Prisma Access Browser: SASE의 필수 요소

브라우저에서의 작업 증가는 조직의 위험 증가를 의미합니다.

업무 방식이 바뀌었습니다. 점점 더 많은 SaaS 및 웹 애플리케이션을 통해 클라우드의 기업 리소스에 액세스하고, 인스턴트 메시징을 통해 동료와 채팅하고, AI를 사용하여 이메일을 작성하는 방식은 새로운 업무 패러다임에서 현실이 되었습니다. 업무 수행을 위해 사용하는 디바이스가 사무실의 노트북에서 이동 중에도 사용할 수 있는 스마트폰으로 확장되었습니다.

최신 인력은 바뀌었습니다. 직원 증강, 타사 비즈니스 파트너, 컨설턴트, 아웃소싱으로 인해 '동료'라는 단어는 최신 인력에서 완전히 새로운 의미를 갖게 되었습니다. 현대 업무 공간은 경계가 없습니다.

이러한 모든 변화에 따라 보안도 변화해야 하며, 변화해야만 합니다. 중앙 집중식 사무실 환경에서 간단하게 구현하고 시행할 수 있었던 정책과 제어가 이제는 전 세계 가장 먼 곳까지 확장되었습니다. 여러 위치에서 다양한 디바이스를 사용하는 신입 직원에게도 본사의 동료와 동일한 수준의 보호와 주의가 필요하며, 표준화되고 구성하기 쉬운 보안을 통해 업무에 방해가 되지 않도록 해야 합니다. 그렇지 않으면 원격 근무자든 아니든 생산성을 유지하기 위해 이러한 보안 제어를 우회하게 됩니다.

이러한 환경에서 확장된 하이브리드 업무 모델과 AI 지원은 이제 업무 공간에서 생산성의 핵심 요소입니다. 최신 인력은 다양한 SaaS 앱과 디바이스에 의존하여 비즈니스 속도를 유지합니다. 그리고 이 작업이 이루어지는 장소는 어디일까요? 마찬가지로, 바뀌었습니다. 이제 작업은 거의 전적으로 브라우저에서 이루어집니다.

Palo Alto Networks의 최근 조사에 따르면 직원들이 업무 시간의 85% 이상을 웹 브라우저에서 보내는 것으로 나타났습니다.[1] 브라우저는 모든 사람의 일상에서 중심적인 역할을 합니다. 그러나 이로 인해 브라우저는 사이버 공격의 주요 표적이 되고 있으며, 설문조사에 참여한 조직의 약 95%가 모든 디바이스에서 브라우저 기반 위협을 보고했습니다.[2] 위험 비율이 왜 이렇게 높을까요? 전통적으로 웹 브라우저는 보안 솔루션과 이를 사용하는 팀에게 사각지대였기 때문입니다.

사실, 따라잡기가 어려웠습니다.

이러한 취약점 증가에 대응하기 위해 Palo Alto Networks는 SASE의 핵심 요소로 Prisma® Access Browser를 도입했습니다. 이 보안 브라우저는 SASE의 잠재력을 최대한 발휘하여 몇 분 안에 모든 디바이스에 포괄적인

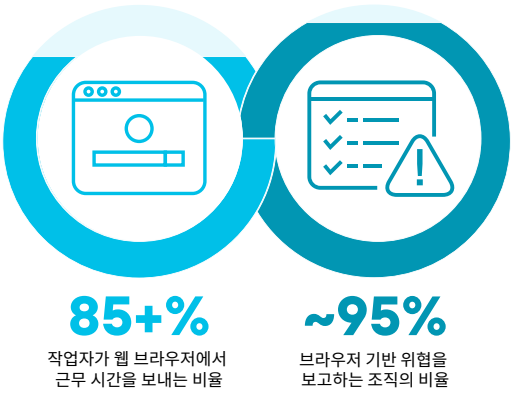

그림 1: 작업자가 안전하지 않은 웹 브라우저에서 대부분의 시간을 보냅니다.

보안을 제공합니다. SASE 프레임워크에 기본적으로 통합된 최초이자 유일한 보안 브라우저로, 조직은 사용자 마찰을 최소화하면서 필수 웹 애플리케이션에 안전하게 액세스하고 여러 개인정보 및 데이터 규정을 준수하는 동시에 위협으로부터 인력을 보호할 수 있습니다.

1. *Optimizing Security for Modern Workforces*, Palo Alto Networks 및 Omdia, 2025년 1월.
2. Ibid.

보안 액세스의 진화

레거시 보안 솔루션은 그 솔루션이 나온 시대에는 효과가 있었지만 더 이상 오늘날의 인력에게 필요한 보호 기능을 제공하지 못합니다. 관리되지 않는 디바이스, 클라우드 기반 인프라, 새로운 네트워크 프로토콜에 대한 의존도가 높아지면서 이러한 구식 솔루션의 한계가 드러나고 있습니다. 그 결과 보안의 공백과 열악한 사용자 환경이 지속되어 조직이 취약해지고 생산성이 저하됩니다.

기존의 보안 구현은 브라우저 기반 위협에 대한 포괄적인 보호 기능을 제공하지 못하여 조직이 클라우드 네이티브 애플리케이션 및 확장 프로그램의 공격에 노출되어 있습니다. 브라우저가 주요 작업 공간이 되면서 민감한 기업 네트워크 침해를 노리는 공격자들에게 유리한 표적이 되고 있습니다. 이러한 변화에는 SASE 원칙을 브라우징 환경에 직접 통합하는 새로운 접근 방식이 필요합니다.

웹 브라우저 내에서 더 많은 작업이 수행되고 SaaS 애플리케이션에 대한 의존도가 높아짐에 따라 오래된 SASE 접근 방식의 격차를 줄이는 것이 중요합니다. 완벽한 SASE 솔루션은 브라우저로 확장되어 SaaS 및 비관리형 디바이스를 사용하는 최신 인력을 위한 안전한 정책 적용 액세스 및 라스트 마일 데이터 제어를 보장해야 합니다. 웹 및 클라우드 애플리케이션 내에서 사용자 상호 작용에 대한 완전한 가시성과 제어가 없으면 조직은 데이터 노출 및 규정 준수 문제의 위험이 증가합니다. 기업이 클라우드 환경과 하이브리드 업무로 전환함에 따라 포괄적인 보안과 사용자 작업 전반의 취약성을 줄이기 위해서는 모든 브라우저 기반 활동을 포함하도록 SASE를 확장하는 것이 필수적입니다. SASE를 브라우저로 확장하면 네트워크, 엔드포인트, 브라우저 등 다계층 다차원 보안 전략에 계층이 추가되어 강력한 보호를 보장합니다.

