

# 가장 민감한 자산인 데이터 보호



## 데이터를 검색, 분석, 감지하고 보안 및 규정 준수 위협으로부터 보호할 수 있는 중요한 뷰를 제공하는 Vormetric 및 Informatica 솔루션

### 업계 초점

Vormetric Data Protection 로그와 Informatica

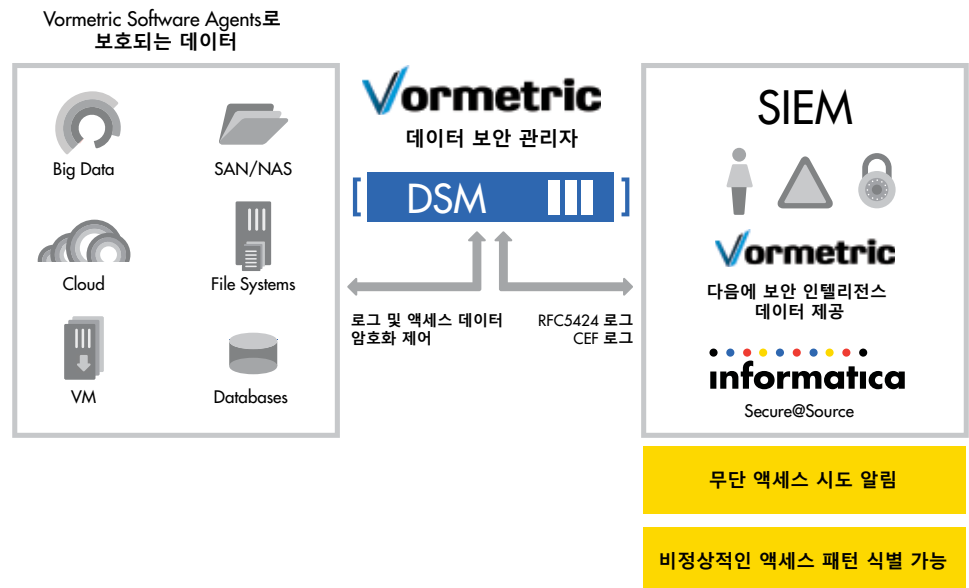
Secure@Source를 함께 활용하여 상세 사용자 및 프로세스 액세스 정보를 얻어 조직을 위협에 처하게 하는 위협으로부터 적극적으로 보호

### 이점

- 프로세스가 악성 바이러스에 의해 감염되었음을 나타낼 수 있는 비정상적인 사용 패턴을 확인하기 위해 민감한 데이터를 모니터링 및 분석하여 위협 발견
- 정책 보고를 통해 Informatica의 Secure@Source에 포괄적인 내부 뷰를 더해 추가적인 통찰력 확보
- 권한없이 무단으로 액세스하려는 악의적인 내부자 발견-근본 원인 또는 슈퍼 유저 단계의 사용자까지 파악 가능
- 위험한 데이터 사용 패턴 및 전송을 감지하여 규제 및 개인 정보 보호 규정 준수 보장
- 감사 기능을 통해 악성 바이러스 또는 악의적인 내부 사용자를 나타내는 보호된 데이터에 대한 비정상적인 사용자 액세스 패턴 감지 및 파악

수 년간 데이터 보호 방법은 간단했습니다. 즉, 강력한 경계를 구축하여 외부의 침입을 차단했습니다. 일반적인 해커는 해킹 세계에서 이름을 알리려 하거나 단순히 장난을 치는 개인들이었습니다. 그러나 지금은 모든 것이 완전히 바뀌었습니다.

오늘날의 해커는 돈 때문에 해킹을 합니다. 그들은 더 이상 개인이 아니며, 보통 데이터를 유출해서 사용하거나 최고 입찰자에게 판매하여 수익을 올리는 수십억 달러 규모의 산업을 구성하는 전문가 또는 그룹으로 이루어져 있습니다. 이러한 현상과 더불어 경계가 더 이상 존재하지 않기 때문에 경계 방어가 더 이상 효과적이지 않다는 사실은 조직이 허용할 수 없는 위협에 처했음을 의미합니다. 이러한 공격에 맞서 싸우는 데 가장 효과적인 몇 가지 툴은 Informatica의 SecureSource와 같은 고급 데이터 상관 관계의 위협 및 보안 인텔리전스 기능입니다. 이 솔루션은 비정상적인 사용 패턴을 찾고 잘못된 탐지를 줄이기 위해 가능한 위협을 파악하고, 필요할 때 조직에 알리기 위해 민감한 데이터를 검색, 분석 및 모니터링하는 기능을 제공합니다.



