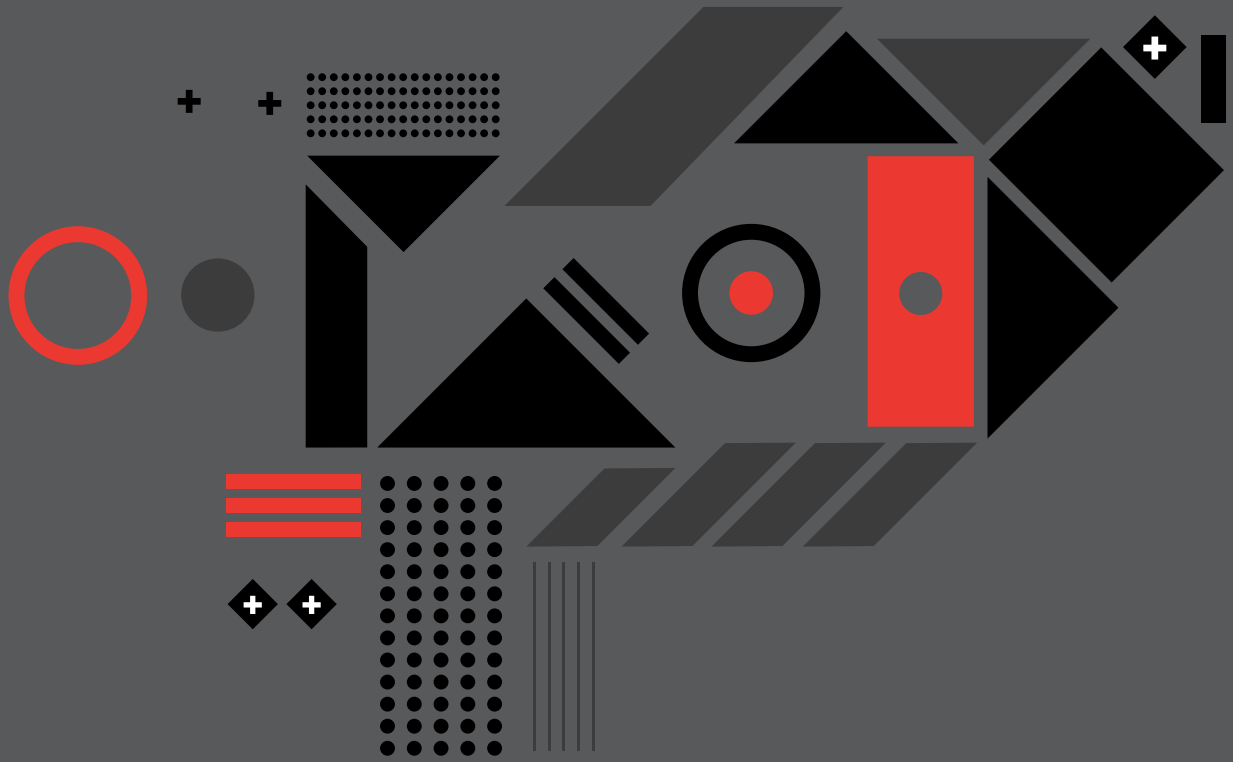
Libro electrónico



TRABAJA DESDE CUALQUIER LUGAR CON TOTAL SEGURIDAD

PROTEGE A TU PLANTILLA HÍBRIDA Y TUS DATOS, Y REFUERZA LA RESILIENCIA DE TU NEGOCIO CON LA PLATAFORMA CROWDSTRIKE FALCON EN AMAZON WORKSPACES

CROWDSTRIKE | aws

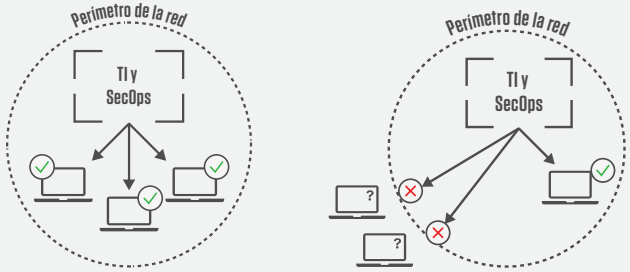
ÍNDICE

LAS PLANTILLAS REMOTAS ABREN UNA BRECHA EN EL PERÍMETRO DE SEGURIDAD

El teletrabajo ha llegado para quedarse y se impone un modelo híbrido en el que algunos empleados trabajan siempre a distancia, otros vuelven a la oficina y otros combinan las dos opciones y solo van a la oficina algunos días de la semana. En este mundo en el que se puede trabajar desde cualquier lugar, los retos para garantizar la seguridad y la resiliencia del negocio se multiplican, especialmente ahora que la mayoría de las empresas se afanan por cumplir objetivos recortando gastos.

