INFORME

McAfee

Informe de adopción de la nube y riesgos

Edición relativa al teletrabajo

Informe de adopción de la nube y riesgos

Edición relativa al teletrabajo

La reciente exigencia de trabajar desde casa ha cambiado de manera radical nuestra manera de vivir y trabajar. Las empresas están innovando para poder seguir funcionando con productividad en un momento en el que la mayoría de los empleados teletrabajan. En condiciones normales, la mayoría de los empleados estarían trabajando en la oficina, dentro de la red interna. En el caso de los que trabajaran desde casa, se recurriría al uso de una VNP para acceder a las aplicaciones internas. En cualquier otro momento, solo un pequeño porcentaje de empleados estarían teletrabajando[1]. COVID 19 ha instaurado una nueva realidad. Ahora reina un vacío inquietante en oficinas, cines, calles y tiendas, y nuestras mesas de trabajo y salas de conferencias están acumulando polvo.

Pero, ¿cómo afecta esto al uso de los servicios en la nube? En marzo de 2020, casi al mismo tiempo que la mayoría de las grandes empresas imponían restricciones de viaje, se cancelaban grandes eventos empresariales, algunos países y estados dictaban orden de confinamiento, y un número mayor de personas empezaban a trabajar a distancia, Microsoft hacía público que sus servicios en la nube experimentaban un crecimiento del 775 %[2]. Si bien parte de este crecimiento puede considerarse normal, no cabe duda de que se ha producido un cambio fundamental en la actividad empresarial. El teletrabajo es la nueva normalidad. Incluso después de la pandemia, es posible que nuestra forma de trabajar no vuelva a ser nunca la misma.

Para aportar más información del impacto del teletrabajo en la adopción y uso de los servicios en la nube, McAfee ha utilizado datos de uso de la nube acumulados y anonimizados procedentes de más de 30 millones de usuarios de McAfee® MVISION Cloud en todo el mundo entre enero y abril de 2020. Este conjunto de datos representa a empresas de todos los sectores principales, incluido el de servicios financieros, atención sanitaria, sector público, educación, minoristas, tecnología, fabricación, energía, servicios, legal, inmobiliario, transporte y servicios empresariales.

Descubrimientos Principales

- En general, el uso empresarial de servicios en la nube experimentó un repunte del 50 %, con las empresas de fabricación y los servicios financieros a la cabeza.
- El uso de servicios de colaboración registró un aumento del 600 %. No sorprende que el sector de la educación sea el motor de este aumento, aunque seguido de cerca por el sector público y los servicios financieros.
- Los ataques externos contra cuentas en la nube aumentaron un 630% siendo los sectores público, de transporte y la fabricación los más afectados.

Síganos

Aumenta el uso general de servicios en la nube

Nuestros datos muestran un aumento global del 50 % en el uso empresarial de la nube en todos los sectores. En particular, el sector de la manufactura experimentó el mayor aumento con un 144 %, seguido del de la educación con el 114 %. Nuestro análisis mostró un aumento en todas las categorías de nube. Por ejemplo, en el sector de servicios financieros, el uso de servicios de colaboración, como Microsoft 365, aumentó un 123 %, mientras que también lo hacía el de servicios empresariales como Salesforce en un 61 %.

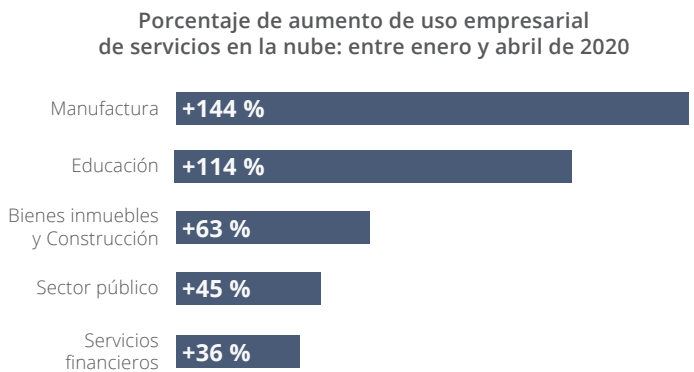


Figura 1. Aumento del uso de servicios en la nube por sector vertical.

