데이터 시트

Cloud Access Security Broker(CASB)

사용자가 안전하게 SaaS 플랫폼에 액세스할 수 있습니다.

오늘날 인터넷과 브라우저에서 거의 모든 업무가 수행됩니다. 고도로 분산된 모바일 사용자는 동적이고 유연한 SaaS(Software-as-a-Service) 플랫폼을 통해 연결하고 공동 작업을 수행합니다. 이 플랫폼은 비즈니스를 수행하는 어디서나 작업자에게 강력한 기능과 성능을 제공합니다. 그러나 SaaS 플랫폼은 사용자와 플랫폼을 직접적이면서 영구적으로 연결해야 하며 이로 인해 위험이 초래됩니다. 기업의 가시성과 통제력이 미치지 않는 상황에서 악의적인 공격자들이 SaaS를 공격 벡터로 악용할 수 있기 때문입니다. 따라서 보안 팀에게는 오늘날의 고도로 분산된 공동 작업 방식의 업무 환경을 방해하지 않으면서 사용자의 SaaS 액세스를 보호할 수 있는 새로운 방식이 필요합니다.

3가지 중요 사항:

오늘날의 사용자는 클라우드 앱 및 서비스 형태의 최신 애플리케이션을 사용하여 비즈니스를 수행하는 어디서나 중요한 비즈니스 정보와 도구에 액세스할 수 있습니다.

이러한 앱은 일반적으로 사용자와 플랫폼을 직접적이면서 영구적으로 연결해야 하며 이 과정에서 기업 보안 팀은 배제됩니다.

Menlo Security CASB를 사용하면 고도로 분산된 모바일 사용자는 SaaS 플랫폼에 중단 없이 안전하고 자신 있게 액세스할 수 있습니다.

제품 개요

Menlo Security Cloud Access Security Broker(CASB)를 사용하면 사용자는 SaaS 플랫폼에 안전하게 액세스할 수 있으며 보안 팀은 경로 내 멀웨어를 차단하는 데 필요한 심층적인 가시성과 제어 기능을 확보할 수 있습니다. CASB는 Menlo의 격리 기반 방식을 사용하므로 사용자는 최신 애플리케이션에 안전하게 액세스할 수 있으며 인터넷 트래픽을 중앙 데이터 센터로 백홀하지 않아도 됩니다. 따라서 조직은 분산된 원격 사용자에게 클라우드 기반의 안전한 로컬 인터넷 액세스 지점을 제공할 수 있습니다.

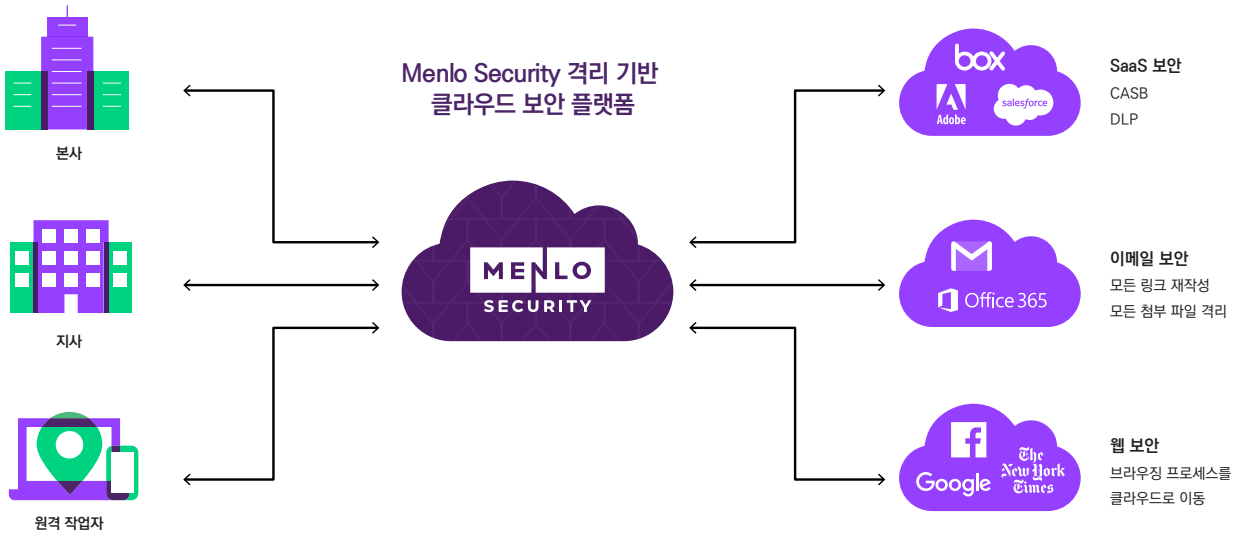
사용자는 클라우드 기반의 이 유연한 모바일 로컬 인터넷 액세스 지점을 통해 데이터 센터를 보호하는 모든 동일한 보안, 가시성 및 제어 기능으로 SaaS 플랫폼에 직접 안전하게 연결할 수 있습니다.

