한눈에 보기

Cisco ISE(Identity Services Engine)

엔터프라이즈 네트워크는 더 이상 4면으로 둘러싸인 벽안에만 존재할 수 없습니다. 네트워크는 직원이 있는 곳 그리고 데이터가 이동하는 모든 곳으로 확대되고 있습니다. 오늘날의 직원들은 더 많은 장치에서 더 많은 비엔터프라이즈 네트워크를 통한 업무 리소스에 대한 액세스를 요구하고 있습니다. 모빌리티와 IoE(Internet of Everything)를 통해 삶의 방식과 작업 방식이 변화하고 있습니다. 수많은 보안 위협과 널리 알려진 데이터 보안 침해로 인해 나날이 진화하는 엔터프라이즈 네트워크에 대한 액세스 보안의 중요성이 그 어느 때보다 강조되고 있으므로, 기업에서는 새로운 네트워크 사용 디바이스의 확산을 지원해야 하는 과제에 직면해 있습니다.

현대의 네트워크 확대에 따라 리소스 보호, 개별 보안 솔루션 관리 및 위협 제어의 복잡성도 함께 증가하고 있습니다. IT 리소스가 이미 제한된 상태에서 IoE 연결이 보편화되는 것을 고려하면, 보안 위협을 식별하고 치료하지 못한 결과로 발생할 수 있는 영향의 범위가 커질 것이라는 것은 자명합니다.

진화하는 모바일 엔터프라이즈의 관리와 보안을 모두 유지하려면 다른 접근 방식이 필요합니다. 바로 Cisco® ISE(Identity Services Engine)가 그 해결책을 제시합니다.

위험 노출 범위 축소 및 위험 감소

가시성 및 제어를 바탕으로 위협에 한발 앞서 대처하십시오. 여기에는 네트워크에 액세스하는 사용자 및 디바이스에 대한 상세한 가시성을 확보하고 동적 제어를 통해 적절한 디바이스를 사용하는 올바른 사용자만 엔터프라이즈 서비스에 액세스할 수 있도록 하는 것이 포함됩니다.

이 재설계된 ISE 2.0을 사용하면 유무선 멀티벤더 네트워크와 원격 VPN 연결 전체에서 보안 액세스 제어를 일관되게 제공하는 작업이 간소화됩니다. 광범위한 지능형 센서와 프로파일링 기능을 통해 Cisco ISE는 네트워크에 심층적으로 연결하여 리소스에 액세스하는 대상에 대한 월등한 가시성을 제공합니다. 에코시스템 파트너 통합과 중요한 상황 데이터를 공유하고 소프트웨어 정의 세분화를 위한 Cisco TrustSec 정책을 구현하여 Cisco ISE에서는 네트워크를 단순한 데이터 전달자에서 보안 정책 시행자로 전환함으로써, 네트워크 위협을 감지하는 시간과 해결하는 시간을 단축시킵니다.

혜택

- **중앙 집중화 및 통합을 통한 고도로 안전한 액세스 제어**: 비즈니스 역할을 기반으로 고도로 안전한 액세스 제어를 중앙 집중화 및 통합하여 유무선 네트워크 또는 VPN을 통해 연결하는 최종 사용자에게 일관적인 네트워크 액세스 정책을 제공합니다.
- **가시성 개선 및 더 정확한 디바이스 식별**: Cisco® ISE(Identity Services Engine) 디바이스 프로파일링 및 디바이스 프로파일 피드 서비스를 통해 가시성을 개선하고 더 정확하게 디바이스를 식별하여 알 수 없는 엔드포인트 수를 감소시킵니다.
- **게스트 환경 간소화**: 완벽한 맞춤형 기능을 제공하는 브랜디드 모바일 및 데스크톱 게스트 포털을 통해 게스트 환경을 간소화하는 한편 게스트 온보딩 및 관리를 더욱 더 쉽게 합니다. 이러한 포털은 동적이고 시각적인 워크플로우를 통해 몇 분 안에 생성이 가능하며, 게스트 환경을 쉽게 관리할 수 있습니다.

