격리 방식으로 취약한 인터넷 사용으로 인한 위협 방어

자유롭게 인터넷을 사용하면서 기업의 보안 수준을 유지하는 것은 양립할 수 없습니다.

오늘날의 위협 환경:

- 매일 새로운 웹페이지들이 생겨났다 사라지고 끊임없이 업데이트되고 있습니다. 이에 따라 분류가 어려운 동적 웹 환경이 조성되고 있습니다.
- 웹 페이지가 계속 업데이트되고 제3자 콘텐츠가 추가됨에 따라 위협 인텔리전스는 이를 따라가기 벅찬 상황입니다.
- 또한 이메일의 링크 또는 첨부 파일 형태에 관계없이 무기화된 문서가 이를 인식하지 못하는 사용자 장치에 악의적인 멀웨어가 다운로드되도록 하고 있습니다.

기업 딜레마: 무제한 또는 통제된 웹 액세스

웹으로부터 멀웨어를 차단하는 데 따른 위협은 매우 실질적인 것입니다. 멀웨어에는 매년 5억 개가 넘는 변종이 생겨나며 신뢰할 수 있는 사이트조차도 일반 사이트에 숨겨진 악의적인 콘텐츠 저장소가 될 수 있습니다. 멀웨어는 매우 쉽게 전파되고 이로 인해 최근 일어난 많은 대표적인 침해 사례에서 중대한 역할을 해왔습니다. 이러한 침해에 따른 비용은 수백만, 때로는 수십억 달러 수준이므로 기업은 점점 더 엄격한 웹 보안 정책을 채택해야 하는 압력을 받고 있습니다.

위험한 웹은 보안 관리자를 승산이 없는 전쟁의 상황으로 몰아가고 있습니다. 웹 접속을 통제하는 것으로 생산성이 저해되고 관리자들에게 복잡성을 안겨주는 상황에서 보안 관리자들은 악의적인 콘텐츠로부터 기업 보호와 사용자들에게 작업 수행에 필요한 웹 기반 도구와 정보에 대한 무제한적인 액세스 허용 사이에서 올바른 결정을 내려야 하는 과제에 직면하고 있습니다.

허용 또는 차단 접근 방식에 기초한 기존 도구

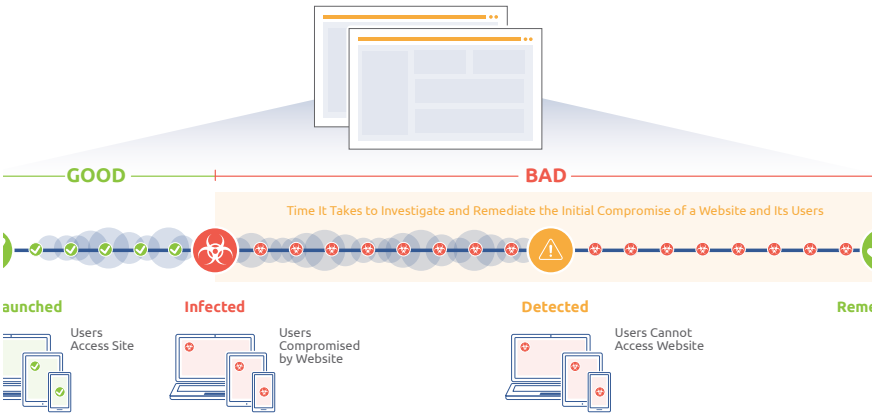
전통적인 보안 웹 게이트웨이(SWG) 솔루션은 사이트 액세스 허용 또는 차단을 결정하는 데 웹사이트 분류를 활용합니다. 그러나 합법적인 웹사이트라고 해서 모두 적절히 분류할 수 있는 것은 아닙니다. 오늘날의 인터넷은 매일 새로운 웹페이지들이 생겨났다 사라지며 그에 따라 실시간 분류가 어려운 동적 웹 환경이 조성되고 있습니다. 사용자는 새로운 고객 사이트 또는 기존 분류에 해당하지 않는 사이트에 액세스해야 할 수도 있습니다. 따라서 기업들은 너무 엄격하여 생산성을 저해하거나 너무 관대하여 멀웨어 감염 위험을 증가시키는 보안 정책을 수립하게 됩니다.

