HP WOLF ENTERPRISE SECURITY

CONFIANZA CERO CON HP WOLF ENTERPRISE SECURITY[1]

PORQUE LOS CLICS SON INEVITABLES

El concepto de confianza cero se acuñó hace una década. Desde entonces, ha evolucionado de manera constante y legítima para entrar en la arquitectura de seguridad de IT de las empresas modernas. HP presenta en este documento una descripción general de la confianza cero y analiza cómo profundiza en este concepto para ordenadores.

TABLA DE CONTENIDO

CONTEXTO

La confianza cero es una herramienta esencial en la lucha incesante contra las amenazas cibernéticas. El principio de confianza cero consiste, como el propio término implica, en no confiar en nada al pie de la letra y en verificar todo lo que pueda ser verificado. Aprovecha las identidades de los usuarios y los dispositivos, la configuración del firmware y el software, y una información contextual más amplia para tomar decisiones relativas a la seguridad y el acceso.

Este informe técnico describe de forma sencilla cómo HP ofrece en exclusiva una confianza cero de manera eficaz y eficiente desde el punto de vista operativo.

HP WOLF ENTERPRISE SECURITY[1]

CONFIANZA CERO APLICADA EN EL ORIGEN

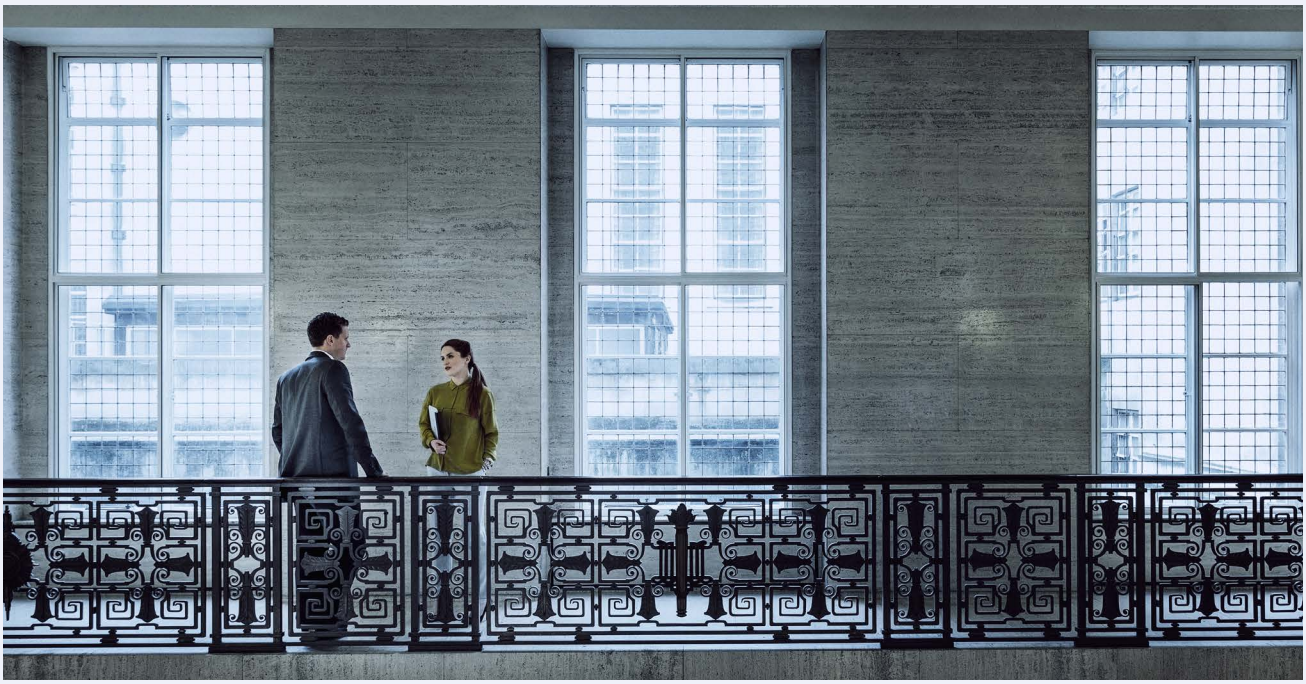
El enfoque de HP a la confianza cero se basa en el concepto de que debe implementarse lo más cerca posible de las fuentes de ataques. Al igual que las olas de un estanque son mucho más pequeñas cerca de su origen, restringir una amenaza muy cerca de su punto de origen es mucho más sencillo que hacerlo desde otro lugar. Cuanto más rápido podamos limitar la libertad de movimiento de los atacantes, menos daño podrán hacer. Puesto que la mayoría de atacantes comienzan en los ordenadores de los usuarios finales, es importante extender el concepto de confianza cero a los dispositivos.

