MENLO SECURITY

데이터 시트

Menlo IRIS 브라우저 확장 프로그램

업무의 중심인 브라우저에서 사용자와 데이터, 기업을 지키는 핵심 보안



브라우저 교체 없이 기존 환경 그대로

주요 보안 기업이 신뢰하는 Menlo 엔터프라이즈 플랫폼 기반

브라우저 전용 통제와 가시성으로 기존 보안 체계 강화

업무의 중심, 보안의 사각지대 브라우저

생성형 AI를 통한 데이터 유출, 악성 확장 프로그램, 피싱, 소셜 엔지니어링, 멀버타이징, 계정 정보 탈취, 파일·데이터 보안까지. 브라우저를 둘러싼 보안 과제는 어느 기업에나 있습니다. 브라우저는 사실상 또 하나의 운영체제이자 거의 모든 업무의 출입구가 되었지만, 보안 책임은 어느 팀에도 명확히 속해 있지 않습니다. 브라우저는 IT팀이, 웹 트래픽 필터링은 네트워크 보안팀이, 디바이스는 엔드포인트 보안팀이, 로그인은 ID 관리팀이, 데이터 보호는 컴플라이언스팀이 맡습니다. 각 팀은 문제의 일부만 보고, 나머지는 기존 보안 체계가 막아 줄 것이라 생각합니다. 공격자가 노리는 것이 바로 이 브라우저 보안 공백입니다.

새로운 웹 도구가 정책보다 빠르게 쏟아지면서 이 공백은 갈수록 커지고 있습니다. 생성형 AI가 대표적입니다.

> 기업 디바이스에서 AI를 정기적으로 사용하는 직원은 1년 새 15%에서 45%로 3배 늘었고, 이 중 67%는 개인 계정으로 이용합니다. 기업당 평균 15% 이상의 사용자가 승인되지 않은 AI 브라우저 확장 프로그램을 설치해 쓰고 있습니다.[1]

> 침해 사고 5건 중 1건은 섀도우 AI와 관련이 있었으며, 섀도우 AI 사용이 많은 기업은 평균 침해 비용이 USD 670,000 더 높았습니다.[2]

[1] Verizon 2026 Data Breach Investigations Report (DBIR) [2] IBM Cost of a Data Breach Report 2025, Ponemon Institute 조사

주요 이점

PoV부터 실제 도입까지, 수개월이 아닌 단 몇 시간

복사·붙여넣기·업로드·다운로드·인쇄·스크린샷 시점의 데이터 유출 차단

승인된 생성형 AI 도구 사용 유도 및 입력 데이터 통제

DLP 위반, 바이러스, 멀웨어 파일 인라인 검사

콘텐츠 무해화(CDR) 애드온으로 안전한 파일을 그대로 활용

HEAT Shield 애드온으로 알려지지 않은 피싱·제로데이 위협까지 사전 차단

임직원이 설치한 모든 브라우저 확장 프로그램과 위험도를 한눈에 파악

사용자·디바이스·접속 대상·활동별 웹 세션 로그 중앙 수집

기존 보안 체계가 브라우저를 놓치는 이유

방화벽, SWG, EDR은 네트워크와 엔드포인트를 위해 설계되어 브라우저 세션 안에서 벌어지는 일은 보지 못합니다. 복사, 붙여넣기, 업로드, 인쇄, 스크린샷 같은 일상 행위가 사각지대에 놓이고, 그 대상이 생성형 AI라면 위험은 더 커집니다. 브라우저를 오가는 파일은 민감 데이터를 밖으로 내보내고 멀웨어를 안으로 들여올 수 있습니다. 게다가 대부분의 기업은 사용자가 설치한 확장 프로그램 현황조차 파악하지 못합니다. 소리 없는 업데이트 한 번으로 언제든 달라지는 확장 프로그램별 위험도를 판단하기란 더욱 어렵습니다.

