솔루션 개요

ARUBA CLEARPASS POLICY MANAGER

유무선용 액세스 가시성 및 보안

IT가 든든한 문지기 역할을 하며 엄격한 정책과 통제된 에코시스템으로 환경을 지배하던 때를 기억하십니까? 이러한 시대는 지나갔습니다. 오늘날 IT와 사용자 소유의 장치는 경계 보안 안팎에서 연결되어 있습니다.

수많은 노트북, 스마트폰, 태블릿 및 IoT(사물 인터넷) 장치가 업무 환경에 넘쳐나고 있습니다. 이러한 상황에서 데이터를 보호하려면 무엇보다도 네트워크상에 무엇이 존재하는지 파악할 수 있어야 합니다. 자동 정책 이행을 사용하면 정상 사용자 및 장치의 연결만 허용할 수 있으며, 내외부 감사 및 컴플라이언스 요구 사항을 안전하게 준수하려면 실시간 위협 보호가 필요합니다.

전문가들의 전망이 맞다면 유무선 네트워크상에서 IoT 장치가 사용됨에 따라 IT'의 중점 분야가 변경되고 있습니다. 대부분의 조직에서는 무선 네트워크와 장치에 대한 보안은 적용했지만 회의실, IP 전화, 프린터 등의 유선 포트는 방치하고 있는 실정입니다. 또한 IoT 장치에는 보안 속성이 부재하고 외부 관리 리소스가 액세스해야 할 수 있기 때문에 유선 액세스가 새로운 리스크로 부상하고 있습니다.

IT에서 제어력을 유지하려면 기본 인프라를 프로그래밍하고 알려졌거나 알려지지 않은 IoT 및 모바일 장치에 대한 네트워크 액세스를 제어하는 적절한 툴이 필요합니다. 오늘날의 보안 솔루션은 프로파일링, 정책 이행, 게스트 액세스, BYOD 온보딩 등의 기능을 통해 IT에서 워크로드를 오프로드하고, 위협으로부터 더욱 효율적으로 보호하고, 향상된 사용자 환경을 제공해야 합니다.

모빌리티와 IoT로 인한 NAC에 대한 인식 변화

IT 도메인의 경계는 이제 엔터프라이즈의 벽을 넘어서고 있습니다. 기업들은 보안을 그대로 유지하면서 언제 어디서나 연결을 제공하기 위해 노력하고 있습니다. IT가 비즈니스 및 사용자 환경에 영향을 주지 않으면서 가시성과 제어력을 유지하려면 어떻게 해야 할까요? 다음과 같은 3단계 계획을 살펴보십시오.

1. **식별** 어떤 장치가 얼마나 사용되고 있으며, 어디에서 접속하고 있고, 어떤 운영 체제가 지원되는지 식별해야 합니다. 이것이 모든 것의 기초가 됩니다. 또한 변경되는 내용과 네트워크를 오가는 장치에 대한 지속적인 인사이트가 시간이 흐름에 따라 요구되는 가시성을 제공합니다.
2. **이행** 사용자, 장치 유형 또는 위치에 상관없이 사용자와 장치에 적절한 액세스를 제공하는 정확한 정책을 이행함으로써 기대에 부응하는 사용자 환경을 제공할 수 있습니다. 스마트폰이든 감시 카메라든, 기업들은 오늘날 끊임없이 발전하는 장치 및 그 용도에 맞추어 적응할 수 있어야 합니다.
3. **보호** 동적 정책 제어, 그리고 타사 시스템으로 확장되는 실시간 문제 해결을 통해 리소스를 보호해야 합니다. 보호는 퍼즐의 마지막 조각입니다. 새벽 3시에도 예상치 못한 네트워크 동작에 대비되어 있으려면 트래픽을 차단하고 장치의 연결 상태를 변경하는 통합 접근 방식이 필요합니다.

기업에서는 기존 문제는 물론 예상치 못한 문제에 대해서도 미리 대비해야 합니다. 사용자가 원격에서 근무하거나 새 스마트폰을 구입해야 할 때 IT와 헬프 데스크 직원들이 수동으로 개입하는 방식은 현실적이지 않습니다. NAC는 이제 더 이상 알려진 장치가 액세스하기 전에 평가를 수행하기 위해서만 존재하지 않습니다.

