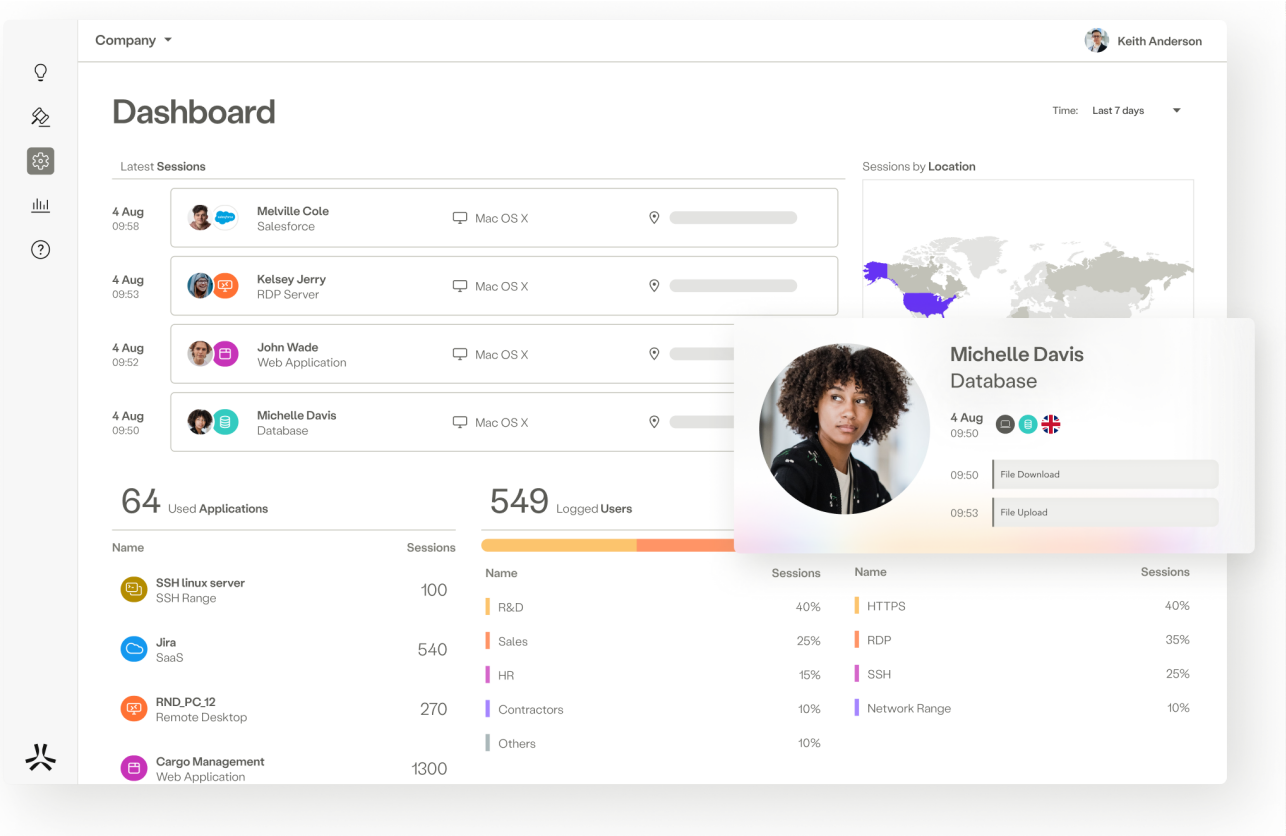
HPE Aruba Networking SSE

HPE Aruba Networking SSE를 통해 어디서나 모든 사용자, 장치, 애플리케이션에 대해 중단 없는 보안 액세스를 지원할 수 있습니다



언제 어디서나 사무실과 똑같이 연결되면 다음이 가능합니다.

분산된 기업 지원

94%

직원이 주로 하이브리드 또는 완전히 재택 근무를 한다고 답한 조직의 비율입니다.[1]

제3자 액세스 보호

1/3

사용자가 파트너, 공급업체, 벤더 또는 고객인 비율입니다. 네트워크 액세스를 확장하거나 에이전트를 설치할 필요 없이 비즈니스 에코시스템이 민감한 데이터에 안전하게 액세스할 수 있도록 지원하세요.

