MENLO SECURITY

멘로시큐리티
글로벌 브라우저 보안 솔루션

The Secure Enterprise Browser Solution

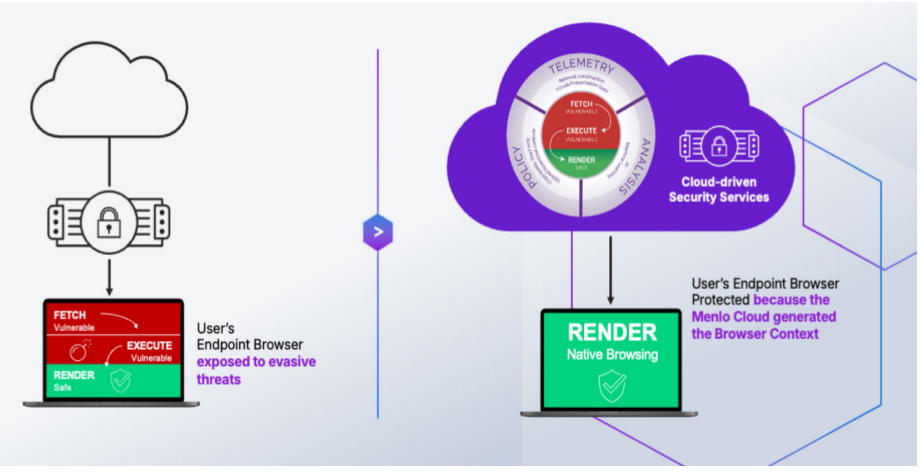
Secure **The Browser.**
Secure **The Enterprise.**

Menlo Remote Browser Isolation

브라우저 기반 악성 소프트웨어 및 피싱 위협 차단으로 안전한 업무 환경 실현

기업의 핵심 애플리케이션, 하지만 보안의 가장 큰 도전 과제 – 바로 브라우저입니다.

인터넷은 오늘날 기업에 필수적인 업무 도구입니다. 전 세계의 분산된 사용자들은 일상적인 업무를 위해 웹사이트, 클라우드 앱, SaaS(Software-as-a-Service) 플랫폼에 빠르고 안정적으로 접근해야 합니다. 그러나 인터넷은 악성 위협과 교묘하고 적응력 있는 위협(HEAT) 공격으로 가득 차 있어 기업에 큰 위험을 안겨줍니다. 보안 팀은 사용자들이 어디서든 더 효율적이고 스마트하게 작업할 수 있도록 하면서 웹 브라우징을 안전하게 보호할 수 있는 새로운 접근 방식이 필요합니다.



Menlo Secure Cloud Browser Isolation으로 회피형 위협을 엔드포인트에서 완벽 차단

주요 이점

- 안전한 업무 환경 제공
- 생산성 극대화
- 비지니스 연속성 보장
- 제로 트러스트 보안 원칙 준수

기존 탐지 기반 보안 방식으로는 최신 위협을 완벽히 막기 어렵습니다. 이제 HEAT 공격, 랜섬웨어, 제로데이, 자격 증명 탈취와 같은 정교한 위협에도 강력하게 대응할 수 있는 보안이 필요합니다.

Menlo Remote Browser Isolation과 Menlo Secure Cloud Browser는 근본적으로 차원이 다른 접근 방식을 통해 브라우저 기반 위협을 완벽히 제거하고, 한 발 앞선 보안을 제공합니다.

주요 기능

브라우저 기반 위협에 대한 선제적 보호

- 보안이 강화된 클라우드 환경에서 모든 웹 콘텐츠를 실행하여 기존 브라우저 보안의 취약점을 최소화합니다. Menlo는 JavaScript나 은닉 코드에 숨겨진 악성 콘텐츠 및 동적 페이로드가 엔드포인트에서 실행되지 않도록 차단하여, 기존 보안 솔루션을 우회하는 고급 악성 코드로부터 강력한 보호를 제공합니다.

