Cisco ISE(Identity Services Engine)

제품 개요

Cisco® ISE(Identity Services Engine)는 IT 전문가가 엔터프라이즈 모빌리티 과제를 해결하고 성장하는 네트워크를 전반적인 공격으로부터 보호하도록 지원합니다. Cisco ISE는 최고의 보안 정책 관리 플랫폼으로서 고도의 보안 액세스 제어를 통합하고 자동화하여 네트워크 및 네트워크 리소스에 대한 역할 기반 액세스를 실행합니다. 이 제품은 엔터프라이즈 모빌리티 환경을 간소화하는 탁월한 사용자 및 디바이스 가시성을 제공하며 Cisco pxGrid (Platform Exchange Grid) 기술을 사용하여 빠르게 위협을 식별, 차단, 교정 하도록 중요 상황 데이터를 통합 에코시스템 파트너 솔루션과 공유합니다.

모바일 엔터프라이즈에서의 보안

엔터프라이즈 네트워크는 더 이상 폐쇄적인 보안 장벽으로 보호할 수 없습니다. 오늘날 직원들은 개인용 노트북 컴퓨터, 태블릿 및 스마트폰을 포함한 다양한 미디어의 이용하여 홈 네트워크 및 모바일 네트워크에서 엔터프라이즈 리소스에 액세스하기를 원합니다. 특히 모빌리티로 인하여 네트워크가 엄청난 공격과 데이터 보안 침해에 노출될 수 있으며, 그 결과 조직에 큰 경제적 손실을 미칠 수 있습니다. 하지만 오늘날 모바일 직원들은 경쟁력을 유지하고 생산성을 높이기 위해 언제 어디서나 일할 수 있어야 합니다. 이러한 확장된 네트워크의 복잡성 증가와 "사물 인터넷(Internet of Things)"의 출현, 그리고 사설 및 공용 네트워크에 연결하는 모든 종류의 네트워크 지원 디바이스로 인해 네트워크 보안 위협 요소를 식별하고 대처하지 못할 때의 피해 가능성은 기하급수적으로 커지고 있습니다.

이와 동시에 IT 전문가는 더 빠듯한 예산으로 엔터프라이즈 모빌리티 이니셔티브를 지원하면서 정부, 산업 및 기타 규정준수 요건을 충족해야 합니다. 이러한 요건으로 인해 네트워크 액세스에 대한 명확한 가시성과 엄격한 액세스 제어가 필요해졌습니다. 위협이 발생할 때 이를 식별하거나 보안 침해나 공격이 발생한 후 포렌식 작업을 지원하는 데 중점을 두고, 기업 네트워크 전반에 보안 포인트 솔루션을 대량으로 분산하고 구축하고 있습니다. 감염된 디바이스 또는 사용자의 네트워크 액세스를 차단하는 데 중점을 두는 보안 솔루션은 일반적으로 매우 복잡하고 시간이 오래 걸리며 구축 비용이 높습니다. 네트워크가 성장하고 확장해 나갈 때 이렇게 서로 다른 포인트 솔루션은 네트워크의 성장에 맞춰 빠르게 확장할 수 없습니다. 성장하는 모바일 엔터프라이즈를 관리하고 보호하려면 다른 접근 방식이 필요합니다. 이를 위한 솔루션이 바로 Cisco ISE(Identity Services Engine)입니다.

기능 및 장점

Cisco ISE는 네트워크 액세스 보안에 대한 종합적인 접근 방식과 함께 다음과 같은 기능을 제공합니다.

- 모든 사용자 및 디바이스의 정확한 식별
- 모든 디바이스를 간편하게 온보딩 및 프로비저닝
- 누가, 언제 그리고 어떤 디바이스로 액세스하는지와 같은 사용자 액세스를 제어하는 중앙 집중형 상황 인식 정책 관리
- 연결된 사용자 및 디바이스에 관한 더 상세한 상황 데이터를 통해 위협 요소를 더 빠르게 식별, 차단 및 교정

표 1은 네트워크에서 Cisco ISE를 구축하여 운영할 때 고객이 얻는 이득입니다.

