PRISMA SaaS
BY PALO ALTO NETWORKS

Prisma SaaS: Resumen

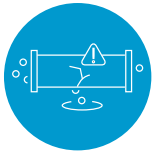
Desafíos de la Seguridad SaaS

El concepto del alojamiento de los datos de una organización en un solo lugar centralizado ya no aplica mayormente hoy en día. Los datos se distribuyen a través de múltiples ubicaciones, muchas fuera del control de la organización. Dondequiera que se encuentren los datos, las organizaciones IT continúan siendo responsables de protegerlos a medida que se mueven. Este problema puede verse principalmente en el caso de las aplicaciones de Software-as-a-Service (Software como Servicio – SaaS), cuyo uso es difícil de controlar y cuya visibilidad es difícil de mantener con la seguridad tradicional. Como los usuarios finales configuran y usan las aplicaciones SaaS directamente, no requieren permiso para acceder a ellas ni para mover datos corporativos confidenciales hacia ellas. Esto constituye un desafío importante, ya que los usuarios finales actúan como sus propios departamentos IT y controlan su uso de estas aplicaciones sin tener necesariamente experiencia en la evaluación y prevención de riesgos de datos o amenazas.

Habilite Aplicaciones SaaS de Manera Segura con Prisma SaaS

Al ofrecer una protección avanzada de datos y consistencia a través de todas las aplicaciones, Prisma™ SaaS controla los riesgos. Responde a las necesidades de su Cloud Access Security Broker (Agente de Seguridad de Acceso a la Nube – CASB) y provee capacidades avanzadas para el descubrimiento de riesgos, la prevención de pérdida de datos, la garantía de cumplimiento, el control de datos, el monitoreo del comportamiento de usuarios y la protección avanzada contra amenazas. Ahora, usted puede mantener el cumplimiento y al mismo tiempo evitar las filtraciones de datos y la interrupción del negocio a través de una implementación CASB multimodo.

Profunda visibilidad de riesgos de la nube: Los paneles de uso de SaaS fáciles de navegar y los informes detallados ayudan a controlar las shadow IT. Descubra riesgos a un nivel más profundo con visibilidad completa de toda la actividad de usuarios, carpetas y archivos en las aplicaciones SaaS, generando análisis detallados que le permiten determinar rápidamente la presencia de riesgos de datos o violaciones a políticas relacionadas con el cumplimiento.



Protección de datos y prevención contra filtraciones: Defina un control de políticas minucioso, que tenga en cuenta el contexto para impulsar su cumplimiento y poner en cuarentena a los usuarios y datos apenas ocurran las violaciones. Prisma SaaS es capaz de asegurar sus aplicaciones clasificando los datos y supervisando el uso mediante el aprendizaje automatizado y un motor avanzado de data loss prevention (DLP).

Control de acceso granular y adaptativo: Políticas fáciles de gestionar le proporcionan un control granual sobre el acceso a sus aplicaciones SaaS para definir qué aplicaciones están permitidas, así como el comportamiento aceptable dentro de ellas. Esto le permite bloquear el acceso a las aplicaciones no autorizadas mientras mantiene un control sobre las aplicaciones toleradas.

Control de datos y garantía de cumplimiento: Usted puede cumplir rápida y fácilmente con los requisitos de cumplimiento sobre riesgos de datos, como aquellos relacionados con los datos GDPR, PCI, PII o PHI, mientras se mantienen los beneficios de las aplicaciones basadas en la nube.

Supervisión del comportamiento del usuario: El monitoreo trasversal del comportamiento de usuarios y la generación de alertas le permite identificar fácilmente las conductas sospechosas, como accesos desde regiones imprevistas, volúmenes inusualmente grandes de actividades de uso o múltiples intentos fallidos de acceso, que indiquen intentos de robo de credenciales.

Prevención de amenazas avanzadas: bloquear el malware conocido, además de identificar y bloquear el malware desconocido dentro de las aplicaciones SaaS.