안전한 클라우드 문서 및 아카이브 뷰어

- 파일을 엔드포인트에 다운로드하지 않고도 안전하게 문서를 열고 확인할 수 있습니다. Menlo의 보안 문서 및 아카이브 뷰어는 고품질 보안 버전의 파일을 제공하며, 인쇄, 검색, 복사/붙여넣기, 공유 기능을 지원하여 데스크톱과 모바일 환경에서도 원활한 작업이 가능합니다.

엔드투엔드 브라우저 가시성 제공

- Menlo는 회피형 위협 정보와 실시간 대응 가능한 경고를 SOC 팀에 제공하여 가시성을 극대화하고 인시던트 대응 능력을 향상시킵니다. 상세한 위협 인텔리전스 및 브라우저 포렌식 데이터는 기존의 로그 통합, 자동화 및 보안 오케스트레이션 도구와 연계되어 최적의 성능을 보장합니다.

통합 브라우저 포렌식 지원

- 인시던트 대응 팀은 Menlo Browser Forensics를 활용하여 브라우저 세션의 전체 시각적 타임라인을 기록할 수 있습니다. 이를 통해 스크린샷, 사용자 키 입력, 페이지 리소스 등 상세한 탐색 정보를 확인하고, 위협 발생 시 신속하게 대응할 수 있습니다.

유연한 배포 및 간편한 관리

- Menlo는 모든 브라우저와 모든 데스크톱 및 모바일 디바이스에서 지원되므로, 사용자는 기존 브라우저를 그대로 활용할 수 있습니다. 추가적인 엔드포인트 소프트웨어 설치가 필요하지 않으며, 활성화 후 관리 포털에서 손쉽게 정책을 설정하고 모니터링할 수 있습니다.

원활한 API 및 서드파티 연동

- Menlo는 SSO, SIEM, MDM, 방화벽, 프록시, AV, 샌드박스, CDR, SOAR, SD-WAN, SASE 등 다양한 보안 솔루션과 유연한 API 연동을 제공합니다.

브라우저 내부 위협 차단 및 위험한 사용자 활동 방지

- 사용자의 기기에서 직접 웹 콘텐츠를 실행하는 대신, Menlo의 RBI 기술은 안전한 가상 컨테이너 내에서 콘텐츠를 처리하여 회피형 악성 코드, 정교한 피싱 공격, 기타 보안 위협이 엔드포인트에 도달하는 것을 원천 차단합니다. 이러한 접근 방식 덕분에 사용자는 웹사이트 및 애플리케이션과 원활하게 상호작용할 수 있으며, 보안은 더욱 강력해지고 브라우징 성능에는전혀 영향을 주지 않습니다.

Menlo Security 브라우징 포렌식

브라우저 트래픽의
완벽한 가시성 확보

필요한 정보만 빠르게
복잡한 데이터 분석 없이
바로 활용

브라우저 트래픽 가시성 확보의 도전 과제

전통적인 보안 솔루션은 기업 네트워크, 엔드포인트, 애플리케이션을 강력하게 보호할 수도록 설계되었습니다. 하지만 브라우저 콘텐츠는 여전히 기존 보안 시스템에서 보이지 않는 영역으로 남아 있습니다.

- ✓ 피싱 공격을 통해 사용자가 자격 증명을 입력하도록 유도하고, 이를 활용해네트워크에 접근합니다.
- ✓ 데이터 또는 지적 재산(IP) 유출이 발생했을 때, 보안팀은 유출 사실은 파악할 수 있지만, 정확히 어떻게 발생했는지는 알기 어렵습니다.
- ✓ 인시던트 대응팀은 공격을 감지하지만, 해커가 어떻게 네트워크에 침투했는지 추적하기 어렵습니다.
- ✓ 피싱 공격이 탐지되더라도, 사용자가 어떻게 반응했는지, 어떤 계정 정보가입력되었는지, 어떤 자산이 노출되었는지 불분명합니다.

이제 위협을 포착하고, 강력하게 보호하세요

Browsing Forensics는 Menlo Cloud기반에서 동작하며, Secure Cloud Browser를 활용해 사용자의 로컬 브라우저와 동일한 강화된 디지털트윈을 동적으로 생성합니다. 차세대 Remote Browser Isolation 기술을 적용한 Secure Cloud Browser는 지연 없이 실시간 보호를 제공하며, 사용자 경험에 영향을 주지 않습니다.