표 1. 고객 주요 혜택

Cisco ISE의 장점	
강력한 디바이스 분류 기능	**Cisco** ISE는 각 엔드포인트를 식별하는 업계 최초의 통합 디바이스 프로파일러를 제공합니다. 엔드포인트를 해당 사용자나 부서, 시간, 위치, 네트워크 등의 기타 속성에 연결하고, 네트워크에서 누가 무엇에 액세스할 수 있는지 IT가 정확하게 제어할 수 있도록 상황적 신원을 만듭니다. Cisco ISE는 자동화된 디바이스 피드 서비스가 적용되어 실시간으로 업데이트하기 때문에 새로운 디바이스가 출시되는 즉시 식별될 수 있도록 보장합니다.
광범위한 정책 적용	Cisco ISE를 통해 조직은 액세스 정책 규칙을 편리하고 유연하게 정의하여 끊임없이 변화하는 기업의 비즈니스 요건을 충족시킬 수 있습니다. 예를 들어, IT 관리자는 Cisco ISE에 게스트 사용자와 디바이스를 등록된 사용자 및 디바이스와 구분하는 정책을 정의할 수 있습니다. 이를 통해 게스트 사용자에게는 전체 네트워크에 대한 제한된 액세스를 제공하고 등록된 사용자에게는 해당 정책에 지정된 액세스를 제공할 수 있습니다. 또한 Cisco ISE의 정책에서는 등록된 사용자가 소유한 신뢰할 수 있는 디바이스 또는 컴플라이언트 디바이스에만 네트워크 액세스를 허용할 수 있습니다. Cisco ISE에서 사용자 또는 디바이스의 상황적 신원을 기반으로 네트워크 진입점에 고도의 보안 액세스 규칙을 전송하므로 IT에서는 위치에 관계 없이 사용자나 디바이스가 네트워크 액세스를 시도하면 일관되게 정책을 적용할 수 있습니다.
게스트 환경 능률화	Cisco ISE에서는 게스트 관리 및 온보딩 기능을 즉시 사용할 수 있습니다. 관리자는 게스트가 경험하게 될 포털 화면과 단계를 실시간 미리보기 할 수 있는 동적인 시각 툴을 사용하여 게스트 포털을 몇 분만에 맞춤화할 수 있습니다. 이 툴을 통해 관리자는 설정 변경이 사용자에게 미칠 영향을 정확하게 볼 수 있습니다. Cisco ISE는 광고, 배너, 테마, 브랜딩 등 완벽한 게스트 페이지 맞춤화 기능, 게스트 계정과 만료 관리 기능, 게스트 계정 및 네트워크 활동에 대한 철저한 감사 기능을 제공합니다. Cisco ISE에서는 핫스팟부터 SMS 확인을 사용한 직원 추천 게스트 액세스까지, 가능한 모든 유형의 게스트 워크플로우가 지원되므로 게스트 액세스가 용이합니다.
셀프 서비스 디바이스 온보딩	Cisco ISE를 사용하면 IT 직원은 엔터프라이즈의 BYOD(Bring-Your-Own-Device) 또는 게스트 정책을 구현하는 방법을 유연하게 결정할 수 있습니다. Cisco ISE는 IT에서 정의한 비즈니스 정책에 따라 사용자가 새 디바이스를 등록하고 프로비저닝할 수 있는 셀프 서비스 등록 포털을 제공합니다. 이를 통해 IT는 보안 정책 준수에 필요한 디바이스 프로비저닝, 프로파일링 및 보고를 자동화할 수 있으며 직원은 IT의 지원 없이 자신의 디바이스를 네트워크에 간편하게 연결할 수 있습니다.
보안 컴플라이언스	단일 관리 콘솔을 통해 회사 네트워크 전체에서 정책 생성, 가시성 및 보고가 간소화됩니다. 따라서 감사, 규제 요건 및 IEEE 802.1X 표준에 대한 연방 정부 법규 가이드라인의 준수 여부를 편리하게 확인할 수 있습니다.
