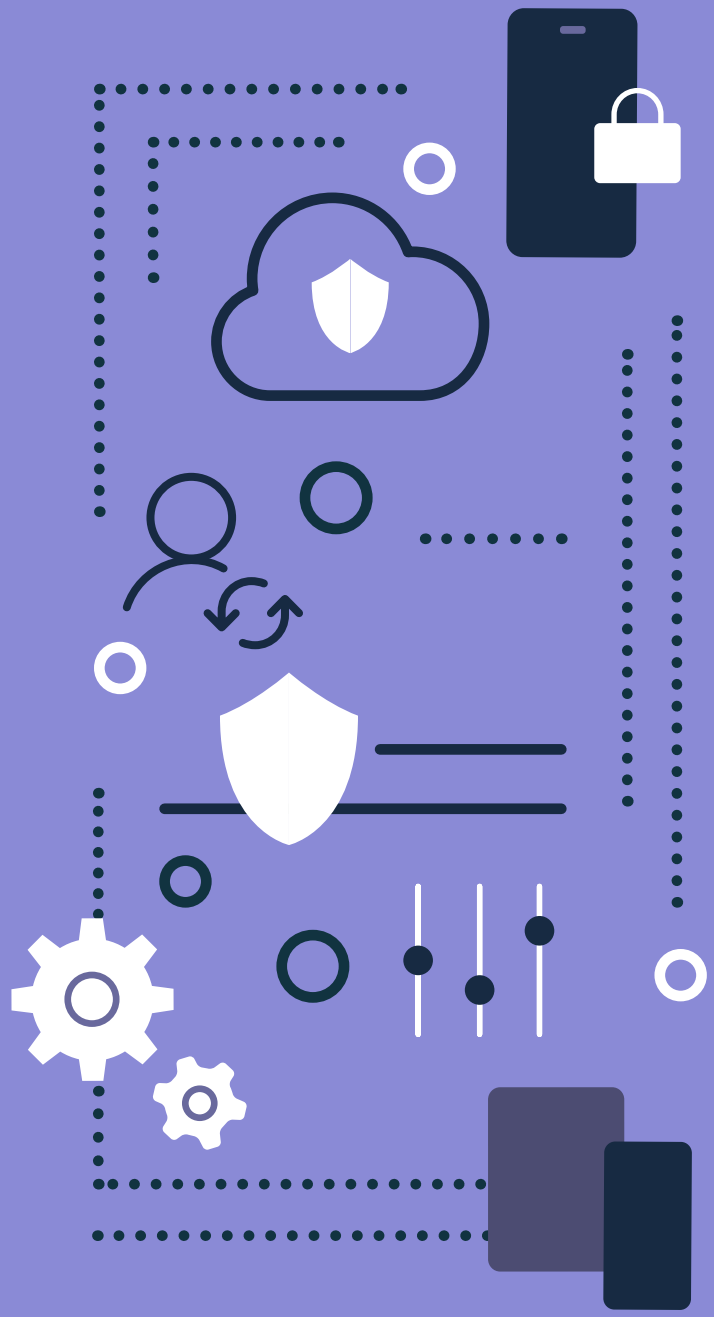


jamf

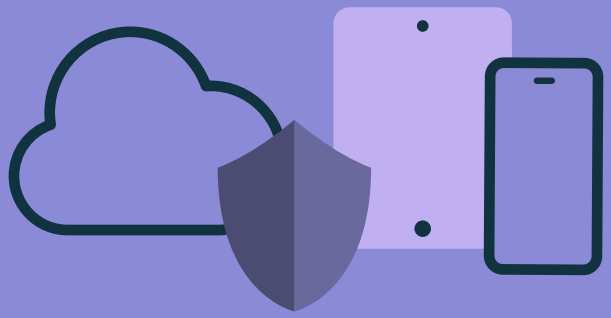
Guía esencial para

Antivirus para Mac

LA PREVENCIÓN DE MALWARE DIRIGIDA A DISPOSITIVOS MAC ES ESENCIAL A MEDIDA QUE LAS EMPRESAS SIGUEN AMPLIANDO SU FLOTA APPLE.