한곳에서 모든 것을 파악하고 관리

ClearPass 정책과 AAA 솔루션은 내장 장치 프로파일링, 웹 기반 관리 인터페이스, 그리고 실시간 경보와 함께 종합적인 보고를 제공합니다. 또한 수집된 컨텍스트 데이터를 활용하여 액세스 방법이나 장치 소유자와 관계없이 사용자와 장치에 적절한 액세스 권한을 부여합니다.

내장 프로파일링 엔진은 장치 카테고리, 벤더, OS 버전 등의 정보를 비롯한 실시간 데이터를 수집합니다. 이제 더 이상 유무선 네트워크에 몇 대의 장치가 연결되었는지 막연히 추측할 필요가 없습니다. 정밀한 가시성을 통해 감사에 통과하고 성능 및 보안 리스크의 원인을 파악하기 위해 필요한 데이터가 제공됩니다.

THE POWER OF CLEARPASS EXCHANGE

독립 실행형 ClearPass Universal Profiler는 정책을 완전히 이행할 준비가 되지 않은 조직과 ClearPass가 처음부터 구축되지 않은 원격 지사에도 동일한 수준의 프로파일링 가시성을 제공합니다.

IT는 템플릿 기반 정책 이행 기능을 사용하여 사용자 역할, 장치 유형, MDM/EMM 데이터, 인증 상태, 위치, 요일 등을 활용하는 유무선 중심 정책을 구축할 수 있습니다. 직원, 학생, 의사, 게스트, 경영진, 그리고 각 사용자가 지참하는 각 장치 유형에 대해 간편하게 정책을 이행할 수 있습니다.

ClearPass OnConnect는 조직에서 비AAA 이행을 사용하여 수많은 유선 포트를 차단할 수 있도록 해 주는 내장 기능입니다. 이 기능을 사용하기 위해서는 따로 장치를 구성할 필요가 없이 스위치에 명령 한 줄만 입력하면 됩니다. 유선과 무선에 대해 표준 AAA/802.1X 방법도 지원됩니다.

따라서 사일로화된 AAA, NAC 및 정책 솔루션으로는 불가능한 일관적인 정책 이행과 엔드-투-엔드(end-to-end) 접근 방식이 가능해집니다. Microsoft Active Directory, LDAP 호환 디렉토리, ODBC 호환 SQL 데이터베이스, 토큰 서버 및 내부 데이터베이스를 비롯한 단일 정책 서비스에서 복수의 ID 저장소를 사용할 수 있다는 것 또한 ClearPass 레거시 솔루션과 차별화되는 지점입니다.

IT 개입 없이 장치 프로비저닝

BYOD 환경을 위해 개인 장치의 온보딩을 관리하는 일은 IT와 헬프 데스크 리소스에 부담이 될 수 있으며, 보안 문제를 유발할 수도 있습니다.

ClearPass Onboard를 사용하면 사용자가 스스로 안전한 네트워크에서 장치를 사용하도록 구성할 수 있습니다. 또한 장치별 인증서 덕분에 사용자들이 하루종일 로그인 자격 증명을 반복적으로 입력해야 할 필요가 없어집니다. 이러한 편의성 하나만으로도 엄청난 이점이 제공됩니다. 인증서 사용을 통해 추가되는 보안은 보너스입니다.

장치 온보딩을 수행할 수 있는 사용자, 이러한 사용자가 온보딩할 수 있는 장치 유형, 그리고 인당 몇 대의 장치까지 온보딩 가능한지는 IT 팀에서 정의하게 됩니다. IT는 내장된 인증 기관 덕분에 내부 PKI처럼 빠르게 개인 장치를 지원할 수 있으며, 이때 추가적인 IT 리소스는 요구되지 않습니다.

빠르고 간단한 게스트 액세스

BYOD에는 단지 직원 장치만 포함되는 것이 아닙니다. 유선이나 무선 네트워크 액세스가 필요한 게스트 장치도 BYOD에 포함됩니다. IT는 브랜드 포털에 장치를 푸시하고, 액세스 자격 증명 프로비저닝을 자동화하고, 동시에 엔터프라이즈 트래픽을 별개로 유지하는 보안 기능이 제공되는 간단한 모델이 필요합니다.