새로운 SASE를 통한 최신 인력 지원

현재의 업무 환경을 최우선으로 고려하여 구축된 솔루션, 어제가 아닌 오늘날의 작업자의 요구에 맞춘 유연하고 분산된 글로벌 솔루션, 그리고 가장 중요한 것은 브라우저에서 작업이 수행되는 위치에 대한 가시성, 보안 및 제어를 제공하는 솔루션 등 완벽한 SASE 솔루션의 필요성이 그 어느 때보다 분명해졌습니다.

Palo Alto Networks는 관리형 및 비관리형 디바이스 모두에서 안전한 업무 공간을 구축할 수 있도록 기본적으로 통합된 보안 브라우저를 갖춘 업계 유일의 SASE 솔루션을 제공합니다. 처음으로 모든 사용자가 모든 디바이스에서 SaaS 및 개인 애플리케이션에 일관되고 지속적으로 마찰 없는 제로 트러스트 액세스를 즐길 수 있으며, 관리자는 사용자와 데이터가 만나는 지점을 제어할 수 있습니다. 이제 어디서나 모든 작업자에게 동일한 보안 정책과 경험을 제공할 수 있습니다.

솔루션 설계의 핵심은 특정 직무에 맞게 세분화된 보안 정책을 배포할 수 있는 브라우저의 기능입니다. 직원은 자신의 역할에 필요한 데이터와 애플리케이션에만 액세스할 수 있으며, 민감한 정보는 마스킹 처리되고 불필요한 앱과 웹사이트는 차단됩니다. 이 최소 권한 액세스 정책은 모든 작업자의 업무 수행에 영향을 주지 않으면서도 강력한 보안을 보장합니다.

Prisma Access Browser의 주요 기능

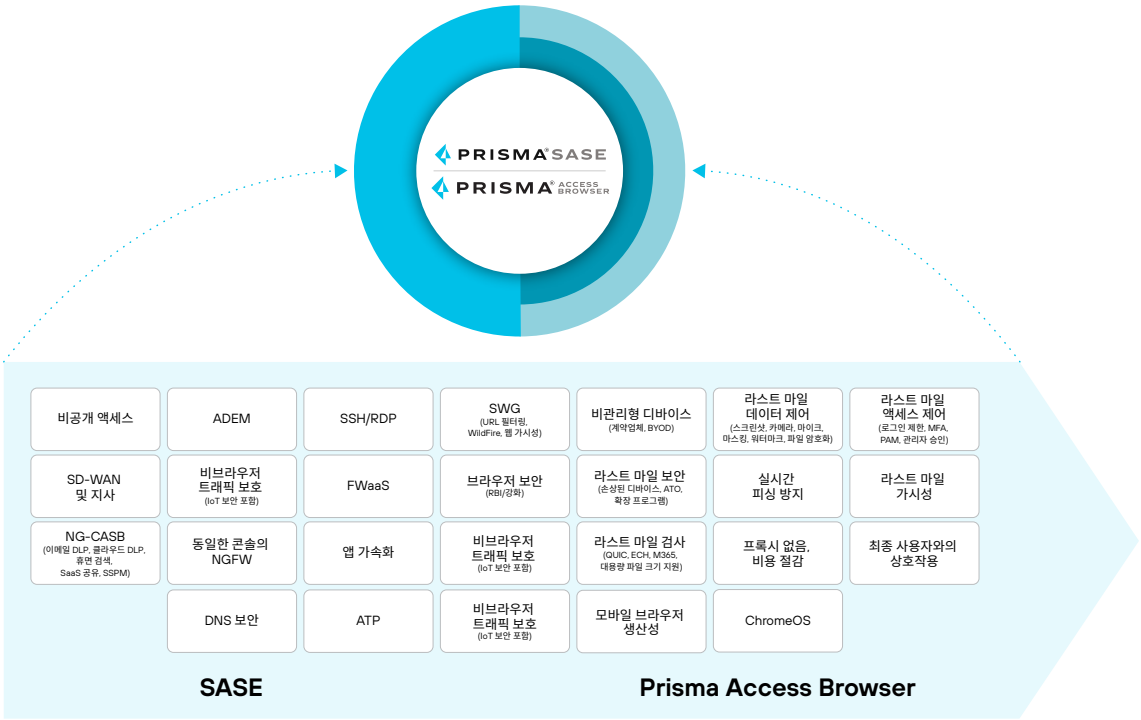

그림 2: Prisma Access Browser는 SASE를 확장하고 브라우저를 통해 보안을 확장하여 탁월한 보호 기능을 제공합니다.

모든 디바이스에서 다방향 보안

손상된 엔드포인트에 대한 보호

Prisma® Access Browser는 관리형 및 비관리형 디바이스 모두에 향상된 보안을 제공하여 회사 디바이스든 개인 스마트폰, 태블릿, 노트북이든 모든 디바이스에 안전한 작업 공간을 만들어 줍니다. 이를 통해 사용자는 기업 네트워크의 무결성을 손상시키지 않고 어느 위치에서나 안전하게 작업할 수 있습니다. 브라우저는 신뢰할 수 없는 엔드포인트의 잠재적 위협으로부터 기업 애플리케이션을 격리하여 데이터 유출 및 멀웨어 침입의 위험을 줄입니다.

관리형 디바이스에서는 오래된 소프트웨어, 사용자 오류 또는 정교한 피싱 공격으로 인해 취약성이 여전히 발생할 수 있습니다. 피싱은 여전히 가장 중요한 위협 중 하나로, 공격자가 그럴듯한 이메일과 웹사이트를 제작하여 직원을 속여 민감한 정보를 공개하거나 멀웨어를 설치하도록 유도합니다. 피싱 수법이 점점 더 정교해짐에 따라 포괄적인 보호 기능을 갖추는 것이 중요합니다. Prisma Access Browser는 고급 보안 기능을 브라우저에 직접 내장하여 이러한 위협에 대응합니다. 자동화된 웹 모니터링 및 위협 탐지 기능을 제공하여 피싱 시도 및 기타 위협을 신속하게 식별하고 차단합니다.

위협으로부터 보호

Prisma Access Browser는 브라우저 계층에 암호화 계층을 추가하여 키로거, 화면 스크레이퍼, 신뢰할 수 없는 인증서 및 공용 네트워크의 위협으로부터 보호합니다. 민감한 브라우저 구성 요소를 비활성화하여 공격 표면을 줄이고 악성 확장 프로그램을 방어함으로써 브라우저는 작업이 항상 보호되도록 합니다. 90초마다 디바이스 상태를 확인하고 위협 추적 및 포렌식을 위한 웹 인사이트를 수집하는 등 Prisma Access Browser의 선제적 보안 조치는 보안을 더욱 강화합니다.

