한눈에 보기

장점

- **중앙 집중화 및 통합을 통한 보다 안전한 액세스 제어**: 비즈니스 역할기반을 바탕으로 유무선 네트워크 또는 VPN으로 어떤 방법으로 접속하든 상관없이 최종 사용자에게 일관된 네트워크 액세스 정책을 제공합니다.
- **향상된 가시성 및 더 정확한 디바이스 식별**: Cisco ISE(Identity Services Engine) 디바이스 프로파일링과 디바이스 프로파일 피드 서비스를 통해 엔드포인트를 더 정확히 구별할 수 있습니다.
- **게스트 환경 간소화**: 완벽한 커스트마이제이션이 가능한 모바일 및 데스크톱 게스트 포털을 통해 더 편리한 온보딩과 관리가 가능합니다. 이러한 포털은 게스트 환경을 편리하게 관리할 수 있는 동적이고 직관적인 워크플로우를 통해 몇 분 안에 생성됩니다.

Cisco Identity Services Engine

변화하는 네트워크를 보호하고 관리하는 새로운 방법

엔터프라이즈 네트워크는 더이상 4면의 안전한 벽에 둘러 싸여있지 않습니다. 네트워크는 직원이 있는 곳 그리고 데이터가 이동하는 모든 곳으로 확대되고 있습니다. 오늘날의 직원들은 더 많은 디바이스에서 그리고 더 많은 엔터프라이즈 이외의 네트워크를 통해 업무 리소스에 액세스 하는 것을 요구하고 있습니다. 모빌리티, 디지털화, 사물 인터넷(IoT)으로 인해 삶의 방식과 업무 방식이 변화하고 있습니다. 기업에서 새로운 네트워크 기반 디바이스의 도입 시, 수많은 보안 위협과 널리 알려진 데이터 보안 침해 때문에 엔터프라이즈 네트워크에 대한 액세스 보안의 중요성이 그 어느 때보다 강조되고 있습니다.

현재의 네트워크 확장에 따른 리소스 보호, 서로 다른 보안 솔루션 관리 및 위협 제어의 복잡성도 함께 증가하고 있습니다. IT 리소스가 이미 제한된 상태에서 기업 소유가 아닌 디바이스의 연결이 보편화하는 것을 고려하면, 보안 위협을 식별하고 치료하지 못해 발생할 수 있는 영향의 범위가 매우 커질 것입니다.

진화하는 엔터프라이즈 네트워크의 관리뿐만 아니라 보안에도 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.

ISE 2.1은 유무선 멀티벤더 네트워크와 VPN 연결 전반에 일관되고 뛰어난 보안 액세스 제어를 더욱 단순화합니다. 광범위한 지능형 센서와 프로필 구축 기능을 통해 Cisco ISE는 네트워크 리소스에 액세스하는 대상에 대한 최고의 가시성을 제공합니다. 기술 파트너 통합과 중요한 상황 데이터를 공유하고 소프트웨어 정의 세그멘테이션를 위한 Cisco TrustSec® 정책을 구현하여 Cisco ISE에서는 네트워크를 단순한 데이터 전달 통로에서 보안 정책 시행 도구로 전환함으로써, 네트워크 위협을 탐지하고 해결하는 시간을 단축합니다.

- **BYOD(bring-your-own-device) 및 엔터프라이즈 모빌리티 가속화**: 간편한 아웃오브더박스(out-of-the-box) 설정, 셀프서비스 디바이스 온보딩 및 관리, 내부 디바이스 인증서 관리 및 온프레미스와 오프프레미스 모두의 디바이스 온보딩을 위한 통합된 EMM(Enterprise Mobility Management) 파트너 소프트웨어를 제공합니다.
- **네트워크 위협을 격리하는 소프트웨어 기반(SDN) 세그멘테이션 정책 구성:** Cisco TrustSec 기술을 사용하여 라우팅 및 스위치 레이어에서 역할 기반 액세스 제어를 시행합니다. 여러 개의 VLAN 사용으로 인한 복잡성이나 네트워크를 재설계하지 않고도 액세스를 동적으로 분할할 수 있습니다.
- **사용자와 디바이스 정보를 에코 파트너 및 보안 솔루션과 공유:** 전반적인 효율성을 향상하고 네트워크 위협을 제어하는 데 소요되는 시간을 단축합니다.
- **자동으로 위협 격리**: Cisco Firepower Management Center 및 다른 기술 파트너와의 통합을 통해 ISE에서 감염된 엔드포인트를 자동으로 격리합니다.

중요한 ISE 2.1 업데이트 및 개선 사항은 다음과 같습니다.

- **위협 대응형 NAC(Network Admission Control):** ISE에서는 이제 취약성 평가와 위협 인시던트 인젤리전스를 통합하여 네트워크 정책에 영향을 줄 수 있습니다. 또한 이를 통해 엔드포인트의 위협 점수가 변경될 경우 ISE가 네트워크 권한을 동적으로 변경할 수 있습니다.
- **Cisco TrustSec과 ACI(Application Centric Infrastructure) 정책 통합:** 이제 전사적으로 일관된 보안 정책을 적용하여 애플리케이션 상황 정보를 사용자 역할과 디바이스 유형과 함께 통합할 수 있습니다.
- **EasyConnect:** 엔드포인트가 802.1X를 지원하지 않을 경우 신속하고 쉽고 유연하게 사용자를 인증하는 방법입니다.
- **간소화된 가시성:** 간단하고 유연하면서 쉽게 사용할 수 있는 인터페이스를 통해 네트워크에 있는 사용자와 디바이스에 대해 즉시 사용 가능한 가시성을 확보합니다.

Cisco Rapid Threat Containment: Cisco Rapid Threat Containment는 이제 Cisco ISE 2.1과 Cisco Firepower™ Management Center 6.1의 통합을 지원하여 위협이 네트워크에 더 확산되기 전에 자동으로 위협을 동적으로 차단합니다.

또한 ISE에서는 Cisco pxGrid(Platform Exchange Grid) 기술을 사용하여 풍부한 상황 데이터를 통합된 기술 파트너 솔루션과 공유합니다. 이 기술을 통해 광범위한 네트워크 전체의 보안 위협을 신속하게 식별, 차단 그리고 치료할 수 있습니다. 전체적으로는 보안 액세스 제어를 중앙 집중화하고 간소화하여 중요한 비즈니스 서비스를 더욱 안전하게 제공하고, 인프라 보안을 개선하고, 컴플라이언스를 시행하며, 서비스 운영을 능률화할 수 있습니다.

최고의 SIEM(Security Information and Event Management) 및 위협 방어 솔루션과의 통합, 심층적인 네트워크 가시성, 그리고 보안 액세스 제어 기능을 통해 ISE는 Cisco Cyber Threat Defense, Network-as-a-Sensor 및 Network-as-an-Enforcer 솔루션의 중요한 역할을 합니다. 궁극적으로 ISE는 중앙에서 네트워크에 대한 모든 액세스를 제어하고, 사용자 및 디바이스 세부사항을 확인 및 공유하고, 위협을 차단 및 억제하고 공격의 전 범위를 대상으로 하는 보안을 효과적으로 구현할 수 있도록 합니다. 여기에는 공격이 발생하기 전에 네트워크 액세스를 관리하고, 공격 도중 위협에 대한 가시성을 제공하고, 공격 후 격리에 소요되는 시간을 개선하는 작업이 포함됩니다.

다음 단계

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

C45-654884-14 06/16