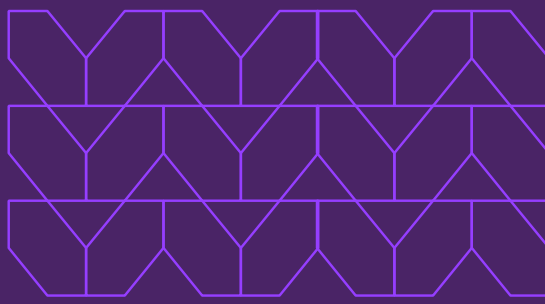
MENLO SECURITY

데이터 시트

# 브라우저 격리

## 인터넷 멀웨어의 위협을 제거하여 업무를 보호할 수 있습니다.

선택의 문제가 아닙니다. 인터넷은 오늘날 기업 운영에 있어 필수적인 업무용 도구입니다. 넓게 분산되어 있는 사용자들은 일일 업무를 완료하기 위해 웹사이트, 클라우드 앱 및 SaaS(Software-as-a-Service) 플랫폼에 빠르고 안전하게 액세스할 수 있어야 합니다. 그러나 인터넷은 기업에 막대한 위험을 초래하는 악의적인 위협으로 가득 차 있습니다. 보안 팀에게는 어디서나 업무를 보다 완벽하고 스마트하게 처리할 수 있는 직원 역량에 영향을 미치지 않으면서 사용자들의 웹 브라우징을 보호할 수 있는 새로운 방식이 필요합니다.



### 3가지 중요 사항:

사용자는 생산성 유지를 위해 웹 기반 정보, SaaS 애플리케이션, 온라인 문서, 공동 작업 및 기타 비즈니스 도구에 안전하고 안정적으로 액세스할 수 있어야 합니다.

기존의 감지 기반 보안 방식은 제로 데이 공격, 자격 증명 도용 및 랜섬웨어와 같은 최신 위협을 방어하지 못합니다.

Menlo Security 브라우저 격리는 근본적으로 다른 방식을 사용하여 공격을 사전에 차단하고 이러한 위협을 완전히 제거합니다.

## 제품 개요

Menlo Security 브라우저 격리는 기업 보안 팀에서 인터넷 멀웨어를 방어하는 제로 트러스트 방식을 이행하는 데 필요한 가시성과 제어 기능을 제공합니다. 브라우저 격리는 멀웨어가 경계를 침투하는 시점에서 위협을 식별하는 방식이 아닌 모든 웹 트래픽을 클라우드 기반 원격 브라우저를 통해 라우팅하여 단말에 안전한 콘텐츠만 전달함으로써 제로 트러스트를 구현합니다. 웹 콘텐츠의 적법성이나 위법성 여부 또는 분류나 비분류 여부는 중요하지 않습니다. Menlo Security 브라우저 격리는 모든 콘텐츠를 악의적인 것으로 간주하고 그에 따라 처리하는 제로 트러스트 원칙을 채택합니다.

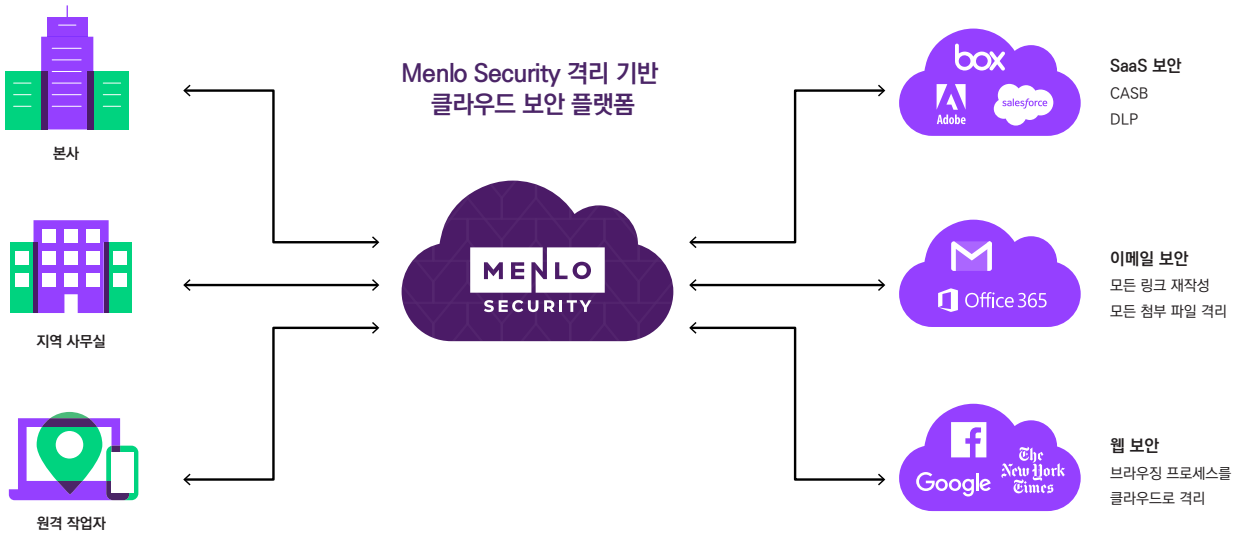
Menlo Security는 브라우저 격리와 함께 모든 보안 웹 게이트웨이 기능을 단일 클라우드 네이티브 플랫폼(예: CASB, DLP, RBI, Proxy, FWaaS 및 개인 액세스)으로 통합하여 확장 가능한 API와 정책 관리, 보고, 위협 분석을 위한 단일 인터페이스를 제공합니다.

