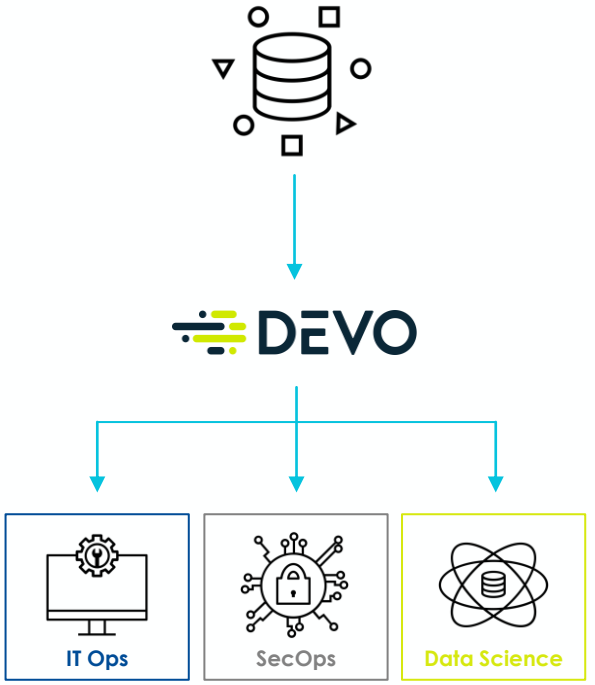
진정한 멀티테넌시

- 대규모 조직 또는 서비스 제공업체의 경우 Logging-as-a-Service를 제공합니다.
- 단일 Devo 배포에는 여러 테넌트가 있을 수 있습니다. 각 테넌트는 해당 데이터에만 안전하게 액세스할 수 있지만 상위 테넌트는 모든 테넌트의 데이터에 액세스하여 전체 비즈니스를 볼 수 있습니다.

Devo 아키텍처가 제공하는 것

하나의 데이터 세트, 다양한 용도

- 데이터 가치를 배가하고 단일 데이터 세트로 많은 다운스트림 팀(IT Ops, SecOps)을 활성화합니다.
- Devo를 사용하면 사용자 유형에 따라 데이터 액세스 및 마스킹을 쉽게 조정할 수 있습니다.



Devo 아키텍처가 제공하는 것

풍부한 시각적 기반 분석

- Devo를 사용하면 비즈니스 분석가에서 IT 관리자에 이르기까지 모든 기술 수준의 사용자가 정보에 입각한 빠른 결정을 내리는 데 필요한 정보를 모을 수 있습니다.
- 대화형 Activeboard이든 코드 없는 쿼리 기능이든 Devo를 사용하면 페타바이트 규모의 데이터에서 실시간으로 쉽게 답변과 통찰력을 얻을 수 있습니다.

Devo 서비스 운영

복잡한 IT 환경에서 보다 신속하게 근본 원인 파악

조직의 IT 운영 전반에 걸친 상황별 전체 스택 가시성

- 실시간 인사이트
- ML 기반 분석
- 복원 워크플로
- 근본 원인 분석
- 시각적 서비스 평가 모델
- 사전 패키징된 분석

FORRESTER®
WAVE LEADER 2020
Artificial Intelligence For IT Operations

Devo 보안 운영

분석가가 중요한 사항에 집중할 수 있는 워크플로를 제공하여 SOC를 혁신합니다.

단일 솔루션에 완전한 가시성, 분석가 중심 워크플로 및 풍부한 조사를 결합한 최초의 클라우드 네이티브 차세대 SIEM입니다.

- 보안 분석
- 오케스트레이션 및 자동화
- 위협 인텔리전스
- Devo 콘텐츠 스트림
- 탐지 및 경고
- 엔터티 분석
- 조사 워크플로
- 포렌식 분석

Devo로 할 수 있는 일

보안 운영

위협 탐지 및 사냥

손상을 일으키기 전에 위협 및 침해 징후 식별

위협 조사

자동으로 강화된 신뢰도 높은 경고로 위험 분류 속도를 높여 분석가가 중요한 사항에 대한 조사에 집중

포렌식 분석

포렌식 증거를 중앙 집중화하고 분류하여 기업에 영향을 미치는 위협을 심층적으로 이해합니다.

보안을 위한 로그 관리

확장 가능한 멀티 테넌트 클라우드 플랫폼에서 모든 보안 데이터와 컨텍스트를 중앙 집중화

IT 운영

애플리케이션 모니터링

클라우드 및 하이브리드 앱에서 성능 문제를 식별하여 신속하게 문제를 감지하고 선점합니다.

인프라 모니터링

기존의 가상화된 클라우드 인프라를 대규모로 검색 및 모니터링하여 가동 중지 시간을 제거합니다.

비즈니스 서비스 모니터링

복잡하고 비즈니스 크리티컬한 시스템 전반에 걸친 전체적인 고객 여정을 시각화하고 이해합니다.

IT 운영을 위한 로그 관리

확장 가능한 멀티테넌트 클라우드 플랫폼에서 전체 IT 스택의 로그, 메트릭 및 경고를 수집하고 집계합니다.

DEVO

More data. More clarity. More confidence.

Contact :
㈜한국밸런스
김 형덕 영업대표
Mobile : 010-7138-8889
Email : hdkim@valence.co.kr