브라우저 내장 보안 기능도 도움은 되지만 특정 벤더의 브라우저에서만 동작하며, 대부분의 기업은 여러 브라우저를 함께 씁니다. 제로데이 익스플로잇 방어나 완전한 콘텐츠 무해화(CDR)도 지원하지 않습니다. 브라우저를 지켜보는 장치가 없다면 침해나 데이터 유출이 일어난 뒤에야 문제를 알게 됩니다.

원인은 결국 하나입니다. 임직원이 이미 쓰는 모든 브라우저에 빠르게 적용할 수 있는 엔터프라이즈급 브라우저 보안이 없었다는 점입니다. 지금 필요한 것은 도구 재정비나 브라우저 교체, 수주간의 집중 작업 없이 바로 도입해 운영할 수 있는 브라우저 단의 가시성과 통제입니다.

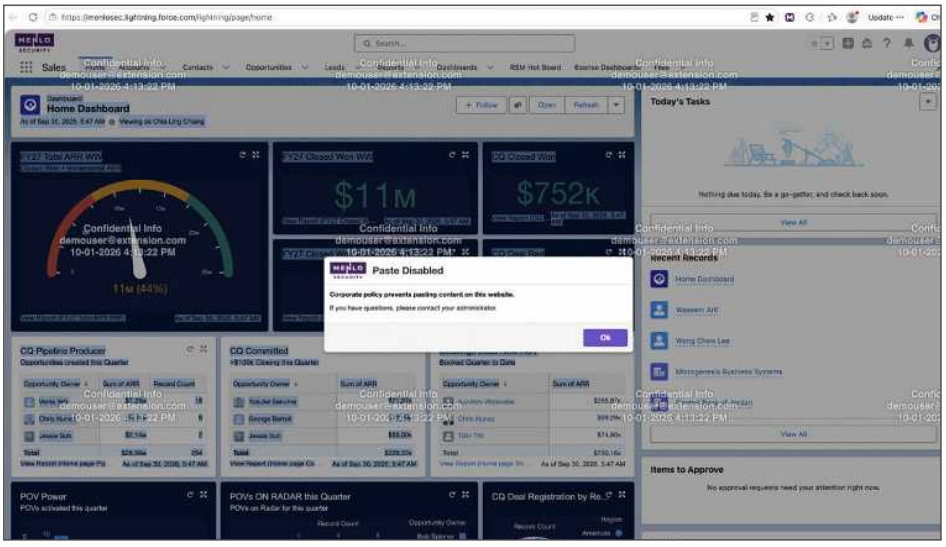
확장 프로그램 하나로 엔터프라이즈급 브라우저 보안

Menlo IRIS는 보안 엔터프라이즈 브라우저의 핵심 기능을 배포가 간편한 확장 프로그램으로 구현해, 사용자가 이미 쓰는 브라우저에 그대로 제공합니다. Chrome Web Store, MDM, Intune, JAMF 등 UEM 도구로 설치하고, 데이터 보호·파일 보안·웹 거버넌스·위협 차단·확장 프로그램 가시성을 업무 현장에서 바로 적용하며, 모든 정책은 단일 콘솔에서 관리합니다. 사용자는 익숙한 브라우저와 도구를 그대로 쓰며, 공격이 차단되는 순간까지 Menlo IRIS의 존재를 거의 느끼지 못합니다. 프록시나 인라인 복호화 없이 기존 네트워크, 엔드포인트, ID 보안 도구와 함께 동작하므로 통제 중복 없이 빈틈만 정확히 메웁니다.

