ZIMPERIUM®

# Manual del CISO para habilitar el acceso de O365 en dispositivos móviles:

## Gestionado o BYO (Traído por uno mismo)

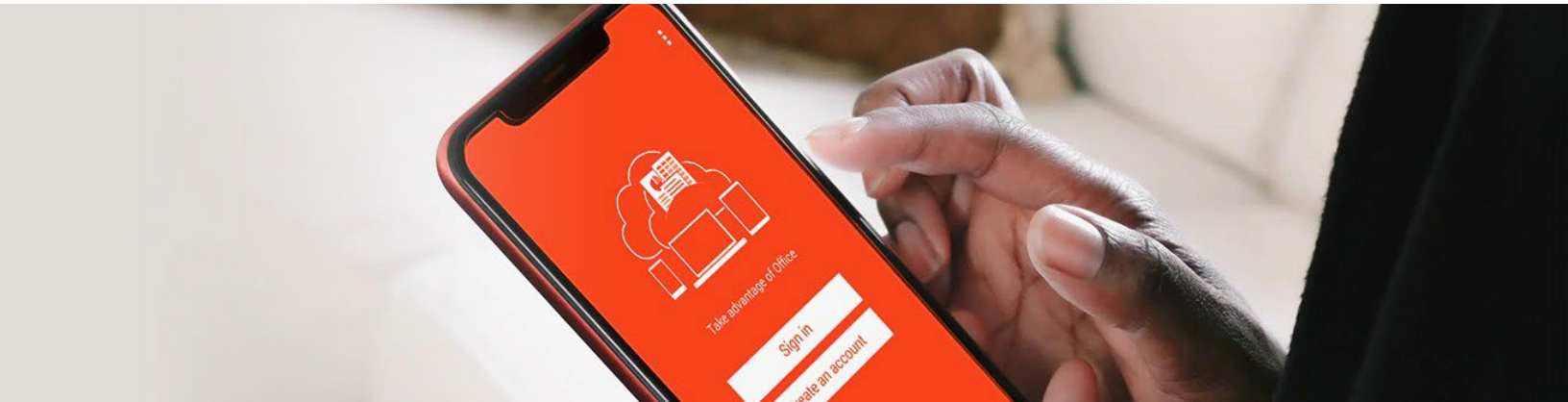
# Introducción

Aproximadamente el 84 % de las organizaciones tienen Office 365 (O365) habilitado en los dispositivos móviles de los empleados, pero más del 50 % no han implementado soluciones de defensa contra amenazas móviles (MTD) para evitar que se vean comprometidas. Teniendo esto en cuenta, pedimos a Eric Green, que trabaja en la protección de operaciones comerciales en TikTok, que comparta sus perspectivas sobre lo que las organizaciones deberían hacer ahora para garantizar que el acceso móvil a O365 sea transparente y seguro.

**Z (Zimperium): Preparemos el escenario y establezcamos un contexto para este tema, ya que asegurar de manera efectiva el acceso móvil a O365 había sido un desafío, incluso antes de que llegara la pandemia. ¿Cuál fue el ambiente, su actitud y la de su equipo cuando comenzó el confinamiento en marzo de 2020?**

**Eric:** Me encontraba en mi octavo mes como Jefe Global de Mobile & Mac Security en HSBC. Nadie estaba preparado para los enormes desafíos operativos y de seguridad a los que en poco tiempo nos enfrentaríamos. Casi de la noche a la mañana, tuvimos un aumento masivo en el número de empleados que necesitan acceso móvil a O365. Eso fue problemático ya que **O365 en el móvil proporciona a los usuarios el mismo nivel de acceso a los datos empresariales confidenciales y personales, como ordenadores de sobremesa y portátiles totalmente seguros.** Tuvimos que actuar muy rápidamente para garantizar que el acceso fuera seguro. Afortunadamente, ya teníamos una sólida estrategia de MTD.

[1] Preguntas de encuesta rápida, diciembre de 2021 y enero de 2022 - home.pulse.qa -



## Z: ¿Cómo gestionaban sus homólogos la seguridad del acceso móvil O365 en otras compañías?

**Eric:** La mayoría de las organizaciones adoptaron el enfoque tradicional, implementando soluciones UEM (incluyendo MDM y MAM), como Microsoft Intune para controlar el acceso a O365 y otros recursos de teléfonos móviles, tabletas y ordenadores portátiles.