핵심 포인트

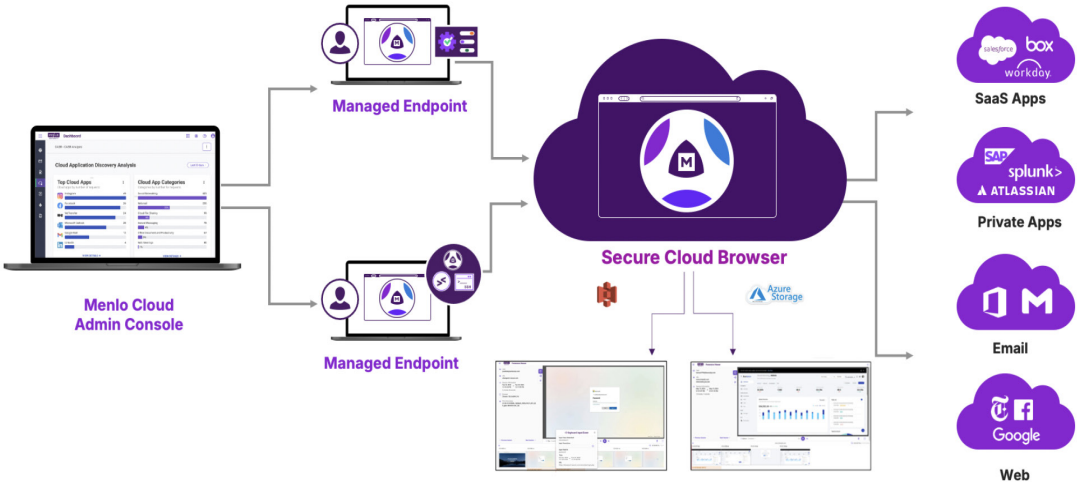
확실한 증거로 보안 경고에 대응

사용자가 잠재적 위협 사이트와 어떻게 상호작용하는지 공격자가 침투하기 전에 확인하세요.

앱과 데이터에 대한 사용자 접근이 정책을 준수하도록 보장하세요.

Secure Application Access와 함께 사용하면 내부 애플리케이션과 데이터를 더욱 안전하게 보호할 수 있습니다.

Menlo Protect와 HEAT Shield AI를 결합하면, 피싱 공격이 랜섬웨어나 협박으로 발전하기 전에 내부를 완벽히 파악할 수 있습니다.



보안 사고를 신속하게 해결하세요!

원클릭으로 브라우징 세션 데이터를 확인하여 조사 시간을 획기적으로 단축할 수 있습니다.

Browsing Forensics의 주요 활용 사례:

- Phishing incident response
- Data security
- Threat hunting
- Generative AI sites
- Security research
- Insider threats
- Audit and compliance

보안 인시던트가 해결되지 않는 시간마다 조직의 위험 노출은 더욱 커집니다.

Menlo Browsing Forensics를 통해 브라우징 정보와 사용자 활동을 확인하여 인시던트가 어떻게 발생했는지 정확히 파악할 수 있습니다. 사용자의 브라우징 세션 내 행동을 분석함으로써, 실수로 인한 행동인지 또는 악의적인 의도가 있었는지 신속하게 판단할 수 있습니다.

지금 바로 활용할 수 있는 인사이트

보안 이벤트와 인시던트를 명확하게 확인하세요. 보안 이벤트가 발생한 원인과 인시던트의 세부 내용을 정확히 파악할 수 있습니다. Menlo Browsing Forensics는 웹 세션과 사용자 활동을 자동으로 기록하여, 언제든지 브라우저 세션의 전체 이력을 확인할 수 있도록 지원합니다. 기록된 데이터는 즉시 AWS, Azure 또는 원하는 저장 위치로 전송되며, SIEM과 연동할 수도 있습니다. 또한, Menlo는 자체적으로 기록을 보관하거나 열람하지 않으므로, 조직과 사용자의 프라이버시가 완벽히 보호됩니다.