필요한 기능을, 운영하기 쉬운 형태로

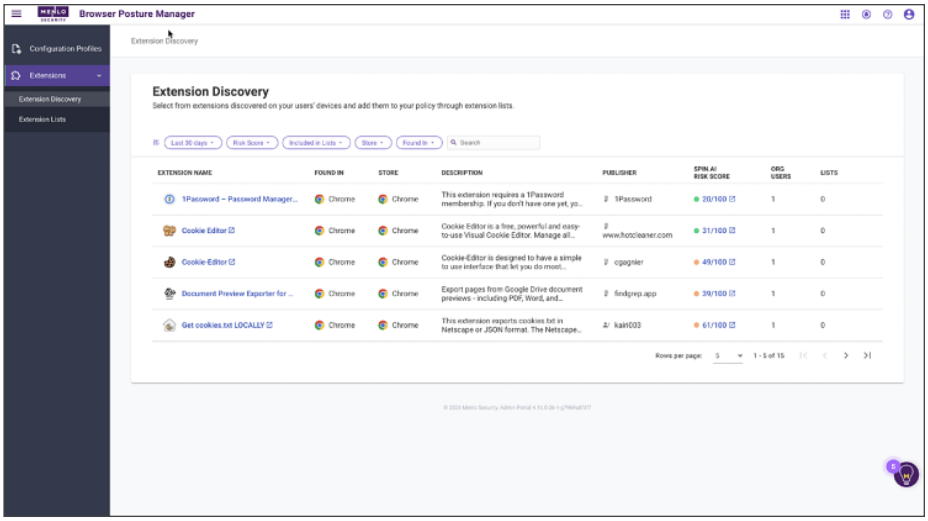
데이터 유출 방지

Menlo IRIS는 브라우저 세션 안에서 DLP 정책을 직접 적용하며, 사용자·그룹·도메인·위치별로 세분화해 설정할 수 있습니다.



- 클립보드(복사/붙여넣기), 파일 업로드/다운로드, 워터마크, 인쇄, 읽기 전용 페이지, 개발자 도구 제한, 스크린샷 방지 기능을 제공하며, 기본 사전과 사용자 정의 사전으로 핵심 자산을 보호합니다.
- **핵심 포인트:** 일상적인 행위, 특히 생성형 AI로 향하는 데이터는 반드시 관리하고 통제해야 합니다. Menlo IRIS는 사용자가 시도한 행위까지 보여 줍니다.

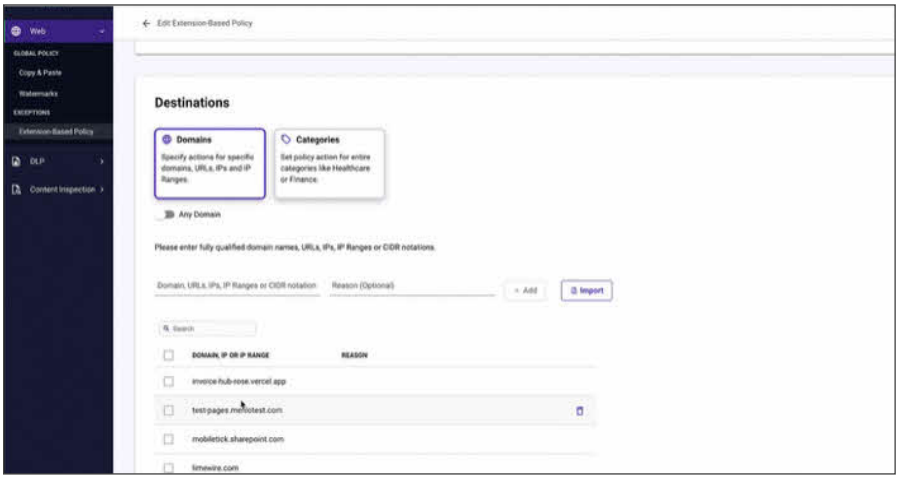
서드파티 확장 프로그램 가시성·위험 관리



Menlo IRIS는 엔드포인트에서 동작하므로 사용자 디바이스에 설치된 다른 확장 프로그램까지 파악합니다.

- 전사 서드파티 확장 프로그램 현황과 항목별 위험도를 한눈에 관리합니다.

- **핵심 포인트:** 확장 프로그램은 해킹당하거나, 개발자 라이선스가 탈취되거나, 공격자에게 인수될 수 있습니다. 업데이트가 웹 스토어에서 자동으로 조용히 배포되기 때문에 기업도 사용자도 뒤늦게 알게 됩니다.