전체 SASE 제품군과의 통합으로 Prisma Access Browser의 보안 기능이 더욱 강화되었습니다. 업계 최대 규모의 클라우드 기반 멀웨어 방지 엔진인 Advanced WildFire®는Palo Alto Networks Precision AI™를 기반으로 7700만 개 이상의 새로운 파일을 분석하고 매일 최대 45만 개의 새로운 고유 악성 파일을 예방합니다. AI 기반 URL 필터링은 업계 최대 규모의 순수 AI 기반 위협 인텔리전스 데이터베이스를 활용하여 매일 1억 5100만 개의 악성 URL을 차단합니다. 고급 Threat Prevention 기능은 딥 러닝 모델을 통해 정교한 위협을 실시간으로 방어하며 인젝션 공격의 90%를 방지합니다.

오늘날의 업무 환경에서는 조직이 어떤 디바이스에서든 안전하게 작업할 수 있도록 지원하는 것이 매우 중요합니다. 이러한 유연성은 비관리형 엔드포인트와 관련된 보안 위험을 완화하는 동시에 선호하는 디바이스를 사용할 수 있도록 하여 작업자의 생산성과 만족도를 높입니다. 모든 디바이스에서 포괄적인 보호 기능을 제공함으로써 조직은 강력한 보안 태세를 유지하고 데이터 손실 위험을 줄이며 규제 요건을 준수할 수 있습니다.

SaaS 및 웹 앱 전반의 가시성 및 제어 강화

Prisma Access Browser는 SaaS 및 웹 애플리케이션 내의 모든 사용자 활동에 대한 가시성과 제어 기능을 강화하여 모든 앱에서 수행되는 모든 작업으로 컨텍스트 기반 제로 트러스트 정책을 확장합니다. 이를 통해 데이터, ID, 권한 액세스 제어를 전반적으로 일관되게 적용하고 시행할 수 있습니다. 제로 트러스트를 모든 사용자 및 디바이스 속성, 모든 웹 애플리케이션, 모든 작업 및 라스트 마일 제어로 확장함으로써 조직은 포괄적인 감독을 유지하고 우발적이거나 의도적인 데이터 유출로부터 보호할 수 있습니다.

선도적인 데이터 분류 엔진, 다단계 인증(MFA), 모든 제어에 대한 적시(JIT) 권한으로 탁월한 보안 범위를 제공합니다. 우발적이든 고의적이든 데이터 유출은 광범위한 결과를 초래할 수 있습니다. 실제로 조직의 55%는 지난 12개월 동안 우발적인 데이터 유출을 경험한 적이 있다고 답했습니다.[3]

Prisma Access Browser는 강력한 기능 세트로 데이터 손실을 완화합니다. 보안팀은 사용자와 기업 리소스의 상호작용에 대한 세분화된 인사이트를 확보하여 잠재적인 위협을 실시간으로 모니터링하고 대응할 수 있습니다. 사용자/그룹, 디바이스 상태, 네트워크 및 위치를 포함한 모든 사용자 및 디바이스 속성을 볼 수 있습니다. 이러한 가시성을 통해 조직은 엄격한 데이터 보호 조치를 구현하고 사용자 역할, 컨텍스트 및 행동에 따라 민감한 정보에 대한 액세스를 제어할 수 있습니다. 무단 데이터 액세스 및 유출을 방지하여 권한이 있는 직원만 고위험 작업을 수행할 수 있도록 합니다.

특히 민감한 데이터와 중요한 애플리케이션을 다룰 때 보안과 규정을 준수하는 환경을 유지하려면 향상된 가시성과 제어 기능이 필수적입니다. Prisma Access Browser를 사용하면 조직은 암호 해독 없이도 모든 웹 및 SaaS 트래픽을 기록, 모니터링, 제어할 수 있습니다. 또한 조직은 Prisma Access Browser를 통해 파일 업로드/다운로드, 복사/붙여넣기, 텍스트 입력, 텍스트 마스킹, 인쇄, 스크린샷/공유, 카메라/마이크 사용에 대한 제어 기능을 설정할 수 있습니다. 이 브라우저는 1,000개 이상의 내장 데이터 분류기와 고급 ML/NLP, OCR, EDM, IDM 기능을 포함하는 Palo Alto Networks DLP와 통합하여 강력한 콘텐츠 기반 보호를 보장합니다. 또한 HIPAA, PII, GDPR, PCI 등 22개의 사전 정의된 규정 및 규정 준수 프로필을 지원합니다.

3. *The State of Workforce Security: Key Insights for IT and Security Leaders,* Palo Alto Networks 및 Omdia, 2025년 2월.

모든 애플리케이션에 라스트 마일 데이터, ID 및 액세스 제어를 적용함으로써 조직은 사용자의 위치나 디바이스에 관계없이 보안 정책을 일관되게 적용할 수 있습니다. 패스키 및 관리자 승인 프로세스를 포함한 단계별 MFA 및 JIT 권한은 특히 권한 있는 사용자를 보호하기 위해 보안 계층을 추가합니다.

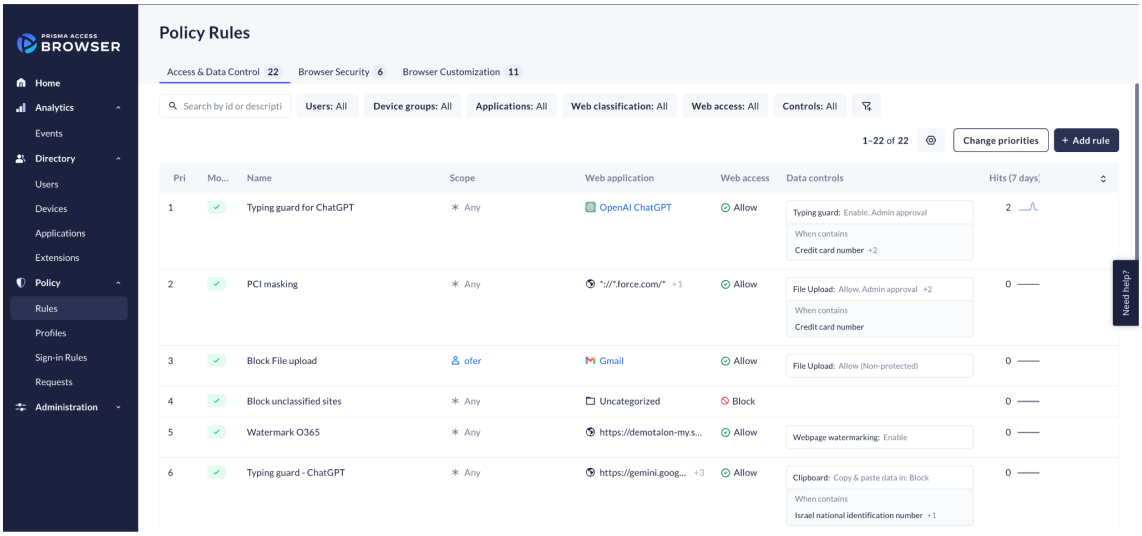

그림 3: 매우 자세히 설정 가능한 규칙은 모든 앱의 모든 사용자 및 디바이스 속성에 적용됩니다.

