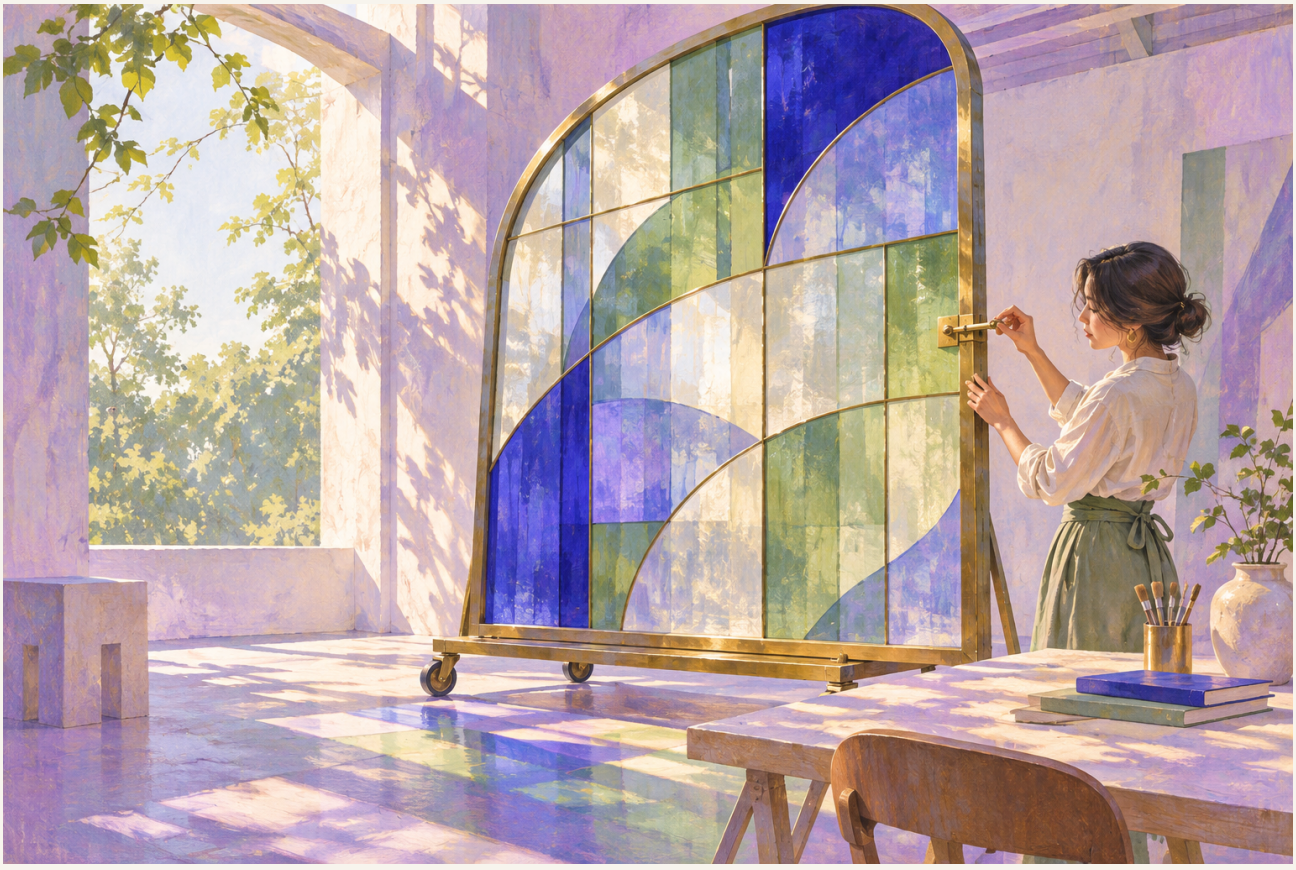
A DAILY PERSPECTIVE ON AI

AP *News*

AI 도구의 확장, 권한과 완료 근거를 함께

아티팩트의 앱 설치, 서버에 맡기는 장기 작업, PR의 리뷰와 수정까지 AI의 실행 범위가 넓어지고 있습니다. 제공 단계·권한·비용·검증 결과를 나누어 읽고, 실제 운영에서 확인할 경계를 살펴봅니다.