El uso de servicios de colaboración experimentó el mayor crecimiento

El uso empresarial de servicios de colaboración en la nube ha aumentado más del doble desde principios de año con Zoom (+350 %), Microsoft Teams (+300 %) y Slack (+200 %) ocupando las primeras posiciones en cuanto a ganancias. Aunque Zoom ha recibido últimamente la mayor atención mediática, hemos observado un aumento incluso mayor en el uso de Cisco Webex, con una subida del 600 % durante el mismo período. Por segmentos sectoriales, los mayores incrementos del uso de servicios de colaboración se produjeron en los sectores de la manufactura y la educación. Si bien casi todos los sectores tienen una mayor necesidad de herramientas de colaboración remota, el sector de la educación ha sido el que ha experimentado cambios más drásticos, con clases online para estudiantes de todos los niveles.

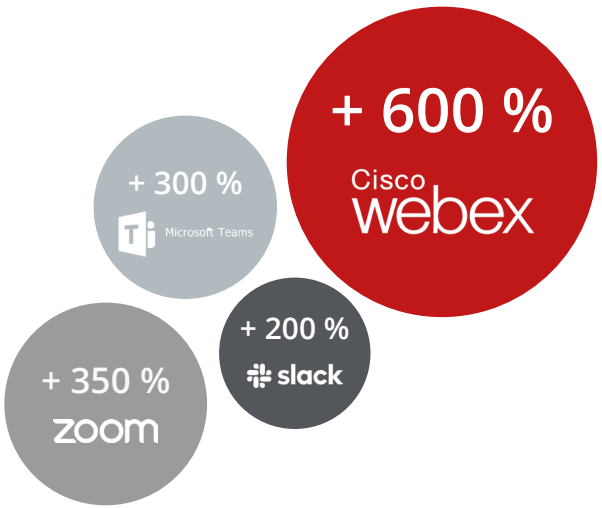


Figura 2. Incremento del uso de servicios de colaboración en la nube medido en la semana 11 de 2020.