즐거운 사용자 경험 제공

Prisma Access Browser는 최대 가동 시간과 대폭 향상된 성능을 특징으로 하는 탁월한 사용자 경험을 제공하도록 설계되었습니다. 완전히 분산된 인프라는 안정성과 속도를 보장하여 사용자에게 원활하고 생산적인 브라우징 환경을 제공합니다. 공용 및 SaaS 앱부터 비공개 및 SSH/RDP 애플리케이션에 이르기까지 모든 업무용 애플리케이션에 브라우저에서 바로 액세스할 수 있습니다. Prisma Access Browser는 일반적으로 생산성을 저해하는 보안 조치를 최소화함으로써 사용자가 프로토콜을 우회할 필요 없이 규정 준수를 유지할 수 있도록 지원합니다. 또한 GenAI 애플리케이션에 대한 수요가 증가함에 따라 브라우저는 이러한 고급 도구에 대한 안전하고 효율적인 액세스를 지원하여 보안을 유지하면서 생산성을 향상시킬 수 있습니다.

사용자는 기존 솔루션보다 최대 5배 향상된 성능으로 애플리케이션에 더 빠르게 액세스할 수 있습니다. 이렇게 향상된 성능은 직원들이 더 빠르고 효율적으로 작업을 수행할 수 있어 생산성 향상으로 이어집니다. 브라우저는 가장 관련성이 높은 콘텐츠를 선제적으로 미리 가져와 빠르고 원활한 상호 작용을 보장합니다. 또한 인프라 변경 없이 몇 분 만에 완료할 수 있는 간소화된 온보딩 및 오프보딩 프로세스는 노트북을 배송할 때보다 총 소유 비용을 약 80% 절감하여 IT 운영을 더욱 간소화합니다.

즐거운 사용자 경험을 제공하는 것은 사용자 채택과 만족도를 높이는 데 매우 중요합니다. 직원들이 빠르고 안정적인 브라우징 환경을 경험하면 해결 방법을 찾기보다는 보안 조치를 받아들일 가능성이 높아집니다. 이는 전반적인 생산성을 향상시킬 뿐만 아니라 보안 정책을 준수하도록 보장합니다. 단일 장애 지점 없이 최대 가동 시간을 유지하는 Prisma Access Browser의 기능은 사용자의 신뢰와 만족도를 더욱 높여줍니다.

IT 비용이 절감되고 디바이스 관리가 간소화되면 조직은 다른 전략적 이니셔티브에 더 많은 리소스를 할당하여 전반적인 비즈니스 성장과 효율성을 높일 수 있습니다. 이 브라우저를 사용하면 조직 전체에서 정책을 쉽게 정의하고 확장할 수 있습니다. 자율적 디지털 경험 관리(ADEM)는 디바이스 성능, 네트워크 성능, Wi-Fi 문제 등을 표시하여 애플리케이션 성능 문제를 선제적으로 해결합니다.

ADEM의 일부인 실제 사용자 모니터링(RUM)은 페이지 로드 및 렌더링 시간과 같은 추가적인 성능 인사이트를 통해 브라우저에서 중단 없는 생산성을 보장합니다. AI Access Security™와의 통합을 통해 직원들에게 안전한 AI 도입을 지원하고, 어떤 AI 앱을 누가 사용하는지 확인하여 AI 사용에 대한 완벽한 실시간 가시성을 제공하며, 공유 데이터, 기밀 및 IP를 스캔하여 포괄적인 데이터 보호를 제공합니다. 손끝에서 액세스 제어를 통해 승인되지 않은 앱을 차단하고, 정보 보안 정책을 적용하고, 데이터를 보호하여 안전하고 즐거운 사용자 경험을 보장할 수 있습니다.

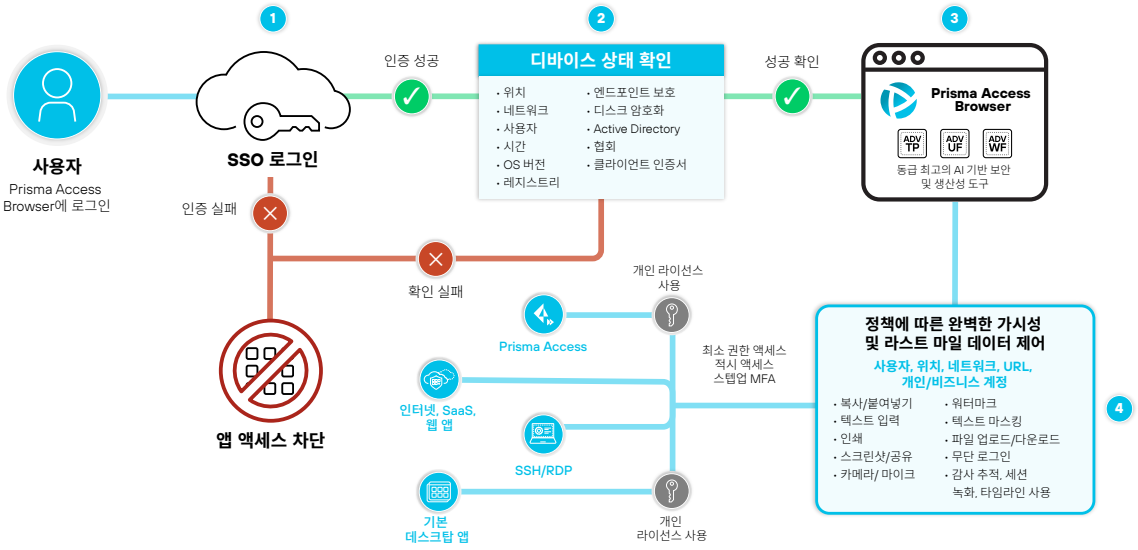

그림 4: 사용자가 Prisma Access Browser로 작업에 액세스하는 방법 예시

Prisma Access Browser 실제 사용 사례

독립 작업자

Prisma Access Browser는 타사와 계약업체가 안전하고 효율적으로 액세스할 수 있도록 설계되어 모든 기기에서 몇 분 안에 SaaS 및 비공개 애플리케이션에 연결할 수 있습니다. 이 기능은 인수합병, 콜센터, 일선 및 현장 근무자 등 다양한 시나리오에서 매우 중요합니다. 관리 권한이 필요한 기존 솔루션과 달리 Prisma Access Browser는 사용자의 개입 없이도 원활한 액세스와 보안을 제공합니다.

