#ACCEDE

2.

PRISMA ACCESS

Prisma Access es una solución SASE que brinda servicios de conectividad y seguridad en red desde la nube para proteger a las organizaciones que emplean tecnología en la nube y plataformas de movilidad.

Esta solución protege de una forma coherente todo el tráfico, en todos los puertos y desde todas las aplicaciones, permitiendo:

- Evitar que los ciberataques alcancen sus objetivos.
- Inspeccionar todo el tráfico de las aplicaciones de manera bidireccional, incluido el tráfico cifrado con SSL/TLS, en todos los puertos, tanto si la comunicación se produce con internet, la nube o sucursales.
- Beneficiarse de la inteligencia integral sobre amenazas, basada en datos de amenazas automatizadas de Palo Alto Networks y cientos de fuentes de terceros

Un usuario solo ha de conectarse a Prisma Access para acceder con seguridad a internet, a las aplicaciones del centro de datos y a las alojadas en la nube, tanto si están desplazándose como si trabajan desde la sede central. Prisma Access ofrece funciones de red para todas las aplicaciones y una seguridad coherente que permite aplicar las mismas políticas en todo momento. Proporciona conectividad y acceso seguro a todas las aplicaciones, ofreciendo flexibilidad y escalabilidad en la nube para adaptarse a todos los requerimientos de la empresa.

CARACTERÍSTICAS

Firewall como servicio (FWaaS):
Prisma Access funciona como un servicio de cortafuegos que protege las sucursales frente a las amenazas al tiempo que presta los servicios de seguridad.

Puerta de enlace web segura (SWG) en la nube:
Diseñada para garantizar la visibilidad de todos los tipos de tráfico y detener las evasiones que puedan esconder amenazas.

DNS Security:
Ofrece una combinación de análisis predictivo, aprendizaje automático y automatización para combatir las amenazas sobre el tráfico DNS. Las organizaciones pueden bloquear determinados dominios, predecir los maliciosos y detener la tunelización de DNS.

Prevención de pérdida de datos (DLP):
Combina la integración con controles de prevención de pérdida de datos basados en API y en línea. Estas políticas de DLP permiten a las organizaciones clasificar los datos y establecer políticas que eviten su pérdida.

Agente de seguridad de acceso a la nube (CASB):
Controles que combinan seguridad en línea, seguridad basada en API y controles contextuales para determinar el acceso a la información confidencial.