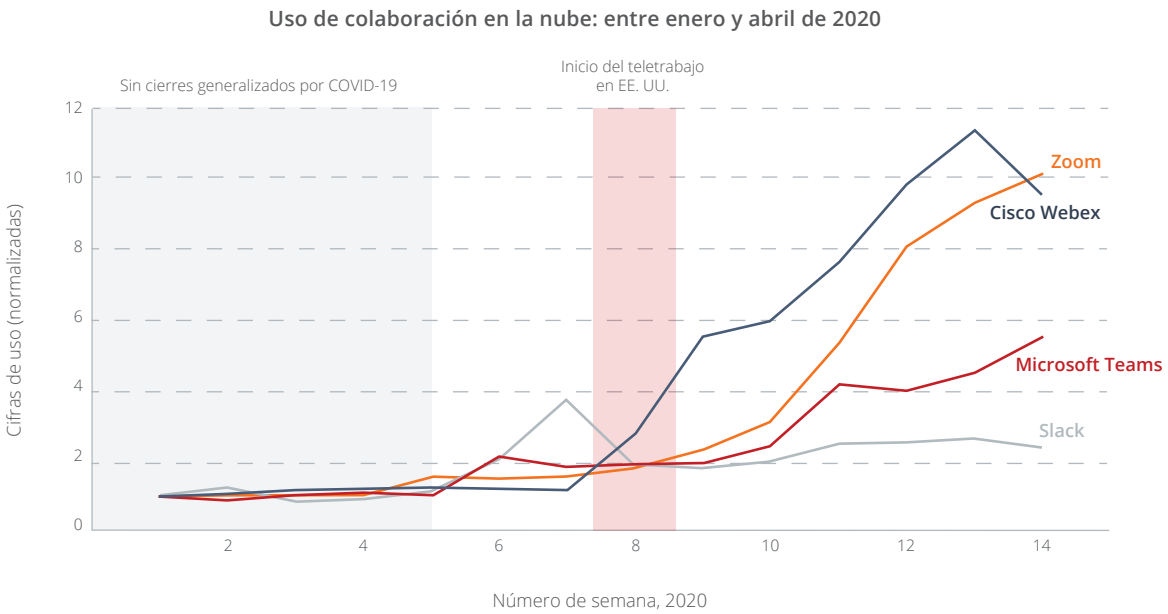


Figura 3. Uso de servicios de colaboración en la nube por semana.

El uso empresarial de la nube desde dispositivos no gestionados se multiplica por dos

También observamos que se duplicó el tráfico en la nube desde dispositivos no gestionados en todos los sectores verticales, lo que supone un aumento del riesgo cuando estos dispositivos acceden a los servicios en la nube fuera de las redes corporativas gestionadas.

No existe forma de recuperar los datos confidenciales de un dispositivo gestionado, por lo que este aumento del acceso podría dar lugar a la pérdida de datos si los equipos de seguridad no controlan el acceso a la nube por tipo de dispositivo.

Los autores de amenazas tienen a la nube en el punto de mira

La cantidad de amenazas de actores externos que atacan servicios en la nube aumentó un 630 %, con la mayor concentración en servicios de colaboración como Microsoft 365. A efectos de este análisis, hemos clasificado estas amenazas externas en dos categorías: uso excesivo desde una ubicación anómala y comportamiento superhumano sospechoso. Ambas requieren normalmente el uso de credenciales:

- **Uso excesivo desde una ubicación anómala.** Empieza por un inicio de sesión desde una ubicación que no se ha detectado anteriormente y que es anómala para la empresa del usuario. El ciberdelincuente entonces comienza a acceder a grandes volúmenes de datos y/o con privilegios.
- **Comportamiento superhumano sospechoso.** Se trata de un intento de inicio de sesión desde más de una ubicación geográficamente distantes, a las que es imposible viajar dentro de un período de tiempo determinado. Hemos observado este comportamiento en multitud de servicios en la nube; por ejemplo, si un usuario intenta iniciar una sesión en Microsoft 365 desde Singapur y después lo hace en Slack desde California cinco minutos más tarde.

Las categorías de amenazas internas han permanecido invariables. Esto indica que los empleados no actúan fuera de control e intentan robar más datos porque estén trabajando desde casa. La mayoría de los ataques que hemos observado son externos, amenazas nativas de la nube que atacan cuentas en la nube directamente.

