cisco
SECURE

Cisco Secure Access

클라우드 애자일 보안으로 하이브리드 인력을 보호하세요.

2024년 2월

목차

하이브리드 업무 및 보안 서비스 엣지 3
제품 개요 3
기능 및 이점 5
패키징 옵션 12
자세한 내용 14

@ 2024 Cisco and /or its affiliates. All rights reserved.

클라우드 애자일 보안으로 하이브리드 인력을 보호하세요.

하이브리드 업무 및 보안 서비스 엣지

하이브리드 업무의 새로운 시대에는 보안에 대한 새로운 접근 방식이 필요하며, SSE(보안 서비스 엣지)는 모든 조직의 하이브리드 업무 전략의 핵심 요소입니다. SSE는 클라우드에 여러 보안 기능을 결합하여 어느 위치에서든 근무하는 직원, 계약자 또는 파트너를 보호하고 중요한 리소스를 보호합니다. 세션에 포함된 애플리케이션이 프라이빗 데이터 센터에 있든, SaaS 위치에 있든, peer-to-peer, IaaS 또는 인터넷 사이트에 있든 SSE는 여러 가지 유형의 악의적인 활동을 식별하고 방지하는 "보안 중개자" 역할을 합니다. 엔드 유저에게는 사무실, 가정, 이동 중 등 어디에서나 안전하고 투명한 사용자 경험이 보장됩니다. SSE 솔루션은 세 가지 주요 요구 사항을 해결해야 합니다: 우수한 사용자 경험 제공, IT 복잡성 감소, 보안 효율성 향상.

제품 개요

Cisco Secure Access는 제로 트러스트에 기반한 통합 클라우드 보안 SSE 솔루션으로, 장소에 구애받지 않고 원활하고 투명하며 안전한 액세스를 제공합니다. 수상 경력에 빛나는 Cisco의 Umbrella 보안 인터넷 액세스 솔루션이 더 광범위한 Secure Access라는 이름으로 확장되어 더 많은 SSE 관련 기능을 포괄합니다. 이제 하나의 라이선스 및 관리 플랫폼에 모든 핵심 SSE 구성 요소(SWG, CASB, ZTNA, FWaaS)와 확장 기능(멀티모드 DLP, DNS 보안, RBI, 샌드박싱, DEM 인사이트, Talos 위협 인텔리전스 및 AI 사용 보안 조치)이 포함되어 있습니다. 조직에서는 하나의 클라우드 제공 플랫폼에서 이러한 기능을 모두 활용하여 다양한 보안 문제를 해결할 수 있습니다. 이제 사용자는 프로토콜, 포트 또는 사용자 지정 수준에 관계없이 필요한 모든 리소스와 앱에 안전하고 원활하게 액세스할 수 있습니다.

Cisco Secure Access는 다른 시너지 구성 요소와의 상호 운용성을 용이하게 하는 공통 관리 제어, 데이터 구조 및 정책 관리로 설계되었습니다. 예를 들어, 모든 SAML 기반 서비스(AD, Azure AD, Okta, Ping 등)를 포함한 다양한 ID 공급자(IDP)가 ID 확인 및 컨텍스트를 제공할 수 있습니다. 이 솔루션은 SD-WAN, XDR, 디지털 경험 모니터링 등 다른 Cisco 제품 및 타사 기술과 함께 작동하여 고객 성과를 개선합니다.

Secure Access는 최신 사이버 보안을 시행하는 동시에 위험을 근원적으로 줄이고, IT 운영의 복잡성을 크게 간소화하며, 최종 사용자가 수행하는 작업을 최소화합니다.

더 나은 사용자 경험

Cisco Secure Access는 사용자 환경을 획기적으로 개선하여 마찰을 없애고, 필요한 보안 절차를 우회할 수 있는 가능성을 극복하며, 생산성을 높입니다. 이 솔루션은 사용자 연결 방식을 간소화하는 통합 클라이언트를 사용하여 사용자가 인증한 후 원하는 애플리케이션으로 바로 이동합니다. 이러한 '모든 액세스' 기능은 최소 권한 개념, 사전 구성된 보안 정책 및 관리자가 제어할 수 있는 적응형 시행 조치와 자동으로 연결됩니다.

세션에서 특정 비표준 앱에 대해 ZTNA를 사용하든 VPNaaS를 사용하든 관계없이 사용자는 추가 단계를 수행할 필요가 없습니다. 성가신 확인 작업을 반복할 필요가 없습니다. 이를 통해 별도의 클라이언트를 시작해야 하거나 다른 로그인 프로세스 조건이 제거되는 경우, 서로 다른 리소스에 어떤 액세스 방법이 필요한지 등의 문제와 관련된 사용자 번거로움을 최소화합니다. 모든 애플리케이션에 대한 중앙 집중식 액세스는 사용자가 연결하기 위해 수행하는 프로세스를 크게 간소화하고, 사용자 및 디바이스 태세 상태 검증을 비롯한 보안을 보장하며, 생산성을 향상시킵니다.

© 2024 Cisco and /or its affiliates. All rights reserved.