자동화된 디바이스 컴플라이언스 점검	Cisco ISE는 Cisco AnyConnect® 4.0 Unified Agent를 사용하여 디바이스 보안 상태 점검 및 교정 옵션을 제공합니다. 이와 함께 데스크톱과 노트북 컴퓨터 점검을 위한 고급 VPN 서비스는 물론 업계 모바일 기기에 최고의 EMM(Enterprise mobility management) 솔루션과의 통합도 제공합니다. 이 기능을 사용하면 사용자 디바이스의 보안 및 정책 준수를 보장할 수 있습니다.
어디서나 안전하게 액세스	Cisco ISE는 네트워크 액세스 디바이스에 실시간으로 정책을 적용하므로, 모바일 또는 원격 사용자는 유선 및 무선 연결 모두에서 일관되게 서비스에 액세스할 수 있습니다.
운영 효율성	온보딩 및 보안 자동화, 중앙 정책 제어, 가시성, 문제 해결, Cisco Prime™ 솔루션과 통합 등의 기능이 제공되므로 IT와 헬프 데스크에서는 사용자 및 네트워크 보안 수정에 소요되는 시간을 크게 줄일 수 있습니다.
내장된 실행 기능	대부분의 Cisco 스위치 및 무선 컨트롤러에는 디바이스 감지 기능이 내장되어 있어서 오버레이 어플라이언스 또는 인프라 교체 비용 및 관리 없이 진입점에서 네트워크 전체로 프로파일링을 확장할 수 있습니다.
Cisco TrustSec® 정책 네트워킹을 사용하여 액세스에서 데이터 센터로 정책 확장	Cisco ISE는 네트워크 보안의 복잡성을 해결하기 위한 정책 정의 네트워크 세그먼테이션을 제공하는 고유한 Cisco TrustSec 네트워크 기술의 정책 관리 지점입니다. Cisco TrustSec 기술을 통해 고객은 여러 VLAN을 관리하거나 네트워크 아키텍처를 변경하는 대신 역할 기반 액세스 정책을 사용하여 네트워크를 비즈니스 규칙에 따라 논리적 및 동적으로 분할함으로써, 지속적으로 변화하는 확장된 네트워크 전체에서 매우 안전한 액세스를 간편하게 구현할 수 있습니다.
멀티 벤더 인프라 지원	Cisco ISE는 RADIUS 및 IEEE 802.1X 표준을 준수하는 멀티 벤더 인프라(예를 들어, 스위치 및 무선 액세스 포인트)와 상호 운용됩니다. Cisco 및 Cisco의 파트너는 모범 사례 가이드라인은 물론 상세한 실제 설계 가이드라인을 제공합니다. 기업 고객은 Cisco TrustSec 기술과 함께 Cisco에서 설계한 네트워크 인프라가 적용된 Cisco ISE를 사용하여 네트워크에서 더 뛰어난 인텔리전스와 향상된 가시성을 얻을 수 있습니다.
Cisco pxGrid 상황 공유	Cisco ISE는 네트워크 전체에서 동적 상황 데이터를 수집하며 강력한 상황 공유 플랫폼인 Cisco pxGrid 기술을 사용하여, 연결된 사용자 및 디바이스에 대한 좀 더 심층적인 상황 데이터를 외부 및 내부 에코시스템 파트너 솔루션과 공유합니다. 단일 API를 사용하여 Cisco ISE 네트워크 및 보안 파트너는 자체 네트워크 액세스 기능을 개선하고 네트워크 위협을 식별, 차단 및 교정하는 솔루션 기능을 촉진하기 위해 이 데이터를 사용합니다.