En general, Apple se defiende bien teniendo en cuenta que las detecciones están aumentando en todas las plataformas informáticas, mientras que las detecciones de malware específico parecen estar en calma en comparación con otros tipos de amenazas de malware más específicas.

A medida que las organizaciones han ido adoptando fuerzas laborales en remoto e híbridas, el panorama tecnológico ha cambiado drásticamente. En respuesta, los autores de malware y los actores de amenazas se están adaptando a estos cambios, modificando el alcance y la escala de las herramientas de malware de su arsenal. Al conjuntar varios tipos de amenazas a la vez, los agresores añaden complejidad, mientras que la mayor dependencia en la automatización permite que los objetivos se amplíen para incluir las herramientas de colaboración en las que los usuarios confían para seguir siendo productivos.



EN ESTA GUÍA, HABLAREMOS DE LO SIGUIENTE:

- Definiremos los antivirus (AV) enfocados en Mac
- Destacaremos cómo las amenazas de malware afectan cada vez más a los usuarios de Mac
- Explicaremos por qué comprender estas tendencias es tan vital para proteger los datos privados y...
- ...compartiremos lo que Jamf le ofrece para garantizar la protección de sus dispositivos Mac

ANTIVIRUS ENFOCADOS EN MAC

El antivirus es un requisito básico para que la mayoría de los dispositivos de la organización proporcionen una seguridad básica. Apple incluye un mecanismo antivirus básico en macOS con XProtect, Gatekeeper y MRT. Sin embargo, estas herramientas se actualizan de manera esporádica y las organizaciones carecen de visibilidad respecto a sus acciones. Las organizaciones requieren capacidades antivirus más sofisticadas para prevenir y poner en cuarentena el malware dirigido a dispositivos Mac y supera con creces lo que las soluciones destinadas a Windows son capaces de ofrecer en macOS.
Y no deberían esperar a que surgieran problemas de malware, adware u otro software no deseado.

Necesitan implementar un antivirus que identifique y remedie eficazmente los ataques específicos de Mac sin invertir valiosos recursos en la búsqueda de amenazas para Windows en un dispositivo Mac. Tanto para la seguridad como para la experiencia del dispositivo es vital contar con capacidades antivirus para Mac que sean eficaces, eficientes e integrales.

Ejemplos como la retransmisión de coordenadas GPS, el registro de mensajes descifrados y el monitoreo/grabación de llamadas telefónicas son solo algunos de los muchos problemas de privacidad que se vulneran, según un informe de Kaspersky Labs.

UN CAMBIANTE PANORAMA DE AMENAZAS

Se ha producido un notable aumento de las campañas de phishing que se aprovechan de las crisis contemporáneas, alimentándose de los temores y preocupaciones de las personas, sobre todo cuando se trata de bienes cuyo suministro ha sido limitado o afectado por la escasez mundial, incluidas las estafas relacionadas con el soporte técnico.

