aruba
a Hewlett Packard Enterprise company

솔루션 오버뷰

제로 트러스트 보안을 갖춘 Aruba ESP

에지를 위한 보안

사용자의 탈중심화 현상이 증가하고, 더 정교하고 지속적인 공격이 등장함에 따라 네트워크 보안 과제는 지난 몇 년간 대폭 심화되었습니다. 네트워크의 경계에 주로 중점을 두는 종전의 보안 접근방식은 독립형 보안 전략으로서의 효용성이 없어지고 있습니다. 최신 네트워크 보안은 끊임없이 변화하는 다양한 사용자와 디바이스는 물론, 네트워크 인프라의 기존의 "신뢰할 수 있는" 부분을 표적화하는 훨씬 더 만연해진 위협을 다루어야 합니다.

제로 트러스트는 모든 사용자, 디바이스, 서버, 네트워크 세그먼트가 원래부터 안전하지 않고 잠재적으로 공격을 가할 수 있다고 가정함으로써, 현대 기업의 변화하는 보안 요구사항을 훨씬 더 잘 해결할 수 있는 효과적인 모델로 부상하고 있습니다. 제로 트러스트 보안을 갖춘 Aruba ESP는 기존의 신뢰할 수 있는 네트워크 리소스에 더욱 엄격한 보안 모범 사례 및 제어를 적용하여 전반적인 네트워크 보안 상태를 개선합니다.

ARUBA ESP: 제로 트러스트 핵심 원칙

제로 트러스트는 고려하는 보안 분야가 어디인지에 따라 크게 달라집니다. 애플리케이션 레벨 제어가 제로 트러스트의 중점이 되긴 했지만 종합적인 전략은 네트워크 보안 및 연결된 디바이스(재택 근무 환경 포함)의 수가 증가하는 문제를 다루어야 합니다. 제로 트러스트 보안을 갖춘 Aruba ESP는 종합적인 가시성, 마이크로 세분화 및 제어에 대한 액세스 최소화, 지속적인 모니터링 및 시행을 통합합니다. 캠퍼스 또는 지점 네트워크에 동일한 제어를 보장하고, 이를 재택 또는 원격 근무자에게도 확장하여 기존의 VPN 솔루션도 개선합니다.

IoT 시대에는 올바른 네트워크 보안의 기본 원칙을 구현하는 게 어려울 때가 많습니다. 가능한 경우, 모든 디바이스와 사용자를 식별하고 네트워크 액세스를 허용하기 전에 올바르게 인증해야 합니다. 인증 외에도, 사용자 및 디바이스가 네트워크에 있을 때에는 업무상 중요한 활동을 수행하는 데 필요한 최소한의 액세스 권한만 제공해야 합니다. 이는 지정된 사용자 또는 디바이스가 어떤 네트워크 리소스 및 애플리케이션에 액세스할 수 있는지 권한을 부여하는 것을 의미합니다. 마지막으로, 최종 사용자와 애플리케이션 간의 모든 통신을 암호화해야 합니다.

종합적인 가시성의 필요성

IoT 채택이 증가함에 따라 네트워크상의 모든 디바이스와 사용자에 대한 폭넓은 가시성을 갖기가 점점 더 어려워지고 있습니다. 가시성이 없으면 제로 트러스트 모델을 뒷받침하는 중요한 보안 제어를 적용하기가 어렵습니다. 자동화, AI 기반 머신 러닝, 디바이스 유형을 신속하게 식별할 수 있는 기능은 매우 중요합니다.

아루바 클리어패스 디바이스 인사이트(Aruba ClearPass Device Insight)는 능동 및 수동검색을 조합하고 프로파일링 기법을 사용하여 네트워크에 연결되어 있거나 연결을 시도하는 디바이스를 폭넓게 감지할 수 있습니다. 여기에는 노트북 및 태블릿 같은 일반적인 사용자 기반 디바이스도 포함됩니다. 이 솔루션이 기존 도구와 다른 점은 오늘날 네트워크에서 점점 더 보편화되고 있는 다양한 IoT 디바이스를 확인할 수 있는 기능입니다.

"액세스 최소화" 및 마이크로 세분화 채택

가시성이 자리 잡은 이후 매우 중요한 다음 단계는 "액세스 최소화" 및 마이크로 세분화와 관련된 제로 트러스트 모범 사례를 적용하는 것입니다. 이는 네트워크에 있는 각 엔드포인트에 최상의 인증 방법을 사용하고(예: 사용자 디바이스에 대한 완전 802.1X 및 다단계 인증), 해당 디바이스 또는 사용자에게 꼭 필요한 리소스에만 액세스 권한을 부여하는 액세스 제어 정책을 적용하는 것을 의미합니다.