간소화된 IT 업무

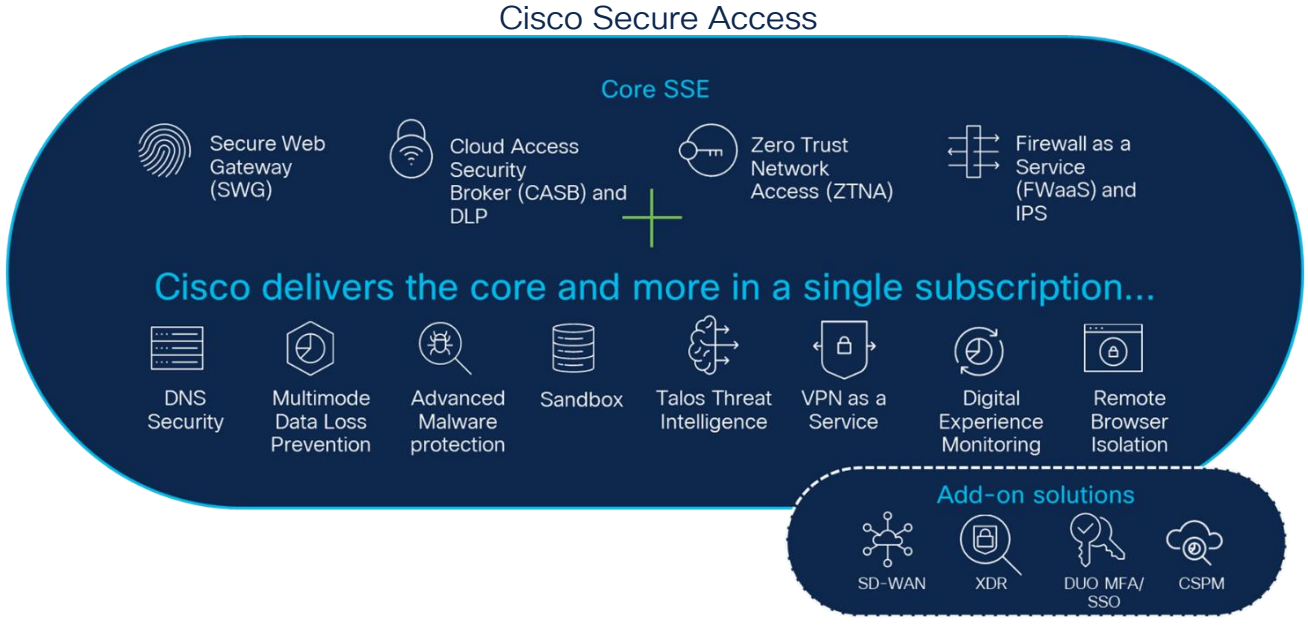
오늘날 IT 팀은 과도한 보안 툴을 통합하는 데 어려움을 겪고, 여러 관리 콘솔 및 정책 엔진이 필요하며, 각 최종 사용자 디바이스에 여러 소프트웨어 에이전트를 구축하고 관리해야 합니다. 이러한 문제는 각 보안 포인트 제품에서 발생하는 별도의 보고, 알림 및 인시던트에 의해 확대됩니다.

Cisco Secure Access는 단일 클라우드 관리 콘솔, 통합 클라이언트, 중앙 집중식 정책 생성 프로세스 및 통합 보고를 통해 보안 및 IT 팀의 운영을 간소화하고 자동화합니다. 이제 IT에서는 서로 다른 수많은 제품을 구축하는 대신 하나의 툴만 관리하면 됩니다. 이를 통해 측정 가능한 효율성 향상으로 이어짐으로써 비용을 절감하고 유연한 IT 환경을 통해 비즈니스 민첩성을 높일 수 있습니다. IT 부서는 이제 수동 집계 작업을 줄이면서 최종 사용자 활동에 대한 가시성을 개선하는 동시에 위협을 더욱 신속하게 탐지 및 차단하고, 조사를 신속하게 진행하며, 문제 해결 작업을 최소화할 수 있습니다. 이를 통해 다양한 위치에 있는 사용자 또는 그룹을 매니지드 디바이스와 관리되지 않는 디바이스를 포함해 여러 대상(인터넷, SaaS(Software as a service) 앱, 프라이빗 앱)으로 이동시킬 수 있는 세분화된 상황 인식 제어가 가능합니다.

모두를 더 안전하게 보호

Cisco Secure Access는 최종 사용자와 온프레미스 리소스 모두에 업계 최고의 보안 효능을 제공합니다. 심층 방어 아키텍처형 접근 방식의 확장된 기능은 다양한 사이버 보안 위협으로부터 보호합니다. 엔드 유저는 감염된 파일, 악의적인 웹사이트는 물론 피싱 및 랜섬웨어 체계와 같은 위험으로부터 보호됩니다. IT 및 보안 팀은 공격 표면을 줄이고, 최소 권한 제어를 시행하고, 보안 상태 검증을 활성화하고, 분산된 환경에서 보안 공백을 제거할 수 있습니다.