기업인수 합병

기업 인수 합병 시에는 서로 다른 IT 시스템과 리소스를 빠르고 안전하게 통합하는 것이 중요합니다. 또한 M&A 성공의 핵심 지표인 가치 실현 시간을 단축하기 위해 전환 기간 동안 직원들의 생산성을 유지하는 것도 중요합니다. Prisma Access Browser는 새로 인수한 팀이 관리형 또는 비관리형 모든 디바이스의 중요 애플리케이션에 보안을 손상시키지 않고 몇 분 안에 액세스할 수 있도록 지원하여 이러한 작업을 용이하게 합니다. Prisma Access Browser를 통해 기업, SaaS 및 GenAI 앱에 빠르게 안전하게 액세스하면 노트북 및 VDI 배송에 비해 저렴한 비용으로 직원들이 M&A 프로세스 내내 생산성을 유지할 수 있습니다. 세분화된 보안 정책을 적용하고 고급 위협 방지 기능을 활용함으로써 조직은 통합 전반에 걸쳐 중요한 데이터를 보호할 수 있습니다.

콜센터

콜센터에는 고객 데이터와 기업 애플리케이션에 빠르고 안전하게 액세스해야 하는 정규직 직원, 계약직 직원, 타사 공급업체가 혼합되어 있는 경우가 많습니다. Prisma Access Browser는 모든 디바이스에서 안전한 컨텍스트 기반 액세스를 지원하여 솔루션을 제공합니다. 이를 통해 콜센터 상담원은 데이터 보호 규정을 준수하면서 효율적으로 업무를 수행할 수 있습니다.

일선 및 현장 근무자

일선 및 현장 근무자는 기존의 보안 조치가 비현실적인 환경에서 근무하는 경우가 많습니다. Prisma Access Browser를 사용하면 모바일 디바이스에서 기업 애플리케이션과 데이터에 안전하게 액세스하여 업무를 효과적으로 수행하는 데 필요한 도구를 확보할 수 있습니다.

Prisma Access Browser는 타사 및 계약업체를 위한 SaaS 및 비공개 애플리케이션에 대한 안전한 액세스를 제공함으로써 조직이 기존의 경계를 넘어 보안 경계를 확장할 수 있도록 지원합니다. 이 기능은 운영의 민첩성과 유연성을 지원할 뿐만 아니라 위치나 기기에 관계없이 모든 사용자가 안전하고 효율적으로 작업할 수 있도록 보장합니다.

개인 디바이스 사용

Prisma Access Browser는 직원들이 자신의 디바이스를 업무에 유연하게 사용할 수 있도록 지원하여 언제 어디서나 비즈니스 애플리케이션에 안전하게 액세스할 수 있도록 합니다. 이러한 BYOD 기능은 인력 민첩성 향상, 디바이스의 자유, 모바일 지원, 비용 절감, VDI에 대한 의존도 감소 등 몇 가지 주요 이점을 제공합니다.

인력 민첩성

오늘날과 같이 빠르게 변화하는 비즈니스 환경에서는 직원들이 이동 중에도 회사 리소스에 액세스할 수 있는 기능이 필요합니다. Prisma Access Browser는 직원들이 개인 디바이스에서 SaaS 및 비공개 애플리케이션에 안전하게 연결할 수 있도록 지원하여 이러한 민첩성을 실현합니다. 재택근무, 출장, 사무실 근무 등 어떤 상황에서든 직원들은 특정 디바이스나 장소에 얽매이지 않고 생산성과 연속성을 유지할 수 있습니다.

디바이스 자유도

Prisma Access Browser를 사용하면 직원들은 더 이상 회사에서 지급한 디바이스만 사용하지 않아도 됩니다. 선호하는 스마트폰, 태블릿, 노트북에서 비즈니스 애플리케이션에 액세스할 수 있어 더욱 개인화되고 편리한 업무 환경을 제공합니다.

모바일 디바이스 사용

모바일 디바이스 사용은 기존 사무실 환경 밖에서 비즈니스 애플리케이션에 액세스해야 하는 직원에게 매우 중요합니다. Prisma Access Browser는 모바일 디바이스를 기업 네트워크에 안전하게 통합하여 필수 도구와 정보에 원활하게 액세스할 수 있도록 지원합니다. 이 기능은 모바일 디바이스에 의존하여 연결성과 생산성을 유지하는 현장 근무자, 영업팀, 원격 근무자에게 특히 유용합니다.

노트북 배송비 절감

원격 근무 직원에게 회사 노트북을 배송하는 것은 비용이 많이 들고 물류적으로 어려울 수 있습니다. Prisma Access Browser는 새로운 직원이 이미 가지고 있는 모든 개인 디바이스에서 안전하게 액세스할 수 있도록 지원하여 이러한 필요성을 없애줍니다. 이는 특히 대규모 IT 통합 또는 임시직 근로자의 경우 하드웨어 프로비저닝 및 배송과 관련된 비용을 크게 줄여줍니다.

Prisma Access Browser의 BYOD 기능은 직원들이 자신의 디바이스를 자유롭게 사용할 수 있도록 지원하여 인력의 민첩성과 생산성을 향상시킵니다. 비즈니스 애플리케이션에 대한 안전하고 유연한 액세스를 제공함으로써 조직은 비용을 절감하고 IT 운영을 간소화하며 모바일을 사용하는 최신 인력을 지원할 수 있습니다.

안전한 GenAI

생성형 AI 도구는 비즈니스 운영을 혁신하고 있지만, 잠재적인 보안 위험도 내포하고 있습니다. Prisma Access Browser는 웹 기반 GenAI 도구를 사용하기 위한 안전한 환경을 제공하여 위험을 줄입니다. 브라우저의 라스트 마일 DLP 제어를 통해 브라우저 내에서 AI 플랫폼과의 데이터 상호 작용이 보호됩니다.

안전한 데이터 상호 작용

작업자가 실수로 중요한 기업 데이터를 GenAI 앱에 업로드할 수 있으므로 데이터 보호는 매우 중요합니다. Prisma Access Browser는 라스트 마일 데이터 보호 기능을 적용하여 복사-붙여넣기를 차단하고 파일 업로드를 비활성화하며 앱에 민감한 정보를 입력하는 것을 방지합니다. 사용 중인 데이터를 보호하는 것은 사용자가 실수로 민감한 정보를 AI 시스템과 공유할 경우 발생할 수 있는 데이터 유출을 방지하는 데 있어 매우 중요합니다.

가시성 및 액세스 제어

GenAI 도구를 사용할 때 가장 큰 어려움 중 하나는 섀도우 AI에 대한 가시성을 확보하고 사용자 액세스 제어를 유지하는 것입니다. Prisma Access Browser는 AI 도입 및 사용에 대한 가시성을 제공하여 IT 보안팀이 ChatGPT와 같은 플랫폼과의 상호 작용을 모니터링하고 관리할 수 있도록 지원합니다. 이러한 가시성은 민감한 정보를 보호하고 직원들이 허용되는 사용 정책을 준수하도록 하는 데 매우 중요합니다. 이는 조직에서 관리되지 않는 디바이스의 사용을 허용할 때 특히 유용합니다.