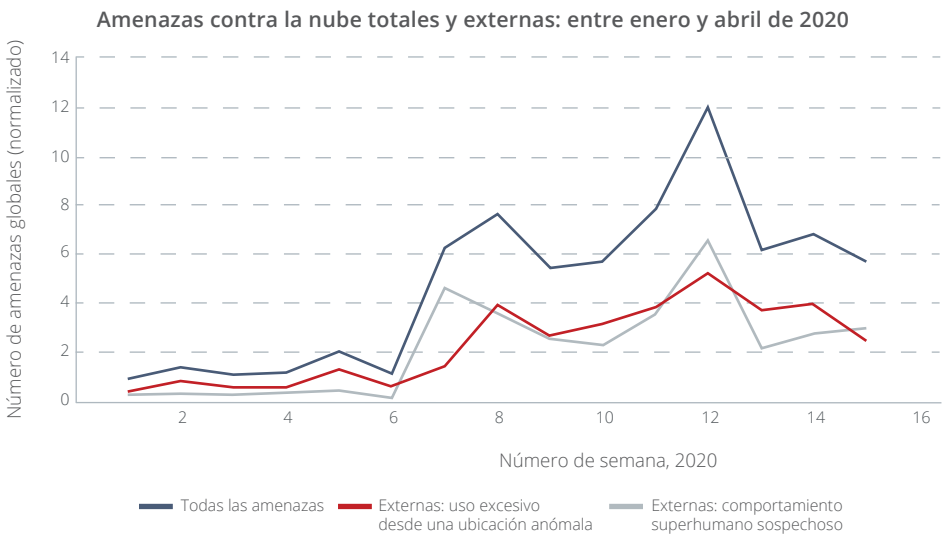


Figura 4. Eventos de amenazas contra la nube en todos los sectores.

Mercado vertical: amenazas contra la nube

Por sector vertical, vemos que el transporte y la logística, la educación y el sector público experimentaron los mayores incrementos en número de eventos de amenazas en sus cuentas en la nube, aquí mostrados tanto para amenazas internas como externas. Lógicamente, a medida que estos sectores se inclinan cada vez más por servicios en la nube para aumentar la productividad, los agresores les siguen el paso con intentos de acceder a sus cuentas y filtrar datos.

Aumento en porcentaje de amenazas contra la nube por sector vertical: entre enero y abril de 2020

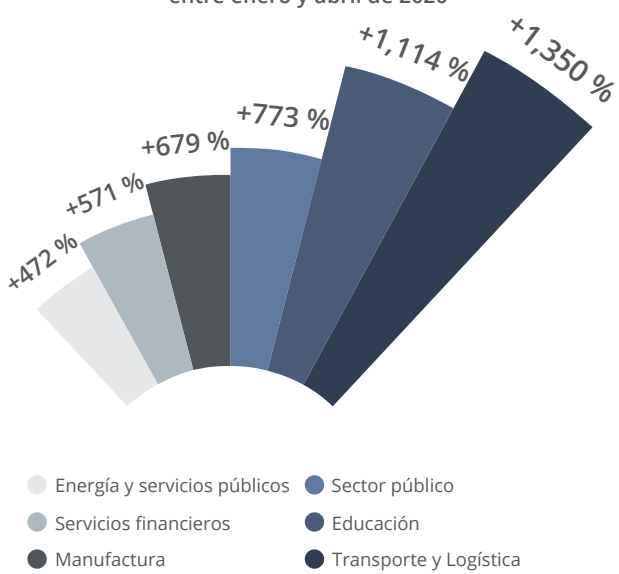


Figura 5. Aumento de los eventos de amenazas contra la nube por sector.

Centrándonos de nuevo solamente en las amenazas de actores externos, llevamos a cabo un análisis de las direcciones IP utilizadas en esos ataques para conocer las ubicaciones de las que procedían. Si bien la dirección IP de origen no puede utilizarse para determinar la atribución de un ataque, sigue ofreciéndonos una visión útil de los datos que puede ayudar con la implementación de controles de seguridad. Las direcciones IP supervisadas no se utilizaron solamente para atacar cuentas en la nube, sino también para otra actividad maliciosa, lo que apunta a la reutilización de la infraestructura delictiva para múltiples ataques.

En primer lugar, observemos los datos de forma global. En el siguiente gráfico, el tamaño del círculo indica el número de direcciones IP utilizadas para lanzar ataques, y la profundidad del color indica el número máximo de eventos de amenazas dirigidos contra una sola organización desde estas direcciones IP.

Geolocalización de direcciones IP de origen para amenazas contra la nube externas: entre enero y abril de 2020

Figura 6. Visión global de las fuentes de ataques externos contra cuentas en la nube por geolocalización de dirección IP.