보안 팀은 무단 섀도 IT 운영 및 승인되지 않은 애플리케이션 사용에 대한 가시성을 확보하고 그러한 활동을 차단할 수 있습니다. 내부 리소스를 은폐하고 해커가 그 존재를 발견하지 못하도록 함으로써 IT 부서는 추가적인 보안 계층을 확보할 수 있습니다. 이 모든 기능은 독보적인 원격 측정, 광범위한 연구, 고급 AI를 통해 위협을 식별하고 차단하며 신속한 해결을 지원하는 Cisco Talos 위협 인텔리전스의 지원을 받습니다. 조직은 보안 위험을 완화함으로써 비즈니스 연속성을 유지하고 반복과 보안 침해로 인한 재정적 영향을 방지합니다.



코어 SSE(Security Service Edge)를 뛰어넘어 비즈니스 연결 및 보호 개선

© 2024 Cisco and /or its affiliates. All rights reserved.

기능 및 이점

표 1. 기능 및 이점

기능	이점
제로 트러스트 네트워크 액세스(ZTNA)	온프레미스 데이터 센터 또는 클라우드/IaaS(Infrastructure as a service) 환경에 있는 프라이빗 애플리케이션에 대한 세분화된 앱별 액세스를 제공합니다. 정의된 액세스 제어 정책을 기반으로 하는 ID 인식 프록시 설계는 최소 권한 원칙과 상황별 인사이트를 사용하여 기본적으로 액세스를 세부적으로 거부하며 명시적으로 허용되면 위치에 상관없이 애플리케이션에 대한 사용자 액세스를 중개합니다. • 두 가지 액세스 방법: 클라이언트 기반 및 클라이언트 없는 브라우저 기반 액세스, 세분화된 사용자 및 애플리케이션 기반 액세스 정책, SAML 인증, ID 공급자(IdP), 상황별 액세스 제어. • 클라이언트 기반 액세스는 통합 Cisco Secure 클라이언트를 활용합니다. • 디바이스 태세 상태 확인이 수행된 후 세션별 보안 액세스를 설정합니다. • 안전한 암호화된 터널을 통해 사용자를 인증하며, 사용자는 액세스 권한이 있는 애플리케이션과 서비스만 볼 수 있습니다. • 애플리케이션 프록시는 애플리케이션을 인터넷에 노출하지 않고 투명하고 안전한 원격 액세스를 제공합니다. 심지어 프라이빗 앱에 액세스하는 클라이언트로부터 프라이빗 앱의 네트워크 세부 정보도 숨깁니다. 이렇게 하면 공격자가 클라이언트 기기를 침해한 경우에도 IP 정찰에서 아무것도 알 수 없게 됩니다. • 횡적 공격자 이동을 방지합니다. • 위치 및 디바이스별 액세스 제어 정책을 구현하여 보안이 침해되었을 가능성이 있는 디바이스의 서비스 연결을 방지합니다. • 관리자는 외부 이동 기능 없이 계약자 및 직원에게 액세스해야 하는 리소스에만 액세스 권한을 할당합니다. • 관리자는 엔드포인트 OS 유형 및 버전에 대한 포스처 프로파일, 브라우저 유형 및 버전 , 액세스 결정에 사용할 지리위치 정보를 구성할 수 있습니다. • 거부된 액세스의 원인을 설명하는 유용한 정보를 사용자에게 제공하고 제안된 교정 단계를 제공합니다. • 관리자는 대시보드를 통해 특정 사용자 및 디바이스 조합에 대한 ZTNA 액세스를 취소할 수 있습니다. • 관리자는 특정 애플리케이션에 대한 최대 인증 간격을 설정하여 해당 애플리케이션에 대해 추가 사용자 인증을 수행할 수 있습니다.
VPNaaS	모든 프라이빗 앱에 ZTNA를 적용할 수 있는 것은 아닙니다. 웹 인터넷 트래픽이 아닌 트래픽에 대한 안전한 원격 액세스 및 안전한 인터넷 액세스를 위한 VPNaaS 클라우드 기반 옵션이 포함되어 있습니다. • 기능의 예는 다음과 같습니다: 사용 사례 지원(분할 터널링 및 터널 모두 지원, P2P 통신, 신뢰할 수 있는 네트워크 감지, BYO 인증서, 분할 DNS, 동적 분할 DNS), 여러 인증 방법(SAML, 인증서, Radius), 사용자 사용 편의성(항상 VPN, 로그온 전 시작), IT 운영 단순화(로컬 IP 풀, 여러 VPN 프로필). • 원격 사용자가 Cisco Secure 클라이언트를 사용하여 보안 액세스 패브릭을 통해 프라이빗 애플리케이션에 액세스할 수 있습니다. • ID 기반 액세스 제어는 고객의 IdP를 통해 SAML 인증에 사용할 수 있습니다. • 엔드포인트 보안 상태도 평가됩니다. 이를 통해 프라이빗 리소스에 대한 세분화된 액세스 제어가 가능합니다. • 애플리케이션 별 액세스 제어를 지원합니다. • 헤드엔드 또는 터널 유형을 선택할 필요 없이 연결성을 간소화합니다. • 사용자가 PC에 기록하고 비밀번호 재설정을 수행할 때 VPN 터널을 가져와 온프레미스 Active Directory에 원활하게 인증하는 데 사용되는 관리 터널을 지원합니다. • 데스크톱 관리팀은 사용자 VPN 로그인 없이 관리 터널을 사용하여 소프트웨어 업데이트를 PC에 다운로드할 수 있습니다. • ISE(Identity Services Engine)와의 통합 및 RADIUS 인증 지원.