새로운 접근 방식: 인터넷 격리

격리 방식은 멀웨어가 감염되거나 악성 웹사이트, 이메일 첨부 파일 또는 문서를 통해 멀웨어가 사용자 장치에 도달할 수 있는 가능성을 제거합니다. 즉 웹 격리는 탐지 및 분류 기반의 허용 또는 차단 방식에 의존하지 않고 모든 웹 콘텐츠를 위험하다고 간주하며 클라우드 기반 격리 플랫폼에서 가져오기 및 실행 명령을 수행합니다. 안전하고 멀웨어가 없는 콘텐츠만 사용자 장치에 미러링되므로 웹사이트, 문서 또는 보안이 중요한 다른 합법적인 콘텐츠를 차단하지 않고 완벽하고 안전한 웹 경험을 제공할 수 있습니다.

20%

Menlo 연구소의 연구에 따르면 Menlo Internet Isolation Platform으로 격리시킨 URL의 최소 20%가 안전한 사이트에서 안전하지 않은 사이트로 변경된 것으로 밝혀졌습니다.



웹 격리 기능을 기존의 SWG에 통합하면 관리자가 사용자에게 인터넷을 더 허용하면서 공격 위험을 제거할 수 있습니다.

분류되지 않은 웹사이트	무기화된 문서
원리: URL을 알 수 없는 URL, 새로운 URL 또는 기존 범주에 해당하는 URL로 분류할 수 있습니다.	**원리:** 위협 행위자는 사용자가 정상적인 문서 파일을 가장하여 사용자 장치에 강제로 멀웨어를 다운로드하게 하는 무기화된 문서를 전달합니다.
기존 솔루션의 비효율성: 분류되지 않은 웹사이트를 처리하려면 많은 노동력이 필요한 프로세스가 필요합니다. 보안 전문가가 웹사이트를 계속 분류하고 사용자의 접근 차단 해제 요청에 대응해야 하므로 년간 수백만 달러의 관리 비용이 발생합니다.	**기존 솔루션의 비효율성:** 최근 수법은 감염된 XML 파일을 Word 문서로 위장하는 것입니다. Word 문서를 신뢰하는 사용자가 멀웨어를 자동으로 다운로드하는 악성 매크로를 활성화하므로 샌드박스와 AV 솔루션을 효과적으로 피할 수 있습니다.
솔루션: 웹 격리에서는 조직을 위험한 상황에 빠뜨리지 않고 사용자가 원하는 웹사이트에 액세스할 수 있게 해줍니다. 따라서 웹사이트를 분류하고 탐지에 의한 보안 경고를 처리하는 데 따른 비용이 제거됩니다.	**솔루션:** 웹 격리는 사용자 장치와 멀리 있는 격리된 환경에서 모든 활성 콘텐츠를 실행합니다. 사용자는 또한 정책에 따라 안전하고 깨끗한 문서(Safe PDF Document) 또는 원본 문서(Original Document)를 다운로드할 수 있습니다.

Menlo Security 회사 소개

Menlo Security는 웹, 문서 및 이메일에서 멀웨어 위협을 제거하여 사이버 공격으로부터 조직을 보호합니다. Menlo Security의 클라우드 기반 격리 플랫폼은 사용자 단말에 소프트웨어가 필요하지 않으며 최종 사용자 환경에 영향을 주지 않고 기업 규모에 관계없이 확장 가능한 포괄적인 보호 성능을 제공합니다. Menlo Security는 포춘지 선정 500대 기업과 금융 서비스 기관을 비롯한 세계 주요 기업을 지원하고 있습니다.

문의
menlosecurity.com
Korea@menlosecurity.com