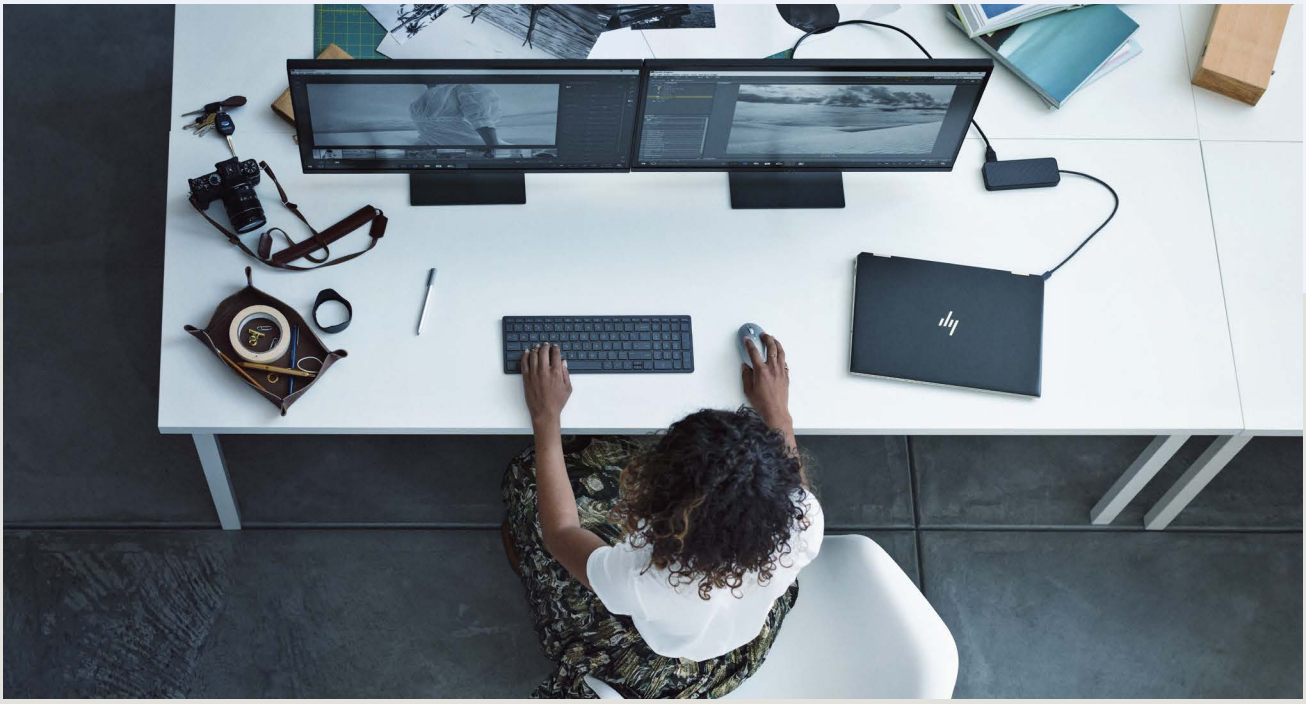
Pero, ¿qué es un atacante? Está bastante documentado que la mayoría de atacantes entran aprovechándose del comportamiento de los usuarios. Los casos más habituales son engañar a las personas para que hagan clic en enlaces o abran archivos adjuntos del correo electrónico que contienen malware a través de phishing.

Esto deja claro que los atacantes son en realidad los propios empleados de una organización, solo que ellos no lo saben. Los programas de formación de personal pueden ayudar, pero dado que el adversario solo necesita tener éxito una vez para entrar, estos programas no pueden eliminar el riesgo por completo.