© 2024 Cisco and /or its affiliates. All rights reserved.

보안 웹 게이트웨이(전체 프록시)	포트 80/443을 통해 모든 웹 트래픽을 기록하고 검사하여 차원이 다른 투명성, 제어, 보호를 지원합니다. IPsec 터널, PAC 파일 및 프록시 체인은 전체 가시성, URL 및 애플리케이션 수준 제어, 고급 위협 보호를 위해 트래픽을 전달하는 데 사용됩니다. • 범주 또는 특정 URL로 콘텐츠를 필터링하여 정책 또는 컴플라이언스 규정을 위반하는 대상을 차단합니다. • 다운로드한 모든 파일에 악성코드 및 기타 위협을 검사합니다. • Cisco Secure Malware Analytics 를 이용한 샌드박싱은 알 수 없는 파일을 분석합니다(Cisco Secure Malware Analytics 전용 섹션 참조). • 파일 유형 차단(예: .exe 파일 다운로드 차단). • 숨겨진 공격과 시간이 많이 소요되는 감염으로부터 보호하기 위한 전체 또는 선택적 TLS 해독 . • 일부 앱에서 특정 사용자 활동을 차단하는 세분화된 앱 제어(예: Dropbox에 파일 업로드, Gmail에 첨부 파일, Facebook의 게시물/공유). • 전체 URL 주소, 네트워크 ID, 허용 또는 차단 작업, 외부 IP 주소 등이 포함된 세부적인 보고. • 맞춤형 제어 및 트래픽 경로 옵션을 사용하여 인터넷 기반 SaaS(Software as a service) 앱의 다중 모드 보호 .
CASB(Cloud Access Security Broker)	사용 중인 생성형 AI 앱을 포함해 클라우드 애플리케이션을 탐지하고 보고하여 섀도우 IT를 노출합니다. 클라우드 도입을 관리하고, 위험을 줄이고, 공격적이거나 비생산적이고 위험하거나 부적절한 클라우드 애플리케이션의 사용을 차단합니다. 사용자 /그룹 활동을 탐지, 로그 및 제어하는 멀티 모드 기능. • DLP(Data Loss Prevention)는 클라우드 또는 아웃바운드 웹 트래픽에서 민감한 엔터프라이즈 데이터가 권한이 없는 사람에게 유출되는 것을 차단합니다. (별도의 DLP 섹션 참조). • 검색된 각 앱의 공급업체 범주, 애플리케이션 이름 및 활동량에 대한 보고서. • 웹 평판 점수, 재정적 실행 가능성, 관련 규정 준수 인증과 같은 앱 세부 정보 및 위험 정보. • 클라우드 기반 파일 스토리지 애플리케이션에서 악성코드를 탐지하고 제거하는 클라우드 악성코드 탐지. • 특정 클라우드 애플리케이션을 차단/허용하는 기능. • 모든 사용자 또는 특정 그룹/개인이 액세스할 수 있는 SaaS(Software as a service) 애플리케이션의 인스턴스를 제어하기 위한 테넌트 제한 • 70개 이상의 생성형 AI 애플리케이션의 사용 또는 사용 시도를 검색 및 제어. 사용을 차단하거나 이러한 앱의 사용 방식을 제어하는 정책을 만들고 시행.

© 2024 Cisco and /or its affiliates. All rights reserved.

데이터 손실 방지(DLP)	멀티모드 데이터 손실 방지. 민감한 데이터를 인라인으로 분석하여 조직에서 나가는 민감한 데이터에 대한 가시성 과 제어 기능을 제공. 클라우드에 있는 미사용 데이터 OOB(Out of Band) 분석을 위한 API 기반 DLP 기능. 보다 효율적인 관리 및 규정 준수를 위한 통합 정책 및 보고를 포함. • PII, PHI, PCI 및 기타 규정의 컴플라이언스를 위한 600개 이상의 내장형 식별자 및 HIPAA, PCI, 개인정보 보호정책, PII를 위한 내장형 데이터 분류. • 임계값 및 근접 기능이 있는 맞춤형 내장형 콘텐츠 분류자를 통해 오탐을 조정 및 감소. • 맞춤형 구문이 포함된 사용자 맞춤화 사전(예: 프로젝트 코드 이름). • 민감한 데이터 사용에 대한 탐지 및 보고, 오용을 식별하는 데 도움이 되는 드릴다운 보고서를 제공. • DLP 정책을 AI 애플리케이션에 할당하여 사용자가 챗GPT 같은 공개적으로 사용 가능한 AI 서비스를 더욱 안전하게 사용하도록 지원하여, 위험한 콘텐츠를 탐지 및 차단하여 IP 손실 또는 IP 감염을 방지하는 기능. • 클라우드 앱 및 웹 트래픽 콘텐츠를 검사하고 데이터 정책을 시행. • API 기반 기능은 Microsoft 365(SharePoint 및 OneDrive), Google Drive, Webex, Box 및 Dropbox를 지원합니다. • 챗GPT의 경우 권한이 없는 사용자에게 유출되지 않도록 전용 소스 코드의 업로드를 차단합니다. • 사용자가 챗GPT에서 소스 코드를 생성하여 다운로드하고 조직 코드 저장소에 커밋하는 것을 방지하기 위해 챗GPT에서 생성된 콘텐츠의 다운로드를 차단합니다.