# Vormetric 및 Informatica – 귀하의 조직을 보호하기 위한 다음 단계

Vormetric Data Security가 제공하는 상세한 정보 없이는 조직의 보호된 데이터가 위협에 처할 수 있습니다. 엔터프라이즈 데이터 보안 솔루션의 리더인 Vormetric은 물리적, 가상, 클라우드 및 빅 데이터 환경 등 데이터가 존재하는 곳 어디서나 전례 없는 데이터 가시성, 제어 및 보안을 제공하여 중요한 정형 및 비정형 데이터를 보호합니다. Vormetric 에이전트는 이러한 모든 환경에서 암호화 규칙과 데이터 액세스 제어를 적용하는 동시에 이를 보호하는 Vormetric 인프라 사용에 대한 세부 정보뿐 아니라 사용자 및 프로세스별 데이터 액세스에 대한 정보를 수집하고 기록합니다.

Vormetric이 제공하는 자세한 정보는 위협이 될 수 있는 사용 패턴을 식별하기 위한 Informatica Secure@Source의 인텔리전스 기능으로 분석할 수 있는 중요 데이터를 나타냅니다. 이러한 기능에는 다음이 포함되지만 이에 국한되지 않습니다.

- 개인 정보 보호/보안 정책 적용
- 효율적으로 중요 데이터 비용 확인
- 복잡하고 민감한 데이터 위험 분석 수행
- 데이터 위험, APT, 악의적인 내부자, 악성 바이러스의 근본 원인 및 다운스트림 영향 파악

Vormetric 정책 로그, 감사 로그 및 인텔리전스 데이터와 Informatica의 Secure@Source 솔루션 조합은 비정상적인 활동에 대한 인식을 넘어 다음 단계를 수행할 수 있는 전례 없는 가시성과 제어를 제공합니다.

- **탐색:** 악성 바이러스 위협이나 사용자의 데이터 및 커뮤니케이션에 대한 액세스 권한을 얻으려는 내부자를 차단하기 위해 민감한 데이터가 있는 위치 및 액세스를 확산시키고 제어할 수 있는 위치를 탐색
- **분석:** 잠재적인 정책 위반이나 정상 범위에서 벗어난 의심스러운 행동을 찾아내어 위험 분석
- **감지:** 사용자의 데이터 액세스와 같은 비정상적인 행동 또는 관리 사용자가 보호된 데이터 액세스 권한으로 새로운 계정을 생성하는 것처럼 관리 계정 손상을 나타낼 수 있는 기타 의심스러운 행동 감지
- **보호:** 암호화, 토큰화 및 데이터 마스킹을 배포하는 방식의 새로운 첨단 사이버 범죄 기법뿐 아니라, 기존 해킹의 대상이 되는 민감한 저장 상태 데이터 보호

가장 민감한 자산을 보호한다는 것은 특히 거의 매일 변화하는 위협 환경에서는 박찬 일일 수 있습니다. Informatica와 Vormetric이 공동으로 개발한 솔루션이 현재뿐 아니라 미래에도 조직이 발전하고 새로운 위협이 등장함에 따라 계속해서 조직을 보호해 줄 확장 가능한 플랫폼으로 데이터를 안전하게 보호할 수 있습니다.

## Vormetric 소개

데이터 보안 솔루션의 리더인 Vormetric(@Vormetric)은 물리적, 가상, 빅 데이터 및 클라우드 환경에서 저장 상태 데이터를 보호합니다. 10년 이상 기업과 정부의 신뢰를 받아 온 Vormetric Data Security Platform은 포춘지 선정 50대 기업 중 17개 기업을 포함해 1,500개가 넘는 글로벌 기업의 데이터를 보호하고 있습니다. 단일한 인프라 및 관리 환경인 Vormetric은 파일, 볼륨 및 클라우드 스토리지 암호화, 동적 데이터 마스킹을 통한 토큰화, 현장 수준의 애플리케이션 암호화, 복잡한 액세스 제어 정책, 타사 및 통합 암호화 키 관리로 데이터가 상주하는 곳 어디에서나 데이터를 보호합니다. 자세한 내용은 [www.vormetric.com](http://www.vormetric.com)을 참조하십시오.

## Informatica 정보

Informatica는 모든 데이터의 미래를 위한 변화의 혁신을 제공하는 선도적인 독립 소프트웨어 공급업체입니다. 전 세계의 기업들이 Informatica와 함께 정보의 잠재력을 실현하고 중요한 비즈니스 과제를 해결하고 있습니다. 5,800개 이상의 기업이 Informatica를 통해 소셜 네트워크를 포함한 인터넷, 클라우드 및 기업 내에 있는 정보 자산을 최대한 활용하고 있습니다.



한국인포매티카 06611 서울시 서초구 서초동 강남대로 465 교보타워 B동 13층, 대표 전화: +82 2 6293 5001  
[informatica.com/kr](http://informatica.com/kr) [linkedin.com/company/informatica](https://www.linkedin.com/company/informatica) [twitter.com/Informatikr](https://twitter.com/Informatikr) [facebook.com/informatikr](https://www.facebook.com/informatikr)

© 2016 Informatica LLC. All rights reserved. Informatica® 및 Put potential to work™는 미국 및 전 세계 관할 국가 내에서 Informatica Corporation의 상표 또는 등록 상표입니다. 다른 모든 회사 및 제품 이름은 상품명 또는 등록 상표일 수 있습니다.