Menlo Security CASB는 승인 및 미승인 애플리케이션과 관련된 사용자 활동에 대한 가시성과 제어 기능을 실시간으로 제공합니다. 완전 통합형 서비스는 정책 만들기와 관리를 간소화하므로 알려진 기존 위협은 물론 알려지지 않은 미래의 위협까지 차단할 수 있습니다.

Menlo만의 Isolation Core™는 파일과 문서 등 SaaS 콘텐츠로 승인 받지 않은 애플리케이션으로부터 사용자를 보호하며 Menlo Security 클라우드 플랫폼을 통해 안전하게 액세스할 수 있습니다. Menlo Security는 안전하고 승인된 콘텐츠만 최종 사용자 브라우저에 효율적으로 전달하며 애플리케이션 환경에 아무런 영향을 미치지 않습니다.

또한 Menlo Security의 CASB는 실제 위치나 기본 연결에 관계없이 보안 팀에게 모든 트래픽에 적합한 보안 제어 기능을 적용할 수 있는 역량과 가시성을 제공합니다. OneDrive, Google 드라이브, Box 및 Dropbox와 같은 클라우드 공유 사이트로 민감한 정보를 업로드하는 것을 제어할 수 있는 데이터 손실 방지(DLP) 기능과 더불어 로그인, 업로드, 다운로드, 공유, 만들기, 삭제와 같은 애플리케이션 기능 제어가 대표적입니다. 관리자는 미승인 앱보다 승인 앱에 정책을 보다 유연하게 적용할 수 있으며 그 과정에서도 Menlo의 문서 격리, 콘텐츠 검사 및 통합 DLP를 통해 위협 보호 기능을 계속 유지할 수 있습니다.

무엇보다 Menlo는 성능에 대한 영향은 물론 IT 오버헤드까지 야기하는 취약한 VPN 서비스나 물리적 보안 어플라이언스를 사용하지 않고 최신 앱에 대한 가시성과 제어 기능을 제공합니다.



Menlo Security Cloud Access Security Broker: 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.
문서 격리	모든 활성 콘텐츠나 위험한 활성 콘텐츠를 단말과 격리된 클라우드에서 실행하여 문서를 안전하게 볼 수 있습니다.
	안전하게 정리된 버전이나 원본 문서를 다운로드할 수 있습니다.
	세분화된 정책으로 필터 유형과 사용자에 따라 문서 액세스를 제한합니다.
클라우드 보안 플랫폼	모든 장치의 모든 사용자에게 즉각적으로 적용되는 웹 보안 및 액세스 정책을 중앙에서 구성합니다.
	하이브리드 배포를 지원하며 동일한 정책을 적용합니다.
URL 필터링 및 허용 가능 사용 정책(AUP)	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 등 문서 액세스를 제어합니다.
대역폭 제어	대역폭을 예측대로 제어하는 사용자/그룹 정책으로(예: 동영상 콘텐츠) 사용자 환경을 강화합니다.
콘텐츠 및 멀웨어 분석	파일 해시 검사, 바이러스 백신 및 샌드박싱을 사용하는 통합 파일 분석
	기존 서드파티 바이러스 백신 및 샌드박싱 솔루션과 통합됩니다.
	위험한 콘텐츠를 검사하고 다운로드한 모든 원본 문서의 악의적인 행동을 감지합니다.