CASB Multimodo, Entregado en la Nube

Prisma SaaS actúa como un CASB multimodo que ofrece protección en línea, basado en API, que trabaja en conjunto para minimizar el rango de riesgos en la nube que pueden provocar brechas. Con un enfoque de CASB completamente basado en la nube, puede proteger sus aplicaciones SaaS al utilizar:

- **Protecciones en línea** para proteger el tráfico en línea con una profunda visibilidad de aplicaciones, segmentación, acceso seguro y prevención de amenazas. Este enfoque combina funciones de inspección de usuarios, contenidos y aplicaciones dentro del servicio de seguridad para habilitar funciones CASB. La tecnología de inspección asocia usuarios a aplicaciones para hacer un control minucioso del uso de aplicaciones en la nube, independientemente de la ubicación o del dispositivo. Otras funciones incluyen control de funciones específicas de las aplicaciones, filtrado de URLs y contenidos, políticas basadas en el riesgo de las aplicaciones, políticas basadas en el usuario, Data Loss Prevention (Prevención de Pérdida de Datos – DLP) y prevención de malware conocido y desconocido. La asistencia ida y vuelta brindada por proxies garantiza estas capacidades exhaustivas, donde quiera que vayan los usuarios y cualquiera sea el dispositivo que usen.
- **Protecciones basadas en API** para conectarse directamente con las aplicaciones SaaS para la clasificación de datos, DLP y detección de amenazas. Prisma SaaS aprovecha este enfoque fuera de banda basado en API que permite la inspección minuciosa de todos los datos en reposo en la aplicación en la nube, así como también el monitoreo continuo de la actividad del usuario y las configuraciones administrativas. Este modo de implementación preserva la experiencia del usuario en la aplicación en la nube porque no es intrusivo, no interfiere ni depende de la ruta de datos hacia la aplicación en la nube.

Para conocer más por favor visite www.paloaltonetworks.com/prisma.

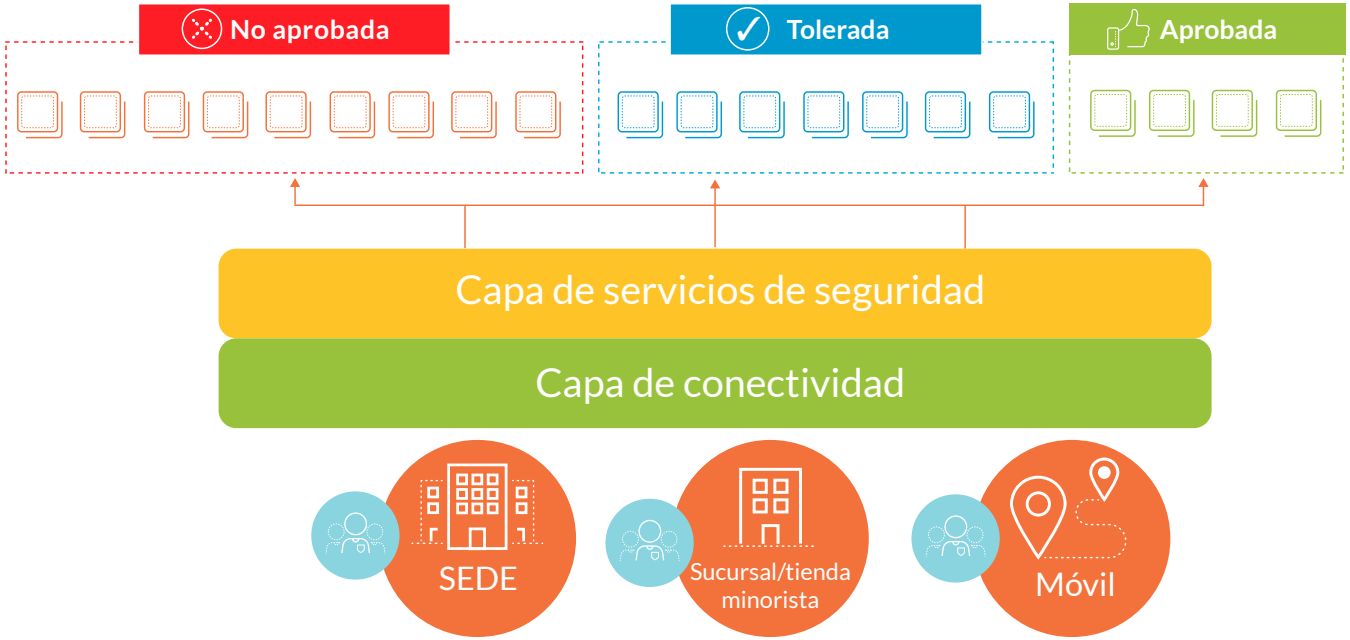


Figura 1: Modelo Prisma SaaS