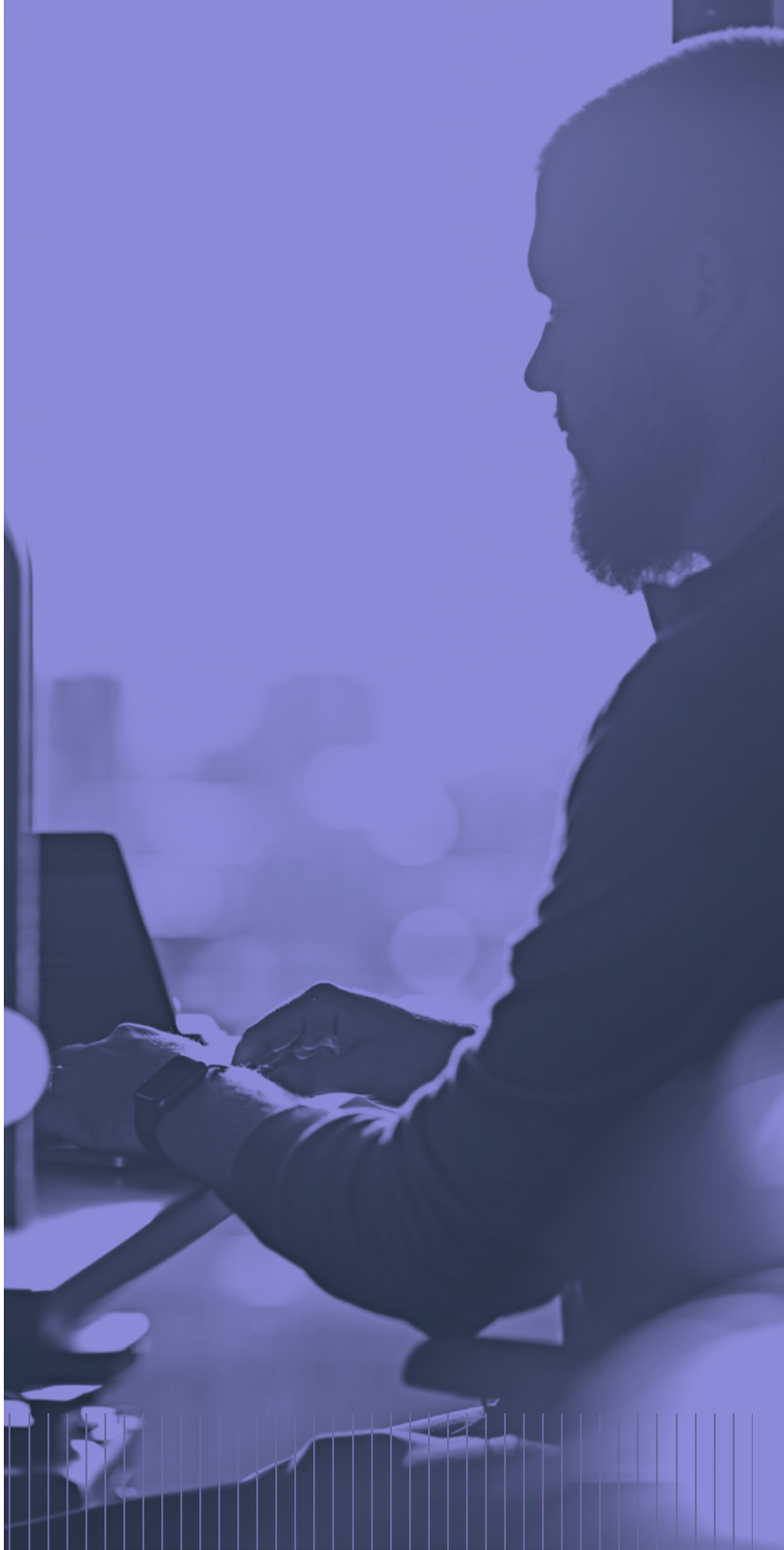
FISGONEO EN LÍNEA

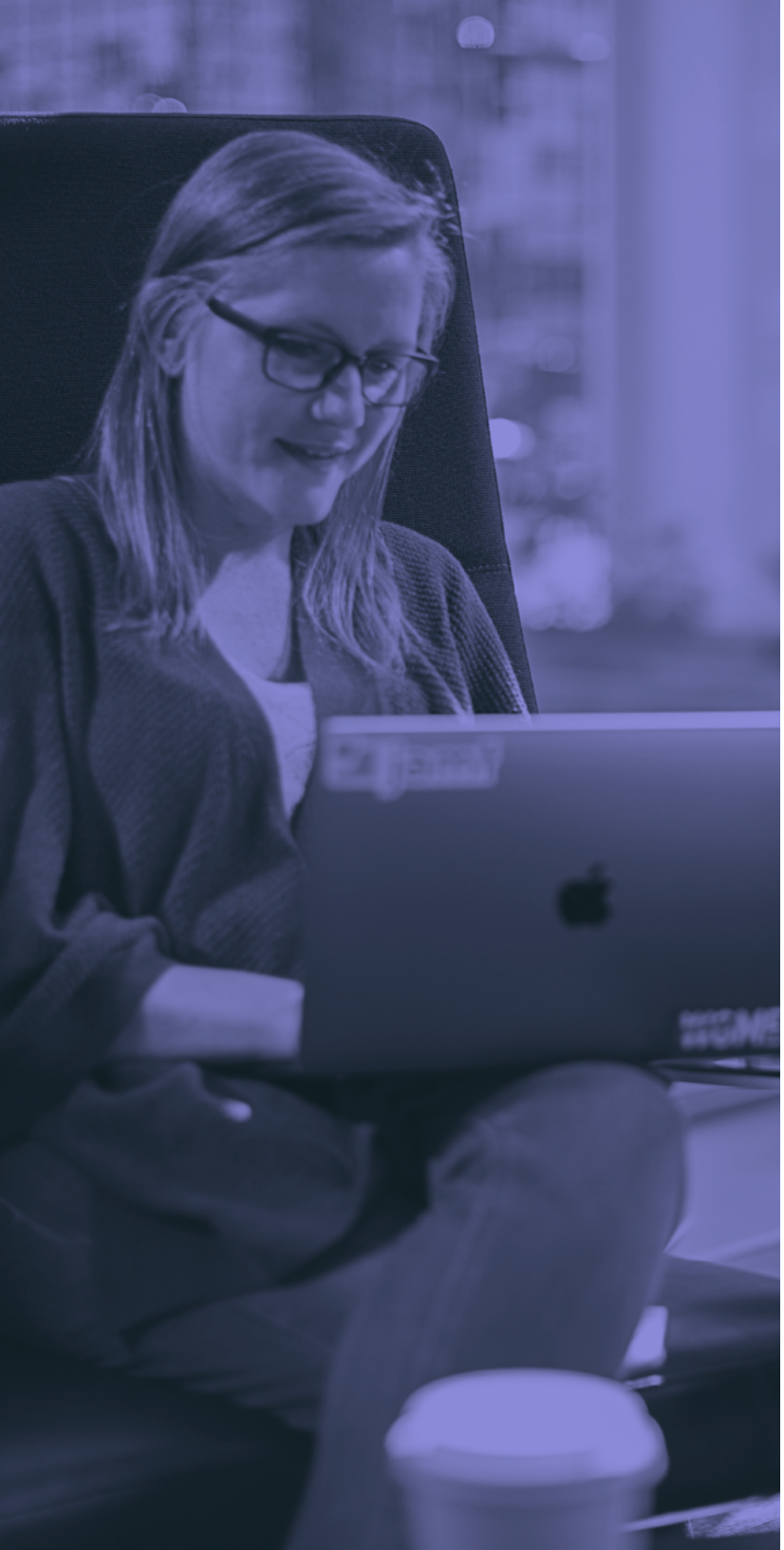
Adware, spyware, stalkerware son todos tipos de malware utilizados para obtener y extraer datos sobre los usuarios de computadoras. Este último, el stalkerware, se ganó el apodo de "fisgoneo en línea" porque aprovecha todo tipo de datos de identificación personal en tiempo real.

SE TRATA DE AJEDREZ, NO DE DAMAS

Al revisar esta información, es importante tener en cuenta que las amenazas suelen jugar a largo plazo, lo que significa que las campañas de ataque pueden durar tanto como sea necesario para tener éxito. No se limitan a introducir una sola pieza de malware en un dispositivo, sino que pueden seguir intentando obtener acceso y aprovechar cualquier punto de apoyo existente. Esto les permite disponer de tiempo para realizar los cambios necesarios en su estrategia o herramientas de ataque, reunir toda la información que deseen y, en última instancia, permitir que el malware se incruste más profundamente en los sistemas afectados.

Es cíclico: cada faceta influye directamente en la siguiente y la alimenta.





