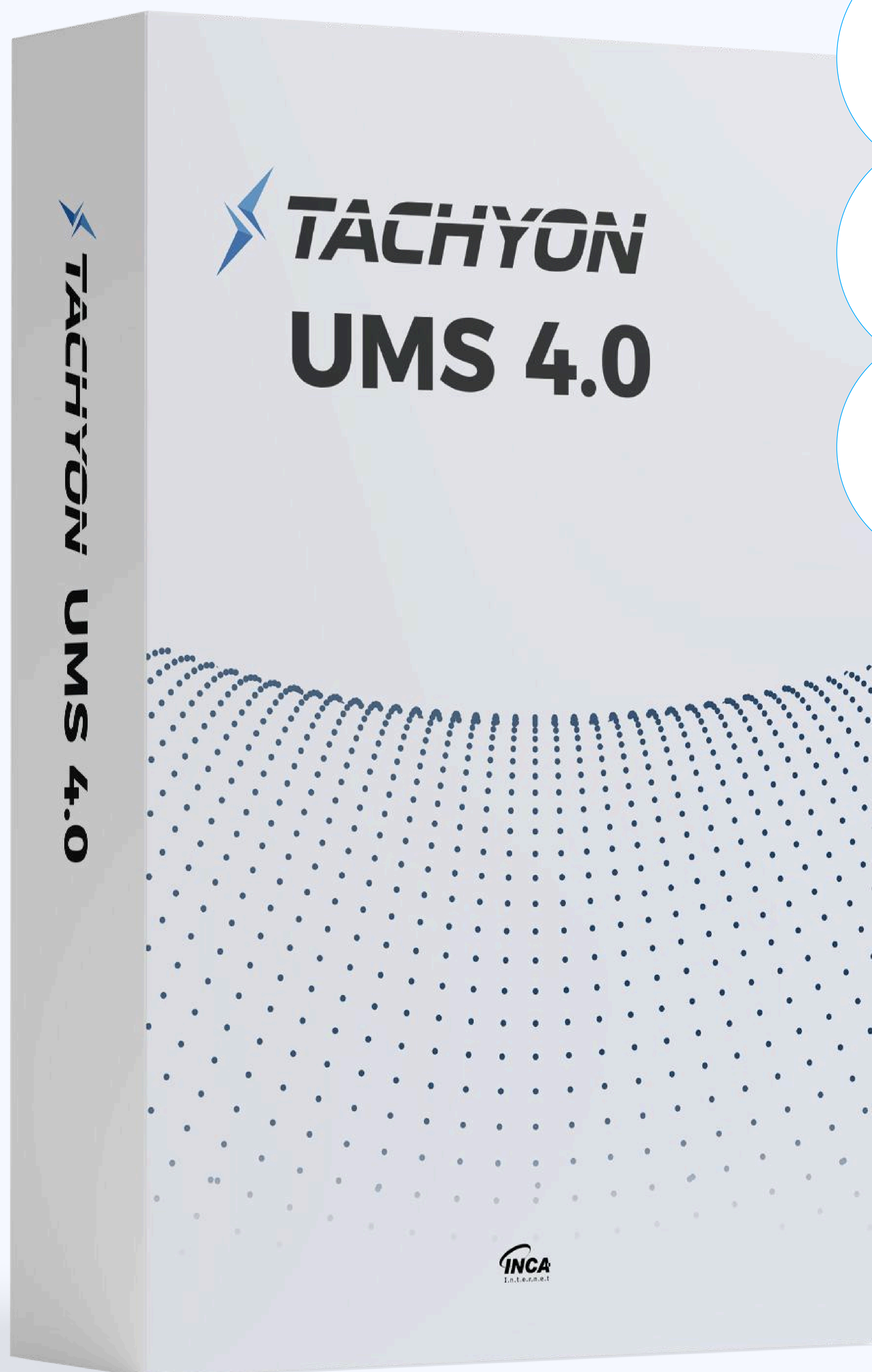


TACHYON UMS 4.0

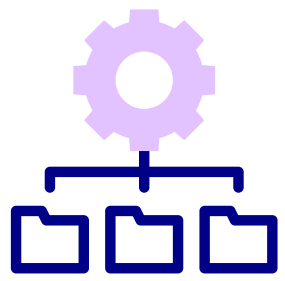
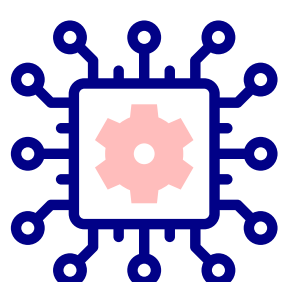
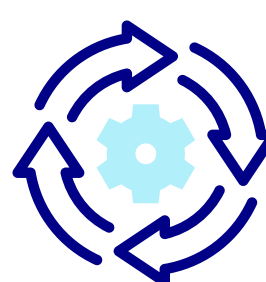
기업의 주요 정보가 보조관리 매체를 통해
유출되지 않도록 중앙 통제 및 관리, 보안 사고 위험 최소화를 위한
매체제어·보안 USB 솔루션



TACHYON UMS 4.0

TACHYON UMS는 조직 별·기간 별 유연한 보안 정책으로 보안USB를 비롯한 다양한 이동식 저장 매체의 반출입 등 사용을 효과적으로 제어하여 비인가된 이동식 저장매체를 통한 기업 정부 유출을 방지할 수 있는 중앙 관리 엔드포인트 보안 제품입니다.

주요기능

 보조기억 매체 관리 보조기억장치 등록 미등록 보조기억장치 사용 차단 보조기억장치 사용현황 파악 및 관리	 내부정보 유출 방지 보조기억장치 관리체계 구축 허가안된 보조기억장치를 사용한 내부정보 유출 방지	 분실시 데이터 자동 삭제 보조기억매체 분실 시 사용 통제 및 데이터 삭제 내부정보 유출 사고 위험 최소화
 강화된 매체제어 시스템 무선 랜 제어 기능, 데이터 케이블 매체 제어, 특정 프로세스에 대한 매체제어 예외 처리, 스마트폰 테더링 차단 기능	 보안USB 전용 보안 탐색기를 통한 보안 영역(Hidden Security Area)에 파일 압/복호화 강화된 보안 기능 제공	 유기적인 설정 관리 관리자는 보안정책을 설정하고 사용자의 요청에 따라 반출입 및 사용 권한 승인 / 반려 효율적이고 체계적인 매체 관리 가능

도입효과