**Menlo Security 클라우드 플랫폼은 Menlo 만의 Isolation Core™를 기반으로 하여 기업 요구 사항에 따라 사용자 다수를 빠르게 수용하고 지원할 수 있는 탄력적인 확장성을 제공합니다.**

또한 용량 계획 사이클이나 복잡한 클라이언트 구성을 단말 장치에 배치하지 않고도 급변하는 인력 요구 사항과 트래픽 양을 수용할 수 있습니다. 따라서 자동으로 세분화된 액세스 정책과 보안 정책을 이행하고 데이터 유출을 방지하며 클라우드 앱의 안전성을 확보하고 모든 장치와 위치에서 규정을 준수할 수 있습니다. 동시에 사용자는 필요한 웹 기반 정보와 생산성 도구에 기본적으로 액세스할 수 있습니다.

Menlo Security 브라우저 격리는 일반 사용자의 업무 방식을 완벽하게 지원할 뿐만 아니라 손상된 웹사이트, 사이버스쿼팅, 파일 업로드 및 다운로드, 소셜 게시 및 기타 알려지지 않은 위협 등 악의적인 활동을 차단하도록 관리자에게 허용 가능한 사용 정책을 설정하는 기능을 제공합니다. 사용자, 그룹, 파일 형식, 웹사이트 분류 또는 클라우드 애플리케이션에 따라 정책을 적용하여 콘텐츠가 차단되거나 읽기 전용 모드에서 렌더링되는 경우 또는 최초 콘텐츠에 대한 액세스를 허용해야 하는 경우를 판별할 수 있습니다. Menlo Security 브라우저 격리는 여기에 탁월한 성능과 확장성까지 겸비하고 있습니다.

브라우저 격리는 직접 클라우드(direct-to-cloud) 인터넷 액세스를 지원하면서 핵심 프록시 기능을 제공합니다. 게이트웨이가 웹 프록시로서 인터넷 트래픽을 종료 및 프록시 처리하며 URL, 필터링, 샌드박싱, 데이터 손실 방지, 바이러스 백신 검사, 클라우드 액세스 보안 브로커(CASB) 및 보안 웹 게이트웨이(SWG)로 제공되는 기타 통합 기술 등 보안 검사를 통해 해당 트래픽을 처리합니다.