La adopción acelerada de la nube favorece el trabajo híbrido

Entre las empresas que han optado por el teletrabajo, muchas se han visto obligadas a acelerar la adopción de las tecnologías en la nube, por ejemplo, trasladando sus modelos de ciberseguridad locales a soluciones alojadas en la nube. Ahora que el teletrabajo se ha implantado definitivamente, estas empresas observan que los enfoques que aplicaron en condiciones de urgencia y presión operativa extremas ya no bastan para proteger a largo plazo a su personal híbrido ni sus datos.



Como respuesta, las empresas con visión de futuro están adoptando un enfoque de ciberseguridad nativa en la nube basada en una infraestructura que protege a todo el mundo, en cualquier lugar.

Protección en tiempo real

Prevención de amenazas, detección de la actividad sospechosa y respuesta a los incidentes, todo en tiempo real, dondequiera que se encuentren tus empleados o dispositivos.

Protección de endpoints

Eliminación de la complejidad, simplificación del conjunto de soluciones de seguridad y despliegue en tiempo récord. Activa de manera inmediata la gestión de vulnerabilidades y la higiene de TI con Falcon Spotlight™ y Falcon Discover™.

Para todos los dispositivos

Un solo agente ligero de Falcon funciona en cualquier lugar, incluso en cargas de trabajo en la nube y en datacenters, protegiendo a los usuarios tanto en los dispositivos propiedad de la empresa como en los suyos propios.

Seis factores clave que pueden garantizar la ciberseguridad de los teletrabajadores

1. Asegúrate de contar con una política de ciberseguridad actualizada que incluya el teletrabajo.
2. Planifica el uso de los dispositivos propiedad de los empleados (BYOD) que se conectan a tu empresa.
3. Ten en cuenta que es posible que se acceda a datos confidenciales a través de redes Wi-Fi no seguras.
4. La visibilidad y la higiene de ciberseguridad son fundamentales.
5. La comunicación y la formación continua de los usuarios son extremadamente importantes, y es recomendable garantizar que los trabajadores a distancia puedan ponerse en contacto rápidamente con el departamento de TI para recibir asistencia.
6. Es necesario que la plantilla remota sea capaz de poner en práctica los planes de gestión de crisis y respuesta a incidentes.

PROTEGE A TU PERSONAL HÍBRIDO CON FALCON Y AMAZON WORKSPACES

Protección de las identidades de tus empleados y tus datos

Con Amazon WorkSpaces, los teletrabajadores disponen de una solución segura de escritorio como servicio (DaaS) que les proporciona acceso a sus equipos dondequiera que trabajen. Instalar el sensor de CrowdStrike Falcon en un entorno de Amazon WorkSpaces mejora aún más tu postura de seguridad y te permite mitigar el riesgo de sufrir amenazas.

Amazon WorkSpaces ofrece una solución DaaS para el personal híbrido.

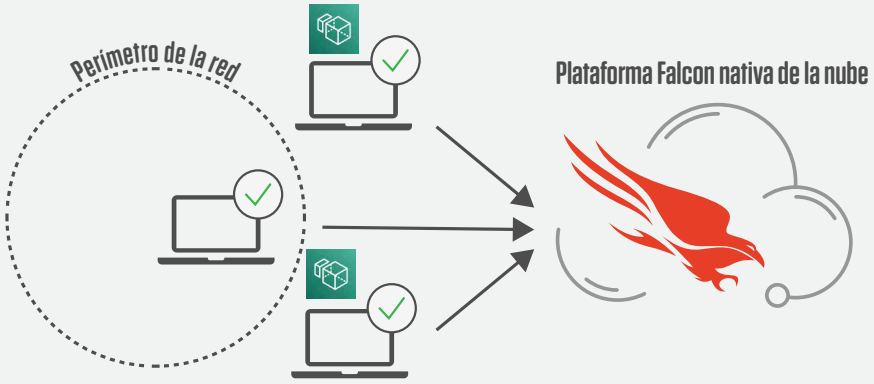
- Un escritorio en la nube al que se puede acceder desde cualquier lugar con una conexión a Internet.
- Se ejecuta directamente en una amplia gama de dispositivos, incluidos PC, Mac y iPads.
- Elimina las tareas administrativas, como el aprovisionamiento, el despliegue y el mantenimiento de los equipos de sobremesa.

