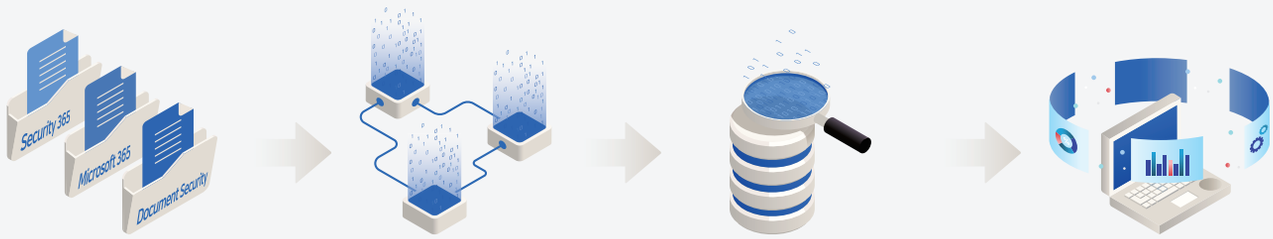
InfoLineage

추적되지 않는 데이터는 통제할 수 없습니다

조직 내 문서가 언제, 어디서, 누구에 의해 사용되는지 추적하고 시각화하는 문서 가시성 플랫폼

엔드포인트와 생성형 AI 및 SaaS 환경에서 발생하는 복잡한 문서 사용 경로를 하나의 흐름으로 추적합니다.
원본·파생 관계를 계보 그래프로 시각화하고 이상징후를 탐지해,
AI 시대에도 문서의 흐름을 가시화해 위험 행위를 효과적으로 식별하고 통제합니다.



1 수집
다양한 환경의 문서 로그

2 표준화
통합 로그로 수집

3 분석
계보 그래프 생성
GraphDB Elastic (ES2Neo)

4 시각화
Web Console 대시보드

흩어진 문서 사용 기록을 하나의 관계도로 파악합니다

사용자·시스템·파일 사이의
상관관계를시각적으로 표현합니다.
누가 문서를 주로 다루는지, 어떤 시스템을 통해 오가는지
흩어진 로그가 아닌 한눈에 보이는 관계도로 파악합니다.

원본에서 파생본까지 문서의 계보를 끝까지 따라갑니다

하나의 문서가 복사·편집되며
만들어낸 파생 문서의 흐름을 추적합니다.
원본과 파생본의 관계를 계보(Lineage) 그래프로 복원해,
문서가 어디까지 퍼졌는지 확인합니다.

InfoLineage

무엇이 위험한지 사용 이력이 말해줍니다

사외 사용·암호 해제·익명 링크 접근은
유출 위험이 큰 행위입니다.
이런 행위가 기록된 위험 가능성이 있는 문서를
놓치지 않고 점검하도록 돕습니다.

문서가 어디로 퍼졌는지 경로를 재구성합니다

문서에 사용 기록이 남아 있다면, 그 이력을 따라
전달 경로와 관련자를되짚어볼 수 있습니다.
사고 조사 시 어디서부터 살펴야 할지
단서를 제공합니다.

Document Lineage

보안 가시성 확보

사용자·시스템·문서 사이의 흐름을
정량적으로 확인합니다. 막연한 추측이 아닌
데이터로 문서 보안 현황을 파악합니다.

Anomaly Detection

사고 시 신속 대응

보안 사고가 발생하면 유출 경로와
관련 사용자·시스템을 빠르게 식별해
대응 시간을 줄입니다.

Risk Detection

감사·내부 통제 강화

사용자·문서 사용 이력을 기반으로
감사 보고서를 작성해 컴플라이언스 대응과
내부 통제를 뒷받침합니다.

InfoLineage 주요 특징

01 통합 대시보드

주의 작업 Top10 · 접근 추이 · 작업 모니터링

작업 발생 문서, 익명 링크 접근 추이, 복호화·삭제·공유 작업 추이 등
핵심 지표를 한 화면에서 모니터링합니다.
문서 보안 현황을 실시간으로 파악합니다.

02 이상징후 탐지 & 알림

업무시간 외 감지 · 실시간 알림

업무 시간 외 발생한 공유·복호화·삭제·익명 링크 접근 등
위험 작업을 자동 감지하고 즉시 알립니다.

03 등급 분석 & 감사 리포트

등급 분포 · 미분류 점검 · 리포트

C·S·O 등급별 문서를 저장소·부서·사용자·PC 단위로 분석하고,
감사 리포트를 CSV·PDF로 제공합니다.

*기밀(C·Classified)·민감(S·Sensitive)·공개(O·Open)

04 유연한 인증 & 연동

통합 로그 보관 · M365 90일 한계 해결 · SIEM 연동

M365 로그와 Security 365 로그를 통합하여 로그 확인 및 추적 관리를 할 수 있습니다.
90일 이상 저장이 필요한 로그관리 컴플라이언스를 E3 라이선스만 있어도 지원이 가능합니다.
SIEM 등 외부 로그 관리 서비스와의 연동 지원을 통해 확장성을 제공합니다.