

제로 트러스트 인터넷

격리 기반 보안 클라우드 변혁으로 제로 트러스트 사고를 지원합니다.

이점:

- 조직이 모든 트래픽에 대한 보안 강화로 더 많은 멀웨어 방지
- 보안 팀이 수동적으로 위협을 기다리지 않고 선제적으로 멀웨어 탐지
- 웹 기반 및 이메일 기반 공격으로부터 사용자 보호
- 제로 트러스트 정책을 명시적이고 의도적으로 즉시 이행

기존 인터넷 관련 사이버 보안의 근본적인 결함

오늘날의 사이버 보안은 이 분야의 초기 방식과 마찬가지로 샌드박스, 화이트리스트 및 URL 필터링과 같은 이전 솔루션으로 멀웨어가 사용자 환경에서 활성화되기 전에 미리 탐지하는 방식을 활용하고 있습니다. 이 방식은 초기 인터넷에는 효과적이었습니다. 당시는 웹사이트가 주로 정적이었으며 멀웨어가 정교하지 않은 기본적인 형태로 쉽게 발견될 수 있었기 때문이었습니다. 오늘날은 웹 페이지에서 다양하고 역동적인 콘텐츠를 제공하며 웹 전체에 흩어져 있는 분산 서버에서 호스팅됩니다. 또한 수많은 진입점과 타사 웹 요소, 여기에 웹 앱과 SaaS(Software-as-a-Service) 기술까지 합쳐져 인터넷 액세스 방식이 크게 변화되었습니다. 오늘날 사용자들은 필요한 곳 어디서나 끊임 없이 지속적이고 직접적인 연결을 요구합니다.

인터넷 마크업의 현저한 변화에는 그에 따른 비용이 발생합니다. 멀웨어는 복잡성과 유행성 측면에서 모두 진화했습니다. 오늘날은 단 몇백 달러만 있으면 위협 요인으로 새롭고 특별한 위협을 쉽게 가할 수 있어 표적을 공격하는 데 비용이 많이 들지 않습니다. 해커들은 멀웨어가 침투할 때까지 여러 번의 공격과 변형으로 표적을 타격할 수 있습니다. 이러한 멀웨어 확대 외에도 해커들은 보안 산업의 최신 탐지 방법을 피할 수 있도록 기술적으로도 진화했습니다. 일례로 최신 멀웨어는 샌드박스에서 활성화 여부를 탐지한 후 사용자 환경에 도달할 때까지 페이로드를 지연합니다.

오늘날 기업들은 다음과 같은 새로운 패러다임에 직면해 있습니다. 인터넷이 빠르게 급변하고 있으며 멀웨어의 복잡성과 강도가 증가합니다. 이러한 새로운 위협에 대처하기 위해 보안 산업은 새로운 방식을 개발했습니다. 바로 제로 트러스트 보안입니다.

제로 트러스트 인터넷

제로 트러스트 아키텍처의 핵심 개념은 조직 내에서 시작된 패킷은 물론 어떤 트래픽도 신뢰해서는 안 된다는 것입니다. 제로 트러스트 인터넷은 모든 브라우저 기반 인터넷 트래픽을 유해한 것으로 간주해야 하며 웹 트래픽을 단말 장치에서 격리시켜야 한다는 개념을 전제로 합니다. 이 새로운 방식은 포괄적인 방식으로, 탐지 기반 보안과 관련된 많은 문제를 제거하지만 이론적으로 많은 관리 오버헤드가 필요합니다.