Las soluciones UEM proporcionan la visibilidad necesaria para monitorear y hacer cumplir la autenticación de usuarios, el acceso a los datos y las políticas de uso aceptable. Cuando se supera un nivel de riesgo, también pueden aplicar soluciones automatizadas, como deshabilitar una aplicación O365, borrar el dispositivo o desconectarlo. **B Pero las soluciones UEM no pueden detectar ataques sofisticados de phishing, malware, dispositivos y redes.** El riesgo para las empresas ha aumentado exponencialmente con el rápido aumento de los dispositivos propiedad de los empleados. La pandemia incrementó drásticamente una superficie de ataque amplia y vulnerable que ya era extremadamente difícil de vigilar y proteger.

## Z: Algunas organizaciones han planteado que las VPN pueden ayudar a proteger O365 en dispositivos móviles. ¿Por qué no proporcionan suficiente protección?

**Eric:** Las VPN son eficaces en situaciones punto a punto, donde es necesario cifrar el tráfico entre dispositivos móviles y recursos locales. **Pero las VPN no pueden detectar ni responder a las amenazas móviles.** Son menos adecuados en escenarios en los que usted accede a servicios en la nube con un navegador, especialmente si tiene que redirigir el tráfico antes de enviarlo a la nube. Eso aumenta rápidamente los costes de red y crea cuellos de botella de rendimiento para los usuarios. Los productos VPN tampoco son infalibles. Si un atacante roba las credenciales VPN de un empleado, adquiere el mismo nivel de acceso a la red corporativa. Las soluciones de MTD pueden ayudar a prevenir las infracciones resultantes al detectar y alertar a los usuarios de que sus credenciales pueden haber sido robadas..

**Las soluciones de MTD pueden ayudar a prevenir las infracciones resultantes al detectar y alertar a los usuarios de que sus credenciales pueden haber sido robadas.**

## Z: ¿Y por lo que se refiere a Microsoft Defender para Endpoint? ¿Con qué eficacia aborda los riesgos de seguridad móviles de O365?

**Eric:** Hay ventajas e inconvenientes. Como aspecto positivo está la integración incorporada entre los productos de Microsoft. Por ejemplo, puede establecer una conexión de servicio a servicio entre Defender e Intune para compartir datos y perfiles de dispositivos. Esto le permite definir niveles de riesgo en Defender que activan controles de acceso condicional en Intune.

**Sin embargo, Defender es un producto relativamente nuevo y las características de MTD son anticuadas.** Por ejemplo, Defender no proporciona suficientes datos sobre el estado de un dispositivo móvil para determinar con precisión si es fiable, si está pirateado o en peligro. Las soluciones avanzadas de MTD ofrecen funcionalidades más completas para detectar y remediar automáticamente las amenazas a nivel de usuario, de dispositivo, de aplicación y de red. También proporcionan los amplios datos forenses y de telemetría que los analistas necesitan para el análisis de la causa raíz y la búsqueda de amenazas.

La flexibilidad y la preparación para el futuro son fundamentales. Las soluciones de MTD deben integrarse fácilmente con su SIEM, proveedor de identidad y otras inversiones en seguridad.

**"Defender no proporciona suficientes detalles sobre el estado de un dispositivo móvil para determinar con precisión si es fiable, si está pirateado o en peligro".**

## Z: ¿Cómo aborda MTD las iniciativas de Zero Trust que muchas organizaciones han acelerado debido al COVID?

**Eric:** El modelo Zero Trust requiere que los usuarios, dispositivos, redes y aplicaciones demuestren que son fiables antes de otorgar acceso a recursos como O365. El desafío es implementar Zero Trust sin exigir que los administradores controlen cada interacción ni obliguen a los trabajadores a superar dificultades para realizar tareas de rutina.