AI Access Security가 적용된 Prisma Access Browser

Prisma Access Browser를 GenAI 전용 솔루션인 AI Access Security와 함께 사용하면 조직은 관리형 및 비관리형 디바이스 모두에서 안전한 AI 도입 및 사용을 지원하고 클라이언트 측과 네트워크에서 민감한 데이터를 보호할 수 있습니다. AI 액세스 보안을 사용하면 제재된 GenAI 앱을 제어할 수 있으며 GenAI 태세 관리, AI 마켓플레이스, 플러그인 등에 대한 추가 보호 기능을 제공합니다. 종합적인 SASE 솔루션의 일부인 이 결합 제품은 브라우저와 디바이스의 자유를 보장하는 동시에 강력한 보안과 제어 기능을 제공합니다.

종합적인 SASE 솔루션의 일부인 Prisma Access Browser는 조직이 강력한 보안 제어를 유지하면서 혁신과 생산성을 높일 수 있도록 지원합니다. 보안과 혁신 사이의 이러한 균형은 AI가 비즈니스 운영에서 더 큰 역할을 계속 수행함에 따라 매우 중요합니다.

VDI 줄이기

VDI 솔루션은 복잡하고 유지 관리 비용이 많이 들 수 있습니다. 브라우저 기반 솔루션을 제공하는 Prisma Access Browser는 VDI 인프라에 대한 의존도를 줄이면서도 비즈니스 애플리케이션에 액세스할 수 있는 안전하고 제어된 환경을 제공합니다. VDI 배포를 줄이면 운영 비용이 절감될 뿐만 아니라 애플리케이션에 더 빠르고 안정적으로 액세스할 수 있어 사용자 경험도 향상됩니다.

리소스 최적화

기존의 VDI 환경은 관리 및 운영에 상당한 리소스가 필요하기 때문에 비용이 많이 들고 인프라가 복잡해지는 경우가 많습니다. Prisma Access Browser는 일상적인 브라우징 활동을 보안 브라우저로 전환하여 이러한 요구를 완화합니다. 이 접근 방식은 VDI 시스템의 부하를 줄여 보다 효율적인 리소스 할당과 전체 인프라 비용을 절감할 수 있습니다.

세분화된 사용자 그룹

모든 직원이 전체 VDI 액세스를 필요로 하는 것은 아니며, 많은 직원이 보안 브라우징 기능만 필요로 합니다. Prisma Access Browser를 사용하면 조직은 사용자 기반을 브라우저 전용 그룹과 전체 데스크톱 그룹으로 세분화하여 사용자 요구에 따라 적절한 수준의 액세스를 제공함으로써 VDI 배포를 최적화할 수 있습니다. 이러한 세분화는 전체 데스크톱 환경이 필요하지 않은 사용자의 비용 절감과 성능 향상으로 이어집니다.

비용 절감

VDI 인프라를 유지 관리하려면 하드웨어와 지속적인 운영 비용 측면에서 비용이 많이 들 수 있습니다. Prisma Access Browser는 비즈니스 애플리케이션에 대한 안전한 브라우저 기반 액세스를 지원하여 비용 효율적인 대안을 제공합니다. 이를 통해 비용이 많이 드는 VDI 배포의 필요성을 줄이고 총 소유 비용을 낮추는 동시에 기업 리소스에 액세스하기 위한 안전하고 제어된 환경을 제공합니다.

Prisma Access Browser는 기존 VDI에 대한 의존도를 줄임으로써 조직이 비용을 절감하고 IT 인프라를 간소화하며 전반적인 사용자 경험을 개선할 수 있도록 지원합니다. 원격 액세스에 대한 이러한 최신 접근 방식은 기업이 보다 유연하고 확장 가능한 IT 솔루션을 계속 채택함에 따라 특히 유용합니다.

비즈니스 연속성

운영 중단 중에도 중요한 비즈니스 애플리케이션에 원활하게 액세스할 수 있도록 하는 것은 운영을 유지하는 데 매우 중요합니다. Prisma Access Browser는 언제 어디서나 모든 디바이스에서 기업 리소스에 안전하고 중단 없이 액세스할 수 있도록 하여 비즈니스 연속성을 지원합니다. 내장된 데이터 보호 기능과 실시간 위협 탐지 기능을 통해 민감한 정보를 보호하고 예기치 못한 이벤트나 중단에도 비즈니스 활동이 원활하게 지속될 수 있도록 보장합니다.

모든 디바이스에서 안전한 액세스

업무 중단에도 불구하고 직원들이 계속 일할 수 있도록 지원합니다. 엔터프라이즈 브라우저를 사용하면 전 세계 어디에서나 관리되지 않는 디바이스를 포함하여 모든 디바이스에서 회사 애플리케이션에 안전하게 액세스할 수 있습니다.

몇 분 안에 활성화

중단이 발생하면 클릭 한 번으로 Prisma Access Browser를 새로운 기본 작업 공간으로 사용할 수 있습니다. 원하는 애플리케이션에 액세스할 수 있는 사용자를 쉽게 구성하여 각 활동에 대한 디바이스 상태 확인 및 보안 요구 사항을 보장할 수 있습니다. 정전이 발생해도 직원들은 지체 없이 안전하게 업무용 도구에 액세스할 수 있습니다.

고급 보안

사이버 범죄자들은 팬데믹, 전쟁, 광범위한 IT 중단과 같은 주요 사건을 기회주의적으로 이용하여 혼란에 빠진 직원과 다른 무고한 사람들을 속이는 데 악용하는 경우가 많습니다. Prisma Access Browser를 사용하면 브라우저 내 활동에 대한 완벽한 가시성과 제어를 통해 안전한 환경에서 비즈니스 운영을 유지할 수 있습니다. 고도로 세분화된 액세스와 데이터 및 ID 제어를 통해 비즈니스 운영을 유지하는 데 필요한 정확한 구성을 정의하고 이벤트 로그, 세션 기록 등을 포함한 전례 없는 가시성을 확보할 수 있습니다.

모든 직원을 위한 원활한 채택

하루 중 85% 이상을 브라우저에서 보내는 직장인에게 Prisma Access Browser에서 작업하는 것은 자연스러운 일입니다. 전 세계 직원들은 시스템을 재부팅하고 노트북을 배송하느라 애쓸 필요 없이 노트북을 열어 생산 환경에 필요한 변화에 신속하게 대응하고, 고객 및 동료와 소통하고, 민감한 정보에 액세스하고, 원격 컴퓨터와 서버를 운영하여 업무 프로세스를 유지하는 등 비즈니스의 원활한 운영에 필요한 기타 중요한 작업을 수행할 수 있습니다.

