MENLO SECURITY

White Paper

브라우저 보안

브라우저에 대한
올바른 보안 접근 방식 제안

지난 몇 십 년 동안, 디지털 변혁(Digital Transformation)은 기업 내에서 근본적인 변화를 촉발시켰습니다. 공급망 재설계, 고객 경험 강화 등이에 속하며, 기업 애플리케이션의 SaaS(Software as a Service) 플랫폼으로의 전환은 디지털 변혁을 더욱 촉진시켰습니다. 이 두 가지 근본적인 변화는 기업이 작업하는 방식을 재정립했습니다.

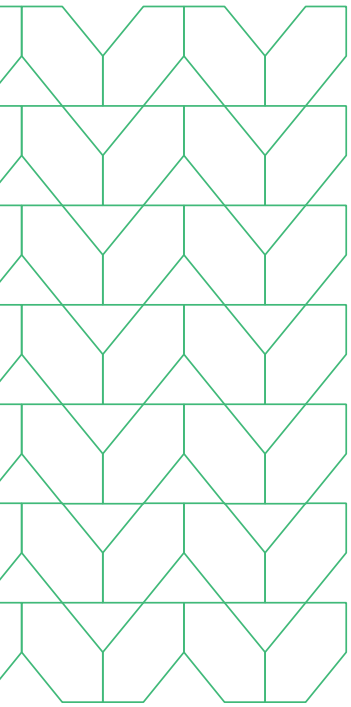
직원들이 일상적으로 사용하는 응용 프로그램은 대부분 브라우저와 관련이 있습니다. Forrester에 따르면 전형적인 기업 근로자는 "기기 사용 시간"의 75%를 웹 브라우저를 사용하는 데 소비한다고 합니다. 이에 비즈니스 중요 응용 프로그램 접근, 업무 이메일에 접근, 파일 공유 등이 포함됩니다.

브라우저는 이제 사용자의 초기 공격 목표입니다. Verizon의 2022 데이터 침해 조사 보고서(DBIR)에 따르면, 웹 브라우저를 통해 주로 액세스되는 웹 응용 프로그램 및 이메일은 보안 침해에서 주요 공격 벡터로, 이러한 사건의 80% 이상을 차지합니다. Google Project Zero가 기록한 내용에 따르면, 2023년에 이용된 클라이언트 측 Zero-day 공격의 대다수는 **브라우저 취약점**입니다. 공격자는 이러한 Zero-day를 활용하여 피해자의 엔드포인트에 악성 코드나 랜섬웨어를 설치하거나 민감한 정보를 도난당할 수 있습니다.

전통적인 네트워크 및 엔드포인트 보안 솔루션인 Secure Web Gateways (SWG), Endpoint Detection and Response (EDR) 솔루션, 방화벽과 같은 솔루션이 브라우저 기반 활동에 대한 제한된 가시성을 갖고 있음이 계속되고 진화했습니다. 왜냐하면 이들의 탐지 방법은 주로 알려진 위협의 패턴 일치 또는 고전적인 네트워크 신호에 의존하며 브라우저 행동에 대한 완전한 가시성이 없기 때문입니다. 예를 들어, URL 평판 엔진을 우회하기 위해 카테고라이즈된 신뢰성 있는 사이트를 사용한 공격이 70% 증가했습니다. 위협 행위자는 소스 및 방법을 다양화시켜 이러한 전통적인 솔루션을 우회하고 있습니다.

보안 및 IT 팀은 이러한 위협에 대응하기 위해 기본 브라우저 정책에 의존해서는 안 됩니다. 기존의 브라우저 정책은 일반적으로 보안 팀이 이러한 위협에 대응하기 위해 시도하는 바와 완전히 일치하지 않습니다. 일반적으로 정책은 강제로 적용하기 어렵고, 어떤 정책이 의미 있는지 파악하기 어렵으며, 사용자 경험은 보안 관리자에게 적합하지 않을 때가 많습니다. 현재의 솔루션은 기업을 보호하는 데 위협을 마주하고 있습니다. 대신, 조직은 브라우저 보안의 모든 측면에 대응하는 포괄적인 솔루션이 필요합니다

브라우저 보안이란?



여러 솔루션들은 브라우저 보안에 대응하기 위해 세 가지 주요 범주로 그룹화될 수 있습니다.

로컬 브라우저

- **주요 브라우저**: Google Chrome, Microsoft Edge, Apple Safari와 같은 브라우저를 포함하며, 각 브라우저 공급업체는 브라우저에 보안 기능을 추가하고 기존 기능을 더욱 안전하게 유지하려고 노력하고 있습니다.
- **기업용 브라우저**: 주로 Chromium을 기반으로 하는 이 브라우저들은 주로 기업 사용자를 대상으로 설계되었습니다. 이러한 브라우저들은 사용자 장치 전반에 걸쳐 기업 정책을 일관되게 시행하는 데 중점을 두고 있습니다.
- **기업용 브라우저 확장 기능:** 이는 브라우저 확장 프로그램 형태로 브라우저에 기능을 추가하는 솔루션으로, 기본적으로 주류 브라우저와 함께 작동하도록 설계되었습니다.

전형적 원격 브라우저 격리(RBI): RBI는 신뢰할 수 없는 웹 콘텐츠(일반적으로 인터넷에서 가져옴)를 사용자 및 사용자 장치에서 분리하기 위해 설계된 웹 솔루션입니다.

클라우드 기반 브라우저 보안: 기업용 브라우저, 브라우저 확장 프로그램 및 원격 브라우저 격리의 기능을 통합한 하이브리드 및 유연한 솔루션으로, 클라우드 기반 서비스로 제공됩니다.

브라우저 보안의 주요 능력

브라우저 보안은 세 가지 주요 요점으로 나눌 수 있으며, 각각은 사용자 보호, 기업 보안, 관리자 및 최종 사용자 모두에게 우수한 사용자 경험을 유지하는 데 중요한 핵심 기능과 사용 사례를 갖추고 있습니다:

- 브라우저 관리
- 사용자 보호
- 액세스 및 데이터 보안

브라우저 관리

브라우저 관리는 새로운 개념이 아닙니다. 사실, 주요 브라우저 관리 플랫폼인 Microsoft Intune과 Google Chrome Enterprise Manager는 중앙에서 제어할 수 있는 수백 가지 관리 매개변수를 제공합니다. 대부분의 기업은 브라우저 버전 및 확장 프로그램 관리 주변의 최소한의 구성 매개변수에 중점을 두고 있으며, 이는 브라우저를 기본 구성으로 남겨두는 것입니다. 브라우저 관리의 모범 사례에는 브라우저를 가장 안전하게 보호하기 위해 추가로 최소한의 매개변수를 구성하는 것이 포함됩니다.