Las 10 principales geolocalizaciones de direcciones IP de origen para ataques externos contra cuentas en la nube desde enero a abril de 2020 (ordenadas por las direcciones IP utilizadas) son:

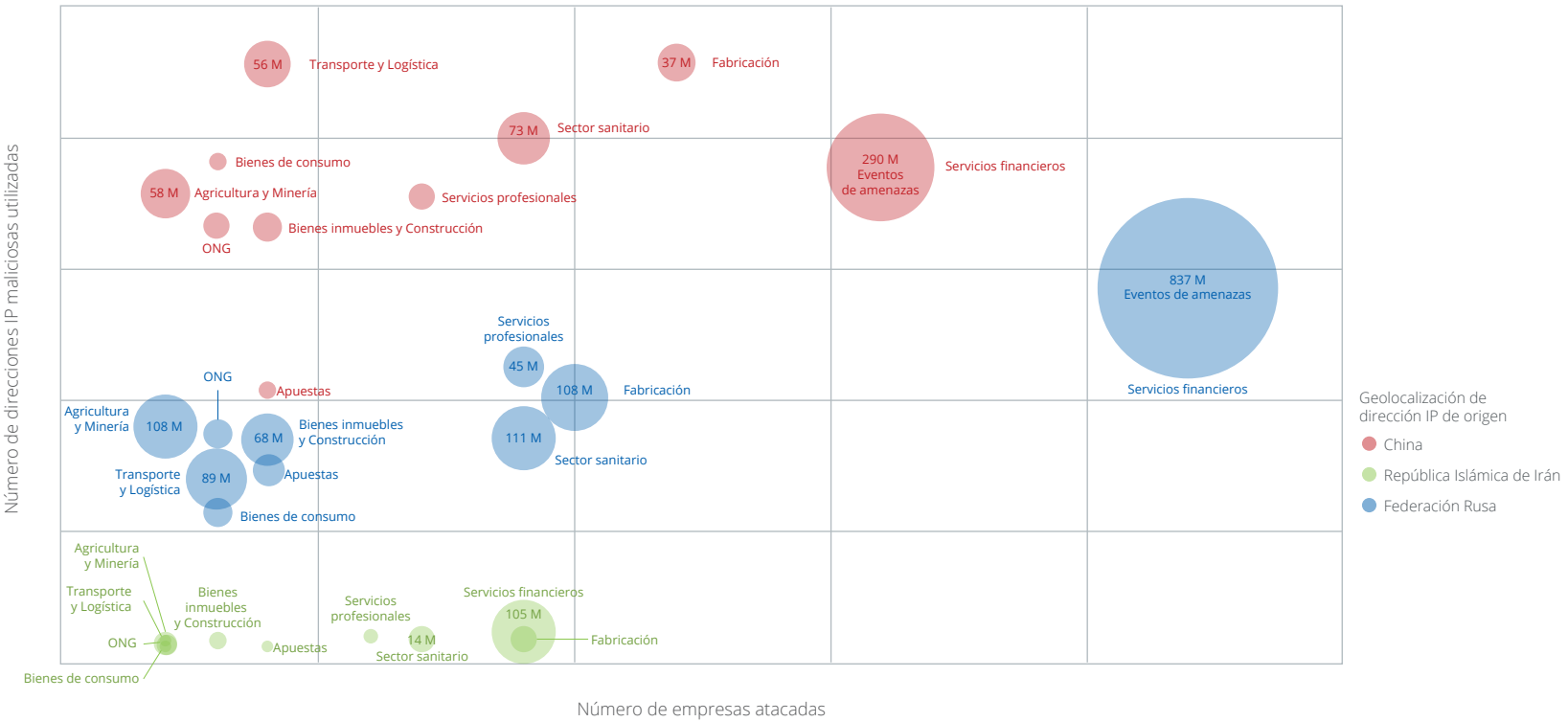
1. Tailandia
2. Estados Unidos de América
3. China
4. India
5. Brasil
6. Federación Rusa
7. Laos
8. México
9. Nueva Caledonia
10. Vietnam

Curiosamente, ninguno de los países de nuestro "top 10" se encuentra en Europa, región en la que se aplican algunas de las normativas más estrictas en materia de protección de datos del mundo. La mayoría procede de países históricamente activos en ciberdelincuencia y otros carecen de los recursos necesarios para aplicar normativas contra la ciberdelincuencia[3].

