솔루션 개요

포괄적 가시성과 제어를 위한 제로 트러스트 액세스

종합 요약

제로 트러스트 액세스(ZTA) 솔루션은 네트워크의 거의 모든 부분에 존재합니다. 그러나 ZTA 제어에 단편적으로 접근해서는 보안에 공백이 생기고 관리하기가 부담스러울 뿐입니다.

포티넷 제로 트러스트 액세스(ZTA) 프레임워크는 긴밀히 통합된 보안 솔루션 제품군을 활용하여 기업에서 네트워크에 액세스하는 모든 사용자 및 기기를 식별, 분류하고, 내부 보안 정책을 준수하는지 평가하고, 이들을 제어 영역에 할당해 네트워크 안팎에서 지속해서 모니터링합니다.

포티넷 제로 트러스트 액세스 제어 프레임워크의 구성 요소

- FortiAuthenticator 사용자 ID 관리 서버
- FortiToken 2단계 인증 토큰
- FortiNAC 네트워크 액세스 제어
- FortiClient 고급 엔드포인트 원격 측정

서론

"제로 트러스트"는 최근 몇 년 사이에 화제가 되었고, 여러 기술 공급업체에서 도입했습니다. ZTA는 ZTA와 보안 중심 네트워크, 다이나믹 클라우드 보안, 인공 지능(AI) 기반 보안 관제를 결합한 전반적인 플랫폼 전략에서 중요한 요소입니다. 기업에서 ZTA의 제약에 따라 액세스를 허용할 경우, 사용자는 자신의 역할에 필요한 리소스에만 액세스할 수 있습니다. 또한, ZTA는 사용자보다 훨씬 많은 수를 차지하는 네트워크에 연결된 기기의 식별, 모니터링 및 제어를 규정합니다.

포티넷은 수십 년 동안 기업이 빠르게 확장되는 네트워크에 보안을 유지하도록 도운 경험을 살려, 매우 효과적인 ZTA 프레임워크를 제공합니다. 이 프레임워크는 3가지 영역(네트워크의 사용자, 네트워크의 기기, 해당 사용자와 기기의 오프라인 활동)에 대한 가시성과 제어 기능을 제공합니다.

효과적이고 실용적인 ID 및 액세스 관리

정상적인 네트워크 사용자와 악의적 행위자는 비즈니스의 성공을 돕느냐, 이를 위협하느냐의 차이만 있을 뿐, CISO에게는 둘 다 걱정거리입니다. 이와 같은 이유로 사용자 ID 관리는 포티넷 보안 패브릭의 주춧돌입니다. 기업에서는 ZTA 프레임워크의 ID 및 액세스 관리(IAM) 부분으로 완전한 사용자 가시성과 효과적인 액세스 정책을 제공할 수 있습니다.

- **FortiAuthenticator**는 인증, 권한 부여 및 계정 관리(AAA), 액세스 관리, SSO, 게스트 관리 서비스의 허브와 같은 역할을 합니다. 로그인, 인증서 및/또는 다단계 입력을 통해 사용자 ID를 설정합니다. FortiAuthenticator는 역할 기반 액세스 제어(RBAC) 서비스와 이러한 입력값을 공유하고 권한이 부여된 사용자와 특정 액세스 권한 및 서비스를 매칭합니다. 또한, FortiAuthenticator는 Security Assertion Markup Language(SAML) 구현을 지원하여 사용자가 서비스형 소프트웨어(SaaS) 솔루션(예: Salesforce, ADP, Microsoft 365)에 안전하게 액세스하도록 합니다.

- **FortiToken**은 하드웨어 토큰 또는 모바일 솔루션을 통해 FortiAuthenticator에 2단계 인증 서비스를 제공합니다. 이 모바일 솔루션은 OAuth를 준수하는 Android 및 iOS 기기용 일회성 비밀번호(OTP) 생성 애플리케이션이며, 시간 기반 토큰과 이벤트 기반 토큰을 모두 지원합니다. 이 공간을 차지하지 않는 솔루션을 사용하면 기업 전체로 다단계 권한 부여 구현을 확장할 수 있습니다.

기업에 포티넷 보안 패브릭이나 다른 보안 인프라가 설치되어 있을 경우, 사용자 ID 및 액세스 관리를 위한 포티넷 ZTA 솔루션이 포티넷 보안 패브릭에 안정적 보안을 제공합니다.