MENLO SECURITY

Menlo Protect with HEAT Shield AI

AI 기반 위협 차단 동적 정책 제어로 더욱 강력하게!

끊임없이 진화하는 공격자보다 한 발 앞서 나가는 솔루션

진화하는 브라우저 기반 위협, 이제는 새로운 보안 전략이 필요합니다! . 공격자들은 끊임없이 전술을 발전시키며, AI 기반 피싱 키트, 제로데이 URL, 그리고 정교한 소셜 엔지니어링 기법을 활용해 가장 경계심이 높은 사용자조차 속이려 합니다. 기존 보안 솔루션은 IP, 도메인 등 오래된 IOC 나 도메인 연령 및 평판과 같은 쉽게 조작 가능한 휴리스틱 방식에 의존하고 있어 점점 효과가 떨어지고 있습니다. 이처럼 빠르게 변화하는 위협환경에서는 **브라우저 보안**을 핵심 방어 전략으로 삼아야 합니다.

최신 회피형 피싱 공격을 막는 AI 기반 위협 차단

Menlo Protect with HEAT Shield AI는 AI 기반 즉시 검사 (On-Click Inspection)와 컴퓨터 비전 기술을 활용하여 웹 콘텐츠를 동적으로 분석하고, 정교한 피싱공격을 실시간으로 탐지 및 차단합니다.

기존 보안 솔루션이 의존하는 IP, 도메인평판 등 정적 지표 대신, 웹 페이지의 동적 요소를 분석하여 신규 URL이나 정교한사칭 공격도 효과적으로 방어할 수 있습니다. 이 기술은 브라우저 내부에서 AI 분석을 수행해, 기존 네트워크 보안 솔루션이 탐지하지 못하는 회피형 위협 신호(evasive threat signals)까지 포착할 수 있습니다. 이를 통해 보안팀은 제로아워 (Zero-Hour) 피싱 공격을 예방하고, 더욱 강력한 가시성을 확보할 수 있습니다.또한, **Menlo Security는 AI 기반 위협 분석을 활용하여 공격 노출 시간을 단축하며, 기업의 보안 환경을 한층 더 강화합니다.**

핵심 포인트

브라우저는 기업에서 가장 중요한 자산입니다. 지난해 브라우저 기반 피싱 공격이 198% 이상 급증했으며, 그중 30%는 기존 보안 솔루션을 우회하는 회피 기술을 활용한 공격이었습니다.

실제로 피싱 링크의 75%가 기존에 알려진 신뢰할 수 있는 웹사이트에서 발생한 것으로 확인되었습니다.

제로아워 피싱 공격이 최초로 등장한 후, 기존 보안 도구의 탐지 메커니즘에 추가되기까지 평균 6일의 지연 시간이 발생합니다.

주요 기능

✓ **제로아워 (Zero-Hour) 피싱 방어**

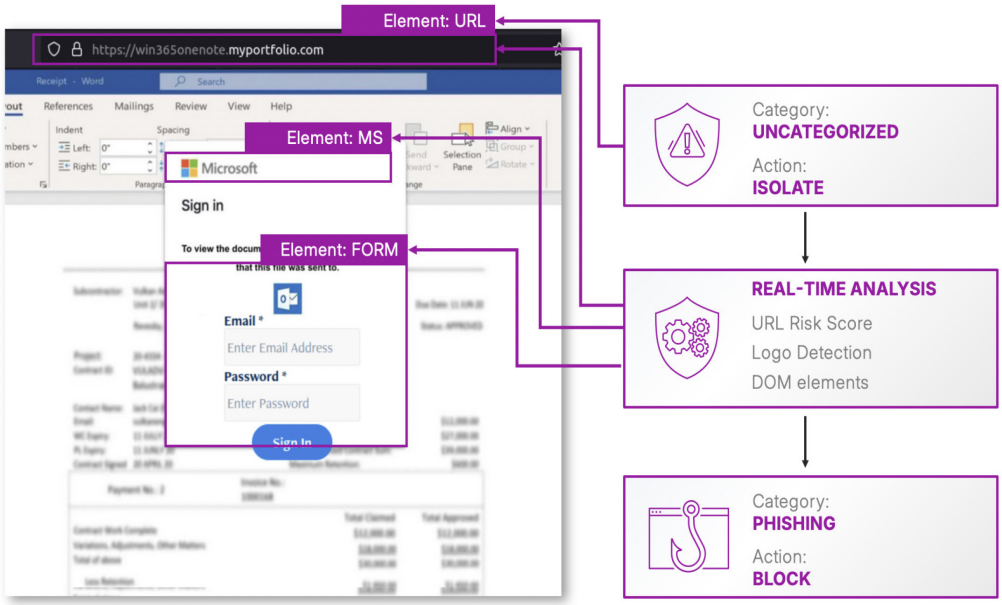
사용자의 로컬브라우저가 웹사이트에 직접 접근하는 대신, 모든 웹 요청은 Menlo Secure Cloud Browser내에서 실행됩니다. 이를 통해 안전하고 깨끗한 콘텐츠만 사용자에게 전달되며, 제로아워 피싱공격을 실시간으로 탐지하고 차단할 수 있습니다.