웹 거버넌스 및 AI 사용 가드레일

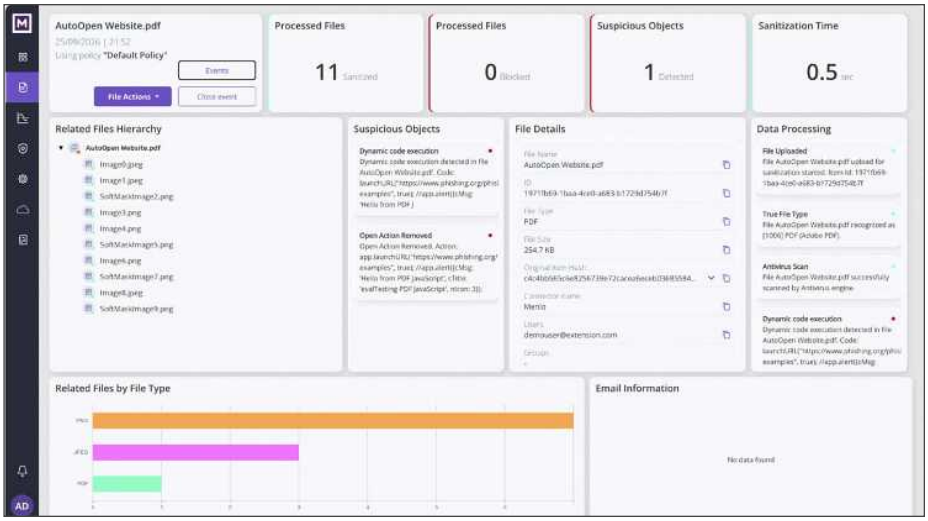
Menlo IRIS로 사용자의 웹 이용을 손쉽게 가이드합니다.

- 도메인·카테고리 기반 정책으로 위험하거나 승인되지 않은 사이트 접속을 막고, 생성형 AI를 포함한 승인된 사이트로 안내합니다.

- 차단 시 사용자에게 사유를 바로 안내해 헬프데스크 문의를 줄입니다.

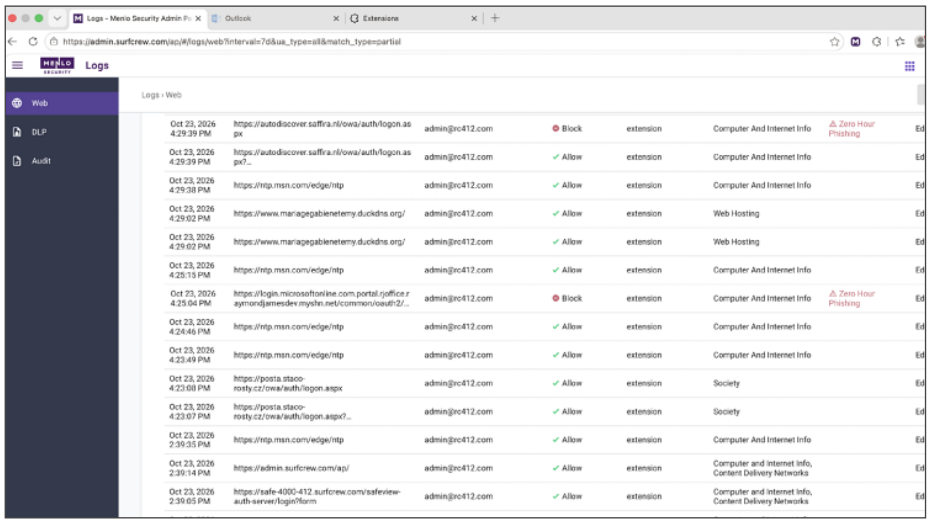
핵심 포인트: 업무에 꼭 필요한 도구를 금지하거나 업무 흐름을 끊지 않고도, 어떤 생성형 AI 도구가 쓰이는지 파악하고 입력되는 데이터를 통제합니다. 같은 통제를 모든 웹사이트에 적용할 수 있습니다.

차단·허용을 넘어선 파일 보안



위험한 파일 차단은 보안의 기본이지만 자칫 업무 흐름을 끊을 수 있습니다. Menlo IRIS는 검사 기능을 내장해 추측이나 요행에 기댈 필요가 없습니다.