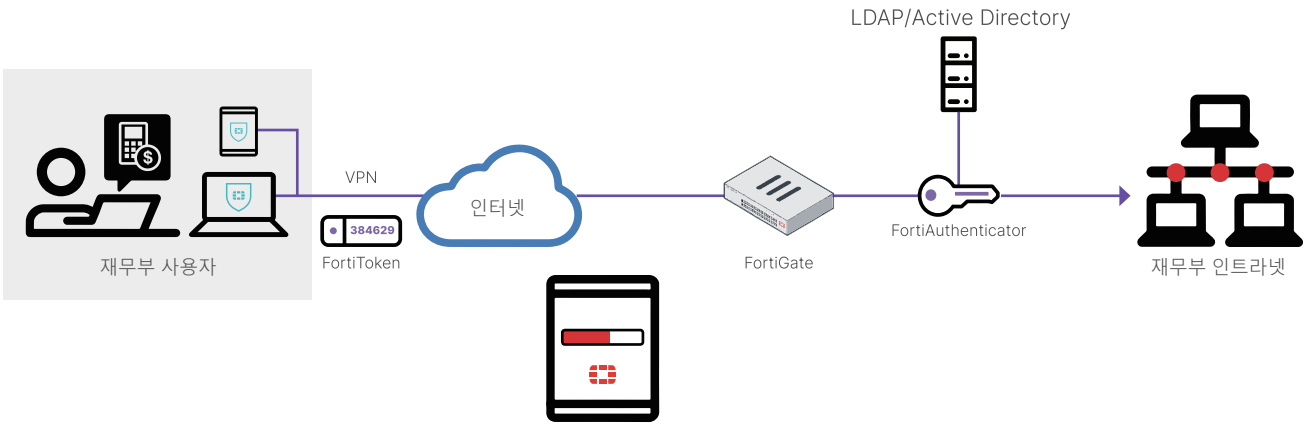

그림 1: 일반적 포티넷 ZTA 사용자 ID 및 액세스 관리 구현.

모든 사물의 보안

포티넷 ZTA 솔루션의 두 번째 목표는 네트워크에 있는 모든 기기의 연속적 가시성과 액세스 제어 기능을 관리하는 것입니다. 기업에서는 이 문제로 인해 상당한 난관을 겪고 있습니다. 네트워크 기기의 증가 속도가 네트워크 사용자의 증가 속도를 넘어섰고, 보안팀의 역량은 넘어선 지 오래입니다. 포티넷 ZTA 솔루션은 보안팀의 부담을 덜어주기 위해 자동화된 통합 탐색, 분류, 세그먼테이션 및 인시던트 대응을 제공합니다.

자동화된 발견 및 분류

FortiNAC 네트워크 액세스 제어 솔루션은 네트워크에 있거나 네트워크에 액세스하려는 모든 기기를 정확히 발견하고 식별합니다. 스캔을 통해 해킹된 기기가 없는지 확인하고, 역할과 기능에 따라 분류합니다. FortiNAC은 기존 에이전트로 기기 정보를 가져옵니다. 하지만 대부분 기업에서는 모든 위치에 에이전트를 설치하고 싶어 하지 않을 수 있고, 이 경우에는 FortiNAC가 먼저 네트워크와 통신하고 나서 나중에 기기를 식별합니다.

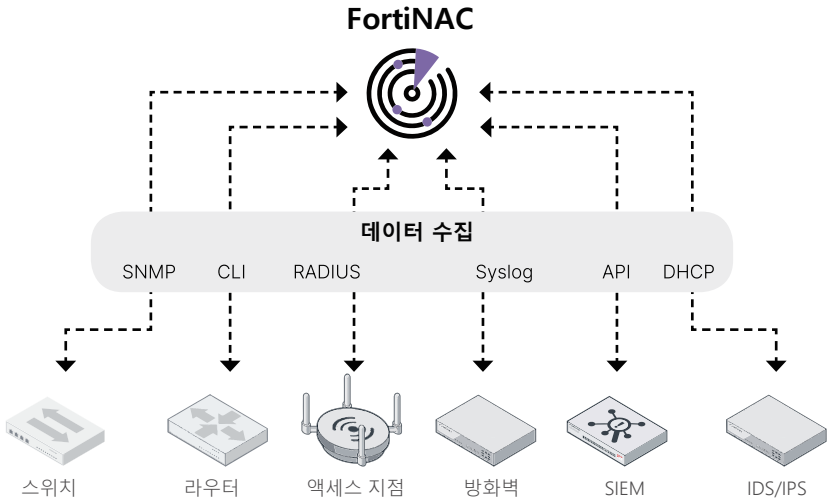

그림 2: 에이전트 없는 데이터 수집을 지원하는 FortiNAC는 네트워크에 있는 모든 것에 광범위한 가시성을 제공합니다.