✓ **AI 기반 즉시 검사 (On-Click Inspection)**

모든 웹 요청은 Secure Cloud Browser에서 실행되며, AI가 JavaScript, DOM 요소, 로고, 입력 필드, URL 경로 등을 분석하여 실시간 보안 검사를 수행합니다. 피싱 또는 악성 코드 위협이 감지되면, 정확한 정책 제어를 통해 사이트를 완전히 차단하거나 읽기 전용 모드로 렌더링하여 데이터 입력을 방지합니다.

✓ **실시간 로고 감지**

Menlo Protect with HEAT Shield AI는 컴퓨터 비전 기술을 활용하여 브랜드 및 서비스 사칭 웹사이트를 식별합니다. 이미지 기반 피싱 공격을 탐지하고, 대규모 동적 공격을 빠르고 정확하게 차단합니다. 또한, 사용자 지정 로고를 지원하여 조직을 표적으로 한 공격으로부터 보호할 수 있습니다.



Menlo Protect with HEAT Shield AI는 분류되지 않은 웹사이트를 실시간으로 분석하여 해당 사이트가 정상적인지 또는 악성인지 판별합니다.

✓ **실시간 위협 경고와 포괄적인 브라우저 가시성**

Menlo Protect with HEAT Shield AI는 회피형 위협 인텔리전스와 실시간 경고를 제공하여 보안 가시성을 높이고 인시던트 대응을 강화합니다. 상세한 위협 인텔리전스 및 경고는 Menlo Security 관리 포털의 대시보드에서 확인 가능하며, API를 통해 SIEM/SOC 도구와 연동하여 더욱 효과적인 보안 운영을 지원합니다.

✓ **간편한 배포 및 쉬운 관리**

Menlo Protect with HEAT Shield AI는 모든 브라우저와 모든 기기를 지원하며, 사용자가 기존 브라우저를 그대로 사용할 수 있도록 합니다. IT 팀이 추가적인 엔드포인트 소프트웨어를 관리할 필요 없이, 활성화 후 관리 포털에서 손쉽게 정책을 정의하고 모니터링할 수 있습니다.

✓ **글로벌 가용성**

Menlo Protect with HEAT Shield AI는 클라우드 네이티브 아키텍처를 기반으로 전 세계 어디서나 사용 가능하며, 기업 내 모든 사용자, 모든 탭, 모든 웹 세션에서 위험 없는 로컬 브라우징 환경을 제공합니다.