인프라 고도화

전환

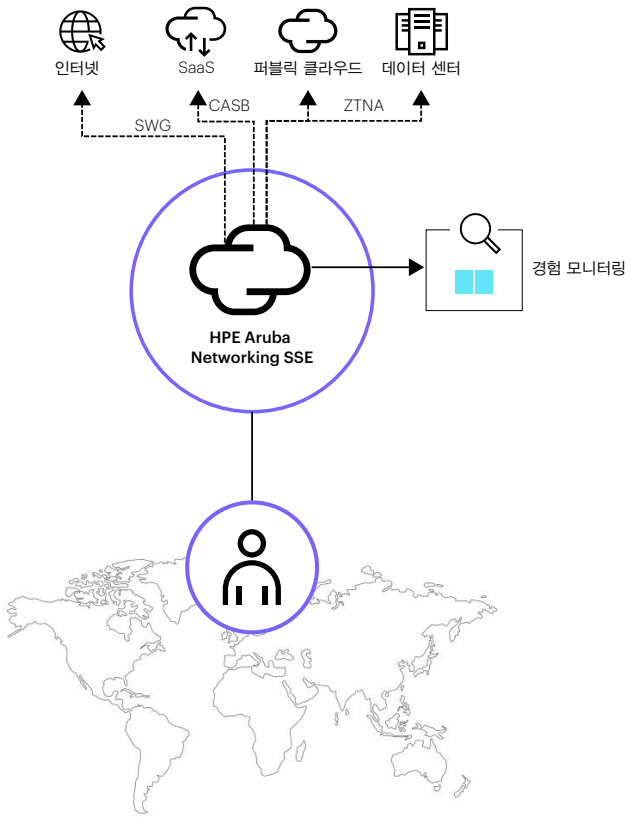
네트워크를 고도화된 클라우드 아키텍처로 바꾸세요. 기존 어플라이언스 교체, 하이브리드-클라우드 채택 간소화, 인프라 비용 절감, 자동화 도입을 시행하세요.

경쟁에서 앞서나가기 위해, IT 팀은 인력과 공급망의 생산성을 유지할 수 있는 서비스에 투자해야 했습니다. 이에 따라 IT 팀에게 사용자를 Microsoft 365, Salesforce, SAP®와 같은 주요 비즈니스 리소스에 연결할 새로운 기술을 정립할 기회가 생겼습니다. IT 리더 중 90%는 직원까지 연결이 확장되는 SaaS 및 하이브리드 클라우드 서비스를 채택할 계획을 가지고 있습니다. 이러한 고도화된 업무 환경에서는 모든 사용자, 애플리케이션, 장치가 인터넷에 연결되어 있습니다.

기존의 네트워크와 달리, IT 팀에서는 인터넷을 제어할 수 없습니다. 따라서 지난 30년 동안 사용해 왔던 네트워크 솔루션은 더 이상 시대에 맞지 않고, 이로 인해 사용자가 네트워크에 있게 되어 인프라가 인터넷에 노출됩니다. 인터넷 액세스를 안전하고 원활하게 제어하려면 새로운 접근 방식이 필요합니다.

HPE Aruba Networking은 SSE(Security Service Edge) 플랫폼과의 보안 연결을 통해 고도화된 업무 환경으로 빠르게 전환하는 것이 목표입니다. HPE Aruba Networking SSE는 500개 이상의 엣지 위치를 사용하여 업무에 필요한 비즈니스 리소스에 사용자, 장치, 서버를 원활하게 연결하는 플랫폼입니다. 이 플랫폼은 ZTNA(Zero Trust Network Access), SWG(Secure Web Gateway), CASB(Cloud Access Security Broker), DEM(Digital Experience Monitoring)을 하나의 클라우드 제공 플랫폼에 정교하게 통합하여 어려움 없이 이용할 수 있으며, 이는 단일 창에서 제어할 수 있습니다.

[1] SSE 도입 보고서, Cybersecurity Insiders, 2024



뛰어난 단순성

복잡성을 최소화하는 SSE

단일 창에서 사용자와 앱을 관리하세요. 클라우드 설계로 IT 팀의 관리 부담이 완화되며 고급 정책 태그 지정 시스템이 갖춰져 있어 사용이 단순합니다.

뛰어난 스마트한 성능

더욱 스마트해지고 강력해진 성능을 증명하는 SSE

IDP의 사이버 보안 메시와 엔드포인트 서비스로 환경과 자동으로 동기화하여 정책을 자동 조율하고 액세스 권한을 막힘없이 조정하세요. SSE는 더욱 스마트해지고 강력해진 성능을 증명하며, 사용자 체감 만족도 문제에도 더 빠르게 대응합니다.

뛰어난 보안

위치에 구애받지 않고 보안을 제공하는 SSE

트래픽을 검사하여 가시성을 높이고 랜섬웨어를 방지하세요. 데이터 유출로부터 보호하고 더 신속하게 감지하고 대응하여 위협을 방지하세요.

HPE Aruba Networking SSE 기능

ZTNA

HPE Aruba Networking ZTNA는 업계 내에서 고도로 발전한 서비스입니다. ID, 정책, 컨텍스트를 사용하여 비공개 앱(VoIP, AS400, ICMP[Internet Control Message Protocol] 포함)에 대한 안전한 일대일 연결을 중개합니다. VPN을 완전히 대체하며 네트워크에 액세스할 필요가 없는 것은 물론 네트워크가 외부로 노출되는 것도 방지합니다.

