CISCO IDENTITY SERVICES ENGINE

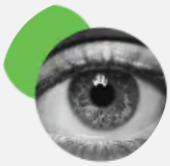
La pieza central en seguridad de confianza cero para el lugar de trabajo

Un componente crítico de cualquier estrategia de Confianza Cero es asegurar el lugar de trabajo al que todos y todo se conectan. Cisco Identity Services Engine (ISE) permite un enfoque dinámico y automatizado para la aplicación de políticas que simplifica la entrega de un control de acceso a la red altamente seguro. ISE permite el acceso definido por software y automatiza la segmentación de la red dentro de los entornos de tecnologías de la Información y de la operación (TI y OT).

Cisco Partner
Select Provider

El CAMINO HACIA EL ACCESO SEGURO A LA RED DE ULTIMA GENERACION

CISCO Identity Services Engine transforma su red con las capacidades necesarias para manejar las demandas digitales de hoy.

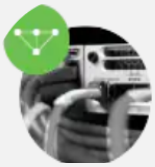


VISIBILIDAD DINÁMICA: mantiene al día con las amenazas y un lugar de trabajo de Confianza Cero

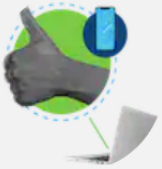
SEGMENTACIÓN DE RED: para aumentar la productividad y reducir su superficie de ataque.

CONTENCIÓN AUTOMATIZADA DE AMENAZAS: se trata de eliminar amenazas, no solo de bloquearlas.

INVITADO Y ACCESO SEGURO INALÁMBRICO SEGURO: Facilita la incorporación (onboarding) y el aprovisionamiento.



ACCESO ALAMBRADO SEGURO: aplica políticas de forma coherente en todas las conexiones



CUMPLIMIENTO DE DISPOSITIVOS: encuentre y repare los dispositivos que ignoran su política de seguridad.

INTEGRACIONES DE ECOSISTEMAS DE SEGURIDAD: aumente el ROI de sus soluciones existentes.

TRAIGA SU PROPIO DISPOSITIVO: los usuarios obtienen el dispositivo que desean --sin el dolor de cabeza de la seguridad.

El DESAFÍO DEL ACCESO SEGURO A LA RED Y LA CONFIANZA CERO

Proporcionar acceso seguro a usuarios de confianza y puntos finales es cada vez más difícil de lograr. El problema de identificar y controlar los puntos finales a medida que solicitan acceso a recursos confiables ha estado exasperado por las tendencias en torno a la migración a la nube, movilidad y la proliferación de dispositivos conectados IoT. Pero como la nube, la movilidad y el IoT poseen grandes posibilidades para desbloquear la innovación y ahorrar recursos organizacionales, estos nuevos paradigmas han introducido más preguntas y complejidad cuando se trata de proteger los datos y mantener el cumplimiento a lo largo del perímetro en expansión.

La Confianza Cero y los privilegios mínimos son un principio vital de ciberseguridad que aborda estos desafíos. Se recomienda otorgar solo el nivel mínimo de acceso al sistema/red basado en el nivel mínimo de privilegio requerido para permitir a los usuarios y puntos finales llevar a cabo sus misiones según lo requieran sus objetivos de negocios. El acceso no requerido amplía la superficie de ataque, aumenta el riesgo para la organización, y permite el movimiento lateral de las amenazas. Al controlar el acceso a solo lo que se necesita para alcanzar los resultados comerciales, se reduce el riesgo organizacional y se asegura el cumplimiento.

boyra
comunica tus sueños

TELEFONOS: 57 601 9156130, 57 350 6137478
DIAGONAL 61c Bis # 24-44 BOGOTA
WWW.BOYRA.COM