# Menlo Security 브라우저 격리: 주요 기능과 이점

| 기능 | 이점 |
|---|---|
| 웹 격리 | 모든 위험한 활성 웹 콘텐츠(JavaScript 및 Flash)를 클라우드 기반 원격 브라우저에서 실행하여 웹사이트를 안전하게 볼 수 있습니다. |
| | 모든 기본 웹 콘텐츠를 스테이트리스(stateless) 웹 세션을 사용하는 일회용 컨테이너에서 삭제합니다. |
| | 스마트 DOM은 DOM 기능을 활용하여 투명한 사용자 환경을 제공하면서 동시에 단말과 격리된 위치에서 활성 콘텐츠를 실행하는 데 따른 보안 이점도 계속 제공합니다. |
| | DOM 재구성으로 모바일 브라우저에 적합한 주요 이점을 스마트 DOM에 제공합니다. |
| | 사용 중인 특정 단말 브라우저와 페이지에서 사용하는 웹 기능에 관계없이 정확하게 렌더링합니다. |
| | 전원 효율적인 렌더링으로 CPU 활용률이 향상되고 전체 전력 소비는 줄어듭니다. |
| | 우선 대역폭 할당으로 스마트 DOM이 배터리 수명을 최적화하도록 네트워크 사용량을 최소화할 수 있으며 동시에 사용자 환경도 유지할 수 있습니다. |
| | 스마트 DOM은 어떤 단말로도 활성 콘텐츠를 보내지 않으므로 최신 공격 익스플로잇이 차단됩니다. |
| | Layer Tree를 의미론적으로 풍부한 DOM으로 변환하므로 다양한 브라우저 에코시스템과 호환됩니다. 따라서 텍스트 노드에 텍스트 의미 체계가 노출되고 앵커 요소가 링크 의미 체계를 내보내며 〈input〉 요소가 암호 관리자 자동 채우기를 트리거합니다. |
| 문서 격리 | 모든 활성 콘텐츠나 위험한 활성 콘텐츠를 단말과 격리된 클라우드에서 실행하여 문서를 안전하게 볼 수 있습니다. |
| | 적용되는 정책에 따라 콘텐츠 검사, CDR 또는 서드파티 멀웨어 엔진 검사를 수행하여 안전하게 정리된 문서나 원본 문서를 다운로드할 수 있는 옵션을 제공합니다. |
| | 세분화된 정책으로 필터 유형과 사용자에 따라 문서 액세스를 제한합니다. |
| | 정화 과정을 거쳐 완벽하게 안전한 고품질 버전의 원본 문서를 제공하며 인쇄, 검색, 복사/붙여 넣기 및 공유 기능을 지원합니다. 데스크톱과 모바일 장치에서 완벽하게 지원됩니다. |
| | 지원되는 다양한 형식의 문서를 웹 기반 보안 문서 뷰어로 렌더링할 수 있습니다. |
| | 격리 방식으로 보관함에 있는 파일을 안전하게 보고 액세스할 수 있습니다. |
| 기본 사용자 환경 | 다양한 브라우저 지원 기능으로 기본 브라우저를 활용할 수 있어 사용자가 기존 방식으로 웹을 계속 사용할 수 있습니다. |
| | 새 브라우저를 설치 또는 사용하지 않아도 됩니다. |
| | 원활한 스크롤과 함께 픽셀화 현상이 나타나지 않습니다. |

| 기능 | 이점 |
| --- | --- |
| 클라우드 보안 플랫폼 | 웹 보안과 액세스 정책을 중앙에서 구성하며 해당 정책은 위치 및 장치에 관계없이 모든 사용자에게 즉시 적용됩니다. |
| | 하이브리드 배포를 지원하며 일관되고 동일한 정책을 적용합니다. |
| Menlo Security 격리 기반 Secure Web Gateway(SWG) | 특정 웹사이트 범주(75개 이상)에 대한 사용자 상호 작용을 제한합니다. |
| | 세분화된 정책(사용자, 그룹, IP)으로 직원 웹 브라우징을 제어합니다. |
| | 보기 전용, 파일 형식에 따른 안전 다운로드 또는 원본 다운로드, 업로드 및 다운로드 제어 등 문서 액세스를 제어합니다. |
| | 짧은 대기 시간, 고대역폭 환경(예: 동영상 콘텐츠)에서 대역폭을 예측대로 제어하는 사용자/그룹 정책을 지원하므로 사용자 환경이 강화됩니다. |
| | 파일 평판 검사, 바이러스 백신 및 샌드박싱을 사용하는 통합 상태 및 동적 파일 분석 |
| | 기존 서드파티 바이러스 백신, 샌드박싱 및 실행 가능한 콘텐츠를 제거하여 문서에 포함된 알려진 위협과 알 수 없는 위협을 모두 방어하는 CDR(Content Disarm and Reconstruction) 솔루션과 통합됩니다. |
| | 위험한 콘텐츠를 검사하고 다운로드한 모든 원본 문서의 악의적인 행동을 감지합니다. |
| | 기본 제공 및 사용자 지정 보고서, 상세 이벤트 로그와 기본 제공 트래픽 분석을 통한 경보 |
| | 유연한 데이터 탐색 및 분석을 위한 기본 제공 및 사용자 지정 쿼리 |
| | API를 사용하여 로그 데이터를 서드파티 SIEM 및 BI 도구로 내보내기 |
| | 최대 1년 동안 유연하게 데이터 보존 |
| | Menlo Query Language를 사용한 사용자 지정 쿼리 만들기 기능 |
| 사용자/그룹 정책 및 인증 | 특정 사용자, 사용자 그룹 또는 콘텐츠 유형(모든 콘텐츠, 위험한 콘텐츠, 비분류)에 대한 정책을 설정하고 미세 조정합니다. |
| | 특정 사용자, 사용자 유형 또는 콘텐츠 유형에 대한 예외를 만듭니다. |
| | SSO 및 IAM 솔루션과 통합되며 사용자 인증에 SAML을 지원합니다. |
| 데이터 손실 방지(DLP) | 인터넷으로 문서 업로드를 제한합니다. |
| | 서드파티 DLP(온프레미스 및 클라우드 기반 DLP 모두)와 통합합니다. |
| | 온프레미스 솔루션에 대한 가시성이 향상됩니다. |
| 클라우드 액세스 보안 브로커(CASB) | 규정 준수를 위해 SaaS 애플리케이션 트래픽에 대한 심층적인 가시성을 제공합니다. |
| | 타사 CASB 솔루션과 통합합니다. |
| | SaaS 애플리케이션에 대한 정책을 세부적으로 제어합니다. |

