SHARE:

Join Our Email List

Noticias y Actualidad Tecnológica

Nuestra misión es mantenerlo informado con las últimas noticias de investigación, productos y actualidad tecnológica, para que esté al día respecto a las tendencias nacionales y globales con énfasis en Ciberseguridad, eHealth y Smart Buildings.

McAfee MVISION Cloud CASB: Seguridad en la nube que agiliza a las empresas

McAfee

Protege los datos y detiene las amenazas en la nube en SaaS, PaaS e IaaS desde un único punto de aplicación nativo de la nube.

McAfee MVISION Cloud: Agente de Seguridad de Acceso a la Nube o Cloud Access Security Broker (CASB) le **permite proteger los datos y detener las amenazas en la nube desde un único punto de aplicación nativo de la nube**.

CASB es un software alojado en la nube o un software o hardware local que actúa como intermediario entre los usuarios y los proveedores de servicios en la nube. Además de proporcionar visibilidad, un CASB también permite a las organizaciones extender el alcance de sus políticas de seguridad desde su infraestructura local existente a la nube y crear nuevas políticas para el contexto específico de la nube. Los CASB se han convertido en una parte **vital de la seguridad empresarial**, lo que permite a las empresas **utilizar la nube de forma segura al mismo tiempo que protegen los datos corporativos confidenciales**.

Con MVISION Cloud eleve las **medidas de seguridad de datos en la nube**:

- **Visibilidad**: Obtenga visibilidad de todos los datos y el uso de la nube.
- **Control**: Tome el control de los datos y la actividad en la nube desde cualquier fuente.

- **Protección**: Protéjase contra las amenazas de la nube y la configuración incorrecta.

En Bafing somos el Partner principal de McAfee en la región sudamericana. McAfee sigue siendo sinónimo de confianza, seguridad e innovación a medida que cumplimos nuestra misión de mantener a las empresas a salvo de las ciberamenazas. La solución **MVISION Cloud** se ubicó como líder en todos los reportes del Cuadrante Mágico de Gartner en la especialidad de CASB, en los años 2018, 2019 y 2020.

Cuadrante Mágico para CASB McAfee en Gartner 2020

Fuente: Gartner, 2020.

Para más información sobre el tipo de análisis realizado por Gartner y los beneficios de la solución CASB, acceda al articulo completo **aquí**.

¿Por qué necesito un CASB?

A medida que los servicios que se ofrecían anteriormente en las instalaciones continúan migrando a la nube, mantener la visibilidad y el control en estos entornos es esencial para cumplir con los requisitos de cumplimiento, proteger a su empresa de ataques y permitir que sus empleados utilicen los servicios en la nube de manera segura sin presentar un alto riesgo adicional para su empresa.

Para mayor información sobre soluciones CASB para su empresa y sobre nuestras soluciones de Ciberseguridad, comuníquese con nosotros.

Contáctenos

Noticias destacadas de la semana

Informe: cuánto daño se produjo a partir de las 50 mayores violaciones de datos de múltiples partes

Riskrecon de MasterCard presentó el informe sobre el daño de los 50 incidentes cibernéticos multipartitos más grandes. En el estudio, se identificaron 50 de los incidentes cibernéticos multipartitos más importantes de los últimos años para comprender sus causas y consecuencias de principio a fin.

El estudio comprende ideas interesantes y resultados claves que incluyen: Los compromisos de la cadena de suministros llevaron a la mayor parte de las pérdidas financieras registradas ($7,4 mil millones) y al mayor número de empresas víctimas secundarias, el costo promedio de estos 50 eventos asciende a $90 millones, las intrusiones al sistema fueron el tipo de incidente más común y también afectaron a la mayoría (57%) de las organizaciones, entre otros. En el siguiente botón podrá descargar el informe completo.

Descarga el informe

Adobe envía alerta de seguridad dominado por parches críticos

Adobe ha lanzado una actualización de seguridad esta semana, abordando 92 vulnerabilidades en 14 productos.

De 92 vulnerabilidades de seguridad, 66 se clasifican como críticas en gravedad, y en su mayoría permiten la ejecución de código. Los más graves pueden dar lugar a la divulgación de información. La escalada de privilegios, la denegación de servicio y las fugas de memoria/divulgación de información también están presentes.

Más información: ThreatPost

Amenazas HTTPS crecen más del 314% hasta 2021

Un reciente informe sobre el estado de los ataques cifrados, destaca el crecimiento de las amenazas HTTPS desde enero, así como otros ataques que enfrentan las empresas de tecnología y los minoristas. Investigadores predicen un aumento de los ataques de ransomware en las plataformas de comercio electrónico durante la temporada navideña.

Se identificó que las amenazas HTTPS han aumentado en más del 314%, mientras que los ataques a las empresas de tecnología crecieron en un 2,300% y las empresas minoristas experimentaron un aumento del 800% en los ataques. Según el informe, la industria tecnológica representó el 50% de todos los ataques que rastrearon. Las instancias de malware aumentaron un 212% y el phishing aumentó un 90%.

Más información: ZDNet

Signal: Ahora permite informar y bloquear mensajes de spam

Signal ha agregado recientemente una forma sencilla para que los usuarios informen y bloqueen el spam directamente desde las pantallas de solicitud de mensajes con un solo clic del mouse. Las solicitudes de mensajes se agregaron a Signal el año pasado para

permitir que los nuevos usuarios se comuniquen con otros usuarios, incluso si no están en sus libretas de direcciones, y brindar más información contextual a los receptores.

Si bien los usuarios ya podían bloquear dichas solicitudes y eliminarlas, Signal ahora ha cambiado el cuadro de diálogo de bloqueo para incluir una opción "Informar de spam y bloquear" para informar mensajes no deseados y no solicitados.

Más información: Bleeping Computer

Facebook se convierte en Meta

El gigante de las redes sociales dio un paso muy importante dejando el nombre Facebook y renombrándose a sí mismo como Meta. El cambio fue acompañado por un nuevo logo corporativo diseñado como un símbolo en forma de infinito azul. Facebook y sus otras aplicaciones, como Instagram y WhatsApp, permanecerán pero bajo el paraguas de Meta.

La medida resalta cómo Mark Zuckerberg, planea reenfocar su compañía en lo que él ve como la próxima frontera digital, que es la unificación de mundos digitales dispares en algo llamado metaverso. Asimismo, cambiar el nombre de Facebook puede ayudar a distanciar a la empresa de las controversias de las redes sociales a las que se enfrenta.

Más información: The New York Times

Contáctenos

Equipo Comercial: info@bafing.com o al +51 969454618
Command Center y SOC: helpdesk@bafing.com o al +51-971500877

www.bafing.com

Acerca de Bafing

Somos una empresa con más de 25 años de experiencia en el mercado de Tecnologías que ofrece soluciones muy especializadas en Ciberseguridad, eHealth y Smart Buildings.