Compliance 준수	- 금융감독원 전산장비 내부 통제 규정 - 금융위원회 보조기억매체 관리 대체 - ISMS 인증 심사 필수 항목 보조저장매체 관리를 통한 데이터 유출 및 보안 사고 방지 - 국정원 보조기억매체 보안 관리 지침 - 금융·공공기관 망분리 가이드 라인
보안감사	- 국정원 지침에 따른 보조기억관리대장을 통해 운영관리 효율성 도모 및 보안 감사에 효과적인 대응 - 보조기억매체에 대한 등록 / 관리를 자산 Lifecycle 제공
사용자 보안의식 고취	- 이동형 저장 매체의 무분별한 사용에 대한 의식 전환 유도로 주요 정보 유출에 대한 자발적인 내부 통제 프로세스 구현

제어매체 종류



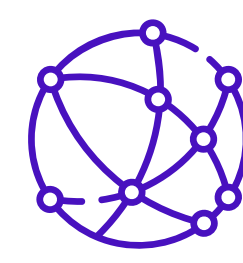
제어 매체 종류	
Wi-Fi 제어	Tathering
USB Network	DATA Cable
네트워크 공유폴더	IEEE 1394
USB 저장장치	스마트 카드
일반 저장 장치	영상장치
MTP 장치	블루투스
PCMCIA 어댑터	Floppy 드라이브
COM 포트	CD/DVD 드라이브
LPT 포트	무선네트워크 HUB
데이터 모뎀	적외선 장치

특장점



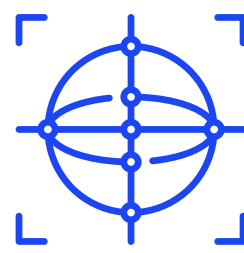
매체제어와 통제

- 비인가 저장 매체와 장치 통제 및 관리
- 무단 반출 장비에 대한 매체 및 네트워크 제어
- 매체 차단 시 일반 USB 예외 신청 연계



연동 API

- 각종 시스템 운영 알림 또는 신청/승인 알림에 대한 API 제공
- 요구 시나리오에 따른 메신저, 업무 시스템 연동



운영/보안 컴플라이언스

- 현황 데이터를 Excel 저장 기능
(예시 - 장기 미접속 조건으로
현황 데이터 저장)