Cisco ISE의 장점	
광범위한 통합 파트너 에코시스템	Cisco ISE는 최대의 파트너 에코시스템을 자랑합니다. 파트너는 Cisco pxGrid를 사용하여 엔드포인트 취약점 교정, 네트워크 포렌식 및 웹 SSO(Single Sign On)를 개선합니다. EMM, SIEM(Security information and event management, 보안 정보 및 이벤트 관리) 및 TD(Threat defense, 위협 방어)의 통합 기술 파트너는 단독으로 해결할 수 있는 것보다 훨씬 많은 사용 사례를 해결하고, 그 결과 자신의 업무를 더 효과적으로 수행하기 위해 Cisco ISE에서 제공하는 심층적 상황적 신원 인식 기능을 활용합니다. Cisco ISE가 있다면, 파트너 플랫폼에서 Cisco 네트워크 인프라에 깊숙이 도달하여 사용자 및 디바이스에 네트워크 작업을 구현할 수 있습니다(예를 들어, 스마트폰 또는 노트북 컴퓨터 격리 및 네트워크 액세스 차단).

Cisco ISE는 포괄적 정책 관리, 디바이스 온보딩 능률화, 파트너 네트워크 솔루션과 공유할 수 있는 풍부한 상황 데이터, 그리고 엄격히 보안된 유선, 무선, VPN 액세스를 보장하기 위한 동적 실행 등을 제공하여 조직의 역량을 강화합니다. Cisco ISE의 기능과 장점은 표 2에 나와 있습니다.

표 2. 기능 및 장점

기능	장점
비즈니스 정책 적용	비즈니스와 관련된 유연한 액세스 제어 정책을 만들기 위해 규칙 기반 속성 중심의 정책 모델을 제공합니다. 사용자 및 엔드포인트 신원, 보안 상태 검증, 인증 프로토콜, 프로파일링 신원이나 기타 외부 속성 소스의 정보가 포함된 미리 정의된 사전에서 속성을 가져와 세밀한 정책을 생성할 수 있습니다. 또한 특성은 역동적인 방식으로 생성해 저장해 두었다가 나중에 사용하는 것도 가능합니다. Active Directory LDAP, RADIUS, RSA OTP 및 인증과 권한 부여를 위한 인증 기관과 같은 여러 외부 신원 저장소와 통합할 수 있습니다.
액세스 제어	dACL(downloadable access control lists), VLAN 할당, URL 리디렉션, 명명된 ACL, Cisco의 TrustSec 기술 지원 네트워크 디바이스의 고급 기능을 사용한 SGT(security group tags)를 포함한 광범위한 액세스 제어 옵션을 제공합니다.
게스트 액세스 기간 관리	게스트 네트워크 액세스를 활성화하고 사용자 지정하기 위한 완전히 새로운 간소화된 환경을 제공합니다. ISE에서 기본적으로 제공하는 핫스팟 워크플로우, 후원 워크플로우, 셀프 서비스 워크플로우 및 기타 다양한 액세스 워크플로우를 통해 광고 및 프로모션이 포함된 회사 브랜드의 게스트 환경을 몇 분 만에 간편하게 만들 수 있습니다. 새 게스트 관리 작업 센터는 디자인의 효과를 실제로 볼 수 있는 실시간의 시각적 흐름을 제공합니다. 시간 제한, 계정 만료, SMS 확인을 통해 추가적인 보안 제어가 가능하며, 완전한 게스트 감사를 통해 보안 및 규정준수 요구에 따라 네트워크 전체에서 액세스를 추적할 수 있습니다.