제어 영역 할당

FortiNAC은 여러 공급업체가 있는 환경에 동적 네트워크 마이크로 세그먼테이션을 제공합니다. 공급업체 170개, 기기 2,400개 이상을 지원하며, 네트워크와 상호작용하여 기기를 적절한 네트워크 세그먼트에서 관리합니다.

또한, FortiNAC는 FortiGate NGFW와 통합되어 인텐트 기반 세그먼테이션을 지원합니다. 이는 비즈니스 목표에 기반한 세그먼테이션 전략입니다. 예를 들어, 일반 데이터 보호 규정(GDPR), 결제 카드 산업 데이터 보안 표준(PCI DSS) 거래 보호 등의 데이터 보호법을 준수하는 것이 해당합니다. 인텐트 기반 세그먼테이션을 구현하고 나면 보안팀이 규정 준수 제한에 따라 자산에 태그를 붙일 수 있습니다. FortiGate는 자산이 네트워크 어디로 이동하든 정책을 적용하여 규정 준수 이행에 들어가는 시간과 비용을 절감합니다. 기업에서는 인텐트 기반 세그먼테이션을 사용하여 네트워크 자체를 다시 구성하지 않고 비즈니스 구조 조정 시 내부 액세스 정책을 관리합니다.

연속적 모니터링

ZTA는 신뢰가 일시적이라고 가정합니다. 기기가 신뢰도를 인증받았더라도 나중에 감염될 수 있습니다. 또한, 기기가 실행하는 애플리케이션 보안이 침해될 수 있습니다. 네트워크에서 모든 기기에 대한 최신 신뢰 상태를 유지하기 위해 FortiNAC은 실시간 인시던트 대응과 더불어 지속적 모니터링을 제공합니다. FortiNAC은 비정상적인 동작을 탐지하면 다양한 대응 조치를 취합니다. 예를 들어, 기기를 격리 영역에 다시 할당하여 해킹된 기기가 위협이 침투하거나 데이터가 유출되는 중심지 역할을 하지 못하도록 하거나, 해당 사용자에 대한 복구 네트워크 세그먼트에 기기를 넣어 탐지된 문제를 해결합니다.

오프라인 안팎에서 자산 보호

노트북, 휴대전화와 같은 최종 사용자 기기의 경우, 포티넷은 FortiClient를 통해 네트워크 안팎으로 모두 ZTA 제어를 확장합니다.

원격 액세스 보안

FortiClient는 안전한 원격 액세스를 지원하기 위해 VPN 연결에 유연한 옵션을 제공합니다. SSL과 IPsec VPN도 모두 지원합니다. 분할 터널링 기능은 일반적 SSL 터널과 달리 회사 VPN 헤드엔드를 통해 트래픽이 통과하지 않고도 SSL VPN의 원격 사용자가 인터넷에 액세스하도록 지원합니다. 이를 통해 지원이 줄어들고 사용자 경험이 개선됩니다. 그와 동시에 FortiClient는 인터넷 기반 트랜잭션이 VPN 연결로 되돌아가 회사 네트워크를 위험에 빠트리지 않도록 보안 기능을 포함합니다.