La plataforma CrowdStrike Falcon detiene las brechas mediante una seguridad sin fricciones y una protección de los endpoints nativa en la nube.

- Instalación rápida desde la nube mediante una solución SaaS para mantener todos los dispositivos protegidos, dondequiera que se encuentren.
- Fácil transición a la protección de todos los modelos de trabajo, sin sacrificar el rendimiento.
- Reducción de la complejidad con una solución SaaS alojada en la nube que no requiere hardware y que ayuda a reducir los costes operativos.

LA ESTRATEGIA DE SEGURIDAD DE CROWDSTRIKE PROTEGE CONTRA LAS BRECHAS

El sensor ligero de Falcon se instala fácilmente en el entorno de WorkSpaces de los usuarios finales y proporciona una configuración segura de teletrabajo. Estas soluciones nativas en la nube combinadas ayudan a garantizar la continuidad de la actividad empresarial protegiendo contra amenazas emergentes, facilitando una solución híbrida y recortando costes gracias a la reducción de los gastos generales.



80 %
de las brechas de seguridad se deben al uso ilícito de credenciales

Acaba con los ciberdelincuentes más nocivos

Las nuevas amenazas aprovechan las vulnerabilidades de la plantilla híbrida, por lo que es esencial contar con la seguridad de una red virtual privada Amazon VPC, además de la protección de endpoints que proporciona Falcon. Protege a tus trabajadores híbridos con una solución de ciberseguridad que combina aprendizaje automático, inteligencia artificial y Threat Hunting proactivo.

Respuesta, recuperación y corrección a distancia

Falcon facilita la protección remota para salvaguardar los datos, cargas de trabajo y dispositivos de tus empleados, con independencia de donde se encuentren. Corrige rápidamente los hosts remotos con una potente solución nativa en la nube.

Contrarresta los costes para reforzar la resiliencia

Las soluciones de escritorio como servicio a través de WorkSpaces y la arquitectura nativa en la nube de Falcon reducen considerablemente tus necesidades de hardware, así como de dispositivos y software. Adopta un enfoque totalmente gestionado para reducir los gastos generales y mejorar la resiliencia de la empresa.

PROTECCIÓN FRENTE A LOS ADVERSARIOS MÁS AUDACES

Detrás de cada ciberataque hay un adversario humano. Estos ciberdelincuentes evolucionan continuamente y aprovechan acontecimientos relevantes para disfrazar sus ataques.

CrowdStrike está siempre al día de las amenazas emergentes y ha elegido el sensor de Falcon para proporcionar una visibilidad profunda de las vulnerabilidades. Integrado con Amazon WorkSpaces, el sensor de Falcon te ayuda a vigilar para garantizar la seguridad de tu personal híbrido y tus datos en la nube.

Seguridad a partir de la nube

Amazon WorkSpaces se despliega en redes Amazon VPC, que proporcionan a cada usuario acceso continuo a volúmenes de almacenamiento cifrado en la nube AWS y que se integran con AWS Key Management Service. No se almacenan datos del usuario en el dispositivo local, lo que mejora su seguridad y minimiza la superficie de riesgo incluso para los trabajadores híbridos.

Detección y prevención de amenazas en tiempo real

Falcon, que incorpora inteligencia de Threat Graph, ofrece funciones extremadamente eficaces de detección y prevención de amenazas conocidas y desconocidas en tiempo real. Los endpoints están protegidos de los ciberdelincuentes 24x7.

Falcon no solo se centra en el malware, ya que emplea una estrategia que no solo identifica los indicadores de compromiso, sino también los indicadores de ataque.