브라우저 관리에는 기업의 전반적인 보안 포지션과 관련된 다음 정책 요소들이 포함됩니다:

- 버전 관리
- 허용되거나 차단된 브라우저 확장 프로그램 나열
- 특정 브라우저 기능 비활성화 – 예를 들어 USB 상호 작용 비허용
- 고급 사용자 기능에 대한 액세스 제한
  – 예를 들어 개발자 도구에 대한 액세스 제한

그리고 이러한 정책들은 기업 내에서 다양한 종류의 브라우저 설치 기반에 대해 일관되게 배포되고 시행되어야 합니다.

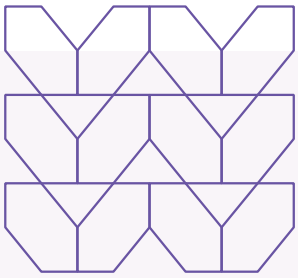
사용자 보호

사용자 보호는 브라우저 보안의 중심에 위치하고 있습니다. 솔루션은 모든 유형의 공격을 예방해야 하며, 일반적인 공격과 고도의 공격을 모두 포함하여 다음과 같습니다:

- 브라우저 취약점의 악용
- 악성 코드 다운로드, 랜섬웨어 포함
- 피싱 (제로아워 보호 포함)

브라우저가 기능을 추가함에 따라 악의적인 행위자가 악용할 수 있는 잠재적인 결함 목록이 계속해서 생성됩니다. 2022년 11월부터 2023년 11월까지 Google은 Chrome에서 175건의 고도로 회피적인 심각한 문제가 발생했으며, Microsoft Edge 와 모든 기업용 브라우저는 기본 브라우저 엔진으로 Chromium을 사용하므로 이러한 취약점이 해당 브라우저에도 영향을 미쳤습니다. 이러한 취약점 중 많은 것들은 악의적인 웹사이트를 방문함으로써 임의의 코드 실행으로 이어질 수 있습니다. 공격자들은 이미 브라우저에 존재하는 방대한 공격 표면을 발견하기위해 집중하며, 여러 해 동안 숨어있었던 취약점을 발견하고 있습니다. 보안 및 IT 팀은 계속해서 증가하는 웹 취약점 목록을 검토하고 대응해야 합니다. 여기에는 브라우저가 단기간 내에 다수의 최종 사용자 장치에 패치되어야 하는 제로데이 취약점도 포함됩니다. 이러한 취약점이 방어되지 않으면 공격자가 대상 시스템에서 원격 코드 실행을 얻을 수 있는 문을 열어두게 되어, 피해자의 시스템에 랜섬웨어와 같은 악성 소프트웨어가 설치될 수 있습니다. 이러한 위험에도 불구하고 기업 사용자가 로드하는 페이지 중 25% 이상이 현재 버전의 Chrome보다 2개 이상의 주요 버전이 낮은 브라우저를 통해 로드되고 있습니다. 즉, 이는 다수의 심각한 취약성을 공개한 브라우저를 사용하는 것입니다.

게다가, 악성 코드와 피싱 공격 측면에서 공격자들은 지속적으로 기술과 인프라를 발전시키고 있습니다. 이는 방어자들이 계속해서 탐지 논리와 시그니처 데이터베이스를 업데이트해야 함을 의미합니다. 이러한 진화하는 공격은 웹 브라우저를 선호하는 진입점으로 활용되고 있습니다.



일부 기업은 관리되지 않는 엔드포인트를 지원하는 특정한 사용 사례를 가지고 있습니다. 예를 들면 단기 계약 근로자들이 노트북과 같은 개인 장치에서 특정 응용 프로그램에 액세스해야 하는 경우입니다. 이 특정 사용 사례는 지역에 따라 다양한 법적 책임 측면에서 일부 도전 과제를 제시할 수 있으므로 본 백서의 목적상 해당 복잡성은 다루지 않을 것입니다. 이 백서는 브라우저 관리는 여러 가지 방법으로 수행될 수 있음을 보여줄 것입니다.

- **관리되지 않는 장치는 기업용 브라우저를 사용하도록 강제될 수 있으며, 사용자는 개인 장비에 응용 프로그램을 설치하도록 강요됩니다.**
- **관리되지 않는 장치는 기존에 선택한 브라우저에 브라우저 확장 프로그램을 추가하도록 강제될 수 있으며, 이로써 엔드 유저의 학습과 경험이 간소화됩니다.**

두 부분 모두 정책 강제가 가능합니다. 이는 주로 사용자 경험, 배포 부담, 그리고 지역 규정과 관련된 문제로 변할 수 있으며, 이에 대한 자세한 내용은 문서의 뒷부분에서 논의됩니다.

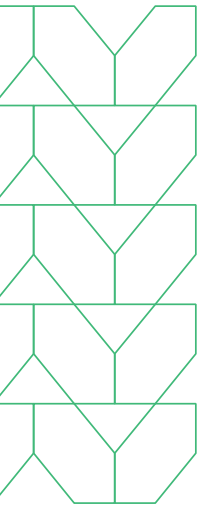
액세스 및 데이터 보안

해당 구성 요소는 일반적으로 제로 트러스트 네트워크 액세스 전략에서 볼 수 있으며, 원격 액세스 전략과 구현을 클래식한 레이어 3 IPSec VPN에서 최소 권한 응용 프로그램 액세스(네트워크 액세스가 아닌 애플리케이션 액세스임에 유의) 패러다임으로 전환한 기업에서 채택되고 있습니다. 이 애플리케이션 별 액세스 제어로의 이동은 기업에 새로운 기회를 제공합니다:

- 응용 프로그램에 대한 세밀한, 최소한의 권한 액세스 - SaaS 제공 및 사설 클라우드
- 관리자를 위한 용이한 관리
- 개선된 최종 사용자 경험
- 인프라 비용 절감

이는 일반적으로 데이터 유출 방지와 연결됩니다.:

- 문서 및 보관된 파일 격리
- 데이터 마스킹
- 워터마킹
- 공유 플랫폼에 대한 읽기 전용 액세스



대부분의 기업 응용 프로그램은 레거시 클라이언트/서버에서 현대적인 웹 기반 응용 프로그램으로 전환되었습니다. 이는 기업이 브라우저 보안을 활용하여 액세스에 대한 간단하면서도 강력한 정책을 만들 수있게 해주며, 세부적인 그룹 및 사용자별 응용 프로그램 특정 정책도 가능하게 합니다. 더 나아가 기업은 응용 프로그램 자체가 해당 수준의 정책을 기본적으로 지원하지 않는 경우에도 이러한 세부적인 정책을 생성할수 있습니다.

가상 데스크톱 인프라(VDI)를 사용하던 기업들은 높은 비용과 불편한 사용자 경험에 대한 대안으로, 익숙한 브라우저 인터페이스로의 전환을 희망하고 있습니다. 이로써 기업은 현대 웹 응용 프로그램에서 기대되는 뛰어난 성능과 사용성을 얻을 수 있습니다. 동시에, 강력한 솔루션은 VDI에서 제공되는 확고한 보안 보장을 유지해야 합니다. 민감한 정보는 화면에 표시되지 않으면 엔드포인트에 도달하지 않아야 하며, 백엔드 서버는 잠재적으로 악성 클라이언트에 직접 노출되지 않아야 합니다.

기존의 웹 응용 프로그램과 미숙한 SaaS 솔루션은 종종 사용자에게 민감한 데이터 노출을 제한하는 데 세밀한 통제가 부족하여 내용 필터링 레이어를 추가로 활용하여 내용을 수정해야 하는 경우가 있습니다. 세밀한 통제가 있더라도 응용 프로그램 단위 또는 응용 프로그램 구성이 보안팀의 통제 밖에 있는 경우가 많습니다.

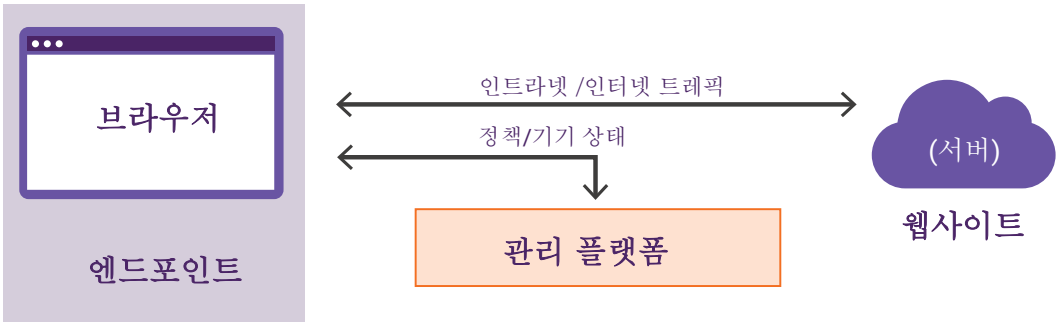
웹 콘텐츠를 보는 것 이상으로 사용자는 몇 페이지만 보기 위해 문서를 다운로드하거나 문서를 열지 않고 다른 웹 응용 프로그램으로 전송해야 할 수 있습니다. 마지막으로 웹 콘텐츠나 문서가 사용자에게 액세스 가능하게 되면 회사 정책에 익숙하지 않아 의도적으로든 의식하지 않고 해당 콘텐츠를 비인가 SaaS 응용 프로그램에 붙여넣거나 업로드할 수 있습니다. 이러한 시나리오에서 브라우저 보안 레이어는 일관되고 견고한 콘텐츠 필터링 정책을 시행하는 데 도움이 되어야 합니다. 믿을 수 없거나 잠재적으로 손상된 엔드포인트로부터 민감한 데이터 노출을 제한하는 것 외에도 기업은 웹 응용 프로그램 서버의 노출을 최소화하려고 합니다. 악의적인 클라이언트는 취약한 서버로 공격 페이로드를 전송할 수 있습니다.

로컬 브라우저 (메인 & 기업용 브라우저)

로컬 브라우저는 브라우저 보안 문제를 해결하기 위해 두 가지 구성 요소로 구성된 솔루션을 제공합니다:

- 중앙 집중식(일반적으로 클라우드 기반) 관리 플랫폼
- 브라우저

일반적으로 브라우저는 주로 Chromium을 기반으로 하며, 기업 중심 기능인 정책 강제, DLP 기능, 지역 브라우저 및 파일 격리 기능 등을 갖추고 있습니다. 특히 기업용 브라우저의 경우 기업을 최우선으로 하는 브라우저를 통해 전체 공격 표면을 줄일 수 있으며, 보안 정책 및 가벼운 보안 기능은 완전한 안전한 서비스 엣지 (SSE) 배포의 필요성을 상쇄하고 기업과 사용자를 적절하게 보호할 수 있다는 전제에 기초합니다.



로컬 브라우저가 브라우저를 관리하는 방법

로컬 브라우저는 Microsoft Intune이나 Google Chrome Enterprise Manager와 같은 온프레미스 또는 클라우드 기반의 관리 플랫폼을 통해 관리될 수 있습니다. 보안 정책 및 다른 설정은 로컬 브라우저로 정의되고 전송될 수 있습니다.