SWG

HPE Aruba Networking SWG는 고급 SSL 검사, URL 필터링, DNS 필터링을 통해 인증된 사용자가 빠르고 안전하게 인터넷에 액세스할 수 있도록 하는 동시에 공격이 주목적인 인터넷 기반 위협으로부터 기업을 보호합니다.

CASB

HPE Aruba Networking CASB를 이용하면 사용자와 클라우드 애플리케이션 사이의 연결을 중재하고 앱의 섀도 IT를 찾아낼 수 있습니다. CASB는 전송 중인 민감한 비즈니스 데이터를 보호하는 동시에 사이버 위협을 방지합니다.

DEM

HPE Aruba Networking DEM은 홉 바이 홉 지표를 측정하고 앱, 장치, 네트워크 성능을 모니터링하여 사용자의 생산성을 유지합니다. IT 팀에서 연결 문제를 쉽게 짚어내고 무결성 확보까지 소요되는 평균 시간을 단축할 수 있습니다.

일원화된 창구

통합된 SSE 대시보드를 통해, IT 팀은 비공개 앱, 인터넷, SaaS 앱, DEM에 대한 액세스를 하나의 콘솔에서 관리할 수 있습니다. 손쉽게 정책을 정의하고 사용자 활동을 추적하며 테넌트를 관리하고 SSE, IDP, 엔드포인트 보안으로 이루어진 사이버 보안 메시를 감독합니다.

모든 트래픽 검사

HPE Aruba Networking ZTNA와 SWG로 공개는 물론 비공개 트래픽을 모두 검사하여 사용자 활동, 다운로드된 파일, 사용된 명령을 확인하고 악의적인 동작을 차단합니다.

애플리케이션 검색

승인되지 않은 애플리케이션과 도메인을 찾고 각각에 대한 정책을 쉽게 정의하며 조직에서 공격에 노출되는 표면을 전반적으로 축소합니다.

자동화된 알림 및 데이터 분류

HPE Aruba Networking SSE는 AI를 사용하여 알림을 생성하고 잠재적인 보안 이벤트를 자동으로 감지하며 데이터 분류를 개선합니다.

에이전트 및 에이전트리스

SSE 에이전트는 트래픽을 HPE Aruba Networking SSE 플랫폼으로 전달하고 장치 상태를 평가하며 기존 엔드포인트 솔루션과 통합합니다. 에이전트는 iOS, Android™, Mac, Windows를 지원합니다. HPE Aruba Networking SSE는 에이전트리스 기능도 강력하여 브라우저 기반 RDP, SSH, Git, 데이터베이스를 포함하여 웹 기반 앱에 안전하게 액세스할 수 있습니다.

서버 간 액세스

HPE Aruba Networking SSE는 사용자 외 엔터티에 제로 트러스트를 적용하여 서버가 다른 서버와 안전하게 통신하도록 합니다.

데이터 유출 방지

파일 다운로드, 복사, 붙여넣기를 차단하며 규정 준수 표준을 지키게 하는 정책을 인라인으로 시행하여 민감한 데이터가 인터넷에 유출되지 않도록 보호합니다. 에이전트 및 에이전트 기반 배포를 지원합니다.

감지 및 대응

고급 맬웨어 스캔 및 감지를 통해 맬웨어 기반 공격을 선제적으로 방지합니다. 향상된 인사이트를 통해 팀에서 그 어느 때보다 보안 이벤트에 빠르게 대응할 수 있습니다.

자세히 알아보기

ArubaNetworks.com/products/sse/

HPE.com 방문하기

채팅 상담하기

© Copyright 2025 Hewlett Packard Enterprise Development LP. 본 문서의 내용은 사전 통지 없이 변경될 수 있습니다. Hewlett Packard Enterprise 제품 및 서비스에 대한 보증의 경우, 해당 제품 및 서비스와 함께 제공된 보증서에 명시된 내용만이 적용됩니다. 본 문서에는 어떠한 추가 보증 내용도 들어 있지 않습니다. Hewlett Packard Enterprise는 본 문서의 기술상 또는 편집상의 오류나 누락에 대해 책임지지 않습니다.

Android는 Google LLC의 상표입니다. Microsoft 및 Windows는 미국 또는 기타 국가에서 Microsoft Corporation의 등록 상표 또는 상표입니다. SAP는 독일 및 기타 국가에서 SAP SE(또는 SAP 계열사)의 상표 또는 등록 상표입니다. 모든 타사 마크는 해당하는 소유자의 재산입니다.

a00133860KOP, 제1차 개정판

HEWLETT PACKARD ENTERPRISE

hpe.com