Ante este reto, nuestro enfoque es sencillo: Aplicamos confianza cero a todas las actividades de riesgo potencial en los ordenadores de los empleados. Nos centramos en las acciones de mayor riesgo:

- Abrir archivos adjuntos en el correo electrónico (documentos de Office, PDF)
- Navegar por la web y hacer clic en enlaces web en clientes de chat
- Abrir archivos en dispositivos USB





HP Sure Click Enterprise,[2], la oferta estrella del portfolio de HP Wolf Enterprise Security y el elemento clave de nuestra estrategia de confianza cero, aplica los principios de confianza cero a la seguridad de los dispositivos para detener incluso las amenazas indetectables. Mediante una tecnología de aislamiento y contención de nivel defensivo y reforzada por hardware, HP Sure Click Enterprise ayuda a las organizaciones a adelantarse a las amenazas modernas que pueden escapar a otras defensas.

HP Sure Click Enterprise coloca cada tarea del usuario (por ejemplo, abrir un archivo adjunto del correo electrónico) en una micro máquina virtual (micro VM) aislada y reforzada por hardware. Esta acción impide que el malware se escape de la tarea por la que llegó, de modo que no puede infectar el ordenador del usuario ni cualquier otra parte de la red. Cuando se completa el proceso, la micro VM se destruye junto con el malware. Lo mejor de todo es que la productividad de los usuarios no se ve afectada, ya que no tienen que hacer nada distinto para beneficiarse de la contención de amenazas de Sure Click Enterprise ni tampoco tienen que estar sujetos a políticas y flujos de trabajo restrictivos. HP lleva el concepto de confianza cero un paso más allá al aprovechar las funcionalidades de seguridad avanzadas que están integradas en todo el hardware de los ordenadores modernos. HP Sure Click Enterprise utiliza el hardware de seguridad asistido en las CPU Intel y AMD actuales para crear la micro VM y establecer un microsegmentación por tarea. Un software de seguridad de los dispositivos que carezca de refuerzo de hardware siempre es susceptible de ser derrotado cuando el sistema operativo o la infraestructura subyacente se ven comprometidos. Sin embargo, HP aplica la confianza cero a toda la pila y crea un modelo de prevención de amenazas que es mucho más difícil de quebrantar. Los departamentos de IT también obtienen inteligencia ante amenazas que pueden procesar para fortalecer la posición de seguridad de la organización.

HP Wolf Security aplica los principios de confianza cero para ofrecer una defensa en profundidad en todo nuestro portfolio de HP Wolf Security, lo que ayuda a mejorar la resiliencia, a limitar la exposición y a minimizar el daño que causa un ciberataque.

CONFIANZA CERO INVERTIDA

PROTECCIÓN DE LAS APLICACIONES Y LOS DATOS DE GRAN VALOR CON HP SURE ACCESS ENTERPRISE[3]

El principio básico de la confianza cero es no confiar en las solicitudes de datos de usuarios o dispositivos no verificados. Pero, además de este caso de uso, HP también es partidaria de darle la vuelta a esta idea y proteger el bueno conocido de todo lo demás.

Un buen ejemplo es la actividad de administración de IT. Una administradora de IT que trabaja desde casa y utiliza una VPN en el centro de datos para desempeñar su trabajo mediante el uso de credenciales de superusuario es la diana perfecta para los atacantes. Si son capaces de encontrar una forma de instalar malware en su portátil, también podrán obtener credenciales de nivel de administrador, acceder directamente a activos confidenciales, establecer una fuerte presencia en el entorno y cosas peores.

HP Sure Access Enterprise protege estos objetivos de gran valor por medio de la capacidad de aislamiento de aplicaciones de HP. Coloca las aplicaciones, como la actividad de administración de IT, en un contenedor virtual seguro y asistido por hardware que no puede ser manipulado por ningún otro proceso del ordenador.

De este modo, aunque un atacante encuentre una forma de entrar y poner en riesgo el ordenador, no podrá acceder a la información confidencial que busca. Y al igual que con Sure Click Enterprise, la protección se consigue sin afectar a la productividad del usuario.

El aislamiento de aplicaciones protege las aplicaciones de gran valor del resto del entorno.

HP WOLF ENTERPRISE SECURITY[1]