| 기능 | 이점 |
| --- | --- |
| 암호화된 트래픽 관리 | TLS/SSL 암호화 웹 브라우징 트래픽을 규모에 따라 가로채서 검사합니다. |
| | 특정 웹사이트 범주에 대한 개인 정보 보호가 강화되도록 SSL 검사 예외를 프로비저닝할 수 있습니다. |
| | 암호화된 세션에서 숨겨진 위협을 노출시킵니다. |
| Global Elastic Cloud | 전 세계 어디서나 원격 사이트와 모바일 사용자를 위한 안전하고 최적화된 웹 액세스를 지원합니다. |
| | 자동 크기 조정과 최소 대기 시간 기반 라우팅으로 어떤 위치로부터의 연결도 모두 지원하며 월간 수십억 개 세션으로 확장됩니다. |
| | 사용자를 신속하게 프로비저닝합니다. |
| | ISO 27001 및 SOC 2 인증 데이터 센터 |
| 연결 방법 및 단말 지원 | PAC(Proxy Automatic Configuration)/에이전트 기반 트래픽 리디렉션 |
| | IPSEC/GRE 네트워크 트래픽 리디렉션 지원 |
| | 우수 SD-WAN 제공업체와 원활한 통합 |
| API 통합 | 웹 세션 보안을 위한 원활한 SaaS 통합 |
| | CDR, SSO |
| | 고도로 확장 가능한 표준 세트 지원, API 및 서드파티 통합 |
| | 콘텐츠 API |
| | 정책 API |
| | 로그 API |
| | 유효성이 검증된 SSO, SIEM, MDM, 방화벽, 프록시, AV, 샌드박스, CDR 및 SOAR의 서드파티 통합 |
| | SD-WAN 및 SASE 통합 |

최신 보안 위협으로부터 보호하는 것이 기업의 최우선 과제인 상황이지만 기존 솔루션은 제한적이고 사후 대응적입니다. Menlo Security는 근본적으로 다른 방식을 사용하여 멀웨어 위협을 완전히 제거하며 클라우드 기반의 탄력적이고 확장 가능한 특별한 격리 기반 클라우드 보안 플랫폼으로 생산성을 완벽하게 보호합니다. 이 플랫폼은 클라우드 보안의 본질을 이행하는 유일한 솔루션으로, 악의적인 공격을 방어하기 위해 가장 안전한 제로 트러스트 방식을 제공하며 최종 사용자가 온라인 작업 과정에서 보안 기능이 실행되는 것을 인식하지 못하고 보안팀의 업무 부담도 없애줍니다.

작업을 보호하는 방법에 자세한 내용은 menlosecurity.com에 방문하거나 Korea@menlosecurity.com으로 문의하십시오.

MENLO SECURITY

**자세한 내용은 다음 연락처로 당사에 문의하십시오.**

**menlosecurity.com**

**(650) 695-0695**

**Korea@menlosecurity.com**

## Menlo Security 회사 소개

Menlo Security는 조직에서 위협을 제거하고 생산성을 완전히 확보할 수 있는 격리 기반의 우수한 클라우드 보안 플랫폼을 제공합니다. 이 플랫폼은 클라우드 보안의 본질을 이행하는 유일한 솔루션으로, 악의적인 공격을 방어하기 위해 가장 안전한 제로 트러스트 방식을 제공하며 최종 사용자가 온라인 작업 과정에서 보안 기능이 실행되는 것을 인식하지 못하고 보안팀의 업무 부담도 없애줍니다. 이제 조직은 조직 내 사용자에게 보안에 대한 걱정 없이 비즈니스 계속 수행할 수 있는 안전한 온라인 환경을 제공할 수 있습니다.

© 2021 Menlo Security, All Rights Reserved.