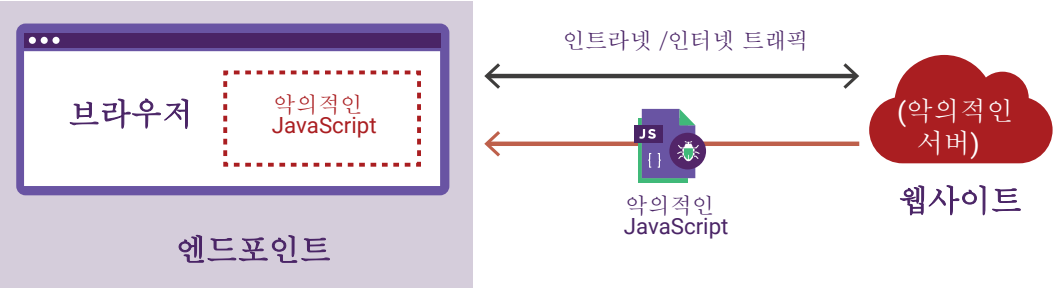
주류 브라우저의 경우 추가 기능을 활성화하려면 라이선싱 복잡성이 있습니다. 예를 들어, Microsoft Intune을 통해 확장 프로그램을 관리하려면 고객은 높은 티어의 엔터프라이즈 라이선스, Microsoft Defender 라이선스 및 그 위에 추가 라이선스가 필요합니다.

로컬 브라우저가 사용자를 보호하는 방법

보안 메커니즘의 소프트웨어 결함이나 취약점은 해당 취약성을 악용할 수 있는 위협 행위자나 특정 공격에 의해 브라우저, 장치 및 네트워크를 위험에 빠뜨릴 수 있습니다.

브라우저 취약성:

일반 및 기업용 브라우저는 로컬에서 실행되는 방어 및 보호 시스템에 완전히 의존합니다. 알려진 위협에 대해서는 효과적일 수 있지만 제로데이 공격에 취약합니다. 이러한 결함을 완화하기 위해 주로 JavaScript의 Just-In-Time 컴파일, WebGL 등과 같은 취약점 소스로 알려진 브라우저 기능을 비활성화합니다. 이러한 기능을 비활성화하면 공격 표면을 줄이지만 이에 의존하는 합법적인 웹 응용 프로그램도 손상시켜 사용자의 시간을 낭비하고 지원 비용 및 전반적인 불만족을 증가시킵니다. Chrome 엔지니어링 팀의 브라우저 보안 문제에 대한 분석 결과에 따르면 이러한 버그들은 우리의 코드베이스 전체에 고르게 퍼져 있습니다. 그 결과, 지난 12개월 동안 수정된 175개의 취약점 가운데 많은 부분은 브라우저의 기능을 심각하게 손상시킨 후에도 여전히 악용 가능했을 것입니다.



멀웨어 (랜섬웨어 포함):

일반 및 기업용 브라우저는 다운로드된 파일을 스캔하여 알려진 악성 콘텐츠를 탐지하는 기능을 제공합니다. 이를 위해 로컬 데이터베이스의 악성 서명을 업데이트하거나 파일을 클라우드 서비스로 전송할 수 있습니다.

피싱 Phishing:

일반 및 기업용 브라우저는 피싱 콘텐츠를 탐지하는 지원을 제공할 수 있습니다. 업데이트된 알려진 피싱 도메인 목록을 기반으로 하며, 페이지가 악성인지를 실시간으로 판단하기 위해 행동 및 콘텐츠 기반 분석을 사용할 수 있습니다. 정책 기반의 조치를 통해 페이지 콘텐츠에 대한 액세스를 차단하거나 사용자 입력을 차단할 수 있습니다.

로컬 브라우저가 액세스 및 데이터를 안전하게 하는 방법

어플리케이션 접근 Application Access:

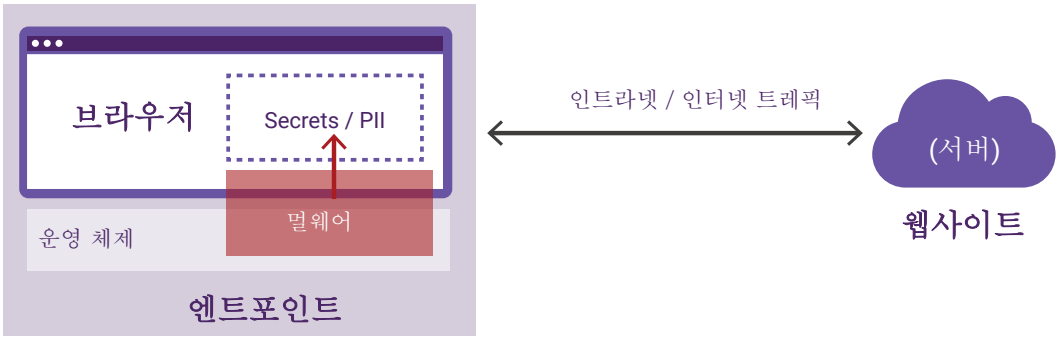
일반 및 기업용 브라우저는 애플리케이션 서버에 대한 액세스를 승인된 브라우저로 제한하기 위해 노력합니다. 이는 일반적으로 클라이언트의 보안 상태를 확인하여 애플리케이션 인증 시에 시도됩니다. 애플리케이션은 Okta와 같은 Identity Provider를 사용하도록 구성되며, Okta는 주류 및 기업용 브라우저의 SaaS 구성 요소에 속하는 IP 주소에서만 인증을 허용하도록 설정됩니다. 사용자가 인증을 완료하면 브라우저에 인증 토큰이 발급되어 애플리케이션에 제시됩니다.

이는 우회될 수 있는 관측에 의한 보안 접근 방식입니다. 승인된 브라우저는 공격자가 완전히 제어하는 브라우저로 위장될 수 있으며, 공격자는 승인된 브라우저의 메모리에서 인증 토큰을 추출하여 완전히 제어하는 브라우저로 전송할 수 있습니다.

데이터 유출 (Data exfiltration):

기업용 브라우저 내에서 민감한 데이터는 사용자에게 표시되지 않도록 "가려질" 수 있습니다. 데이터의 가려짐은 서버가 아닌 기업용 브라우저에서 수행되므로 사용자에게는 가려진 정보가 표시되지 않지만 엔드포인트 메모리에는 여전히 해당 정보가 존재합니다. OS 또는 하이퍼바이저 제어를 가진 공격자는 기업용 브라우저의 메모리를 읽고 정보를 도난당할 수 있습니다. 또한 데이터를 "원래대로 표시"하는 기능을 제공할 수 있습니다. 사용자가 가려진 데이터를 보기로 결정하면 감사 로그 항목이 작성될 수 있습니다.