UN ENFOQUE ÚNICO ALA CONFIANZA CERO EN LOS DISPOSITIVOS

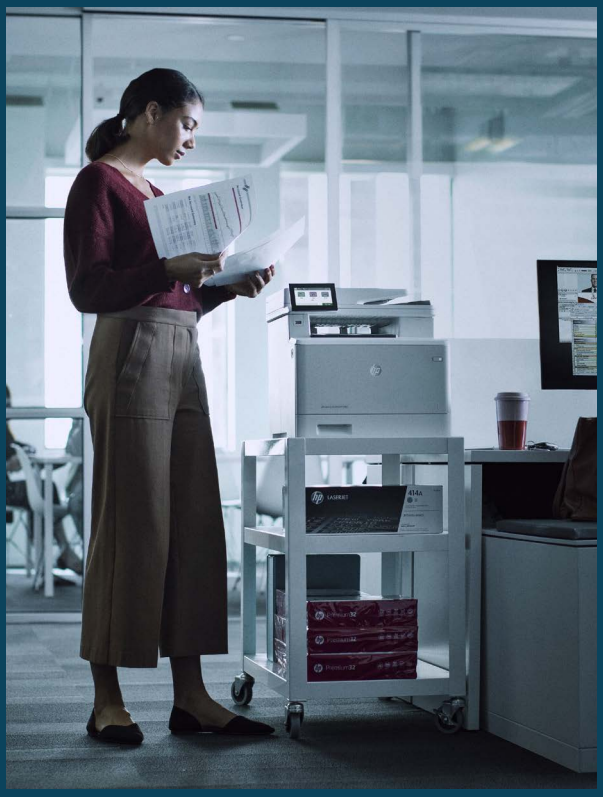
El enfoque de confianza cero de HP combina eficiencia y eficacia de un modo único. A diferencia de las soluciones alternativas, ni Sure Click Enterprise ni Sure Access Enterprise requieren actualizaciones constantes para seguir siendo relevantes; ambos son igual de eficaces a la hora de frustrar los ataques de día cero y ninguno necesita personalizarse en función del uso de la aplicación.

La prevención de amenazas de la confianza cero de HP reduce enormemente la presión sobre el COS y la respuesta a incidentes, ya que elimina la mayor parte del malware antes de que pueda infectar un solo dispositivo Eso se traduce en menos alertas, menos reparaciones de dispositivos y mayor productividad del usuario. También supone un menor gasto de tiempo y dinero en la detección y la respuesta, porque simplemente hay mucho menos que detectar.

EFICIENCIA	EFICACIA
Auténtica prevención, no solo detección	Confianza cero aplicada en el origen
Gestión de políticas sencillas	Asistencia de hardware: Utiliza capacidades de seguridad en todas las CPU modernas
Baja tasa de falsos positivos	Contención de amenazas y aislamiento de aplicaciones en
Integración sencilla con los procesos del COS	Igual de eficaz para los exploits de día cero y generalizados
	Captura de inteligencia ante amenazas en tiempo real

RESUMEN

CONFIANZA CERO PARA EL TRABAJO HÍBRIDO Y LA NUBE HÍBRIDA



Aunque la confianza cero no es un concepto nuevo, es sumamente importante en el entorno de trabajo híbrido actual, donde muchas personas no se encuentran en la oficina.

El enfoque de HP a la confianza cero aplica prevención de amenazas en el origen: el usuario que sin saberlo abre la puerta a un atacante a través de una actividad aparentemente inofensiva. Al situar la protección en el dispositivo, no hay que preocuparse de si el usuario trabaja en remoto o en la oficina, ni de si los datos a los que accede se encuentran en el centro de datos o en la nube. Se detiene a los hackers justo en el ordenador del usuario, de modo que se elimina la necesidad de reparar su ordenador. Eso significa que es eficaz, puede operar a escala y reduce los costes de la gestión de riesgos en las empresas modernas.

Más información en:
hp.com/wolfenterprisesecurity

[1] HP Wolf Enterprise Security requiere Windows 10. HP Sure Click Enterprise es compatible con los navegadores Microsoft Internet Explorer, Edge, Google Chrome, Chromium y Firefox, y aísla archivos adjuntos de Microsoft Office (Word, Excel, PowerPoint) y archivos PDF cuando Microsoft Office o Adobe Acrobat no están instalados. HP Protected App admite actualmente sesiones RDP, sesiones Citrix® ICA y un navegador basado en Chromium.

[2] HP Sure Click Enterprise requiere Windows 10 y es compatible con Microsoft Internet Explorer, Edge, Google Chrome, Chromium o Firefox. Entre los archivos adjuntos compatibles se incluyen los archivos de Microsoft Office (Word, Excel, PowerPoint) y los archivos PDF, siempre y cuando se haya instalado Microsoft Office o Adobe Acrobat.

[3]HP Sure Access Enterprise requiere Windows 10 Pro o Enterprise.

Regístrate para recibir actualizaciones: hp.com/go/getupdated

c07713616, junio de 2021