Menlo Protect with HEAT Shield AI 로 브라우저 기반 피싱 공격을 완벽 차단

Menlo Protect with HEAT Shield AI와 Menlo Secure Cloud Browser는 기업이 기존 브라우저를 효과적으로 관리하고, 사용자를 보호하며, 애플리케이션 접근과 기업 데이터를 안전하게 보호할 수 있도록 지원합니다. 단일 인터페이스에서 정책 관리, 보고, 위협 분석을 간편하게 수행할 수 있어 보안 운영의 효율성을 극대화합니다. 오늘날 기업에게 최신 보안 위협에 대비하는 것은 최우선 과제지만, 기존 보안 솔루션은 제한적이며 사후 대응에 머무르는 경우가 많습니다. Menlo Security는 근본적으로 다른 접근 방식을 통해 브라우저 공격 표면을 제거하며, 클라우드 보안의 가능성을 완전히 실현하는 유일한 솔루션입니다. Menlo는 손쉽게 배포할 수 있는 제로 트러스트(Zero Trust) 보안 모델을 제공하며, 공격을 원천 차단하면서도 보안 운영팀의 부담을 줄여줍니다. 또한, 사용자가 온라인에서 업무를 수행하는 동안 보안이 눈에 띄지 않도록 적용되어 원활한 사용자 경험을 보장합니다.

사용자와 기업을 회피형 위협으로부터 보호하세요.

Menlo Protect with HEAT Shield AI는 제로아워(Zero-Hour) 피싱 공격 및 회피 기술을 사용하는 악성 코드 공격을 실시간으로 식별하고 차단합니다. 기존 보안 솔루션이 막지 못하는 정교한 위협으로부터 사용자와 기업을 안전하게 보호합니다.

MENLO SECURITY

Secure Application Access

안전한 클라우드 브라우징과 글로벌 프라이빗 액세스 아키텍처로 제로 트러스트 접근을 실현!

기존 네트워크 접근 방식의 한계

기업은 기존 네트워크 접근 방식이 초래하는 비용, 복잡성, 보안 위험을 해결해야 합니다. 또한, 제로 트러스트(Zero Trust) 구현을 위해 네트워크 인프라를 직접 제어하거나 복잡한 Security Service Edge(SSE) 배포가 필요한 문제도 고려해야 합니다. VPN과 VDI와 같은 전통적인 접근 방식은 복잡한 아키텍처와 확장성의 한계로 인해 사용자 경험이 저하되는 경우가 많습니다. 또한, 사용자 활동에 대한 가시성을 제한하고, 관리되지 않는 장치에 과도한 접근 권한을 제공할 가능성이 있습니다.

Menlo Secure Application Access (SAA):

쉽고 안전한 엔터프라이즈 애플리케이션 및 SaaS 접근 보안

✓ **제로 트러스트 접근을 가장 빠르게 구현**

보안 및 IT 팀은 복잡하고 비용이 많이 드는 아키텍처 변경 없이, 몇 번의 클릭만으로 엔터프라이즈 애플리케이션에 대한 제어된 접근을 제공

✓ **비즈니스 핵심 애플리케이션과 데이터 보호**

Menlo Secure Cloud Browser 기반의 SAA는 네트워크 분리를 유지하여, 감염된 엔드포인트, 취약한 브라우저, 인터넷 트래픽으로부터 애플리케이션을 안전하게 보호합니다. 또한, Menlo Secure Cloud Browser에서 정책 기반 데이터 제어가 적용되므로, 중요한 데이터가 엔드포인트로 전송되지 않습니다.

✓ **장소와 기기에 관계없이 원활한 업무 지원**

사용자는 별도의 소프트웨어 설치 없이, 기존에 사용하던 브라우저의 포털 또는 확장 프로그램을 통해 허용된 애플리케이션에 접근할 수 있습니다.