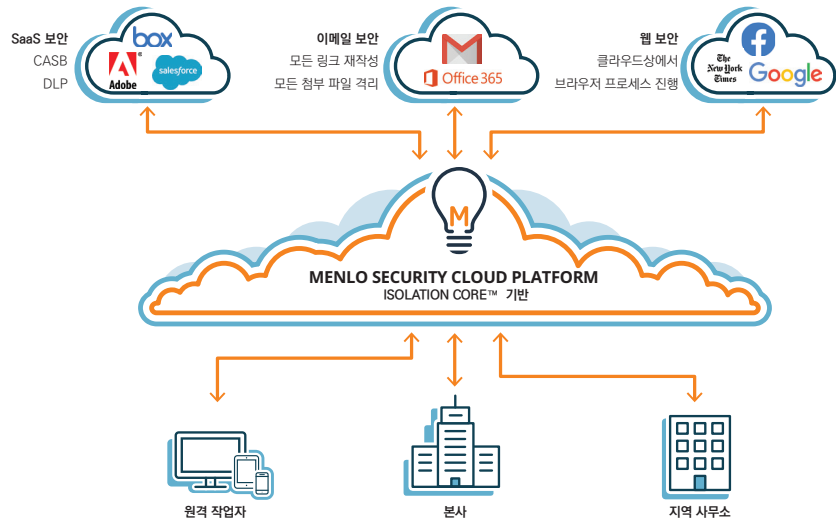


인터넷 격리

격리 기반의 보안 클라우드 변혁은 클라우드 기반 원격 브라우저를 통해 모든 웹 트래픽을 다시 라우팅하는 방식으로 제로 트러스트 인터넷을 지원합니다. 웹 콘텐츠의 안전성 또는 유해성, 분류 또는 미분류 여부는 중요하지 않습니다. 인터넷 격리는 모든 것이 유해하다고 가정하며 유해한 것으로 처리합니다. 클라우드 기반의 격리 플랫폼은 확장성과 민첩성도 크게 향상시킵니다. IT 부서가 하드웨어를 구성하지 않아도 되며 회사가 추가 소프트웨어 또는 컴퓨터 비용을 지불하지 않아도 됩니다. 인터넷 격리는 인력, 비즈니스 주기 또는 트래픽 볼륨 변동에 따라 조직의 클라우드와 같은 규모로 확장될 수 있습니다.

제로 트러스트 인터넷 아키텍처

전통적인 보안 아키텍처와 철학은 더 이상 적용되지 않습니다. 조직 내 수많은 보안 도구에도 불구하고 사이버 범죄는 계속 증가하고 있습니다. 그 이유는 무엇이고 어떻게 해결할 수 있을까요?



조직은 Isolation Core™ 기반의 Menlo Security Cloud Platform을 구현하고 제로 트러스트 인터넷 프레임워크를 활용함으로써 모든 형태의 브라우저 기반 멀웨어를 선제적으로 방어할 수 있습니다. 이 2단계 솔루션은 미래 보안 정책의 중심축으로서, "최초 감염자" 공격과 침해에서 탐지까지 오랜 시간이 걸리던 시대의 종말을 의미합니다.

보안 클라우드 변혁을 통한 제로 트러스트 보안은 미래의 보안 스택으로, IT 팀은 가장 악의적인 해커의 두뇌와 기술력도 극복할 수 있습니다. 웹 보안에 대한 근본적으로 다른 방식, 즉 기본 거부(default-deny) 방식은 모든 패킷을 격리하여 가장 복잡한 멀웨어도 차단할 수 있습니다. 자세한 내용은 menlosecurity.com을 방문하거나

Korea@menlosecurity.com에 문의하십시오.

Menlo Security 회사 소개

Menlo Security는 웹, 문서 및 이메일에서 멀웨어 위협을 제거하여 사이버 공격으로부터 조직을 보호합니다. Menlo Security는 수백여 글로벌 2000대 기업과 주요 정부 기관들이 보안 클라우드 변혁을 달성하도록 지원하고 있습니다. Menlo Security 클라우드 플랫폼은 사용자 단말에 소프트웨어가 필요하지 않으며 최종 사용자 환경에 영향을 주지 않고 기업 규모에 관계없이 확장 가능한 포괄적인 보호 성능을 제공합니다. Menlo Security는 Gartner Magic Quadrant for the Secure Web Gateway의 Visionary 기업으로 선정되었습니다.

© 2019 Menlo Security, All Rights Reserved.

문의

menlosecurity.com

(650) 614-1705

Korea@menlosecurity.com