기능	이점
분석 및 보고	기본 제공 및 사용자 지정 보고서와 함께 상세 이벤트 로그와 기본 제공 트래픽 분석을 통한 경보를 제공합니다.
	유연한 데이터 탐색 및 분석을 위한 기본 제공 쿼리와 사용자 지정 쿼리
	API를 사용하여 로그 데이터를 서드파티 SIEM 및 BI 도구로 내보내기
암호화된 트래픽 관리	TLS/SSL 암호화 웹 탐색 트래픽을 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
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.
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.
웹 게이트웨이	격리 서비스 외에 추가 보안 제어 기능을 적용합니다.
	이메일 격리, DLP, CASB, FWaaS, 전역 클라우드 프록시

기능	이점
Data Loss Prevention(DLP)	인터넷으로 문서 업로드를 제한합니다.
	온프레미스 솔루션에 대한 가시성이 향상됩니다.
Cloud Access Security Broker(CASB)	규정 준수를 위해 SaaS 애플리케이션 트래픽에 대한 심층적인 가시성을 제공합니다.
	서드파티 CASB 솔루션과 통합하는 옵션
	SaaS 애플리케이션에 대한 정책을 세부적으로 제어하고 로그인, 업로드, 다운로드, 공유, 만들기 및 삭제와 같은 앱 기능을 제어합니다.
연결 방법 및 단말 지원	PAC(Proxy Automatic Configuration)/에이전트 기반 트래픽 리디렉션(예: Windows 및 macOS용 단말 에이전트 옵션 포함)
	IPSEC/GRE 네트워크 트래픽 리디렉션 지원
	우수 SD-WAN 제공업체와의 원활한 통합
API 통합	웹 세션 보안을 위한 원활한 SaaS 통합
	고도로 확장 가능한 표준 세트 지원 API 및 서드파티 통합
	콘텐츠 API
	정책 API
	SIEM 지원 로그 API 및 Splunk, IBM QRadar, Menlo iSOC와 같은 로그 분석 도구
	유효성이 검증된 SSO, SIEM, MDM, 방화벽, 프록시, AV, 샌드박스(PAN Wildfire 및 Cisco ThreatGrid), CDR 및 SOAR의 서드파티 통합
	SD-WAN 및 SASE 통합

최신 보안 위협으로부터 보호하는 것이 기업의 최우선 과제인 상황이지만 기존 솔루션은 제한적이고 사후 대응적입니다. SaaS 애플리케이션은 일반적으로 사용자와 플랫폼을 직접적이면서 영구적으로 연결해야 하며 이로 인해 악의적인 공격자가 공격 벡터로 활용할 수 있는 중대한 보안 공백이 발생합니다. Menlo Security의 CASB는 사이버 보안에 대한 격리 기반 제로 트러스트 방식을 지원합니다. 즉 멀웨어와 SaaS 플랫폼에서 시작되는 다른 악의적인 콘텐츠의 단말 액세스를 방지합니다. 또한 Menlo Security는 파일을 클라우드 플랫폼으로 업로드로 인한 데이터 유출을 방지합니다. 무엇보다 최종 사용자가 온라인 작업 과정에서 보안 기능이 실행되는 것을 인식하지 못하며 보안 팀의 모든 작업자를 위한 안전하고 원활하며 효과적인 환경을 유지하기 위한 업무 부담도 줄여줍니다.

작업을 보호하는 방법에 자세한 내용은 menlosecurity.com을 참조하거나 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 조직의 온라인에서 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 보안 팀의 업무 부담도 없애줍니다. 이제 조직은 조직 내 사용자에게 보안에 대한 걱정 없이 비즈니스 계속 수행할 수 있는 안전한 온라인 환경을 제공할 수 있습니다.