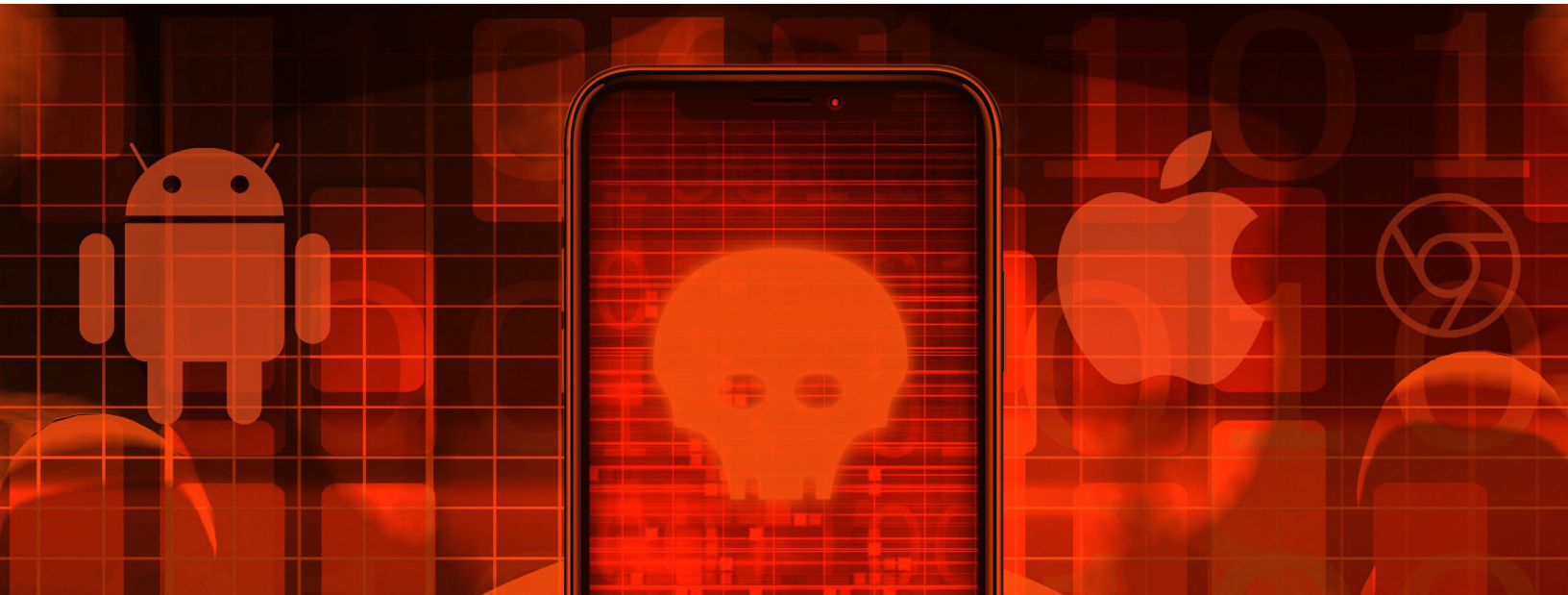
**MTD funciona bien en un entorno de Zero Trust porque supervisa continuamente el dispositivo móvil en busca de malware, exploits de phishing, puntos de acceso fraudulentos, aplicaciones cargadas lateralmente y otras amenazas potenciales.** Si un empleado no está actuando de forma maliciosa o poniendo en riesgo involuntariamente su dispositivo móvil, su acceso a los recursos puede permanecer intacto. Si MTD detecta una amenaza o un riesgo potencial, la amenaza se puede remediar de inmediato, volviendo el dispositivo a un estado en el que se certifique que es fiable.

**Z: ¿Cómo influyen las diferencias entre iOS y Android en su enfoque para proteger O365 en un entorno híbrido?**

**Eric:** Las herramientas y los flujos de trabajo serán diferentes, pero los objetivos serán los mismos. Los perfiles de trabajo administrados de Android separan las aplicaciones y los datos de trabajo de las aplicaciones y los datos personales. Esto permite definir y aplicar políticas de cumplimiento de dispositivos para aplicaciones de espacio de trabajo que se implementen de manera sistemática, si el dispositivo se conecta a un servicio basado en la nube como O365, o a una base de datos ubicada detrás del firewall corporativo. Esto ayuda a reducir los riesgos de los dispositivos BYOD sin quebrantar la privacidad de los empleados. Apple está poniéndose al día con su administrador de perfiles. A la larga, los dos productos alcanzarán la paridad.