MEJORES PRÁCTICAS DE CIBERSEGURIDAD PARA UN MUNDO HÍBRIDO

En un mundo de teletrabajo, la ciberseguridad requiere un enfoque diferente. Los sistemas que protegen a los usuarios en una oficina necesitan herramientas de análisis que consumen un gran ancho de banda para identificar sistemas, evaluar parches y detectar vulnerabilidades. Sin embargo, en el caso del trabajo híbrido, esta configuración no es factible. Cuando los empleados entran y salen de la oficina, y acceden a los datos desde dispositivos gestionados y no gestionados, crean enormes puntos ciegos para el personal de seguridad de TI y generan riesgos que pueden lastrar los esfuerzos para corregir las amenazas.

Para responder a los retos de ciberseguridad que plantea el nuevo modelo de trabajo, los expertos de CrowdStrike ofrecen las siguientes recomendaciones.

Incorpora tecnología para empoderar a tu personal

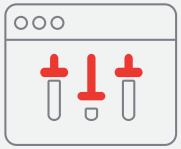
El diseño de una estrategia de ciberseguridad integral y eficaz comienza por el análisis de las políticas, procesos y tecnologías empleadas en todas las funciones de la empresa. Las estrategias de ciberseguridad más eficaces combinan recursos humanos con soluciones tecnológicas avanzadas, como la inteligencia artificial, el aprendizaje automático y otras formas de automatización inteligente, para detectar mejor cualquier actividad anómala y mejorar el tiempo de respuesta y corrección.

Elige tu nube con cuidado

No todas las nubes son iguales en cuanto a cómo aprovechan las ventajas que ofrece esta tecnología, sin poner en riesgo la seguridad. Amazon Web Services (AWS) se creó siguiendo los estándares de seguridad de datos más exigentes, con controles detallados de identidad y acceso, para proporcionar una visibilidad excelente. Las funcionalidades de prevención y detección de CrowdStrike para Amazon Workspaces, líderes en el sector, ayudan a tus teletrabajadores, sin afectar a la continuidad de tu actividad empresarial.

Aplica la respuesta, recuperación y corrección a distancia

Los ataques y las intrusiones no van a desaparecer y debes estar seguro de contar con los recursos y funcionalidades necesarias para responder desde cualquier lugar y mantener así tu empresa protegida. La arquitectura de la nube de Amazon WorkSpaces y Falcon garantiza la protección en tiempo real de cualquier carga de trabajo, dondequiera que se encuentre, incluso si está fuera de un firewall.



Simplifica el uso de DaaS

Al ser un servicio en la nube, con Amazon WorkSpaces hay menos inventario de hardware que gestionar y no se requieren complejos despliegues de infraestructura de escritorio virtual que no se pueden escalar. Amazon WorkSpaces está disponible en 13 regiones de AWS y proporciona acceso a escritorios en la nube de alto rendimiento, allí donde trabajen tus equipos.

LA IMPORTANCIA DE LA GESTIÓN DE COSTES EN TODA ESTRATEGIA DE SEGURIDAD

Una sensación de incertidumbre se apodera de empresas de todo el mundo. Con el objetivo de aumentar la resiliencia del negocio, las empresas han interrumpido las iniciativas encaminadas al crecimiento, han bloqueado presupuestos y han comenzado a acumular reservas de efectivo. Amazon WorkSpaces y Falcon les ofrecen una forma de garantizar las operaciones comerciales con seguridad y contener los costes.

Una arquitectura en la nube rentable

La administración centralizada que ofrece Amazon Workspaces para teletrabajadores ayuda a escalar el acceso a los escritorios en la nube. Y, para continuar apoyando a tu personal híbrido, no hay necesidad de planificar, preparar y adquirir hardware ni software para mantenerse al día, lo que le permite ahorrar tiempo y dinero. Además, con Amazon WorkSpaces no es necesario adquirir demasiados equipos de sobremesa y portátiles, ya que ofrece acceso bajo demanda a escritorios en la nube que incluyen distintos recursos de computación, memoria y almacenamiento adaptado a las necesidades de rendimiento de tus trabajadores híbridos. La plataforma CrowdStrike Falcon analiza todos los endpoints para garantizar su seguridad, con independencia de donde se encuentren y sin afectar al rendimiento.