- **BYOD 및 엔터프라이즈 모빌리티 가속화**: 간편한 아웃-오브-더-박스 설정, 셀프 서비스 디바이스 온보딩 및 관리, 내부 디바이스 인증서 관리 및 온프레미스/오프프레미스 디바이스 온보딩을 위한 통합 EMM(Enterprise Mobility Management) 파트너 소프트웨어 기능을 제공합니다.
- **네트워크 위협을 억제하는 소프트웨어 정의 세분화 정책 구성**: Cisco TrustSec® 기술을 사용하여 라우팅 및 스위치 레이어에서 역할 기반 액세스 제어를 시행합니다. 여러 VLAN을 복잡하게 추가하거나 네트워크를 재설계하지 않고도 액세스를 동적으로 분할할 수 있습니다.
- **상세한 상황별 데이터를 파트너 네트워크 및 보안 솔루션과 공유**: 데이터 공유를 통해 전반적인 효율성을 향상시키고 네트워크 위협의 TTD(Time to Detection) 및 TTR(Time to Resolution)을 가속화합니다.
- **자동으로 위협 억제**: ISE에서 치료, 관찰 또는 제거를 위해 감염된 엔드포인트를 억제할 수 있으므로, Cisco Firepower Management Center와 통합을 통해 자동으로 위협을 억제합니다.

ISE 2.0 업데이트 및 개선 사항은 다음과 같습니다.

- Cisco MSE(Mobility Services Engine)와의 통합을 통해 위치 데이터를 제공하여 위치별 액세스를 생성하고 적용할 수 있게 합니다. 예를 들어, 의료 전문가는 응급실의 환자 의료 기록에만 액세스할 수 있게 합니다.
- 고객이 기존 보안 솔루션을 사용하여 네트워크에서 위협을 식별하여 신속하게 억제하고 치료하기 위해 ISE와 작업할 수 있도록 특정 ISE 에코시스템 파트너의 개방형 아키텍처가 개선되었습니다.
- 더욱 광범위한 네트워크에서 엔드포인트의 규정을 준수하기 위해 ISE의 범위와 연결을 확장하도록 서드파티 네트워크 액세스 디바이스(NAD) 및 IPv6 엔드포인트를 지원합니다.
- TACACS+ 및 RADIUS 액세스 기능을 통한 간소화된 AAA(인증, 권한 부여 및 계정 관리) 디바이스 관리 등의 정책 관리를 간소화하여, 유선 네트워크의 보안 액세스 제어 정책을 훨씬 간편하게 배포합니다.
- Cisco AnyConnect 4.2에는 이전에 오프 프레미스 엔드포인트에서는 사용 불가능했던 애플리케이션 트래픽에 대한 상세 정보를 제공하는 새로운 NVM(Network Visibility Module)이 제공됩니다.

또한 ISE에서는 Cisco pxGrid(Platform Exchange Grid) 기술을 사용하여 풍부한 상황별 데이터를 통합 파트너 에코시스템 솔루션과 공유합니다. 이 기술은 확대된 네트워크 전체의 보안 위협을 신속하게 식별, 차단 및 치료할 수 있도록 합니다. 전체적으로는 보안 액세스 제어를 중앙 집중화하고 간소화하여 중요한 비즈니스 서비스를 안전하게 제공하고 인프라 보안을 개선하고 규정 준수를 시행하며 서비스 운영을 간소화할 수 있습니다.

최고의 보안 정보와 이벤트 관리(SIEM) 및 위협 방어(TD) 솔루션과 통합되었으며, 심층적인 네트워크 가시성과 보안 액세스 제어 기능을 제공하는 ISE는 Cisco Cyber Threat Defense, Network-as-a-Sensor 및 Network-as-an-Enforcer 솔루션의 중요한 역할을 수행합니다. 결과적으로 ISE에서는 기업에서 공격의 전 범위에 걸친 보안(공격 전의 네트워크 액세스 관리, 공격 중의 위협 가시성 확보 및 억제, 공격 후의 TTD(time-to-detection) 및 TTR(time-to-resolution) 개선)을 효과적으로 구현하는 데 필요한 가시성, 상황 및 동적 제어를 제공합니다.

다음 단계

Csco ISE에 대한 자세한 정보는 http://www.cisco.com/go/ise를 참조하거나 해당 지역의 고객 담당자에게 문의하십시오.

C45-654884-13 10/15