Muchos de estos ataques son probablemente oportunistas, y básicamente "bombardean" las cuentas en la nube con intentos de acceso mediante credenciales robadas. Sin embargo, algunos importantes sectores reciben a menudo los ataques de ciberdelincuentes externos, en particular el de los servicios financieros. A menudo, se termina sabiendo que estos ataques proceden de China, Irán o Rusia[4].

Podemos utilizar la geolocalización de direcciones IP de estos tres países para disponer de una visión más profunda de los sectores víctimas de ataques contra la nube externos. En el siguiente gráfico, el eje vertical muestra el número de direcciones IP utilizadas contra cada sector, donde un mayor número de direcciones IP indica una mayor infraestructura y financiación detrás de los ataques. El eje horizontal muestra el número de empresas de un determinado sector que están siendo atacadas, lo que nos da un sentido de la infraestructura de asignación de ataques entre sectores verticales. El tamaño de la burbuja nos muestra el volumen de los eventos de amenazas contra un sector específico, y los colores representan a Rusia, China o Irán.

Comparativa sectorial del volumen de amenazas contra la nube desde fuentes de ataques dirigidos comunes: entre enero y abril de 2020



En nuestro primer examen del impacto en los sectores verticales de las amenazas contra la nube externas, los servicios financieros tenían al quinto mayor incremento en el volumen de ataques. Si observamos las ubicaciones de origen más comunes de los ataques dirigidos, vemos que los servicios financieros experimentan el mayor volumen de ataques respecto a cualquier otro sector, y también tienen el mayor número de empresas afectadas. El sector de la atención sanitaria es el segundo más atacado, seguido del de la fabricación. Todas las empresas, pero en particular las que pertenecen a sectores muy atacados, necesitan supervisar continuamente su actividad en la nube para detectar y bloquear el acceso malicioso a sus datos confidenciales.

Resumen

Estos cambios drásticos en el uso empresarial de la nube están cercenando la eficacia de las soluciones de seguridad y red antiguas que tienen desplegadas muchas empresas. La infraestructura de VPN tiene dificultades para hacer frente a la gran oleada de teletrabajadores[5]. Las aplicaciones modernas como Microsoft 365 se distribuyen directamente a través de la nube y, sin embargo, muchas empresas todavía utilizan una arquitectura radial para enrutar el tráfico de la nube a través de dispositivos de seguridad en su centro de datos. En realidad, los empleados harán lo que sea más fácil y rápido. Desactivarán la VPN y accederán a las aplicaciones en la nube directamente.

Las directrices de teletrabajo e iniciativas de colaboración entre muchos sectores han puesto fin a los modelos arcaicos de conectarse a una red corporativa a través de una VPN antes de ir a una plataforma SaaS, PaaS o IaaS. Los nuevos modelos sin VPN necesitarán controles de acceso condicional para dispositivos personales y suministrados por la empresa, protección de datos completa, análisis reforzado del comportamiento de los usuarios y prevención de amenazas nativa para la nube con respuestas mediante directivas automatizadas para corregir los riesgos.

Los ciberdelincuentes han redoblado sus esfuerzos para aprovechar la distracción y los cambios repentinos provocados por la respuesta a la pandemia a nivel mundial. Hacen falta cambios importantes para implementar nuevos modelos de distribución de la seguridad en un entorno disperso de teletrabajo.

Sin embargo, los datos muestran que el incremento del riesgo de las amenazas nativas de la nube provocado por ciberdelincuentes que atacan servicios en la nube supera al riesgo consecuencia de los cambios en el comportamiento de empleados que simplemente trabajan en una ubicación nueva y remota.