간소화된 디바이스 온보딩	테마가 있는 완전히 사용자 지정 가능하고 브랜드화된 사용자 환경을 제공합니다. 사용자에게 온보딩 프로세스를 안내하며 최종 사용자에게 셀프 서비스 포털을 제공하여 디바이스를 직접 추가 및 관리할 수 있도록 하는 아웃-오브-더-박스 워크플로우를 제공합니다. 표준 PC 및 모바일 컴퓨팅 플랫폼에 대한 자동 요청 프로비저닝 및 인증서 등록을 제공합니다. 디바이스 온보딩이 간소화되어 IT 헬프 데스크의 사례가 감소하며, 사용자에게는 더 쉽고 더 투명한 환경과 더욱 안전한 액세스가 제공됩니다.
AAA 프로토콜	AAA(Authentication, Authorization & Accounting) 목적으로 표준 RADIUS 프로토콜을 사용합니다. PAP, MS-CHAP, EAP(Extensible Authentication Protocol)-MD5, PEAP(Protected EAP), EAP-FAST(Flexible Authentication via Secure Tunneling), EAP-TLS(Transport Layer Security)를 비롯한(이에 제한되지 않음) 다양한 인증 프로토콜을 지원합니다. Cisco ISE는 시스템 및 사용자 자격 증명의 EAP 연결을 지원하는 유일한 RADIUS 서버입니다.
내부 인증 기관	Cisco ISE 내에서 구축하기 쉬운 내부 인증 기관을 제공하므로 조직에서는 복잡하게 외부 인증 기관에 신청할 필요가 없으며 개인 디바이스의 인증서를 간편하게 관리할 수 있습니다. Cisco ISE에는 표준 기반 OCSP(Online Certificate Status Protocol)를 통해 인증서 상태를 확인하는 기능을 이용하여 엔드포인트 및 인증서를 관리하고 디바이스 도난 시 자동 인증서 해지를 제공하는 단일 콘솔이 포함되어 있습니다. 내부 인증 기관은 독립형 구축 및 하위 구축(즉, 기존 엔터프라이즈 PKI 사용)을 지원합니다.
디바이스 프로파일링	IP 전화, 프린터 IP 카메라, 스마트폰, 태블릿 등의 다양한 엔드포인트 유형을 위한 사전 정의된 디바이스 템플릿이 제품과 함께 제공됩니다. 또한 관리자는 자체 디바이스 템플릿을 생성할 수도 있습니다. 이 같은 여러 템플릿을 사용해 엔드포인트가 네트워크에 연결되면 이를 자동 감지, 분류한 후 관리자가 정의한 ID와 연결할 수 있습니다. 또한 관리자는 디바이스 유형에 따라 엔드포인트별 권한 부여 정책을 연결할 수 있습니다. Cisco ISE는 수동적 네트워크 모니터링과 원격 측정, 실제 엔드포인트 쿼리를 통해 또는 Cisco 인프라에서 Cisco Catalyst® 스위치의 디바이스 센서를 이용하여 엔드포인트 특성 데이터를 수집합니다. Cisco Catalyst 스위치의 인프라 중심 엔드포인트 감지 기능은 Cisco ISE 감지 기술의 하위 집합입니다. 이 기능을 통해 스위치에서 엔드포인트 특성 정보를 빠르게 수집한 다음 표준 RADIUS를 사용해 Cisco ISE에 전달하여 엔드포인트 분류 및 정책 기반 적용에 이용할 수 있습니다. 이러한 스위치 기반 감지 기능을 활용하면 엔드포인트 정보를 효율적인 분산 방식으로 수집하여 확장성과 구축 용이성을 높이고 분류 시간을 단축할 수 있습니다.