ClearPass Guest는 직원, 리셉션 담당자, 이벤트 담당자 및 기타 IT 외부 직원들이 하루 동안 지정된 명수의 게스트에 대한 임시적인 네트워크 액세스 계정을 간편하고 효율적으로 만들 수 있도록 해 줍니다. 게스트는 MAC 캐싱으로 인해 게스트 포털에 반복해서 자격 증명을 입력하지 않고도 하루종일 간편하게 접속할 수 있습니다.

셀프 등록 기능이 제공되어 직원들의 업무가 과중되지 않으며, 게스트가 스스로 자격 증명을 만들 수 있습니다. 로그인 자격 증명은 인쇄된 배지, SMS 또는 이메일로 제공됩니다. 자격 증명은 설정된 시간 동안 ClearPass에 저장되며, 지정된 시간이나 일수가 경과하면 자동으로 만료되도록 설정할 수 있습니다.

장치 상태로 액세스 결정

장치가 기업의 바이러스 방지 정책, 스파이웨어 방지 정책 및 방화벽 정책을 준수하도록 하기 위해 인증 과정 중에 특정 장치에 대한 상태 평가를 수행해야 할 수 있습니다. 사용자들은 엔터프라이즈 네트워크에 접속하기 전에 자동화 기능으로 인해 자발적으로 바이러스 백신 검사를 수행하게 됩니다.

ClearPass OnGuard에는 다양한 컴퓨터 운영 체제 및 버전에 걸쳐 취약성을 제거하는 포스처 기반 상태 확인을 수행하는 기능이 내장되어 있습니다. ClearPass는 지속 클라이언트를 사용하든 휘발성 클라이언트를 사용하든 관계없이 무선, 유선 및 VPN 인프라에서 호환 엔드포인트를 중앙 집중식으로 식별합니다.

추가적인 보안을 제공하는 고급 상태 검사의 예:

- 피어투피어 애플리케이션, 서비스 및 레지스트리 키 처리.
- USB 스토리지 장치 또는 가상 시스템 인스턴스의 허용 여부 판단.
- 브리징 네트워크 인터페이스 및 디스크 암호화의 사용 관리.

타사 솔루션 십분 활용하기

ClearPass Exchange는 방화벽, MDM/EMM, MFA, 방문자 등록 및 SIEM 툴 등 널리 사용되는 타사 솔루션을 사용하여 보안 위협 해결을 자동화하거나 서비스를 강화할 수 있도록 지원합니다. 기업에서는 ClearPass에 포함된 컨텍스트 인텔리전스를 바탕으로 장치, 네트워크 액세스, 트래픽 검사 및 위협 보호 수준에서 보안과 가시성을 적용할 수 있습니다.

공통 언어(REST) API, Syslog 메시지 및 ClearPass Extensions라는 내장 리포지토리를 사용하는 자동 워크플로와 의사 결정으로 인해 작업이 간소화되고 기업이 보호됩니다. 더 이상 복잡한 스크립트 언어를 사용하고 반복적인 수동 구성에 신경 쓸 필요가 없습니다. 파트너들은 Extensions로 확장 프로그램을 업로드하여 공동 고객에게 신규 서비스를 실시간으로 제공할 수 있기 때문에 통합도 훨씬 빨라집니다.

ClearPass Exchange로 인해 네트워크는 다음과 같은 작업을 자동으로 수행할 수 있습니다.

- 장치의 탈옥 상태와 같은 MDM/EMM 데이터를 바탕으로 네트워크 연결 가능 여부를 판단합니다.
- 사용자, 그룹, 특정 장치 속성을 바탕으로 방화벽에서 정책을 정확하게 이행할 수 있으며, ClearPass를 사용하여 의심스러운 동작을 보이는 장치에 대해 조치를 취할 수 있습니다.
- 연결된 장치의 인증 데이터가 저장되도록 SIEM 툴을 설정할 수 있습니다.
- 네트워크와 리소스에 정말로 정상 사용자가 연결하는 것인지 확인하기 위해 사용자들에게 다중 인증을 사용하도록 강제할 수 있습니다.