로컬로 다운로드된 파일에서 민감한 정보를 처리하기 위해 파일은 기업용 브라우저에서 사용자의 장치의 나머지 부분으로부터 차단하려고 시도하는 암호화된 영역에 보관될 수 있습니다. 사용자는 내장된 뷰어를 통해 파일 콘텐츠를 볼 수 있지만, 기업용 브라우저에 의해 생성된 울타리 영역 밖으로 원본 파일을 쉽게 복사할 수 없을 수도 있습니다.



스크린샷 및 복사 & 붙여넣기:

기업용 브라우저는 클라이언트 운영 체제에서 제공하는 API를 사용하여 데이터의 스크린샷 및 클립보드로의 복사를 비활성화할 수 있는 유용한 기능을 제공합니다. 그러나 데이터가 로컬 기기에 저장되어 있기 때문에, 기능이 비활성화되기 전에 공격자가 침해된 엔드포인트에서 문서를 네트워크 버퍼에서 "도난" 할 수 있습니다.

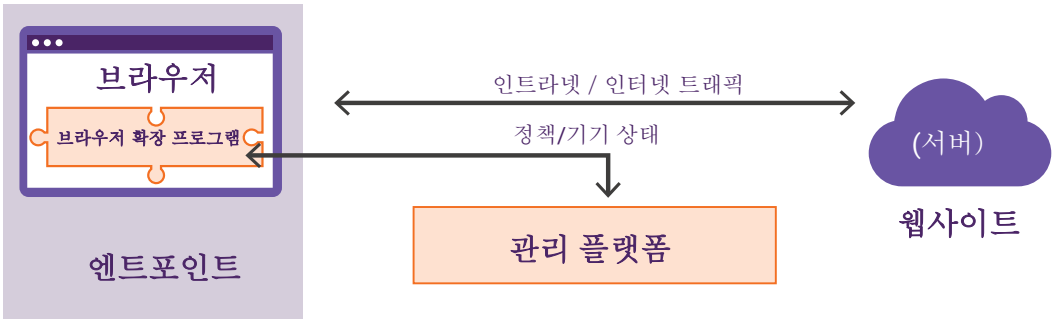
스크린샷 기능의 경우, 기업용 브라우저는 비전문가 공격자에 대해 제어를 제공합니다. 그러나 비전문가 공격자가 자신의 휴대폰을 사용하여 화면을 촬영하는 것은 여전히 간단히 가능하며, 이는 더 많은 제한이 필요한 다른 수단을 통해 방지될 수 있습니다. OS 또는 하이퍼바이저를 제어하는 숙련된 공격자는 기업용 브라우저에서 제공되는 보호를 우회하여 화면으로 전송된 콘텐츠를 쉽게 캡처할 수 있습니다.

브라우저 확장 프로그램

브라우저 확장 프로그램은 기존의 주류 브라우저에 설치되어 주류 브라우저에 대체 구현을 제공하는 의도로 사용됩니다. 시장에는 다양한 수준의 기능을 주장하는 브라우저 확장 프로그램 솔루션이 있습니다. 브라우저 확장 프로그램 및 관련 기능은 브라우저 공급 업체의 API 정책 변경의 영향을 받습니다. 브라우저 보안 확장 프로그램이 활용하는 기능 및 API는 사악한 목적의 당사자가 악성 코드를 작성하는 데 사용될 수 있으며, 이에 따라 브라우저 제작업체는 브라우저 확장 프로그램에 부여된 기능을 제한하기 시작했습니다. 이는 브라우저 벤더에 따라 다릅니다.

브라우저 확장 프로그램이 브라우저를 관리하는 방법

브라우저 확장 프로그램은 최종 사용자와의 상호 작용이 많이 필요하지 않고 대부분의 브라우저를 지원할 수 있도록 설치될 수 있습니다. 그런 다음 확장 프로그램은 중앙 관리 도구와 상호 작용할 수 있습니다.



브라우저 확장 프로그램이 사용자를 보호하는 방법

브라우저 취약점:

한 번 배포된 확장 프로그램은 웹 위협으로부터의 가시성 및 간단한 보호만을 제공합니다. 이러한 확장 프로그램은 다른 브라우저 보안 솔루션에서 제공하는 기능의 일부만 제공합니다. 알려진 나쁜 URL에서 콘텐츠를 차단할 수 있지만 브라우저의 동작을 더 중요하게 변경하여 공격 표면을 줄일 수는 없습니다.

멀웨어 Malware (including ransomware):

다운로드된 콘텐츠는 악성 콘텐츠를 보고 스캔할 수 없으며, 따라서 악성 코드로부터 거의 보호받을 수 없게 됩니다.

피싱 Phishing:

브라우저 확장 프로그램은 피싱 보호에 대해 기업용 브라우저와 유사한 방식을 취합니다.

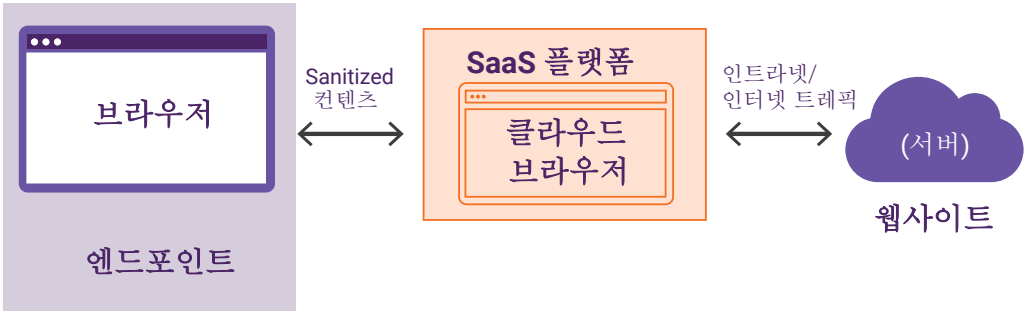
브라우저 확장 프로그램이 액세스와 데이터를 안전하게 하는 방법

어플리케이션 액세스:

브라우저 확장 프로그램은 조직에 애플리케이션 가시성을 제공합니다. 설치된 후, 이러한 확장 프로그램은 민감한 사용자 및 민감한 애플리케이션을 식별하는 데 도움이 되는 정보를 제공합니다. 올바른 정보를 통해 조직은 어떤 조치가 필요한지를 이해하고 애플리케이션에 안전한 액세스를 제공할 수 있습니다. 그러나 확장 프로그램은 관리되지 않는 기기에는 권장되지 않습니다. 왜냐하면 이러한 기기에서는 비교적 쉽게 제거될 수 있기 때문입니다.