주요 이점

1) Zero Trust 보안:
   접속 시 인증 및 권한 확인

2) 암호화 및 민감한 정보 보호

3) 무제한 애플리케이션 접근:
   원격 근무 및 분산 팀 지원

4) 사용자 경험 개선:
   직관적이고 안전한 접근

5) 클라우드 기반:
   확장성과 비용 효율성

6) 자동화된 보안 정보

7) 실시간 위협 탐지 및 대응

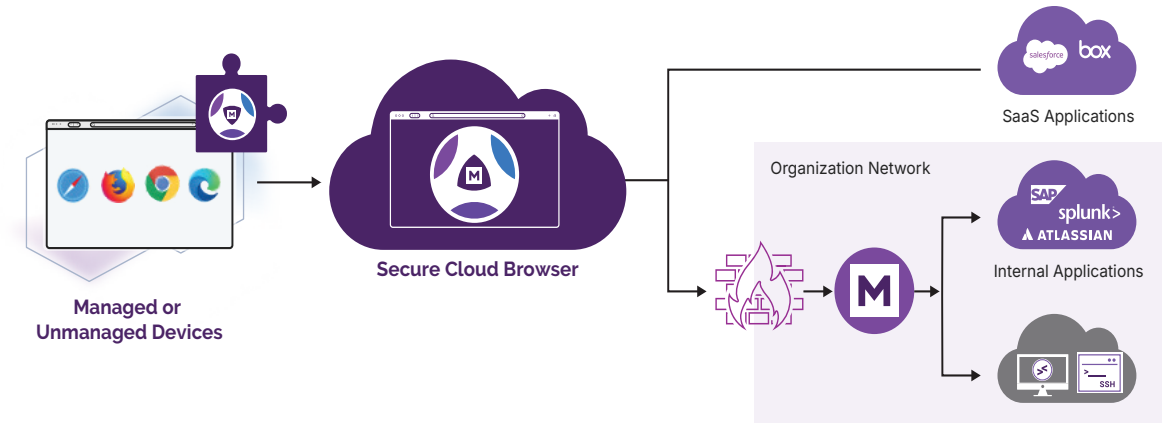
주요 기능

Menlo SAA는 인프라 변경이나 에이전트가 필요 없으며,
복잡성을 줄여주어 조직이 지체 없이 안전하게 애플리케이션에 접근할 수 있도록 합니다.

- 네트워크 재구성이나 방화벽 갱신이 요구되지않음
- DNS 레코드 변경이 요구되지않음
- 인증서 요구되지않음

위협으로부터 애플리케이션과 사용자를 강력하게 보호

Menlo Secure Application Access는 Menlo Secure Cloud Browser 덕분에 크로스 사이트 스크립팅, 쿠키 훔치기, 세션 하이재킹, 감염된 파일 업로드와 같은 데스크탑 위협으로부터 중요 애플리케이션과 데이터를 보호합니다. 또한, Secure Cloud Browser는 웹 필터를 회피하기 위해 도메인을 신뢰 기반으로 분류하는 Legacy URL Reputation Evasion(LURE) 공격과 HTML 스머글링과 같은 콘텐츠 기반 공격으로부터 사용자를 보호합니다. 엔드포인트가 손상되더라도, 위협 행위자는 데이터를 직접 액세스하거나 서버에 요청을 할 수 없습니다. 사용자는 이를 인지하지 못한 채, Menlo Secure Cloud Browser는 사용자 워크플로를 방해하지 않으면서 강력한 보호를 제공합니다.



사용자는 애플리케이션에 직접 접근하는 대신, 포털이나 확장을 통해 애플리케이션의 렌더링을 안전하게 접근합니다.

민감한 데이터를 철저하게 보호

Secure Cloud Browser 내에 구현된 마지막 마일 데이터 손실 방지(DLP) 제어는 민감한 데이터가 조직의 통제 하에 유지되도록 하며, 손상된 엔드포인트나 무단 사용자의 접근으로부터도 안전하게 보호됩니다.
DLP 제어 기능은 다음을 포함합니다:

- 복사/붙여넣기 제어
- 웹 애플리케이션 및 파일 다운로드에 대한 워터마킹
- Data redaction
- 읽기 전용/읽기-쓰기 웹사이트 제어
- 업로드 및 다운로드 제어
- 허용된 업로드 및 다운로드에 대한 DLP (데이터 손실 방지)