특정 네트워크 이벤트가 발생하면 방화벽, SIEM 및 기타 툴에서 ClearPass로 하여금 양방향 동작을 트리거하여 장치에 대한 조치를 취하도록 할 수 있습니다. 예를 들어 사용자가 네트워크 인증에 수차례 실패하는 경우, ClearPass에서 장치로 직접 알림 메시지를 발송하거나 장치가 네트워크에 액세스하지 못하도록 차단할 수 있습니다.

어디서나 안전하게 업무용 앱에 액세스

직원들은 하루 중 언제든지 빠르고 간편하게 업무용 앱에 로그인할 수 있어야 합니다. ClearPass는 이를 위해 SSO 및 ClearPass Auto Sign-On을 지원합니다. Auto Sign-On은 모든 사용자가 앱에 한 번씩 로그인해야 하는 단일 사용자 로그인(SSO) 대신 사용자들이 자동으로 엔터프라이즈 모바일 앱에 액세스할 수 있도록 유효한 네트워크 로그인을 사용합니다. 사용자 장치에는 네트워크 로그인 또는 유효한 인증서만 있으면 됩니다.

단일 사용자 로그인(SSO)이 사용되는 경우 ClearPass를 IdP(ID 프로바이더) 또는 SP(서비스 프로바이더)로 사용할 수도 있습니다.

Bonjour, DLNA 및 UPnP 서비스

사용자들은 Aruba Wi-Fi 인프라에서 DLNA/UPnPL나 Apple AirPlay 및 AirPrint를 사용하는 프로젝트, TV, 프린터 및 기타 미디어 어플라이언스를 공유할 수 있습니다. ClearPass는 이러한 장치를 간편하게 검색하고 공유할 수 있도록 지원합니다.

태블릿에서 프레젠테이션을 보여 주려는 교사에게는 교실에 있는 디스플레이만 표시됩니다. 학교의 다른 곳에 있는 장치들은 표시되지 않습니다. 또한 포털에서 디스플레이를 사용할 수 있는 사용자가 누구인지 확인할 수 있어, 학생들이 임의로 디스플레이를 사용하지 못하도록 할 수 있습니다.

헬스케어 분야에서는 의사들이 병원 어디서나 iPad에서 대형 화면으로 디지털 PACS 이미지를 프로젝션할 수 있습니다. 이로 인해 환자 치료를 위한 협업이 훨씬 간편해집니다.

보안 및 서비스를 위한 적응형 기반

오늘날의 모바일 사용자들에게 원활한 환경을 제공해야 한다는 목표와 IoT 기술의 빠른 확산으로 인해 새로운 IT 문제가 생겨났습니다. 유무선 네트워크에서 언제 어디서나 안전하게 액세스를 지원하기 위해서는 신중한 계획과 적절한 툴, 그리고 강력한 기반이 필요합니다.

ClearPass는 단일 통합 솔루션으로 장치 ID, 정책 제어, 워크플로 자동화 및 자동 위협 보호 기능을 제공하여 이러한 문제를 해결합니다. ClearPass는 실시간 컨텍스트 데이터를 수집하고 상관관계를 분석하여 사용자가 사무실, 캠퍼스, 야구장 등 각각의 환경에 적합한 정책을 정의하도록 지원합니다.

또한 최근 추가된 ClearPass의 향상된 기능으로 인해 IoT 도입으로 인해 새롭게 대두된 네트워크 보안 문제를 해결하고, 모바일 장치 및 앱 인증을 강화하고, 보안 사고에 대한 깊이 있는 가시성을 확보할 수 있게 되었습니다. 이에 더해 자동 위협 보호 및 지능형 서비스 기능 덕분에 최소한의 IT 개입으로도 각 장치에 네트워크 액세스 권한이 정확하게 부여됩니다.

aruba
a Hewlett Packard Enterprise company

1344 CROSSMAN AVE | SUNNYVALE, CA 94089
1.844.473.2782 | 전화: 1.408.227.4500 | 팩스: 1.408.227.4550 | INFO@ARUBANETWORKS.COM

www.arubanetworks.com