아루바 클리어패스 폴리시 매니저(Aruba ClearPass Policy Manager)를 사용하면 IT 및 보안 팀이 지점 또는 캠퍼스의 유선/무선 인프라에 있는 모든 네트워크에 적용된 단일 역할 및 관련 액세스 권한을 사용하는 이러한 모범 사례를 최적화할 수 있는 역할 기반 액세스 정책을 생성할 수 있습니다. 프로파일링이 완료된 디바이스는 적절한 액세스 제어 정책이 자동으로 할당되고 아루바의 다이나믹 세그맨테이션(Dynamic Segmentation) 기능을 통해 다른 디바이스에서 세분화됩니다. 아루바 네트워크 인프라에 내장된 완전한 애플리케이션 방화벽인 아루바의 PEF(Policy Enforcement Firewall)에서 정책을 시행합니다. 아루바 인프라는 무선 네트워크 연결을 통한 WPA3 표준 같은 가장 안전한 암호화 프로토콜도 활용합니다.

ClearPass Policy Manager는 광범위한 인증 솔루션과도 통합되어 다단계 인증 및 네트워크 전체의 주요 포인트에서 재인증을 시행할 수 있는 기능을 사용하도록 지원합니다. 클리어패스(ClearPass) 에코시스템을 통해 고객은 컨텍스트 정보 및 기타 보안 텔레메트리와 관련된 제로 트러스트 요구사항을 충족하는 다른 솔루션과도 손쉽게 통합할 수 있습니다.

이는 ClearPass를 엔드포인트 보안 도구 같은 다양한 솔루션과 통합하여 디바이스의 상태를 기준으로 더욱 지능적인 액세스 제어 결정을 내릴 수 있음을 의미합니다. 액세스 제어 정책은 어떤 유형의 디바이스를 사용 중인지, 사용자가 어디에서 연결하고 있는지, 그리고 그 밖의 컨텍스트 기반 기준에 따라 변경할 수도 있습니다.

지속적인 모니터링 및 시행

세부적인 세분화를 시행할 수 있는 역할 기반 액세스 제어가 자리를 잡으면, 네트워크에 있는 사용자와 디바이스를 지속적으로 모니터링하는 것이 제로 트러스트의 또 다른 모범 사례를 구성하는 요소입니다. 이는 내부자 위협, 지능형 맬웨어 또는 기존의 경계 방어를 우회하는 지속적 위협과 관련된 위험을 해결합니다.