© 2024 Cisco and /or its affiliates. All rights reserved.

FWaaS(Firewall as a Service)	모든 포트 및 프로토콜을 통해 인터넷으로 이동하는 요청에서 발생하는 비 웹 트래픽에 대한 가시성과 제어를 제공합니다. 모바일 앱, 피어 투 피어 파일 공유, 협업(예: Webex 또는 Zoom), O365, 또는 모든 비 웹 또는 비 DNS(Domain Name System) 트래픽을 포함합니다. • Security Access의 단일 통합 대시보드를 통한 구축, 관리 및 보고. • 정책 맞춤 설정(IP, 포트, 프로토콜, 애플리케이션 및 IPS 정책) • 3/4계층 방화벽을 통해 모든 활동을 기록하고 IP, 포트 및 프로토콜 규칙을 사용하여 원치 않는 트래픽을 차단합니다. • 확장 가능한 클라우드 컴퓨팅 리소스를 통해 어플라이언스 용량 문제가 해결됩니다. • 레이어 7 애플리케이션 가시성과 제어를 통해 증가하는 2,800개 이상의 비 웹 애플리케이션 기반을 식별하고 선택적으로 차단 또는 허용합니다. • 검사 전에 트래픽 암호를 해독합니다.
IPS(침입 방지 시스템)	IPS는 SNORT 3 기술 및 서명 기반 탐지를 사용하는 위협 방지 레이어가 추가되어 네트워크 트래픽 흐름을 검사하고 취약성 익스플로잇을 방지합니다. • 통합 대시보드를 사용하여 트래픽을 검사하는 정책을 생성하고 자동화된 작업을 통해 위험한 패킷이 네트워크에 도달하기 전에 이를 포착 및 삭제합니다 . • 인터넷 및 프라이빗 트래픽 모두에 IPS 보호를 제공합니다. • 트래픽 대상에 따라 다양한 맞춤형 프로파일에 대한 액세스 정책 및 옵션을 구성합니다. • Cisco Talos에서 40,000개가 넘는 서명으로 구성된 광범위한 기반을 사용합니다. • 서명은 사전 정의된 템플릿에서 사용할 수 있습니다. • 취약성 악용 탐지 및 차단.
Cisco Secure Malware Analytics	고급 샌드박싱과 위협 인텔리전스를 하나의 통합 솔루션으로 결합하여 악성코드로부터 조직을 보호합니다. 전체 Secure Malware Analytics 콘솔에 대한 액세스를 제공하여 글로브박스에서 악성 파일을 실행하고, 파일 실행 작업을 추적하고, 파일에서 생성된 네트워크 활동을 캡처할 수 있습니다. 보안 분석가는 Investigate와 함께 사용하면 더 나아가 파일의 동작에 매핑된 악성 도메인, IP, ASN을 발견하여 공격자의 인프라, 전술 및 기법을 가장 완벽하게 파악할 수 있습니다. • 숨겨진 공격 방법을 탐지하고 악의적인 파일에 보고하는 기능. • 보안 데이터를 강화하기 위해 XDR 및 일반적으로 사용되는 SIEM과 통합하는 API. • 파일 속성이 변경되는 경우 회귀적 알림(원래는 정상/나중에 악의적인 것으로 간주됨).
원격 브라우저 격리(RBI)	RBI는 브라우저 기반 위협으로부터 사용자와 조직을 보호합니다. 인터넷 위협으로부터 보호하기 위해 브라우징 활동 실행을 사용자에서 원격 클라우드 기반 가상 브라우저 인스턴스로 전환합니다. 웹사이트 코드는 별도로 실행되며 안전한 시각적 스트림만 사용자에게 전달됩니다. 이러한 작업은 엔드 유저에게 완전히 투명합니다. 아직 탐지되지 않은 악성코드에 대해서는 걱정할 필요가 없습니다. • 사용자 디바이스 및 브라우저 기반 위협 간 웹 트래픽 격리 • 제로데이 위협으로부터 보호. • 다양한 위험 프로파일에 대한 세분화된 제어. • 기존 브라우저 설정을 변경하지 않고 신속한 구축. • 추가 사용자를 쉽게 보호하기 위한 온디맨드 확장. • 알려진 위험한 인터넷 사이트에 액세스해야 하는 직원을 보호합니다. 차단으로 인해 생산성이 감소하지 않으며 사용자는 안전합니다.
DNS 레이어 보안	연결을 설정하기 전에 DNS(Domain Name System) 계층에서 필터링을 시행하여 악의적인 원치 않는 대상에 대한 요청을 차단합니다. 위협이 네트워크나 엔드포인트에 도달하기 전에 모든 포트 또는 프로토콜을 통해 차단합니다. • 모든 네트워크 디바이스, 사무실 위치 및 로밍 사용자에서 인터넷 액세스를 보호합니다.