**Por lo demás, las diferencias entre los sistemas operativos no importan. Una solución MTD eficaz debería detectar y solucionar las amenazas, independientemente de que el dispositivo esté ejecutando iOS, Android o ChromeOS (en Chromebooks).** El poder del aprendizaje automático es detectar amenazas en función de sus características detalladas y flujos de procesos. Lo importante es desplegar esos modelos y su lógica de detección y respuesta localmente en cada dispositivo móvil (detección en el dispositivo). Un peligro puede producirse en milisegundos. Uno no puede permitirse la latencia que conllevan las búsquedas en la nube y la coincidencia de firmas.

**"Una solución MTD eficaz debería detectar y solucionar las amenazas, independientemente de que el dispositivo esté ejecutando iOS, Android o ChromeOS (en Chromebooks)."**



## Z: ¿Con respecto a las mejores prácticas en torno a la gestión de parches? ¿Cuál era su enfoque?

**Eric:** A los usuarios no les gusta que se les diga que instalen parches, especialmente si el dispositivo móvil es de propiedad personal. Muchos no cumplirán ni esperarán hasta el último minuto y van a perder el acceso a los recursos corporativos. Algunos dispositivos móviles no se pueden parchear porque el hardware está desactualizado. Se deben establecer prioridades. Las actualizaciones del sistema operativo son cruciales, ya que a menudo proporcionan correcciones de seguridad para vulnerabilidades críticas. Actualizar una aplicación suele ser menos urgente, a menos que se trate de una aplicación autorizada en el lugar de trabajo, como Slack, que los empleados deben usar para ser productivos.

Es más complicado cuando se tiene una mezcla de dispositivos iOS y Android. Los usuarios de Apple suelen ser bastante obedientes. Están acostumbrados a instalar parches y actualizaciones de forma regular. El ecosistema de Android está mucho más fragmentado. Los fabricantes de hardware y los operadores inalámbricos a menudo controlan el tiempo y la disponibilidad de parches y lanzamientos del sistema operativo. Al final, uno juega a golpear el topo. Debe priorizar los parches en función del perfil de riesgo de su organización y los requisitos del caso de uso. No hay soluciones perfectas. El parcheo siempre va a ser reactivo. **Por eso es necesaria una solución que pueda detectar y evitar que los atacantes detonen malware y exploten vulnerabilidades en todos los dispositivos móviles, independientemente del modelo de propiedad o el nivel de cumplimiento.**

## Z: Teniendo en cuenta el panorama de amenazas actual, ¿cómo resumiría sus recomendaciones para los CISO sobre cómo y si deberían estar protegiendo el acceso móvil a O365?

**Eric:** Proteger el acceso móvil a O365 es esencial, pero sinceramente es una pieza de un rompecabezas mucho más grande. Los trabajadores van a seguir accediendo a todos los recursos corporativos desde los dispositivos móviles. Los grupos de amenazas continuarán encontrando nuevas formas de engañarlos para que cometan errores y exploten las aplicaciones móviles y los sistemas operativos vulnerables. La clave es identificar y priorizar las amenazas móviles que plantean los riesgos más significativos para su organización.

Si está utilizando Intune, asegúrese de que sus políticas de administración de dispositivos aborden esos riesgos sin ser demasiado restrictivas. Eduque a los usuarios para que practiquen una buena higiene cibernética. Asegúrese de que ciertos navegadores utilicen el cifrado adecuado para acceder a los servicios en la nube. Acelere su transición a la confianza cero. Esto incluye el bloqueo y la lucha básicos.

**Pero también debe implementar una solución de MTD que haya demostrado ser eficaz para detectar y mitigar las amenazas móviles para usuarios, dispositivos, redes y aplicaciones.** Asegúrese de que la solución que elija funcione bien con su infraestructura de gestión y seguridad existente y preserve la flexibilidad que necesitará a medida que su infraestructura evolucione para cumplir con los nuevos desafíos de seguridad.