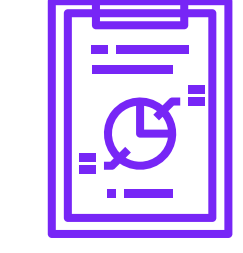
SYSLOG 로그 전송

- 로깅 레벨 별(Critical, Error, Info 등)
세부적인 항목 분류를 포함
- CEF, LEEF 포맷 지원



업데이트로백 기능

- 롤백 버전 지정, 해당 버전으로 롤백 / 업데이트
- 콘솔에서 롤백 명령 시 서버에 저장된 버전 목록에서 지정



대시보드 / 보고서 제공

- 관리서버 관리자 운영 로그 및 다양한 감사 로그
- 에이전트 현황에 Excel 저장 기능 추가
- 관리자를 위한 매체제어 모니터링 대시보드 제공

연관
컴플라이언스

개인정보와 관련한 컴플라이언스는 계속하여 강화되고 있으며 이를 위반한 기업에는 형사처분 또는 과태료 부과 등의 처벌이 내려질 수 있습니다. 기업에서는 컴플라이언스를 숙지하고 반드시 준수토록 해야 합니다.

관련 법규	규정 사항	세부 기능
전자금융감독규정 (금융위원회 2011.10.10)	① 사용자 인증 및 보조기억매체 접근 통제 ② 비상시 보조기억매체등의 전산 자료 안전 지출 및 긴급 파기 ③ 정기적으로 보조기억매체 보유 현황 및 관리 점검	- 사용자 접근 기록 및 매체 통제 - 보안 USB 초기화 - 관리자 권한을 위한 보안 USB / 일반저장매체 등 통합 매체 관리 모니터링 대시보드 제공
전산정보 이용 관련 내부통제 모범규준 (금융감독원 2011.04.01)	① 사용기록 및 승수신 정보 등이 포함된 로그기록을 보관 ② 승인 받지 않은 보조기억매체에 대한 쓰기 금지 운용 ③ 장비 및 사용자 별 비밀번호 사용	- 제품의 감사 로그를 검색 및 조회(에이전트, 매체제어, 방화벽, 자체보호, 서버 등) - 관리자 승인 절차를 통한 철저한 보안 관리 - 보안 USB 및 에이전트 개별 로그인
금융 전산망분리 보안 가이드라인 (금융위원회 2013.12.03)	① 인가된 관리자만 관리 서버 접근 ② 업무용으로 인가된 보조기억장치만 적용 ③ 업무상 보조기억매체 승인 및 반출/입 관리 ④ 인가된 보조기억매체 로깅 3년 이상 보관	- 관리자, 보조 관리자 계정 및 권한 설정 정보 관리 - 관리자 승인 절차를 통한 철저한 보안 관리 - 제품의 감사 로그를 검색 및 조회(에이전트, 매체제어, 자체보호, 서버 등)
USB메모리 등 보조기억매체 보안관리지침 (국가정보원 2009.07.04)	① 사용자 식별 인증 ② 지정 데이터 암호/복호화 ③ 지정된 자료 임의복제방지 ④ 분실 시 데이터보호를 위한 삭제 ⑤ 기타	- 사용자 인증 - USB 내의 비밀문서를 매체 내에 암호화 - KCDSA등의 암호화 표준 준수 - 사용자 및 매체 인증 없이 매체에 접근 불가 - USB 내 파일 완전 삭제(지정 횟수 이상) - 메모리 사용횟수, 기간, PC 등 설정 기능

인증 현황



KCMVP 국정원 검증필 암호모듈
보조기억매체 보안관리지침



GS 인증 1등급 획득
(인증번호 24-0451)

**보안기능
확인서 취득**

보안기능확인서
국정원 기준 보안기능 검증

조달등록



조달청
디지털서비스몰

물품식별번호

25455036 (Manager,1Server), 25455039 (PC Agent,1User)

25455038 (1PC, 8GB), 25455040 (1PC, 16GB), 25455037 (1PC, 32GB)



주 소 서울특별시 강서구 마곡중앙14로 53, 잉카인터넷

홈페이지 <https://www.inca.co.kr>

이 메 일 marketing_sales@inca.co.kr

대표전화 02-6411-8000 / Fax 02-6411-8080

Copyright © INCA Internet Corporation All rights reserved.