- 사전·정규식 기반 인라인 DLP로 브라우저를 오가는 콘텐츠를 검사합니다.
- 해시 매칭, 안티바이러스, 클라우드 샌드박스 분석을 통합해 파일에 자동 적용합니다.
- 콘텐츠 무해화 및 재구성(CDR)을 더하면 한층 강력하게 보호할 수 있습니다. CDR은 파일을 무조건 차단하지 않고, 악성 요소만 제거해 바로 쓸 수 있는 안전한 파일로 재구성합니다.
- **핵심 포인트:** 공격자는 일반적인 필터를 피하려고 파일 안에 링크와 익스플로잇을 숨겨 둡니다.

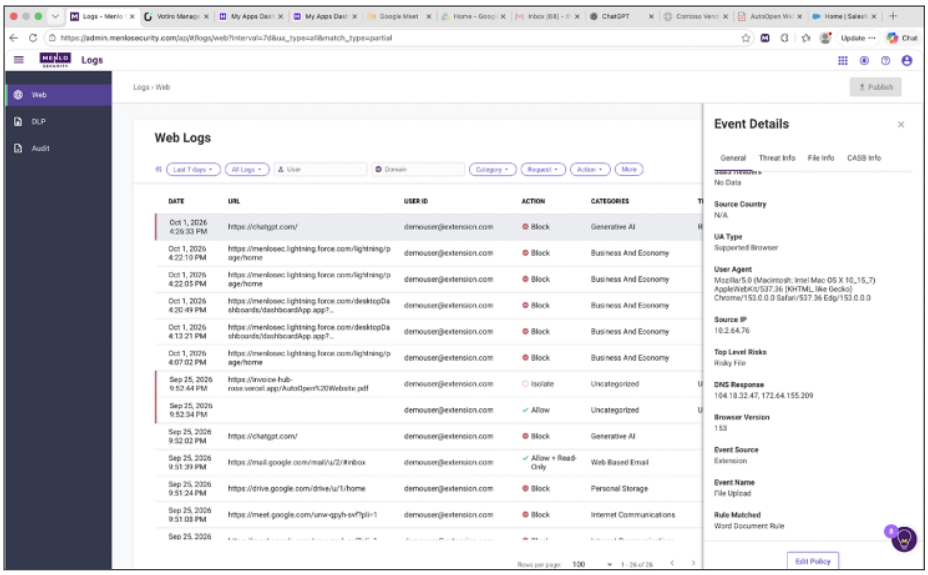


제로데이 위협까지 막아내는 AI 기반 위협 탐지

Menlo IRIS에 HEAT Shield AI를 더하면, AI 기반 탐지로 새로운 익스플로잇이 알려지기 훨씬 전부터 선제 대응할 수 있습니다.

- 의도 기반 실시간 탐지로 피싱, 멀버타이징, 소셜 엔지니어링 공격을 사용자가 클릭하기 전에 차단합니다.
- HEAT Shield는 URL 목록, 시그니처, 침해 지표가 갱신되기를 기다리지 않고 페이지의 실제 동작을 분석합니다.
- **핵심 포인트:** 대부분의 브라우저 보안 도구는 정적 목록에 의존합니다. 선제적 탐지는 아직 아무도 파악하지 못한 악성 행위까지 찾아냅니다.

경영진이 요구하는 가시성과 거버넌스



기존 보안 체계로는 브라우저 안의 사용자 활동을 파악하기가 어렵거나 사실상 불가능했습니다. Menlo IRIS는 모든 브라우저·확장 프로그램 이벤트를 기록하고 언제든 검색할 수 있습니다.

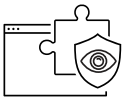
- 사용자, 디바이스, 접속 대상, 활동별 웹 로그를 중앙에서 수집하고, 감사 추적과 전사 확장 프로그램 현황을 언제든 확인합니다.
- SOC 2, HIPAA, GDPR 등 규제 대응을 준비하는 기업은 Insights와 맞춤형 보고서로 필요한 감사 추적을 확보할 수 있습니다.