기능	장점
디바이스 프로필 피드 서비스	Cisco ISE에서 사용할 수 있는 업계 최초의 디바이스 프로필 피드 서비스는 여러 공급 업체의 다양한 IP 지원 디바이스에 대한 Cisco의 검증된 디바이스 프로필을 자동으로 업데이트함으로써 아웃-오브-더-박스 프로파일링 기술을 지원합니다. 피드 서비스에서는 또한 파트너와 고객이 직접 사용자 지정한 프로필 정보를 공유하면 Cisco에서 이를 검사 및 재구축하는 메커니즘도 제공합니다. 이제 기업은 이 자동 업데이트를 통해 사용자가 최신 디바이스를 사용하여 네트워크에 연결을 시도할 때 이러한 모든 디바이스를 감지할 수 있습니다. 이를 통해 매주 쏟아져 나오는 다수의 새로운 디바이스를 처리하는 작업이 간소화되며 IT 관리자의 지원 업무가 크게 줄어듭니다.
엔드포인트 상태	네트워크에 연결하는 PC 및 모바일 기기에 대한 엔드포인트 상태 평가를 확인합니다. 지속적인 클라이언트 기반 에이전트 또는 일시적인 웹 에이전트를 통해 특정 엔드포인트가 회사의 상태 정책과 부합되는지 여부를 검증합니다. 최신 OS 패치, 최신 정의 파일 변수(버전, 날짜 등)를 갖는 안티바이러스 및 안티스파이웨어 소프트웨어 패키지, 레지스트리(키, 값 등) 및 애플리케이션에 대한 확인 작업을 포함하는(이에 제한되지 않음) 강력한 정책 설정 기능을 제공합니다. 또한 Cisco ISE는 엔드포인트가 회사 정책을 위반하지 않도록 PC 클라이언트의 자동 교정 및 정기 평가 시행을 지원합니다.
Cisco pxGrid 및 ISE 에코시스템	Cisco pxGrid는 네트워크 전체에서 이러한 솔루션의 기능을 가속화하기 위해 Cisco ISE가 수집한 심층적인 상황 데이터를 외부 및 내부 에코시스템 파트너 솔루션에 제공하는 Cisco ISE 내의 강력한 상황 공유 플랫폼입니다. 엔드포인트 취약점 평가에서 웹 SSO(Single Sign On)까지, 간단한 통합 프레임워크의 장점을 활용하는 Cisco ISE 에코시스템 파트너의 목록은 계속 확장되고 있습니다.
ISE 에코시스템: EMM 통합	Cisco ISE는 EMM 통합을 통해 Cisco EMM 기술 파트너 솔루션과 연결하여, 네트워크에 연결을 시도하는 모바일 기기가 EMM 플랫폼에 사전 등록되어 있는지와 엔터프라이즈 정책을 준수하는지 확인할 수 있습니다. 또한 사용자가 자신의 디바이스 문제를 해결하도록 지원할 수 있습니다. 규정준수 검사에는 디바이스 암호, PIN 잠금 및 탈옥 상태 검사 등이 포함됩니다.
ISE 에코시스템: SIEM 및 TD	SIEM 및 TD 파트너는 Cisco ISE와의 통합을 통해 사용자 및 디바이스 신원, 네트워크 인증 수준, 보안 상태에 대한 Cisco ISE의 상황 정보로 자사의 네트워크 전체 보안 이벤트 가시성을 보완할 수 있습니다. 따라서 네트워크에서 유해한 디바이스를 차단하는 작업이, 몇 개월이 걸리는 포렌식 이벤트에서 관리자 패널 내에서 보안 조치를 직접 취할 수 있는 실시간 가시성으로 변경됩니다.
ISE 에코시스템: 제어/SCADA 운영 및 보안 정책 통합	제어 및 SCADA(감시 제어 및 데이터 획득) 네트워크 디바이스의 액세스 및 관리를 매우 안전하게 수행할 수 있습니다. Cisco ISE는 제어 및 SCADA 정책 관리자를 위한 상황와 제어를 제공하므로, 침해 발생 시 디바이스의 문제 개선 및 격리가 더 빨라질 뿐만 아니라 악성 디바이스의 식별도 더 용이해집니다.