복호화를 허용하지 않는 보안 앱

오늘날의 기업은 수많은 SaaS 및 웹 애플리케이션에 의존하고 있으며, 이 중 상당수는 운영 효율성을 보장하기 위해 암호화된 채널을 활용합니다. 안타깝게도 공격자들은 이러한 의존성을 악용하여 멀웨어를 숨기고, 명령 및 제어 채널을 설정하고, 민감한 데이터를 유출하기 위해 Microsoft 365, Google Workspace, Slack과 같이 널리 신뢰받는 애플리케이션의 암호화된 채널을 악용하고 있습니다. 현재 사이버 위협의 86%는 암호화된 채널을 통해 전달되므로(4) 이러한 애플리케이션에 대한 가시성은 진정한 제로 트러스트 보안 프레임워크의 중요한 구성 요소입니다.

Palo Alto Networks 보안 솔루션으로 탁월한 복호화

Palo Alto Networks는 차세대 방화벽(NGFW) 및 SASE 솔루션을 통해 웹 및 비웹 트래픽 모두에서 업계 최고의 복호화 기능을 제공합니다. 정밀 AI를 기반으로 하는 이러한 솔루션은 암호화된 트래픽을 심층 검사하여 알려진 위협과 알려지지 않은 위협을 모두 차단하는 동시에 고급 DLP 기능을 통해 강력한 데이터 보호 기능을 제공합니다. 그러나 특정 유형의 트래픽은 애플리케이션 기능, 규정 준수 의무 또는 사용자 경험 요구 사항으로 인해 해독되지 않습니다. 이로 인해 웹 트래픽의 64%가 암호화되어 있으며 숨겨진 위협에 잠재적으로 취약할 수 있습니다.[5]

안전한 가시성을 갖춘 복호화 보완

암호화 해제되지 않은 상태로 남아 있는 트래픽의 문제를 해결하기 위해 Prisma Access Browser는 당사의 선도적인 네트워크 복호화 기능과 함께 작동하여 제로 트러스트 보안을 위한 통합된 다계층 접근 방식을 형성합니다. 유일한 SASE 네이티브 보안 브라우저인 Prisma Access Browser는 트래픽을 해독할 필요 없이 브라우저를 통해 액세스하는 모든 애플리케이션에 대한 가시성과 제어 기능을 제공합니다. 또한 제로 트러스트 정책을 모든 브라우저 기반 활동으로 확장하여 광범위한 네트워크 솔루션을 지원하는 것과 동일한 고급 위협 탐지 및 데이터 보호 기능을 활용합니다. 이 접근 방식을 사용하면 암호화되지 않은 트래픽도 모니터링 및 제어할 수 있으므로 성능에 영향을 주지 않고 위험을 최소화할 수 있습니다.

포괄적인 보호를 위한 이중-계층적 접근 방식

Prisma Access Browser를 Palo Alto Networks 보안 플랫폼과 통합함으로써 조직은 모든 애플리케이션과 통신 채널에서 암호화된 트래픽에 대한 종합적인 가시성과 제어를 확보할 수 있습니다. 네트워크 보안은 탁월한 암호 해독 및 위협 방지 기능을 제공하는 반면, Prisma Access Browser는 암호 해독이 불가능한 브라우저 기반 활동을 보호합니다. 이 둘을 함께 사용하면 암호화된 트래픽이든 암호 해독되지 않은 트래픽이든 사각지대가 발생하지 않습니다.

이 이중 계층 모델은 숨겨진 위협을 탐지하고 중요한 데이터를 보호하며 관리형 및 비관리형 디바이스 모두에서 원활한 보호 기능을 제공합니다. 기업은 Prisma Access Browser를 통해 사용자 경험이나 생산성을 저하시키지 않으면서 모든 트래픽을 처리하는 진정한 제로 트러스트 태세를 도입하여 오늘날의 복잡한 위협 환경에서 탄력적인 보안 태세를 유지할 수 있습니다.

전에 없던 사용 사례

Prisma Access Browser는 고급 보안 기능을 브라우저에 직접 통합함으로써 기존 솔루션으로는 달성하기 어렵거나 불가능했던 다양한 사용 사례를 실현합니다. 이를 통해 조직은 매우 유연한 데이터, 액세스 및 ID 제어를 통해 새롭고 역동적인 시나리오에 신속하게 대처할 수 있습니다. 주요 사용 사례로는 라스트 마일 데이터 보호 지원, 권한 있는 사용자 보호, 내부자 위협 방지, 비즈니스 연속성 보장, GenAI 도구 사용, 섀도우 IT 관리 등이 있습니다.

4. "86% of cyberattacks are delivered over encrypted channels," Help Net Security, 2023년 12월 21일.
5. *The State of Workforce Security: Key Insights for IT and Security Leaders*, Palo Alto Networks 및 Omdia, 2025년 1월.

라스트마일 데이터 보호

데이터 전송 및 액세스의 마지막 단계는 데이터 유출에 가장 취약한 곳입니다. 직원들의 업무 시간 중 평균 85%를 브라우저에서 보내는 만큼, 이 '라스트 마일'을 보호하는 것은 매우 중요합니다. Prisma Access Browser는 브라우저 내에서 직접 암호화, 액세스 제어, 실시간 모니터링과 같은 보안 조치를 원활하게 통합합니다. 이 브라우저의 포괄적인 보호 기능에는 데이터 마스킹, 스크린샷 차단, 협업 도구를 통한 공유 제한, 복사/붙여넣기 기능 제어, 인쇄 방지, 민감한 화면의 워터마크 적용과 같은 고급 제어 기능이 포함되어 있습니다.

권한 있는 사용자 보호

높은 액세스 권한을 가진 권한 있는 사용자는 사이버 공격의 주요 표적이 됩니다. Prisma Access Browser는 중요한 워크플로 단계에서 단계별 다단계 인증, 라스트 마일 데이터 보호, 데이터 무결성을 보장하는 가시성 제어, 디바이스 상태 확인, 모든 활동(세션 녹화 포함)의 상세한 감사 추적과 같은 기능을 통해 이러한 사용자의 보안을 강화합니다. 이러한 종합적인 보안 조치를 통해 권한이 있는 사용자는 안전하고 통제된 환경에서 작업할 수 있습니다.

내부자 위협 완화

고의적이거나 우발적인 내부자 위협은 기업 데이터 보안에 심각한 위험을 초래합니다. Prisma Access Browser는 사용자가 브라우저의 보안 작업 영역에서만 액세스할 수 있는 애플리케이션을 정의하여 이러한 위협을 방지할 수 있는 다양한 제어 기능을 제공합니다. 조직은 비즈니스 작업 공간을 개인 계정과 분리하고 작업자가 공유하거나 액세스할 수 있는 파일 유형을 제어할 수 있습니다. 예를 들어, 기업 앱에서 다운로드한 파일을 암호화하고 기업 외 SaaS 애플리케이션의 액세스를 제한하여 민감한 데이터를 안전한 브라우저 환경 내에서 보호할 수 있습니다.