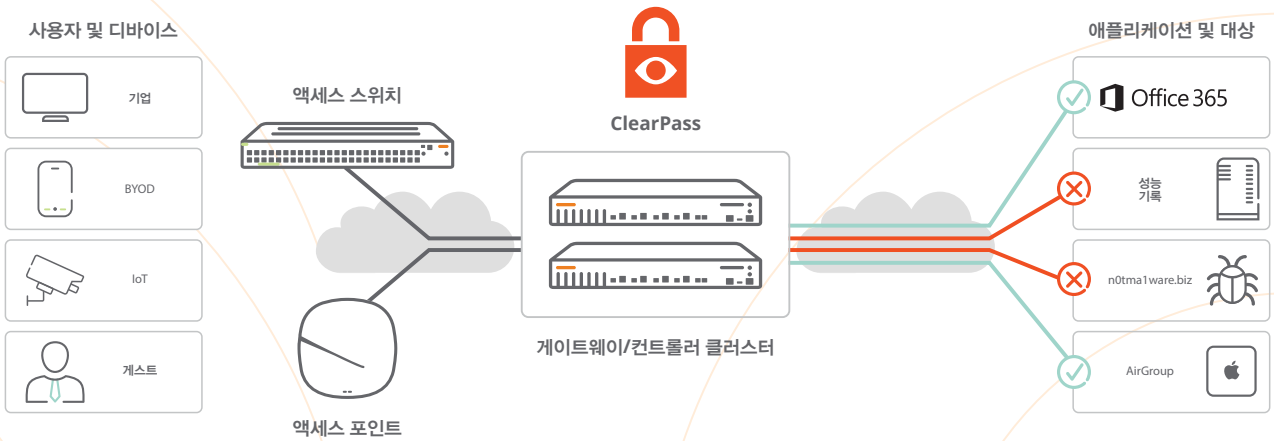

그림 1: Aruba ClearPass는 다이나믹 세그맨테이션을 사용하여 시행되는 역할 기반 액세스 제어 정책을 자동으로 할당함

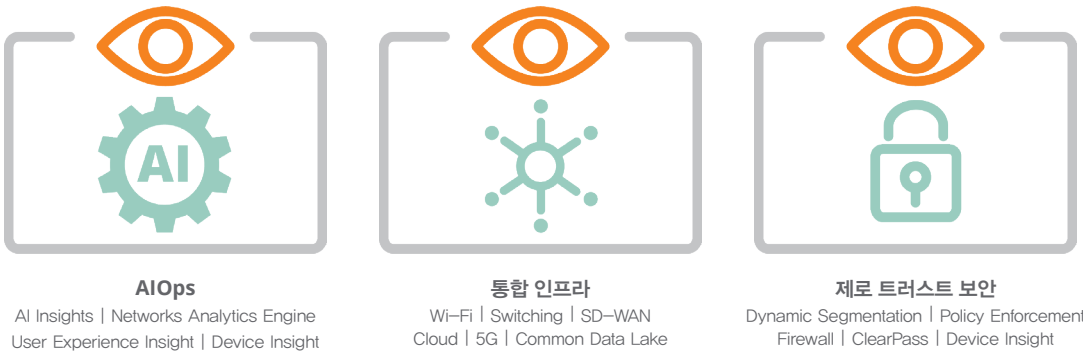

그림 2: 제로 트러스트 보안은 ESP의 주요 구성요소

IDS/IPS를 통한 위협 방어

아루바의 위협 방어 기능은 피싱, 서비스 공격(DoS), 점점 더 확산되는 랜섬웨어 공격을 비롯하여 다양한 위협으로부터 보호합니다. Aruba 9000 SD-WAN 게이트웨이는 Aruba Central, ClearPass Policy Manager, Policy Enforcement Firewall과 연동하여 역할 기반 침입 감지 및 방지(IDS/IPS)를 수행합니다. IDS 기반 IDS/IPS는 내장된 지점 네트워크 보안을 제공하기 위해 게이트웨이를 통과하는 SD-WAN (북-남) 트래픽뿐만 아니라 지점 LAN(동-서) 트래픽에 대해서도 서명 및 패턴 기반 트래픽 검사를 수행합니다. 아루바 센트럴(Aruba Central) 내의 고급 보안 대시보드는 IT 팀에 네트워크 전역에 대한 가시성, 다차원적인 위협 지표, 위협 인텔리전스 데이터, 상관관계 분석 및 사고 관리에 대한 정보를 제공합니다. 위협 이벤트가 해결을 위해 SIEM 시스템 및 ClearPass로 전송됩니다.

360 Security Exchange

보안 운영 및 대응(SOAR) 도구 집합이 포함된 동급 최고의 보안 솔루션으로 구성된 150개 이상의 통합이 포함된 ClearPass Policy Manager는 여러 소스에서 얻은 실시간 위협 텔레메트리를 기반으로 액세스를 동적으로 시행할 수 있습니다. 정책을 생성하여 차세대 방화벽(NGFW), 보안 정보 및 이벤트 관리(SIEM) 도구 및 그 밖의 다양한 소스에서 제공된 알림에 기반한 실시간 액세스 제어 결정을 내릴 수 있습니다. ClearPass 작업은 액세스를 제한(예: 인터넷 전용)하는 단계부터 시작하여 해결을 위해 네트워크에서 디바이스를 완전히 제거하는 단계까지 전체적으로 구성 가능합니다.

ARUBA ESP(에지 서비스 플랫폼)

고객이 에지의 기회를 활용할 수 있도록 지원하기 위해 당사는 에지를 통합, 자동화, 보호할 수 있도록 설계된 업계 최초의 AI 기반 플랫폼인 Aruba ESP를 개발했습니다. 제로 트러스트 보안은 Aruba ESP의 주요 구성요소이며 조직은 이를 AIOps 및 통합 인프라와 결합할 경우 비용을 절감하고, 운영을 간소화하고, 보안을 유지할 수 있습니다.

요약

오늘날의 네트워크 환경 및 위협 환경에는 다른 접근방식이 필요합니다. 과거의 경계 중심 네트워크 보안은 오늘날의 모바일 직원 또는 새로운 IoT 디바이스를 지원할 수 있도록 설계되지 않았습니다. 제로 트러스트 보안을 갖춘 Aruba ESP는 가시성, 제어, 시행을 다루는 종합적인 기능을 제공하여 탈중심화된 IT 기반 네트워크 인프라의 요구사항을 해결합니다.

SO_ZeroTrustSecurity_051120 a00097694enw