© 2024 Cisco and /or its affiliates. All rights reserved.

	• 보안 위협 또는 웹 콘텐츠 유형별로 DNS(Domain Name System) 활동에 대한 자세한 보고 및 수행된 작업을 제공합니다. • 모든 활동의 로그를 유지합니다. • 수천 개의 위치 및 사용자에 대한 롤아웃을 가속화하여 즉각적인 보호를 제공합니다.
Talos 위협 인텔리전스	전 세계적으로 엣지 보안 연구를 제공하는 대표적인 공급자인 Talos는 매일 수천억 개의 DNS(Domain Name System) 요청 및 기타 텔레메트리 데이터를 분석합니다. 이 대규모 데이터베이스에 대해 AI, 통계 및 머신러닝 모델을 지속적으로 실행하여 사이버 위협에 인사이트를 제공하고 사고 응답률을 개선합니다. • 악성 도메인, IP, 멀웨어, URL이 공격에 사용되기 전에 발견합니다. • 인시던트 조사의 우선 순위를 정합니다. • 사고 조사 및 대응 속도를 높입니다. • 공격자의 인프라를 정확히 파악하고 매핑하여 향후 공격의 발원지를 예측합니다.
클라우드 악성코드 탐지	클라우드 기반 파일 스토리지 애플리케이션에서 악성코드를 탐지하고 제거합니다. 악의적인 파일이 엔드포인트에 도달하기 전에 이를 탐지하고 교정하여 보안 보호를 강화합니다. • 보안 관리자의 업무 효율성 및 능률 증가 – 이 기능을 활성화하면 클라우드 기반 서비스의 모든 파일이 자동으로 해시되고 악성코드 스캔을 위해 전송됩니다. 악성코드를 포함하는 모든 파일에는 플래그가 지정되므로 보안 관리자가 격리 및/또는 삭제를 포함하여 교정할 수 있습니다. • Box, Dropbox, Webex, Microsoft 365 및 Google Drive를 지원합니다.
단일 관리 및 보고 콘솔	인텐트 기반 규칙을 포함한 통합 보안 정책 생성, 인터넷, 공용 SaaS 앱, 비공개 앱 액세스 전반에 걸친 관리. 광범위한 기록을 제공하며, 로그를 엔터프라이즈 SOC 등으로 내보내는 기능을 제공합니다. • 모든 앱의 모든 사용자에 대한 정책을 한 곳에서 정의합니다. 보안 정책 구축 프로세스를 간소화하고 전체 조직에 대한 정책 정의의 일관성을 유지합니다. • 통합 소스(사용자, 디바이스)와 통합 리소스(앱, 대상)를 사용하면 연결 지점 및 액세스하는 앱에 관계없이 보안 정책이 사용자를 추적할 수 있습니다. • 진행되는 정책 관리 활동이 감소합니다. • 집계된 보고를 통해 가시성을 개선하고 탐지 시간을 단축합니다. • 전체 SOC/보안 분석 조사 프로세스를 간소화합니다.
AI Assistant*	Secure Access AI Assistant는 대화식 영어 구문을 특정 보안 정책으로 자동 변환합니다. • 보안 관리자는 시간을 절약하고 운영 효율성을 높이며 복잡성을 줄일 수 있습니다. • 여러 사용자가 관리자 그룹을 사용하면 일관되고 효과적인 정책 집합을 만들 수 있습니다. • 비용 절감 및 리소스 절약은 대규모 정책 집합을 생성해야 하는 경우에 더욱 효과적입니다.
리소스 커넥터	리소스 커넥터는 단순한 관리 작업을 통해 프라이빗 애플리케이션에 대한 보안 연결성을 설정합니다. 이 경량 커넥터는 온프레미스 데이터 센터 또는 클라우드에 있는지 여부에 상관없이 Cisco Secure Access와 프라이빗 앱 간의 연결을 관리합니다. 현재 리소스 커넥터는 AWS 및 VMWare 환경만 지원합니다. • 디바이스 및 방화벽 규칙 변경에 대한 네트워크 팀에 대한 종속성을 줄입니다. • 동적 라우팅 또는 중복 서브넷 설정과 같은 라우팅 복잡성은 피하십시오. • 합병과 같은 시나리오에서는 네트워크가 겹치는 IP 등으로 분리되어 있는 경우가 많습니다. 터널을 사용하면 복잡해집니다. 앱 커넥터를 사용하면 이러한 복잡성을 해결할 수 있습니다.

© 2024 Cisco and /or its affiliates. All rights reserved.