기존의 원격 브라우저 격리

'기존의 원격 브라우저 격리'는 신뢰되지 않는 웹 콘텐츠(일반적으로 인터넷에서 가져온)를 사용자 및 사용자 장치로부터 분리하기 위해 설계된 웹 솔루션입니다. 이는 사용자가 악성 웹 콘텐츠에 노출되지 않도록 하고 그들의 장치를 보호하기 위한 것입니다. 이 방식은 사용자의 브라우저가 일종의 가상 환경에서 실행되도록 하고, 웹 콘텐츠는 원격 서버에서 처리되어 실제 사용자 장치로 전달되기 전에 격리된 환경에서 실행됩니다. 이를 통해 악성 콘텐츠가 사용자의 로컬 시스템에 직접 영향을 미치는 것을 방지할 수 있습니다. 이러한 방식으로, 사용자의 웹 브라우징 환경은 실제로 로컬 시스템에서 격리되어 있으며, 원격 서버에서 실행되는 가상 브라우저를 통해 웹 콘텐츠에 접근합니다.



원격 브라우저 격리(RBI)는 사용자를 보호하는 방법

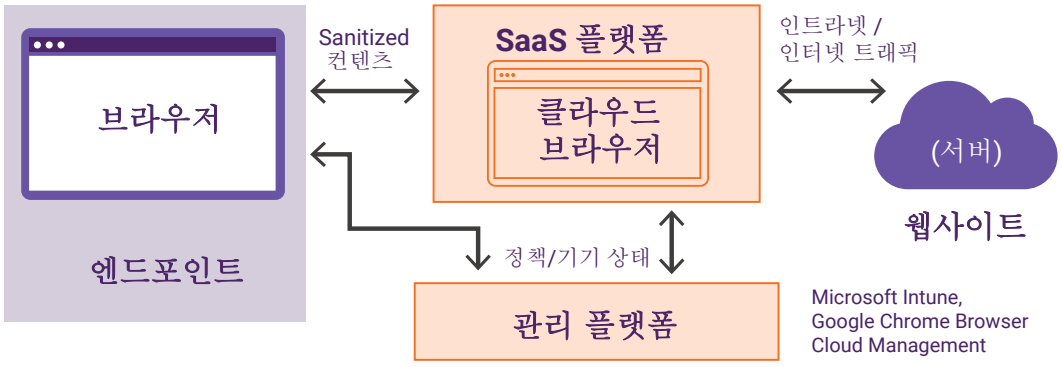
브라우저 취약성, 악성 소프트웨어 및 피싱:

웹 트래픽은 일반적으로 분류되지 않은 채 가상화된 클라우드 환경에서 강제 실행됩니다. 이렇게 함으로써 잠재적으로 악성인 웹 콘텐츠는 사용자에게 도달하기 전에 엔드포인트에서 실행되지 않습니다. 대신 사용자는 악성 사이트나 첨부 파일의 안전하게 렌더링된 버전을 보고 상호 작용합니다.

클라우드 기반 브라우저 보안

클라우드 기반 브라우저 보안은 기업용 브라우저, 브라우저 확장 프로그램 및 원격 브라우저 격리의 기능을 혼합한 형태로 제공됩니다. 브라우저는 모든 웹 트래픽을 클라우드 기반 브라우저 보안 플랫폼으로 라우팅하여 잠재적으로 악성인 모든 활성 콘텐츠를 차단하며 필요한 경우 민감한 정보를 마스킹합니다. 이 접근 방식을 사용하면 어떤 기기 및 어떤 브라우저를 사용하더라도 조직은 브라우저 보안을 활성화할 수 있습니다. 전통적인 RBI와 달리 클라우드 기반 브라우저 보안은 더 효율적인 콘텐츠 기반 RBI를 사용합니다. 이로써 거의 원래의 사용자 경험을 유지하면서 전통적인 RBI의 높은 대역폭 요구 사항을 제거합니다. 결과적으로 이 접근 방식은 종종 위험한 웹 사이트의 일부에만 국한된 전통적인 RBI와는 달리 모든 사용자의 브라우징을 보호하는 데 적합합니다.

예를 들어, Menlo Security 플랫폼은 수백만 사용자의 대다수 웹 활동을 매일 보호하면서 수천 개의 웹 애플리케이션 데이터 액세스를 통제합니다. 보안은 클라우드를 통해 제공되므로 비즈니스가 어디로 이동하든(사무실, 외부, 회의, 고객 사이트 등), 사용자의 엔드포인트의 보안 상태에 관계없이 액세스된 데이터에 대한 보안 보장을 제공합니다. 이는 가상 데스크톱 인프라(VDI)와 같은 더 비싼 및 불편한 접근 방식과 유사한 수준의 보안을 제공합니다.



클라우드 기반 브라우저 보안 관리

관리 기능:

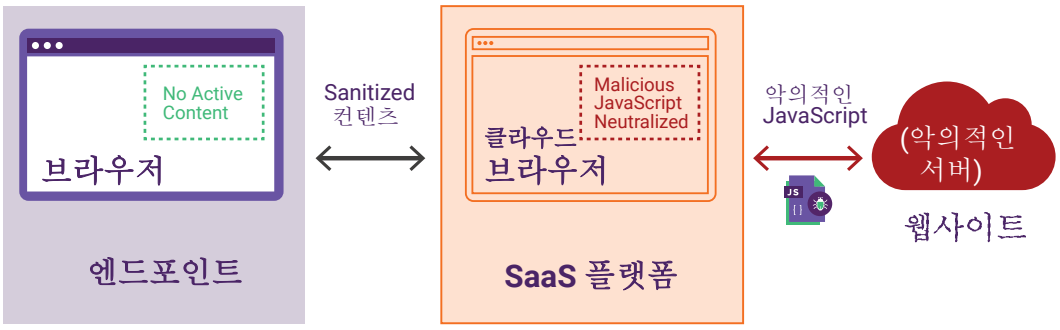
클라우드 기반 브라우저 보안은 브라우저에 중립적인 접근을 취하여 브라우저 관리를 고려할 때 보안을 중점적으로 고려합니다. 클라우드 기반 브라우저 보안은 Google 및 Microsoft와 같은 주류 브라우저 공급업체의 관리 기능을 활용하고 개선합니다.