AI 제작 · 편집 일러스트 · 실제 제품 화면 아님

THE DAILY BRIEF · 5 STORIES

전날인 11월 27일 이후의 미사용 공식 발표만으로 5건을 확보하지 못해 최근 7일로 선정 범위를 넓혔습니다. 오늘은 Anthropic 공식 원문 5건으로, 11월 24일 발표 2건과 23일 발표·가이드·인터뷰 3건입니다. 이전 호의 원문과 같은 이슈를 제외했으며 인터뷰의 기대와 실제 검증 결과를 구분했습니다. AI 작성 및 원문 확인.



AI 제작 · 편집 일러스트 · 실제 제품 화면 아님

01 · AI NEWS

Claude 아티팩트의 앱 설치, 독립 창과 컴퓨터 권한 구분

Anthropic Claude · 발표 2026-11-24

Anthropic은 Mac·Windows에서 아티팩트를 앱처럼 여는 기능을 베타로 배포합니다.

Anthropic은 11월 24일 Install as app을 모든 요금제에 순차 베타 배포한다고 발표했습니다. 설치한 아티팩트는 별도 아이콘·창으로 열리고 원본을 편집하면 갱신됩니다. Claude 요청은 구독 사용 한도에 포함되며 앱을 열려면 온라인·로그인이 필요합니다. 기본 권한·개별 앱 권한·전체 컴퓨터 접근을 구분하고, 갱신 후에는 권한을 다시 묻지만 외부 웹사이트에서 온 부분은 별도로 바뀔 수 있습니다. Enterprise는 소유자가 켜야 하며 HIPAA-ready·하이브리드 배포는 제외됩니다. 일부 문서·슬라이드·시트는 설치할 수 없습니다.

AP의 관점 · AP의 교육·웹 도구 기획에 참고한다면, 가상 업무 도구를 창으로 분리하는 편의와 파일 접근 권한을 따로 검토하는 과제를 제안합니다. 앱 설치를 오프라인·무제한·자동 승인으로 해석하지 않고 버전·권한·사용 한도를 함께 확인할 수 있습니다.

공식 원문 읽기 ↗



AI 제작 · 편집 일러스트 · 실제 제품 화면 아님

02 · AI NEWS

MCP의 Skills·Tasks 확장, 기능마다 제공 단계가 다르다

Anthropic Claude · 발표 2026-11-24

Anthropic은 서버의 안내·장기 작업·중간 입력을 연결하는 MCP 기능을 설명했습니다.

11월 24일 발표에서 Skills over MCP는 Claude·Claude Code의 공개 베타로 소개됐습니다. Pro·Max·Ultra는 기본 활성이고 Team은 관리자 활성화가 필요하며 Enterprise는 추후 제공입니다. Tasks와 Elicitation은 Pro·Max·Ultra에 일반 제공되고 Team·Enterprise에는 순차 배포됩니다. Tasks는 오래 걸리는 일을 서버에 맡긴 뒤 결과를 받게 하고, Elicitation은 도중에 사용자 입력을 요청하게 합니다. 파일을 서버와 주고받는 File Uploads는 곧 배포될 기능으로 구분했습니다. 호환 클라이언트·서버의 지원도 확인해야 합니다.

AP의 관점 · AP의 뉴스레터·서비스 교육에 참고한다면, 가상 작업에서 요청·서버 진행·중간 확인·최종 결과를 따로 표시하는 설계를 제안합니다. 연결 기능이 있다는 사실과 해당 도구에서 실제 장기 작업을 완료한 증거를 구분하고, 비용·삭제 같은 행동은 입력과 승인을 확인하도록 구성할 수 있습니다.

공식 원문 읽기 ↗



AI 제작 · 편집 일러스트 · 실제 제품 화면 아님

03 · AI NEWS

Claude Ship, 리뷰·수정·정책 승인을 나눈다

Anthropic Claude · 발표 2026-11-23

Anthropic은 GitHub PR의 검토·수정·승인 결정을 연결하는 Claude Ship 베타를 소개했습니다.

Anthropic의 11월 23일 발표에 따르면 Claude Ship은 GitHub 저장소를 쓰는 Team·Enterprise에서 제공됩니다. Code Review는 일반 제공, PR Steward와 Claude Approvals는 베타입니다. PR Steward는 검사 실패·충돌·리뷰 피드백을 고치되 승인·병합을 하지 않도록 설계됐고, Approvals는 팀의 저장소 정책으로 승인 여부를 판단합니다. 기존 브랜치 보호와 필수 검사는 유지됩니다. 사용량은 비용을 늘릴 수 있으며 관찰 모드도 사용한 분류기·리뷰에 요금이 생길 수 있습니다. ZDR·HIPAA 구성·고객 관리 암호화 키 조직은 이용할 수 없습니다.