Recomendaciones

La protección de una plantilla de teletrabajadores desplaza los principales puntos de control de seguridad al dispositivo y la nube. Un enfoque nativo para la nube de distribución de la seguridad proporcionará la cobertura más completa, capaz de llegar a dispositivos fuera de la red y que se conectan a servicios en la nube directamente. Las empresas pueden implantar un enfoque de seguridad nativa para la nube si:

1. Implementan un gateway seguro basado en la nube para que se pueda proteger a los dispositivos corporativos contra las amenazas basadas en la Web sin enrutar el tráfico a través de VPN.
2. Permiten a los usuarios conectarse a servicios en la nube autorizados desde sus dispositivos corporativos sin utilizar sus VPN, protegiendo los datos con un agente de seguridad de acceso a la nube (CASB).
3. Definen una directiva en su CASB de manera que los servicios en la nube tengan comprobaciones de dispositivos, controles de datos y estén protegidos contra agresores que pueden acceder a cuentas SaaS a través de Internet.

4. Implementan autenticación multifactor para los servicios en la nube autorizados cuando corresponda para reducir el riesgo de que se utilicen credenciales robadas para acceder a las cuentas.
5. Permiten a los empleados utilizar sus dispositivos personales para acceder a aplicaciones SaaS empresariales para mantener la productividad, con acceso condicional a datos confidenciales en la nube.

Más información

Para obtener más información sobre tecnología de seguridad en la nube, visite los enlaces siguientes:

- Soluciones de seguridad para la nube de McAfee®
- Seguridad para trabajar desde casa
- McAfee® Unified Cloud Edge (Secure Access Service Edge)

¿Está interesado en obtener más información? Póngase en contacto con McAfee para una sesión informativa personalizada con más detalles sobre estos datos, y para saber cómo las tendencias mencionadas en este documento pueden afectar a su empresa.

Metodología

McAfee MVISION Cloud es una plataforma que proporciona seguridad nativa para la nube para los servicios de plataformas SaaS, PaaS y IaaS.

Para ofrecerle estos resultados, se han utilizado datos de uso de la nube acumulados y anonimizados procedentes de más de 30 millones de usuarios de McAfee MVISION Cloud en todo el mundo, que en conjunto generaron miles de millones de transacciones y eventos de directivas diferentes en la nube cada día. Este conjunto datos, recopilados entre enero y abril de 2020, representa a empresas de todos los sectores principales, incluidos el de servicios financieros, atención sanitaria, sector público, educación, minoristas, tecnología, fabricación, energía, servicios, legal, inmobiliario, transporte y servicios empresariales.

1. https://www.owllabs.com/blog/remote-work-statistics
2. https://azure.microsoft.com/es-mx/blog/update-2-on-microsoft-cloud-services-continuity/
3. https://www.researchgate.net/publication/308775653_The_Current_State_of_Cybercrime_in_Thailand_Legal_Technological_and_Economic_Barriers_to_Effective_Law_Enforcement
4. https://www.mcafee.com/enterprise/en-us/about/newsroom/press-releases/press-release.html?news_id=20180221005206
5. https://www.theregister.co.uk/2020/03/11/corporate_vpn_coronavirus_crunch/

Acerca de McAfee

McAfee es una de las empresas de ciberseguridad independientes más importantes del mundo. Inspirándose en el poder de la colaboración, McAfee crea actividades y soluciones de consumo que hacen del mundo un lugar más seguro. Al diseñar soluciones compatibles con los productos de otras firmas, McAfee ayuda a las empresas a implementar entornos cibernéticos verdaderamente integrados en los que la protección, la detección y la corrección de amenazas tienen lugar de forma simultánea y en colaboración. Al proteger a los consumidores en todos sus dispositivos, McAfee protege su estilo de vida digital en casa y fuera de ella. Al trabajar con otras empresas de seguridad, McAfee lidera una iniciativa de unión frente a los ciberdelicuentes en beneficio de todos.

www.mcafee.com/mx.

Av. Paseo de la Reforma No.342 Piso 25
Colonia Juárez, México DF
C.P. 06600
www.mcafee.com/mx