ISE 에코시스템: 네트워크 문제 해결 및 포렌식 간소화	패킷 캡처 시스템에서는 Cisco ISE에서 수집한 상황 데이터를 이용하여 사용자, 디바이스 및 사용자 역할을 캡처된 패킷 데이터에 연결할 수 있습니다. 패킷 캡처는 위협과 네트워크 문제 조사에서 매우 중요한 경우가 많으므로, 상황 데이터를 패킷 캡처에 연결하면 네트워크 문제 해결이 간소화되고 포렌식 조사가 가속화됩니다.
ISE 에코시스템: 엔드포인트 취약점 개선 통합	네트워크 취약점 보고서에서 우선 순위를 지정할 대상과 그 방법을 파악하는 것은 매우 어렵습니다. Cisco ISE의 상황 데이터를 취약점 보고와 공유하면 조사에 필요한 엔드포인트 취약점을 더 효과적으로 식별하고 우선 순위를 지정할 수 있으며 사용자가 신속하게 해결 조치를 취하는 데에도 도움이 됩니다.
ISE 에코시스템: 위험 기반의 적응형 인증 및 SSO(Single Sign On)	상황 중심의 사용자 인증 및 웹 애플리케이션 인증을 사용할 수 있습니다. 페더레이션된 신원, 인증 위험 요소 및 Cisco ISE가 제공하는 상황 데이터를 조합하여 생성된 세밀한 정책만을 기반으로 인증 과제를 줄일 수 있고 심지어 제거할 수도 있습니다. 직원이 비즈니스 자산에 액세스할 때 사용하는 모바일 기기의 확산으로 인해, 보안에 핵심적인 사용자 인증이 번거로워졌습니다. 이러한 통합 덕분에, 반복적인 로그인 없이도 비즈니스 자산에 대해 사용자를 투명하게 인증할 수 있으며 이와 동시에 위험 수준을 기반으로 클라우드 자산 액세스를 차단할 수도 있습니다.
광범위한 다중 포레스트 Active Directory 지원	다중 포레스트 Microsoft Active Directory(AD) 도메인에 대한 포괄적인 인증 및 권한 부여를 제공합니다. 여러 개의 분리된 도메인을 논리적 그룹으로 묶어 복잡한 AD 토폴로지의 구성을 간소화함으로써 끊임없이 변화하는 비즈니스 환경을 지원할 수 있습니다. 또한 원활한 전환과 통합이 가능한 유연한 신원 재작성 규칙도 지원합니다. Microsoft AD 2003, 2008, 2008R2, 2012, 2012R2를 지원합니다.
엔드포인트 보호 서비스	네트워크 내에 위험 요소를 가진 엔드포인트가 있는 경우 관리자가 신속하게 시정 조치(검역 격리, 검역 격리 해제 또는 셧다운)를 취할 수 있습니다. 이를 통해 네트워크 내 위험을 줄이고 보안을 강화할 수 있습니다.
중앙 집중식 관리	관리자가 프로파일러, 상태, 게스트, 인증 및 권한 부여 서비스를 단일 웹 기반 GUI 콘솔에서 중앙 집중식으로 구성하고 관리할 수 있게 하며 단일 창 방식에서 통합된 관리 서비스를 제공함으로써 관리를 대폭 간소화합니다.
모니터링 및 문제 해결	모니터링, 리포팅 및 문제 해결용 내장 웹 콘솔이 사용되기 때문에 헬프 데스크 및 네트워크 운영자들이 신속하게 문제를 파악하고 해결하는 데 도움이 됩니다. 모든 서비스에 대한 강력한 이력 및 실시간 보고, 모든 활동 기록, 네트워크에 연결되어 있는 모든 사용자 및 엔드포인트에 대한 실시간 대시보드 메트릭 기능을 갖추고 있습니다.
플랫폼 선택 사항	물리적 또는 가상 어플라이언스 형태 중에서 선택 가능합니다. 2가지 물리적 플랫폼과 VMware ESX 또는 ESXi 기반 어플라이언스가 있습니다. 물리적 및 가상 폼 팩터를 사용하여 대규모 조직을 위한 Cisco ISE 클러스터를 만들 수 있으며, 중요 엔터프라이즈 비즈니스 시스템에 필요한 규모, 이중화 및 장애 조치를 제공할 수 있습니다.