비관리형 계정에 액세스

조직은 종종 가상 거래실이나 금융 서비스 등 관리하지 않는 계정에 대한 액세스 권한을 제공해야 하는데, 이러한 계정은 보안이 어려울 수 있습니다. Prisma Access Browser는 특허 출원 중인 계정 보호 기능으로 이러한 애플리케이션을 보호합니다. 이 기능은 모든 사용자 비밀번호에 비밀 요소를 추가하며, 이 비밀 요소는 Prisma Access Browser에 저장됩니다. 이렇게 하면 다른 브라우저나 다른 사용자가 계정에 액세스하는 것이 금지됩니다.

섀도우 IT

직원들이 승인되지 않은 애플리케이션과 디바이스를 사용하는 섀도우 IT는 심각한 보안 위험을 초래합니다. Prisma Access Browser는 모든 웹 기반 활동에 대한 가시성을 제공하여 조직이 섀도우 IT를 효과적으로 모니터링하고 관리할 수 있도록 지원합니다. 이러한 종합적인 감독을 통해 데이터 유출을 방지하고 조직 내에서 사용되는 모든 애플리케이션과 디바이스가 보안 정책을 준수하도록 보장합니다.

Prisma Access Browser는 브라우저에서 직접 매우 유연한 데이터, 액세스 및 ID 제어 기능을 제공함으로써 수많은 새로운 사용 사례를 열어줍니다. 이는 보안을 강화할 뿐만 아니라 생산성을 향상시켜 조직이 자신감 있고 민첩하게 동적인 시나리오에 대처할 수 있도록 지원합니다. 기업 보안의 브라우저 격차를 해소하는 Prisma Access Browser는 현대 기업의 복잡한 문제를 해결할 수 있는 강력하고 종합적인 솔루션을 제공합니다.

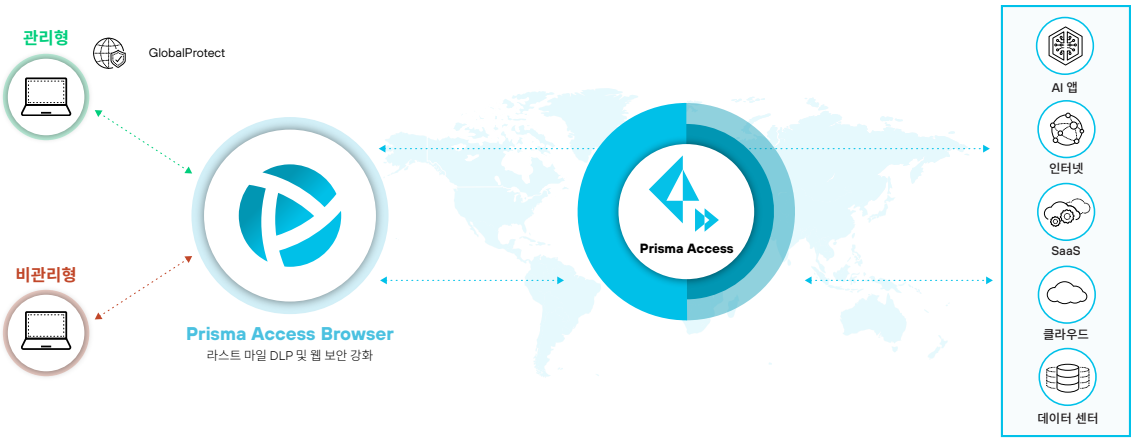

그림 5: Prisma Access Browser로 SASE의 강력한 기능 활용

앞으로의 여정

인력 보안에 대한 모든 변화와 함께 위협도 진화하고 있다는 것은 잘 알려진 사실입니다. 클라우드 리소스 활용부터 일상 업무에 AI 사용까지 새로운 업무 방식에 적응하면서 보안과 생산성을 유지하는 데 직면하는 과제가 점점 더 복잡해지고 있습니다. 보다 정적인 업무 환경을 위해 설계된 기존의 보안 모델로는 더 이상 충분하지 않습니다. 현대의 인력만큼이나 역동적이고 유연한 솔루션이 필요합니다.

Prisma Access Browser는 이러한 문제를 해결하는 데 있어 중요한 진전을 이루었습니다. 브라우저를 통해 SASE를 확장함으로써 관리형 및 비관리형 모든 디바이스에서 전 세계 어디에서나 원활하고 안전한 사용자 경험을 제공합니다.

앞으로 보안 브라우저의 중요성은 더욱 커질 것입니다. Gartner는 "2030년까지 엔터프라이즈 브라우저는 원활한 하이브리드 업무 환경을 위해 관리형 및 비관리형 디바이스에서 직원 생산성 및 보안 소프트웨어를 제공하는 핵심 플랫폼이 될 것"이라고 예측합니다.[6] 이러한 변화는 현대 비즈니스가 요구하는 유연성과 민첩성을 지원하면서 포괄적인 보안을 제공할 수 있는 Prisma Access Browser와 같은 솔루션의 필요성을 강조합니다.

미래의 업무 환경은 브라우저 기반입니다. 조직이 하이브리드 업무 모델을 계속 수용함에 따라 안전하고 효율적이며 사용자 친화적인 도구의 필요성은 더욱 중요해질 것입니다. Prisma Access Browser는 이러한 요구 사항을 충족할 뿐만 아니라 역동적이고 끊임없이 변화하는 업무 환경의 미래 과제까지 예측합니다. 탁월한 보안과 쾌적한 사용자 경험을 제공함으로써 직원들이 어디서 어떻게 근무하든 생산성과 보안을 유지할 수 있도록 지원합니다.

보안 솔루션도 업무와 함께 진화해야 한다는 것은 분명합니다. Prisma Access Browser는 업무가 이루어지는 브라우저 보안을 위한 강력하고 통합된 접근 방식을 제공하여 이러한 진화를 쉽게 만들어줍니다. 고급 기능과 SASE 프레임워크와의 원활한 통합을 통해 엔터프라이즈 보안의 새로운 표준을 제시하며 생산성과 보안이 함께 발전하는 미래를 위한 기반을 마련합니다.

6. Dan Ayoub 외, *Emerging Tech: Security — The Future of Enterprise Browsers*, Gartner, 2023년 4월 14일.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

대표 전화: +1.408.753.4000
판매 문의: +1.866.320.4788
지원 문의: +1.866.898.9087

www.paloaltonetworks.com

prisma_wp_pab-integral-part-of-sase_020425