또한 이 접근 방식은 팀 간 위임을 간소화합니다. 모든 정책 관리를 하나의 팀에서 중앙 집중하는 대신 데스크톱 팀이 일부 정책의 제어를 보안 팀에 위임할 수 있습니다. 클라우드 기반 브라우저 보안은 브라우저에 중립적인 방식으로 정책을 집계하고 간소화합니다. 각 정책을 개별적으로 처리하는 대신 정책은 그룹화되어 여러 브라우저에서 클릭 한 번으로 활성화될 수 있습니다.

클라우드 기반 브라우저 보안은 사용자를 보호합니다.

브라우저 취약점:

클라우드 기반 브라우저 보안은 공격 표면을 크게 줄일 수 있습니다. 기능을 브라우저에서 끄기로 결정하는 대신 기능은 기본적으로 클라우드에서 실행되며 엔드포인트에서 노출되지 않습니다. 클라이언트 측에서 기능을 활용하더라도 해당 기능이 악의적으로 API를 남용할 수 있는 웹사이트에 직접 노출되지 않습니다. 이 접근 방식은 기능을 지원하지 않거나 보안 위험을 창출하는 중에 선택해야 하는 필요성을 제거합니다. 대신 해당 기능은 안전하게 클라우드에서 활용될 수 있습니다. 공격자가 사용자 브라우저에서 코드를 실행할 수 없다는 점은 이전에 언급한 Chrome 취약점을 통해 엔드포인트를 compromise할 수 없다는 것을 의미합니다.

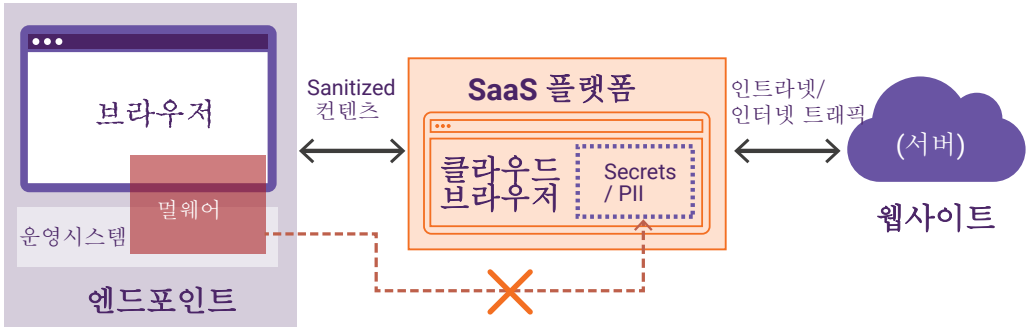


예를 들어 WebGL은 호환되는 모든 웹 브라우저에서 상호 작용하는 2D 및 3D 그래픽을 렌더링하기 위한 JavaScript API로 지원될 수 있으며 WebGL을 보안 문제의 원천으로 식별할 필요가 없습니다. 왜냐하면 WebGL을 활용한 모든 클라이언트 측 콘텐츠 생성이 클라우드 브라우저에서 수행되기 때문입니다. 마찬가지로 Just-In-Time (JIT) 컴파일을 비활성화할 필요가 없습니다. 페이지 JavaScript는 클라우드에서 실행되어 안전하게 JIT 컴파일을 활용할 수 있습니다. 결과적으로 사용자 경험에는 영향을 미치지 않습니다(JIT 컴파일을 비활성화하면 JS 중심 페이지의 성능이 크게 저하될 수 있음).

사용자를 보호하는 데 있어 중요한 부분은 항상 최신 브라우저를 실행하는 것입니다. 이 접근 방식에서 브라우저는 클라우드에서 자동으로 업데이트됩니다. 따라서 사용자 장치가 꺼져 있거나 저대역폭 링크를 통해 연결된 경우에도 브라우저를 업데이트할 수 있으며, 큰 업데이트를 밀어넣는 것이 실용적이지 않은 경우에도 가능합니다. 다시 말해 보안 상의 결정(사용자가 오래된 클라이언트로 브라우징하도록 허용)과 사용자 친화적이지 않은 결정(사용자에게 불안전한 커넥션이 있더라도 브라우징 전에 업데이트를 다운로드하도록 강제) 간에 어떤 상충도 없습니다.

멀웨어 Malware (랜섬웨어 포함):

클라우드 기반 브라우저는 최종 사용자가 다운로드한 모든 파일에 대한 완전한 가시성을 갖추고 파일이 클라이언트로 전송되기 전에 이러한 파일을 분석할 수 있습니다. 주류 및 기업 브라우저와 마찬가지로 파일의 내용은 AV 및 샌드박스 유형의 접근법을 통해 스캔될 수 있습니다. 주류 및 기업 브라우저와 달리 스캔 엔진 및 시그니처 데이터베이스는 클라우드 기반 브라우저 보안 SaaS 플랫폼에서 지속적으로 최신 상태를 유지합니다. 그리고 주류 및 기업 브라우저와 달리 악성으로 판명된 페이로드는 결코 엔드포인트에 닿지 않습니다.



피싱 Phishing:

클라우드 기반 브라우저는 사용자에게 전송된 모든 콘텐츠를 렌더링하고 모든 사용자 입력을 관찰하므로 기업 브라우저와 동일한 유형의 잘 알려진 나쁜 행동 및 콘텐츠 기반 접근 방식을 구현할 수 있습니다. 그러나 엔드포인트에 존재하지 않고 모든 기업 사용자에게 일관된 보호를 제공할 수 있습니다. 탐지에 사용되는 모든 논리 및 시그니처가 클라우드에서 실행되기 때문에 업데이트된 탐지 기능을 전체 브라우저 플리트에 즉시 배포할 수 있습니다. 제로 딜레이 보호는 계속 발전하는 피싱 콘텐츠에 대항하기 위한 핵심입니다.