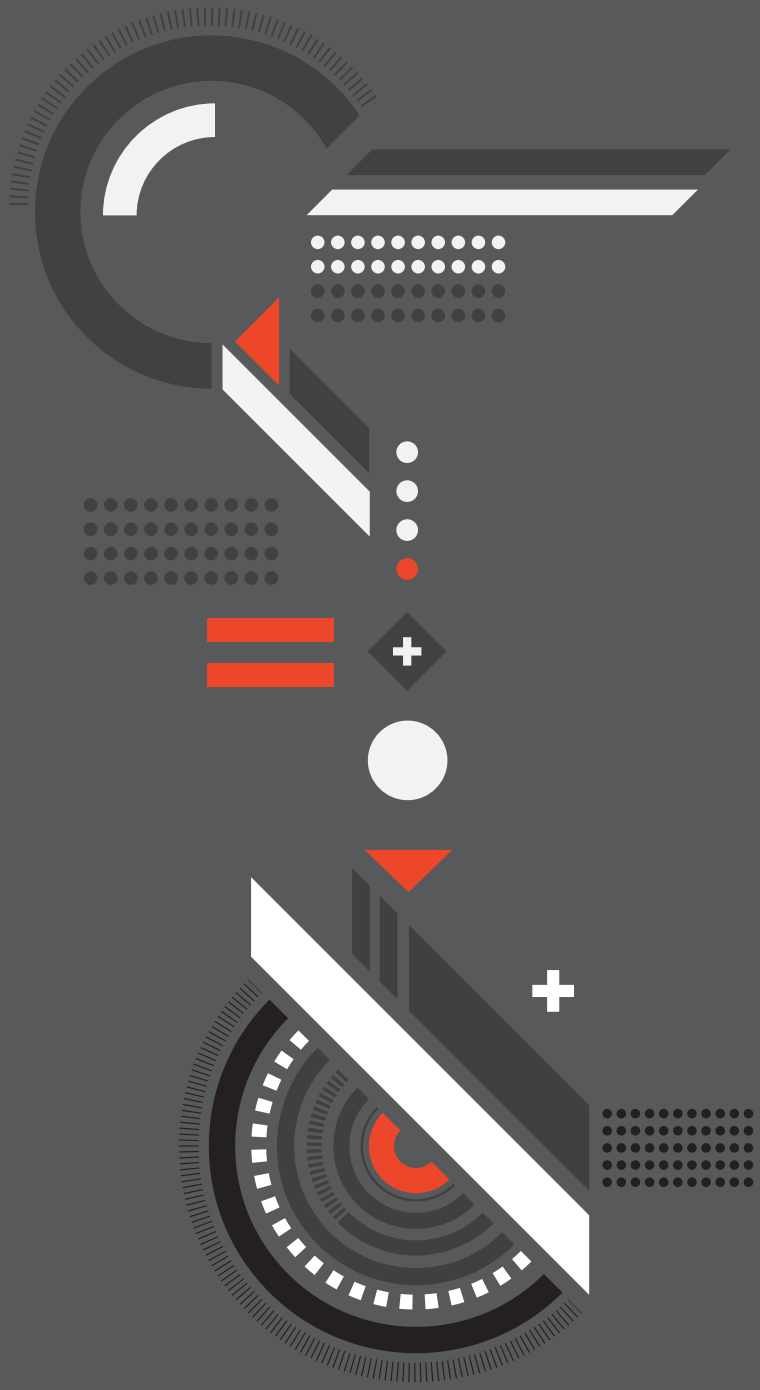
Totalmente gestionado para reducir los gastos generales

Las empresas tienen la opción de reforzar su ciberseguridad desplegando la protección de endpoints de Falcon como un servicio completamente gestionado. Con esta solución puedes confiar la implementación, administración y respuesta a incidentes de seguridad de endpoints al equipo de expertos en seguridad acreditados de CrowdStrike. El resultado es una postura de seguridad que se optimiza de manera instantánea, sin la carga, los gastos generales ni el coste de administrar internamente un programa de seguridad de endpoints global.

HA LLEGADO EL MOMENTO DE PROTEGER EL TRABAJO DESDE CUALQUIER LUGAR

Con CrowdStrike es fácil comenzar. Para obtener más información sobre cómo implementar la plataforma CrowdStrike Falcon y Amazon Workspaces, **utiliza nuestra prueba gratuita de 15 días**.

Para obtener más información sobre las soluciones de CrowdStrike y AWS, visita **CrowdStrike** o **AWS Marketplace**.



aws marketplace