

# DFAS

현장용 정보감사 및 증거분석 솔루션



Argos DFAS는 디지털포렌식 조사 기법을 자동화하여 비전문가라도 손쉽게 이용할 수 있는 휴대용 정보 감사 및 분석 솔루션입니다.

다양한 보안 솔루션의 도입에도 불구하고 정보 유출 사고가 지속해서 발생하고 있으며, 그 피해는 고스란히 기업뿐 아니라 국가적 손실로도 이어질 수 있습니다. 특히 정보 유출은 상당 부분 내부 사정을 잘 아는 직원이나 용역업체 직원들에 의해 주로 발생하고 있습니다. 이에 핵심 정보에 대한 보안강화와 더불어 내부 인력관리에 대한 중요성이 부각되고 있습니다.

이제 행위기반 분석을 통해 위협 요인을 사전에 탐지하고 주요 자료 및 유출 흔적을 다양한 각도에서 분석하는 사후 대응 전략이 필요합니다.

## 주요 기능



### 신속한 분석


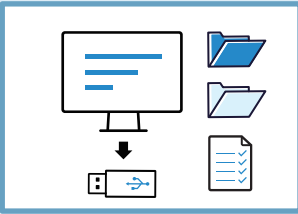

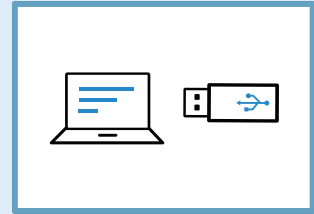

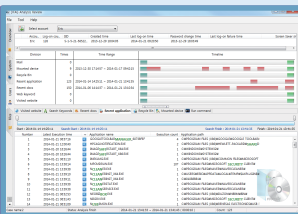
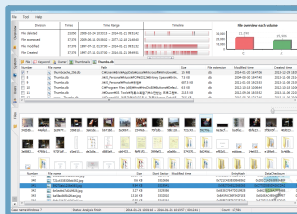
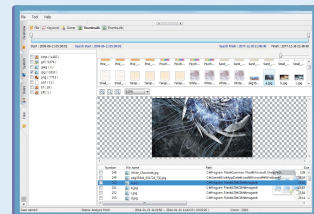
- 암호화(DRM) 문서에 대한 스캔 검색, 분류기능
- 불필요한 파일에 대한 영구삭제 등 관리기능 수행  
파일 내용 암호화 / 복호화 가능
- OS 레벨(레지스트리, 파일시스템 등)의 광범위한 분석을 신속 수행
- 악성코드 감염 진단을 위한 주요 정보 획득 기능 (활성 정보 수집)

### 빠른 사용자 행위 분석 보고서 생성


- 수집된 증거에 대한 자동 보고서 기능 탑재
- 사용자 pc 또는 랩탑에서 연결 구동하고 빠른 분석 보고서를 생성
- 사내 주요 키워드 및 확장자 분석 결과를 통계와 타임라인(시각화) 중심으로 리포팅
- 로고 및 보고서 제목 수정으로 사용자 맞춤형 보고서 출력

특징

“정보감사 및 행위 분석에 최적화된 사용자 편리성 강화”

 <p>비전문가도 손쉽게 사용할 수 있는 UI 제공 (마법사 형태의 분석 정책 설정)</p>	 <p>활성 시스템에 USB 형태로 사용자 행위 정보 수집</p>	 <p>케이스 관리 기능으로 다수의 장치 감사 가능</p>	 <p>무 설치형으로 분석대상 사용자의 PC 부담 최소화</p>
 <p>타임라인 기능으로 특정 시간대 행위 분석</p>	 <p>사용자 계정에서 실행된 프로그램 및 방문한 웹사이트의 검색 키워드, 다운로드 이력 분석</p>	 <p>Thumbnail DB에서 삭제된 이미지에 대한 흔적 확인 가능</p>	 <p>그림 파일 및 문서 파일에 대한 미리 보기 지원</p>

기대효과



**업무 효율성 저하를 최소화하는 정보감사 체계 구축**

- 통제와 룰셋기반 보안 솔루션의 한계/문제점 해소
- 보안 솔루션 확장과 도입에 대한 예산 절감
- 기업의 현실에 맞는 디지털포렌식 활용 대안 제시

**사용자 PC 로그 분석을 통한 다양한 이슈 도출**

- 비정형적인 보안 위협에 대한 사전 예방 및 사후 분석
- 분석이 어려운 행위 로그 및 OS 네이티브 로그 분석
- 정보자산에 대한 목록화로 정보자산 파기, 훼손, 유출 등에 대비하기 위한 정보 현황 관리