	• 해당 위치(IP 주소)를 숨기고 보안 액세스 내에서 제로 트러스트 정책을 통한 연결만 허용하여 프라이빗 앱을 보호합니다. • 리소스 및 네트워크를 격리하여 횡적 이동을 방지합니다.
경험 인사이트: 디지털 경험 모니터링(DEM)	사용자가 리소스에 액세스할 때 엔드포인트, 애플리케이션 및 네트워크 연결의 상태와 성능을 모니터링합니다. 사용자의 엔드투엔드 경험에 대한 세부 정보를 자동으로 마이닝하여 사용자 생산성을 최적화하고 문제 해결을 간소화하며 인시던트 해결 시간을 단축합니다,
	IT/ 보안 담당자가 문제를 신속하게 해결할 수 있습니다. 주요 인사이트 의 예시: • 엔드포인트 성능 - CPU 레벨, 메모리 사용량 및 WIFI 신호의 강도. • 네트워크 성능 - 엔드포인트에서 보안 액세스까지의 경로 시각화 및 성능. • Outlook, Slack, Salesforce, SharePoint를 포함하여 가장 일반적으로 사용되는 SaaS(Software as a service) 애플리케이션(상위 20개). • 사용자별 보안 이벤트. • Webex, Zoom, Microsoft Teams를 비롯한 다양한 앱의 협업 애플리케이션 성능 및 사용자 경험 점수입니다. • 처리량, 레이턴시 및 관리자가 문제 해결을 효율적으로 해결하기 위한 제안된 교정과 같은 메트릭을 사용하여 세그먼트 기반의 문제를 해결합니다. • 네트워크 연결성 패킷 손실을 격리합니다.

© 2024 Cisco and /or its affiliates. All rights reserved.

모바일 디바이스 ZTA 지원*	Apple iOS 디바이스의 매우 효율적인 ZTA(제로 트러스트 액세스)를 지원합니다. Apple과 Cisco는 성능과 보안 이점을 모두 제공하는 고유한 ZTA 프로세스를 개발하기 위해 협업했습니다. • 보안 액세스는 효율적인 등록, 구성 및 문제 해결을 제공합니다. • iOS 디바이스에서 전체 클라이언트를 배포하고 관리할 필요 없이 구축을 간소화할 수 있습니다. • iOS 운영 체제의 내장 기능을 활용합니다. • 더 빠른 트랜짓을 위해 QUIC 및 MASQUE 프로토콜을 활용하고 처리량 향상을 위한 VPP 가속화를 활용합니다. • 빠르고 안전한 액세스를 위해 단일 암호화 레이어를 통해 Apple의 iCloud 프라이빗 릴레이를 활용합니다. • 데스크톱과 동일한 모바일 ZTA 등록 환경. • 관리자는 연결된 iOS 디바이스에서 세부 정보를 볼 수 있습니다. Samsung Galaxy 디바이스에서 ZTA 함수를 지원합니다. • 보안 액세스는 ZTA 등록, 구성, 문제 해결, 트래픽 조정을 제공합니다. • 더 빠른 트랜짓을 위해 QUIC 및 MASQUE 프로토콜을 활용하고 처리량 향상을 위한 VPP 가속화를 활용합니다. • 데스크톱과 동일한 모바일 ZTA 등록 환경. • 문제 해결을 위해 사용자는 클라이언트에서 사용 가능한 로그를 내보내고 헬프데스크와 상호 작용할 때 이러한 로그를 사용할 수 있습니다.
인터넷/SaaS(Software as a service) 앱에 액세스하는 Catalyst SD-WAN 브랜치 사용자	Catalyst SD-WAN과 Secure Access 간의 통합 및 자동화를 사용하면 Cisco Secure Access를 통해 브랜치 사용자에서 웹 및 SaaS(Software as a service) 앱으로 트래픽을 조정할 수 있습니다. • Secure Access의 멀티 레이어 보안 솔루션으로 위협 보호 증가 • 사용자가 로밍 위치와 온프레미스 위치 간을 이동할 때 더 일관된 환경 제공. • Secure Access의 중앙 집중식 정책 관리, 간편한 가동/다운로드 확장성 , 용량 제약 조건 완화를 통해 IT/보안 운영을 간소화합니다.
Identity Services Engine(ISE) 통합	이는 ISE 및 보안 액세스 통합의 첫 번째 인스턴스화입니다. 이 인스턴스는 세분화된 ID 기반 정보를 제공하여 사용자가 무엇을 언제 어떻게 하고 있는지에 대한 가시성을 강화합니다. 이 통합은 다음을 위한 VPNaaS 트래픽에 대한 정책 제어 및 시행을 강화합니다. • 적절한 사용자 또는 디바이스에 대해 적절한 시간에 적절한 정책을 더욱 정확하게 시행할 수 있습니다. • AI 애널리틱스를 제공하여 디바이스 태세/ID의 이상 징후를 탐지하고 올바른 정책을 자동으로 적용합니다. • ISE를 사용한 인증 요청에 대해 RADIUS 지원 • 앞으로 Cisco는 사용자가 작업하는 곳, 연결 방식(유선 또는 무선), 액세스하는 리소스에 관계없이 모든 제품과 기능에 공통된 ID를 적용하는 방향으로 나아가고 있습니다.