ESTADO DE LOS ANTIVIRUS PARA MAC

El crecimiento del malware continúa su tendencia al alza en general, con un total de 1,227,048,144 programas maliciosos identificados —incluidas las aplicaciones potencialmente no deseadas (PUA)— en 2022 por AV-Test.org. ¿El lado positivo para los usuarios de Mac? La distribución por sistemas operativos reveló que solo 220 de los programas maliciosos estaban dirigidos a macOS

Varios factores influyen en este cambio radical, entre ellos:

- El continuo crecimiento del mercado de Apple en el mundo empresarial
- Los consumidores eligen productos Apple de los programas de elección del empleado (o simplemente traen los suyos propios)
- El cambio global hacia trabajos a distancia e híbridos que usan programas para trabajar desde casa ha ampliado la línea de demarcación que solía dividir la oficina y el hogar

¡AÚN NO SAQUE LOS SOMBREROS DE FIESTA!

Aunque los usuarios particulares pueden considerar esta baja como un motivo de celebración, los datos telemétricos recogidos de diversas fuentes indican que los dispositivos utilizados en el espacio personal siguen siendo objeto de programas potencialmente no deseados (PUP), y va a la cabeza el adware.

Esto representa un problema totalmente diferente al que se está viendo en el ámbito empresarial, pero para los usuarios personales de productos Mac, los PUP y el adware representan un intento de atacar la información personal identificable (PII) del usuario —o una preparación para algo mucho peor más adelante— cuando se muestran anuncios maliciosos, se rastrean datos privados o se descarga una aplicación sospechosa que afirma que limpiará su Mac.

MALWARE PARA MEZCLAR Y COMBINAR

Mientras que el último ransomware novedoso conocido dirigido a Mac se detectó hace varios años, 2020 trajo EvilQuest a la vanguardia (también conocido como ThiefQuest). Este malware tiene todas las características de un ransomware, excepto las advertencias de cifrado y la petición de un pago para descifrar los archivos, que no es más que un subterfugio para ocultar su verdadera intención: el robo persistente y selectivo de datos personales y empresariales.

Los programas maliciosos de este tipo pueden evolucionar con el tiempo —al igual que el software normal— para incluir funciones adicionales que causan más daño, al tiempo que aumentan el sigilo para eludir la detección. Incluso puede actualizarse para evolucionar después de haber infectado un dispositivo. EvilQuest tiene todas las trazas de ser una historia en curso que habrá que seguir de cerca para ver cómo cambia en el futuro.

LOS PERROS VIEJOS PUEDEN APRENDER TRUCOS NUEVOS.

Clasificado en la categoría de "molesto por ahora", el malware de tipo adware también está evolucionando. Teniendo en cuenta que las nuevas versiones de macOS de Apple verifican la firma de las aplicaciones antes de permitir su ejecución, algunos autores de malware han hecho todo lo posible por salirse de la norma para acceder a los valiosos datos de su sistema y monetizar los anuncios que vea al navegar por Internet.

Algunos ejemplos de estos tipos de ataque pueden ser: duplicar la aplicación Safari en sí misma, modificándola e instalando extensiones no autorizadas para rastrear a los usuarios; utilizar perfiles de configuración —del mismo tipo que los que utilizan los administradores de IT para administrar los ajustes de los dispositivos—- para engañar a los usuarios y conseguir que los instalen en sus dispositivos; y conceder de forma efectiva a los actores de amenazas los tipos de acceso que necesitan para llevar a cabo más ataques.

También hay que tener en cuenta que, aunque el adware se considera menos peligroso, la combinación de ser la amenaza de malware más común entre los macOS y, al mismo tiempo, mostrar las formas más avanzadas de innovación en la forma de infectar los sistemas, por no hablar de la combinación con la capacidad cada vez más común de añadir remotamente nuevas cargas útiles de malware, puede amplificar su impacto.

TRABAJO MÁS INTELIGENTE, NO MÁS ARDUO

Por desgracia, no existe una solución única que resuelva la escalada de amenazas a la que nos enfrentamos actualmente. Una de las principales conclusiones es que las amenazas no vendrán siempre del mismo sitio. Los actores de las amenazas diversifican cada vez más sus tácticas y se dirigen a los dispositivos y servicios que producirán mayores resultados. Una cosa que afirman los datos es que los atacantes no muestran signos de detenerse.