제품 사양

Cisco ISE를 위한 두 가지 하드웨어 옵션은 표 3에 나와 있습니다.

표 3. Cisco ISE 하드웨어 사양

	Cisco Secure Network Server 3415(소)	Cisco Secure Network Server 3495(대)
프로세서	Intel® Xeon® 쿼드 코어 2.4GHz E5-2609 1개	Intel Xeon 쿼드 코어 2.4GHz E5-2609 2개
메모리	16GB	32GB
하드 디스크	600GB 6Gb SAS 10K RPM 1개	600GB 6Gb SAS 10K RPM 2개
RAID	아니요	예(RAID 1)
CD/DVD-ROM 드라이브	아니요	아니요
네트워크 연결		
이더넷 NIC	통합 기가비트 NIC 4개	통합 기가비트 NIC 4개
10/100/1000BASE-TX 케이블 지원	최대 100m(328피트)의 카테고리 5 UTP	최대 100m(328피트)의 카테고리 5 UTP
SSL(Secure Sockets Layer) Accelerator 카드	없음	Cavium CN1620-400-NHB-G
인터페이스		
전면 패널 커넥터	KVM 콘솔 커넥터 1개(USB 2개, VGA 1개 및 직렬 커넥터 1개 제공)	KVM 콘솔 커넥터 1개(USB 2개, VGA 1개 및 직렬 커넥터 1개 제공)
추가 후면 커넥터	VGA 동영상 포트 1개, USB 2.0 포트 2개, RJ45 시리얼 포트 1개, 기가비트 이더넷 관리 포트 1개, 듀얼 1 Gb 이더넷 포트.	VGA 동영상 포트 1개, USB 2.0 포트 2개, RJ45 시리얼 포트 1개, 기가비트 이더넷 관리 포트 1개, 듀얼 1 Gb 이더넷 포트.
시스템 유닛		
폼 팩터	랙 마운트 1 랙 유닛(1RU)	랙 마운트 1 RU
무게	16.2kg (35.6파운드) 12.1kg (26.8파운드)	15.87kg (35파운드) 완전 구성 시
크기(H x W x L)	1.7 x 16.9 x 28.5인치 (4.32 x 43 x 72.4 cm)	1.7 x 16.9 x 28.5인치 (4.32 x 43 x 72.4 cm)
전원 공급 장치	650W	이중 650W(이중화)
냉각 팬	5	5
온도: 작동	32 - 104°F(0 - 40°C)(작동, 해수면, 팬 고장(fan fail) 없음, CPU 속도 제한 터보 모드 없음)	32 - 104°F(0 - 40°C)(작동, 해수면, 팬 고장(fan fail) 없음, CPU 속도 제한 터보 모드 없음)
온도: 비작동	-40 ~ 70°C(-40 ~ 158°F)	-40 ~ 70°C(-40 ~ 158°F)

플랫폼 지원 및 호환성

Cisco ISE 가상 어플라이언스는 VMware ESX/ESXi 4.x 및 5.x에서 지원되며 표 3에 나와 있는 물리적 플랫폼의 구성과 동일한 하드웨어 또는 그 이상의 하드웨어에서 구동해야 합니다. Cisco ISE에는 최소 메모리 4GB와 하드웨어 드라이브 공간 200GB를 사용할 수 있는 가상 타겟이 필요합니다.

상태 평가 시스템 요구 사항

상태 평가에 사용되는 Cisco AnyConnect 4.0 에이전트의 시스템 요구 사항은 다음과 같습니다.

- Microsoft Windows 7, 8 또는 8.1(32비트 또는 64비트)
- Mac OS X 10.7, 10.8 또는 10.9

주문 정보

제품 주문은 Cisco Ordering Home Page를 방문하십시오. 소프트웨어 업데이트를 다운로드하려면 Cisco Software Center를 방문하십시오.

서비스 및 지원

Cisco는 다양한 서비스 프로그램을 제공하고 있습니다. 이러한 혁신적인 프로그램은 인력, 프로세스, 툴, 파트너의 독특하고 독창적인 조합을 통해 제공되며 높은 수준의 고객 만족을 실현합니다. Cisco 서비스는 고객의 네트워크 투자를 보호하고 네트워크 운영을 최적화하며 새로운 애플리케이션에 맞는 네트워크의 준비를 통해 네트워크 인텔리전스와 고객의 비즈니스 능력 강화에 기여합니다. Cisco 서비스에 대한 자세한 정보는 Cisco 기술 지원 서비스 또는 Cisco 보안 서비스를 참조하십시오.

보증 관련 정보는 http://www.cisco.com/go/warranty를 참조하십시오. 라이센스 정보는 http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-licensing-information-listing.html을 참조하십시오.

추가 정보

Cisco ISE 및 Cisco TrustSec 솔루션에 관한 자세한 내용은 http://www.cisco.com/go/ise를 방문하거나, 현지 Cisco 고객 담당자에게 문의하십시오.

미주 지역 본부
Cisco Systems, Inc.
San Jose CA

아시아 태평양 지역 본부
Cisco Systems (USA) Pte. Ltd.
싱가포르

유럽 지역 본부
Cisco Systems International BV Amsterdam,
네덜란드

Cisco는 전 세계에 200여 개 이상의 지사가 있습니다. 각 지사의 주소, 전화 번호 및 팩스 번호는 Cisco 웹 사이트 **www.cisco.com/go/offices**에서 확인하십시오.

Printed in USA C78-656174-09 10/14