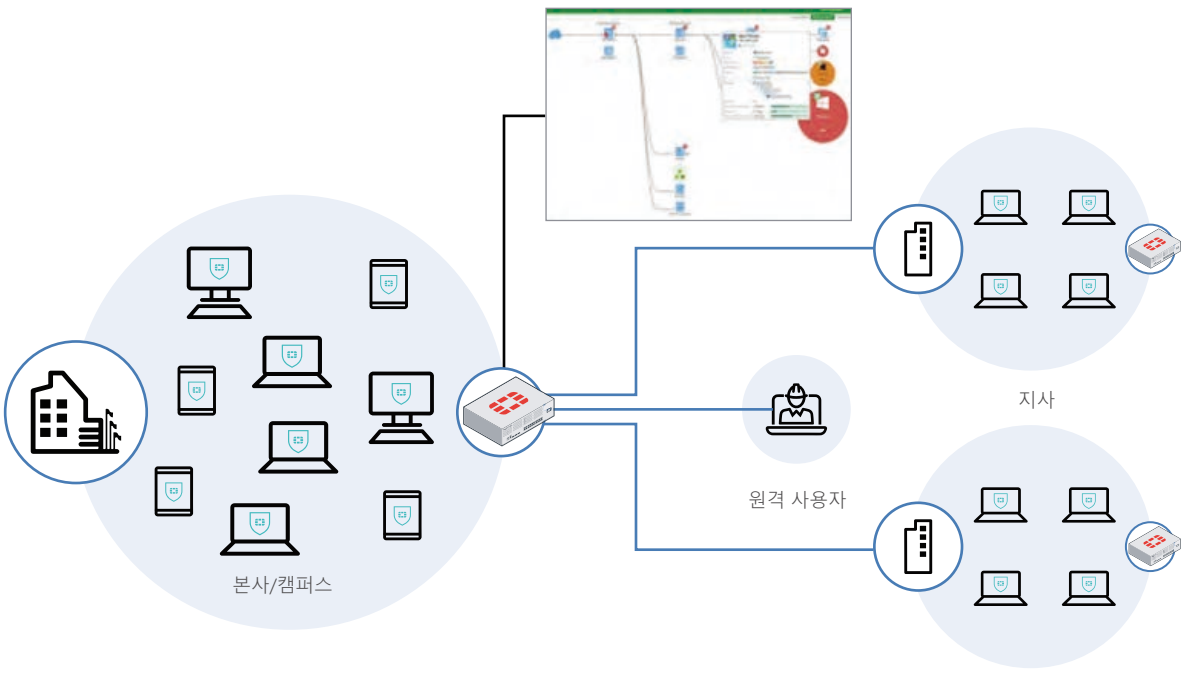

그림 3: FortiClient는 보안 패브릭을 통해 엔드포인트 가시성과 규정 준수를 지원합니다.
또한, 보안 패브릭과 엔드포인트 원격 측정을 공유하고, 통합 엔드포인트에 대한 인식을 강화합니다.

엔드포인트 가시성

최종 사용자 기기가 회사 네트워크에 다시 연결되면 FortiClient 패브릭 에이전트가 엔드포인트 보안 원격 측정 데이터(예: 기기 운영 체제(OS)와 애플리케이션, 알려진 취약성, 패치, 보안 상태)를 FortiGate NGFW 및 나머지 포티넷 보안 패브릭과 공유합니다. 이 데이터는 포티넷 ZTA 도구가 기기의 액세스 규칙을 개선하는 데 도움이 됩니다.

결론

네트워크를 봉쇄하는 것은 있을 수 없는 일이기 때문에 성공적으로 ZTA를 구현하기 위한 열쇠는 보안과 접근성의 균형을 찾는 것입니다. 포티넷 ZTA 솔루션을 사용하면 네트워크에 액세스하는 모든 기기와 사용자를 더욱 손쉽게 정확히 발견하고, 각각의 관련 보안 위험을 관리할 수 있습니다. 따라서 CISO는 네트워크 액세스를 확장하고 새로운 네트워크 연결 기술을 활용하는 디지털 혁신(DI) 이니셔티브를 더욱 효과적으로 지원할 수 있게 됩니다. 제로 트러스트는 그저 유행어나 논란거리에 그쳐서는 안 됩니다. 적절한 솔루션을 선택한다면 진정한 비즈니스 가치를 창출할 수 있습니다.

포티넷 ZTA 프레임워크의 주요 장점

- 네트워크 사용자에 대한 완전하고 연속적인 제어
- 네트워크에 연결된 기기에 대한 완전하고 연속적인 제어
- 유무선 네트워크에 똑같이 작동하는 포티넷 보안 패브릭용 통합 ZTA 솔루션
- 단일 공급업체에서 제공하는 완전한 통합 솔루션

서울특별시 강남구 영동대로 325 에스타워 14 /15층 **전화:** 080-559-8989 **Email:** kr-callcenter@fortinet.com

693461-B-0-KR