AP의 관점 · AP의 웹 구현 교육에 참고한다면, 가상 PR에서 검토 의견·수정 근거·승인 정책을 각각 확인하는 실습을 제안합니다. 한 단계가 성공했다고 전체 배포가 끝난 것으로 보지 않고, 관찰 모드와 실제 권한 부여의 차이도 기록할 수 있습니다.

공식 원문 읽기 ↗



AI 제작 · 편집 일러스트 · 실제 제품 화면 아님

04 · AI NEWS

코딩 에이전트 보안 안내, 모델 밖의 경계도 필요하다

Anthropic Claude · 발표 2026-11-23

Anthropic은 권한·실행 환경·외부 검사·중앙 정책을 겹치는 보안 체계를 설명했습니다.

Anthropic은 11월 23일 Team·Enterprise 조직을 위한 코딩 에이전트 보안 가이드를 공개했습니다. 모델의 거절 판단만 보지 않고, 실행 전 외부 검사·격리 환경·네트워크 경계·중앙에서 강제하는 정책·코드 보안 검토·사건 재구성 가능성을 확인하도록 안내합니다. 자격 증명·과도한 권한·미검토 확장·데이터 유출·프롬프트 주입을 다룹니다. 짧고 좁은 작업 권한과 감사 근거를 강조하는 설계 가이드이며, 안내를 따랐다는 사실만으로 모든 위험이 사라지거나 보안 인증을 받은 것은 아닙니다.

AP의 관점 · AP의 AI 교육·웹 서비스 실습에 참고한다면, 비밀값 없는 가상 환경에서 읽기·쓰기·외부 전송의 허용 범위를 먼저 정하는 과제를 제안합니다. 문서 속 지시와 실제 강제되는 경계를 구분하고, 막힌 행동과 검증 결과를 재현 가능한 기록으로 남길 수 있습니다.

공식 원문 읽기 ↗



AI 제작 · 편집 일러스트 · 실제 제품 화면 아님

05 · AI NEWS

KPMG 인터뷰, 고객 데이터의 수탁 책임과 AI 도입

Anthropic Claude · 발표 2026-11-23

Anthropic은 KPMG의 Todd Lohr가 설명한 도입·감독·데이터 통제 관점을 공개했습니다.

11월 23일 Anthropic이 공개한 인터뷰에서 KPMG US의 Todd Lohr는 고객 자료를 다루는 조직의 AI 도입을 설명했습니다. 그는 엄격한 시험·지속 관찰·사람의 감독·독립 검증을 포함한 Trusted AI 접근을 강조했습니다. 자동 오용 검토를 기존 위험관리의 추가 감독 계층으로 보고, EFS가 조직이 통제하는 클라우드에 자료를 보관하도록 지원할 것이라는 기대를 밝혔습니다. 이는 인터뷰 발언과 전망이며, 모든 고객의 도입 완료나 특정 성능·비용 개선을 입증한 대조 시험으로 읽어서는 안 됩니다.

AP의 관점 · AP의 기업 교육·콘텐츠·Lia Select 업무에 참고한다면, 가상 고객 자료의 소유자·허용 목적·접근 주체·보관·검토 책임을 나누는 점검표를 제안합니다. 공급사 기능 설명과 고객의 실제 계약·운영 조건을 구분하는 연습으로 연결할 수 있습니다.

공식 원문 읽기 ↗

ONE THING TO TAKE AWAY

AP의 시선

AI 도구가 독립 창을 갖거나 서버 작업을 맡는다고 해서 권한·비용·운영 책임까지 자동으로 해결되지는 않습니다. AP의 AI 교육·뉴스레터·웹 서비스와 Lia Select 업무에 참고한다면, 가상 적용안마다 제공 단계·작업 경계·승인 주체·완료 증거를 함께 적는 실습을 제안합니다. 계획이나 요청을 실제 완료로 간주하지 않고, 사람과 시스템이 확인한 범위를 명확히 기록할 수 있습니다.