- **핵심 포인트:** 컴플라이언스 위반은 큰 비용으로 이어지고, 감사 대응에는 많은 시간이 듭니다. 가시성을 확보하려고 SOC를 새로 구축할 필요는 없습니다.

Menlo IRIS 필수 인증

Menlo IRIS는 엔드포인트에서 동작하므로, 사용자가 브라우저로 인터넷, 기업 SaaS, 내부 애플리케이션에 접속하기 전에 인증을 의무화할 수 있습니다.

- Menlo IRIS 인증 의무화를 자동으로 적용합니다.
- 인증 공급자와 연동해 ID 컨텍스트와 로그인을 지원합니다.
- **핵심 포인트:** 모든 사용자가 Menlo IRIS에 인증하도록 해 웹 활동을 모니터링하고 필요한 데이터 보안 통제를 적용합니다



간편한 배포, 간편한 운영

Menlo IRIS는 Chrome Web Store, MDM, Intune, JAMF 등 UEM 도구나 관리형 브라우저 설정으로 배포합니다. 구성이 간단해 PoV에서 실제 도입까지 빠르게 진행할 수 있습니다. 기존 도구로 정책을 배포하고, 단일 콘솔에서 모든 것을 관리하며, 관리형 디바이스와 BYOD 디바이스의 모든 이벤트 로그를 확보합니다. 하드웨어 추가나 브라우저 교체가 필요 없고, 사용자가 기존 브라우저를 그대로 쓰기 때문에 각 벤더의 보안 패치도 배포 즉시 적용됩니다.

엔터프라이즈급 브라우저 보안

브라우저는 업무가 이뤄지는 곳이자, 공격자와 데이터 유출, 위험한 확장 프로그램이 사용자와 맞닿는 지점입니다. Menlo IRIS는 브라우저 전환이나 별도 인력이 필요한 신규 플랫폼 구축 없이, 실제 브라우저 사용 전반에 대한 가시성과 보안, 통제를 제공합니다.

Menlo IRIS는 보안에 가장 엄격한 세계 유수 기업들이 사용하는 Menlo의 검증된 엔터프라이즈 플랫폼을 기반으로 합니다. 위험 환경이 달라지면 차별화된 애드온부터 하이브리드 배포, 완전한 격리까지 단계적으로 확장할 수 있어 언제나 필요한 만큼의 보안을 정확히 갖출 수 있습니다.

Menlo Security 소개

Menlo Security는 사람과 자율 AI 에이전트가 함께 일하는 하이브리드 업무 환경을 관리하기 위해 설계된 업계 최초의 인프라, 브라우저 보안 플랫폼(BSP)을 개척한 기업입니다. 브라우저를 새로운 엔터프라이즈 운영체제로 보고, 사람의 검증 없이 기계 속도로 움직이는 AI 에이전트가 만드는 고유한 위험을 해소하는 “Guardian Runtime”을 제공합니다. Menlo 플랫폼은 레거시 데이터와의 범용 연결과 모든 세션에 대한 통합 제로데이 위협 방어로, 에이전틱 엔터프라이즈가 안심하고 AI를 확대할 수 있도록 지원합니다. 세계 10대 금융기관 중 8곳과 주요 정부 기관을 포함한 1,000개 이상의 글로벌 기업이 Menlo를 신뢰하며, 800만 명 이상의 사용자와 수백만 건의 동시 AI 에이전트 세션을 보호하고 있습니다. 미국 캘리포니아 마운틴뷰에 본사를 두고 JPMorgan Chase, American Express Ventures, Vista Equity Partners 등의 투자를 받은 Menlo는 에이전틱 시대의 브라우저 보안을 이끌고 있습니다. 자세한 내용은 **www.menlosecurity.com**에서 확인하실 수 있습니다.

© 2026 Menlo Security, All Rights Reserved.

자세히 알아보기: https://www.menlosecurity.com
문의하기: ask@menlosecurity.com