액세스 및 데이터 보호:

애플리케이션 액세스:

사용자는 클라우드 브라우저를 통해 보호된 서버와 상호 작용하도록 강제됩니다. 위협 행위자는 클라우드 브라우저를 변조할 능력이 없으며 소프트웨어 스택의 더 많은 권한이 있는 계층을 제어하지 않습니다. 위협 행위자는 클라우드 기반 브라우저의 메모리를 검사하고 세션 토큰을 훔쳐 취약한 애플리케이션과 직접 상호 작용할 수 없습니다. 이는 Browser Security 플랫폼을 통과하는 모든 트래픽을 강제하는 안전한 네트워크 경로가 있기 때문입니다.

이 접근 방식은 공격자로부터 떨어져 안전하게 클라우드에서 소프트웨어가 실행되는 VDI 기반 접근 방식과 유사합니다. 그러나 VDI에서 사용자는 소프트웨어를 설치하려고 하거나 원격 운영 체제를 공격할 수 있습니다. 클라우드 기반 Browser Security 접근 방식에서는 브라우저를 실행하는 기본 운영 체제에 대한 노출이 전혀 없습니다. 이 설정에서 공격자는 클라우드 브라우저를 대상으로 페이지를 클릭하고 양식에 키보드 입력을 입력하는 데로 제한됩니다. 읽기 전용 모드도 강제할 수 있으며 입력이 꺼진 경우 사용자는 마우스 입력만 사용하여 대상 사이트와 상호 작용할 수 있습니다.

데이터 유출:

Cloud Based Browser Security는 민감한 정보를 최종 장치에 전혀 다운로드하지 않습니다. 모호한 데이터에 안전한 보호뿐만 아니라 변조 방지의 신뢰성 있는 감사 로깅을 제공할 수 있습니다. 따라서 사용자가 민감한 필드를 해제하려고 하는 경우 이 작업은 공격자가 변조할 수 없는 방식으로 기록될 수 있습니다. 사용자가 악의적인 경우 훔친 개인 식별 정보(PII)의 폭발 범위 에 대한 정확한 그림을 제공할 것입니다.

이는 파일에도 적용됩니다. 파일은 클라우드에서 완전히 보호된 영역에 유지될 수 있습니다. 사용자는 클라우드 뷰어를 통해 파일의 일부만 볼 수 있으며(플랫폼은 파일의 어느 부분이 표시되었는지 정확하게 추적할 수 있음), 파일이 최종 장치에 전달되지 않고 Gmail 첨부 파일을 Box 폴더에 넣는 등 파일을 웹 응용 프로그램 간에 복사할 수 있습니다.

결론

브라우저를 보호하기 위해 설계된 다양한 솔루션이 있지만 비즈니스 요구 사항을 먼저 식별하고 브라우저 보안의 주요 기능을 이해하여 귀하의 조직에 적합한 솔루션을 찾는 것이 중요합니다. 기업은 보안 도구의 패치워크를 통해 여러 해 동안 브라우저 보안의 측면을 배포해 왔습니다. 그러나 산업이 클라우드 기반 솔루션으로 계속 전환되는 가운데 최종적으로 클라우드 기반 브라우저 보안이 규모에 맞게 브라우저, 사용자 및 응용 프로그램을 대상으로 하는 위협을 가장 효과적으로 해결할 수 있습니다.

브라우저 보안에 대해 더 알아보려면 menlosecurity.com/ko - kr/을 방문하거나 korea@menlosecurity.com으로 이메일을 보내주십시오.

MENLO SECURITY

korea@menlosecurity.com

브라우저 보안 비교표

이 표는 각 언급된 기술이 브라우저 보안의 각 핵심 기능을 지원하는 방식을 보여줍니다. 이러한 기능은 사용자 보호, 기업 보안, 그리고 관리자와 최종 사용자 모두에게 우수한 사용자 경험을 유지하는 데 중요합니다.

		메인 스트림/ 기업용 브라우저	브라우저 확장 프로그램	기존 RBI	클라우드 기반의 브라우저 보안
브라우저 관리	브라우저 설정 구성	🟢	🟠 제한	🔴	🟢 엔터프라이즈 브라우저 관리자에서 제공한 API 를 통한 크로스 플랫폼
	스크린 샷 가능여부	🟠 Bypassable	🔴	🔴	🟠
	장치 상태 확인	🟢	🔴	🔴	🟢 에이전트 필요 할 수 있음
	확정 프로그램	🟢	🟢	🔴	🟢 엔터프라이즈 브라우저 관리자에서 제공한 API 를 통한 크로스 플랫폼
사용자 보호	브라우저 취약성 (제로데이 포함) 보호	🔴	🔴	🟢 클라우드의 모든 활성 콘텐츠	🟢
	멀웨어에 대한 보호	🟢	🔴 다운로드한 파일에 대한 제한된 가시성	🟢 엔진/시그니처 업데이트 가 더 쉽습니다. 크로스 디바이스	🟢 엔진/시그니처 업데이트 가 더 쉽습니다. 크로스 디바이스
	피싱에 대한 보호	🟢	🟢	🟢 엔진/시그니처 업데이트 가 더 쉽습니다. 크로스 디바이스	🟢 엔진/시그니처 업데이트 가 더 쉽습니다. 크로스 디바이스
액세스 및 데이터 보안	데이터 유출로부터 보호	🟠 공격자가 우회할 수 있음	🟠	🔴 Not in scope	🟢 보호된 데이터는 엔드포인트에 닿지않음
	데이터 수정	🟠 공격자가 우회할 수 있음	🟠	🔴 Not in scope	🟢
	워터마킹	🟢	🟢	🔴 Not in scope	🟢
	애플리케이션 액세스	🟠 공격자가 우회할 수 있음	🟠	🔴 Not in scope	🟢 가능 경로는 클라우드 브라우저를 통해서만 가능
	복사 & 붙여넣기	🟠 공격자가 우회할 수 있음	🟠	🔴 Not in scope	🟠
	확장 노출	🟢	🟢	🔴 Not in scope	🟢 클라이언트 확장에 노출되지 않음
	로깅 및 감사	🟠 변조 방지 기능 없음	🟠	🔴 제외	🟢