*정식 출시 예정

© 2024 Cisco and /or its affiliates. All rights reserved.

패키징 옵션

Cisco Secure Access는 Cisco Umbrella SIG의 진화 버전으로, 모든 사용자에게 더 높은 수준의 보안을 제공하는 동시에 IT와 최종 사용자 생산성을 모두 개선하는 단일 구독에서 가장 광범위한 SSE 솔루션입니다. 고객이 조직의 요구 사항에 맞는 적절한 보호 및 커버리지 레벨을 쉽게 선택할 수 있는 패키지로 제공됩니다. 현재 Cisco Secure Access Essentials 및 Cisco Secure Access Advantage의 두 가지 패키지가 있습니다.

표 2. 코어 오퍼 패키지

범주	기능	Secure Access Essentials	Secure Access Advantage
Secure Access	SIA(Secure Internet Access) • SD-WAN DIA 통합 • Secure Client(라이선스 포함) • 로밍 보안(DNS(Domain Name System), 웹 및 Firewall-as-a-Service)	✓	✓
	SPA(Secure Private Access) • Secure Client(라이선스 포함) • ZTNA 클라이언트 • VPN-as-a-Service • ZTNA 클라이언트리스	✓	✓
기본적 보안	DNS 보호	✓	✓
	웹 및 프라이빗 앱의 레이어 3 및 레이어 4 제어를 위한 Firewall-as-a-Service	✓	✓
	보안 웹 게이트웨이(프록시 웹 트래픽, URL 필터링, 콘텐츠 필터링, 고급 앱 제어)	✓	✓
	CASB - 클라우드 앱 검색, 위험 점수 부여, 차단, 클라우드 멀웨어 탐지, 테넌트 제어	✓	✓
	원격 브라우저 격리(위험한 트래픽의 경우에만 라이선스 적용*)	✓	✓
	Secure Malware Analytics(샌드박스)	제한	제한 없음
디지털 경험 모니터링	Experience Insights	✓	✓
고급 보안	레이어 7 Firewall-as-a-Service		✓
	IPS 보호		✓
	생성형 AI/챗GPT 제어를 비롯한 웹 애플리케이션용 DLP(데이터 손실 방지)		✓
	원격 브라우저 격리(모두**)		✓
소프트웨어 지원	이메일과 전화를 통해 연중무휴로 Cisco Software Support-Enhanced에 대한 액세스 지원, Software Support-Premium으로 업그레이드 옵션	✓	✓

*위험: 미분류 웹사이트와 보안 범주(잠재적으로 유해 포함)를 격리합니다.

**모두: 콘텐츠 및 보안 범주, 대상 목록, 애플리케이션, 미분류 등을 포함하여 선택한 대상을 격리합니다.

© 2024 Cisco and /or its affiliates. All rights reserved.

Cisco Secure Access: 소프트웨어 지원 서비스

Cisco Secure Access 제품을 구매 하려면 Software Support-Premium으로 업그레이드할 수 있는 옵션이 있는 별도의 SKU for Software Support-Enhanced용 SKU가 필요합니다.

Cisco Software Support Enhanced

- 기술 지원(Cisco Cloud 보안 지원에 24x7 액세스 - 전화/온라인)
- 소프트웨어 업데이트.
- 솔루션 전문성을 갖춘 주요 연락처.
- 기술 온보딩 및 도입 지원.

Cisco Software Support Premium(선택적 업그레이드)

Enhanced 레벨의 기능 +:

- Enhanced 지원보다 케이스 처리에 우선순위를 둡니다.
- 할당된 전문가가 인시던트 관리, 사전 상담 및 권장 사항을 제공하여 성공적인 보안 소프트웨어 구축과 지속적인 관리 및 최적화를 보장합니다.
- 케이스 분석을 지원합니다.

보안 소프트웨어에 대한 Cisco 지원 서비스에 대해 자세히 알아보려면 여기를 클릭하십시오.

© 2024 Cisco and /or its affiliates. All rights reserved.

자세한 내용

자세한 내용은 Cisco Secure Access를 방문하십시오.

미주 지역 본부

Cisco Systems, Inc.
캘리포니아 주 산호세

아시아 태평양 지역 본부

Cisco Systems (USA) Pte. Ltd.
Singapore

유럽 지역 본부

Cisco Systems International BV Amsterdam,
네덜란드

Cisco has more than 200 offices worldwide. 각 지사의 주소, 전화번호 및 팩스 번호는 Cisco 웹사이트 https://www.cisco.com/go/offices에서 확인하십시오.

Cisco 및 Cisco 로고는 미국과 기타 국가에서 Cisco 및 계열사의 상표 또는 등록 상표입니다. Cisco 상표 목록은 https://www.cisco.com/go/trademarks에서 확인하십시오. 언급된 제3자 상표는 해당 소유자의 재산입니다. '파트너'라는 용어의 사용이 Cisco와 다른 회사 간의 파트너십 관계를 의미하는 것은 아닙니다. (1242051230)

02/24

© 2024 Cisco and /or its affiliates. All rights reserved.