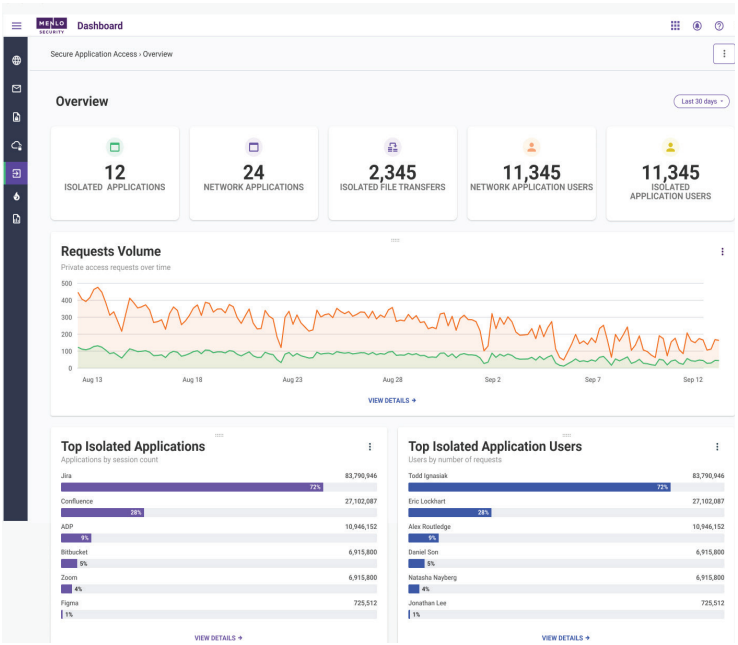
엔드포인트 기반 애플리케이션 접근 기술과 달리, Menlo Secure Application Access는 클라우드 기반으로 작동하며 민감한 정보를 장치에 다운로드하지 않습니다. 이 기능은 공격자가 장치의 메모리에 저장된 데이터에 접근하는 것을 방지합니다.

최소 권한 접근으로 보안을 강화

Menlo Secure Application Access는 사용자, 그룹, 출발지 IP, 및 지리적 위치에 의해 정의된 최소 권한 접근을 적용합니다. 네트워크 기반 서비스와 달리, Menlo SAA는 전체 네트워크나 세그먼트가 아닌 사용자가 필요로 하는 특정 애플리케이션에 대한 접근만 제한합니다. 직원, 파트너, 계약자는 자신이 명시적으로 허가받은 애플리케이션만 보고 접근할 수 있습니다.

애플리케이션 접근 및 사용자 행동에 대한 가시성을 확보

Menlo SAA는 브라우징 활동, 사용자 이름, 출발지 위치 등 모든 애플리케이션 접근에 대한 상세한 로그를 통해 보안 감독을 강화합니다. Menlo SAA는 SIEM, EDR/XDR을 포함한 기존 보안 도구와 통합됩니다. 더 깊은 통찰력을 제공하는 Menlo Browsing Forensics는 사용자 웹 활동에 대한 완전한 가시성을 제공합니다.



Menlo SAA 대시보드는 애플리케이션 사용 추세를 포함한 개요를 제공하며, 가장 자주 접근한 애플리케이션과 **DLP** 위반 사항을 보여줍니다.

레거시 앱 지원

Menlo SAA와 함께 제공되는 Menlo Security Client는 원격 접근 시나리오에서 비웹 기반의 레거시 애플리케이션에 대한 안전한 접근을 확장하며, 이러한 애플리케이션은 Menlo Cloud를 통해 안전하게 터널링됩니다.

Device Posture 점검

Menlo Secure Application Access는 접근 전과 도중에 Posture 점검을 제공하여 보안을 강화합니다.
이 점검은 방화벽 상태, OS 버전, 디스크 암호화 등 중요한 장치 기준을 확인합니다. 또한, CrowdStrike와 통합되어 CrowdStrike의 존재 여부나 ZTA 점수와 같은 추가 요소를 평가하는 엔드포인트 Posture 점검을 지원합니다.
Menlo를 사용하면 조직은 Posture 점검을 위해 클라이언트를 배포할 필요가 없습니다. 대신, Managed Chrome을 활용하여 클라이언트 없는 Posture 점검을 가능하게 하며, IT는 Chrome 구성을 관리하고 장치의 자세에 따라 권한을 부여할 수 있습니다.

제로 트러스트 혁신: 접근을 간소화하고 위험을 줄이세요

Menlo Secure Application Access는 브라우저 보안과 글로벌 프라이빗 접근 클라우드를 기반으로 한 사용자 중심의 제로 트러스트 아키텍처로 애플리케이션 보안을 혁신적으로 변화시킵니다.