¿Qué significa esto para todos los que dependen de las computadoras para vivir y trabajar? En términos sencillos, la seguridad debe configurarse para defender, desviar, prevenir o solucionar todas y cada una de las amenazas que se crucen en su camino. La vigilancia es una parte importante de la ecuación de la seguridad, ya sea que se derive de la capacitación de los usuarios sobre cómo detectar tipos de amenazas comunes, como los intentos de phishing, o de no instalar software desconocido.

Los equipos de IT y seguridad también deben incorporar prácticas de vigilancia en sus flujos de trabajo para reforzar y mantener la postura de seguridad de la organización en todo momento. La confianza en el software de detección para localizar las amenazas basándose en firmas conocidas o en la heurística, que realiza análisis de comportamientos para detectar amenazas desconocidas antes de que se produzcan, proporciona las ideas necesarias para comprender no solo de dónde proceden las amenazas dirigidas a su organización, sino también cómo protegerse contra ellas.

La rapidez de respuesta y la automatización van de la mano para responder rápidamente a las amenazas detectadas, al tiempo que se corrigen los problemas detectados, lo que es esencial para el éxito. Ambos ayudan a minimizar la superficie de ataque y a administrar mejor el riesgo de forma eficaz, al tiempo que añaden otra capa a la estrategia de defensa profunda.

Al fin y al cabo, cuando usamos dispositivos Mac es para hacer algo, probablemente no para escanear miles de líneas de código de una aplicación en busca de errores antes de lanzarla, ¿verdad? Es en estos momentos cuando recordamos que Apple se esfuerza por hacer que su experiencia de usuario sea excepcionalmente fácil de navegar para que los usuarios de Apple puedan crear algo extraordinario. Entonces, ¿por qué el software de seguridad no debería seguir esas mismas pautas?

INTEGRACIÓN JAMF + SOPORTE

Jamf Protect previene el malware y repara el comportamiento malicioso mediante la detección basada en firmas y el análisis del comportamiento en Mac. Con una visión descendente y granular de los dispositivos, los departamentos de IT y seguridad de las empresas pueden ver qué está afectando el rendimiento de los dispositivos desde el punto de vista de la seguridad. Además, cuando se combina con Jamf Pro, se habilita la administración centralizada de parches y la remediación para permitir la resolución de casi cualquier problema que pueda surgir. Por último, Jamf Connect completa esta trifecta de alta seguridad. La solución de Jamf Connect para la administración de identidades y accesos utiliza servicios de identidad basados en la nube para el acceso seguro a dispositivos y recursos.

Una defensa con una estrategia en profundidad que incluya las herramientas integradas de Apple y las amplíe con la potencia combinada de Jamf, le ayudará a mantener una seguridad eficaz de Mac que se integre de manera imperceptible con la experiencia del usuario final sin dejar de proporcionar toda la información y los análisis pertinentes sobre sus dispositivos. Esta estrategia por capas permite a los informáticos tomar la mejor decisión en lo que respecta a la protección de sus dispositivos y la salvaguarda de los datos de los usuarios.

Jamf —el estándar en administración de Apple en el trabajo— tiene los productos y soluciones que le ayudarán a activar la mejor estrategia de seguridad para su organización y sus usuarios.

Lo llamamos Trusted Access.
Más información.

NO SOLO SE CONFORME CON NUESTRA PALABRA,

ponga a prueba la protección antivirus y de terminales.

Cuando esté preparado para proteger su flota de Mac frente a las crecientes amenazas de seguridad, el malware conocido y para corregir comportamientos maliciosos, pruébenos de forma gratuita o póngase en contacto con su distribuidor preferido.

Solicite una prueba gratuita

o comuníquese con tu distribuidor Apple preferido cuando esté listo para reforzar su seguridad.

Más información sobre Jamf Protect y la protección de terminales de Mac en jamf.com/es/