Papel blanco técnico

Empoderar a los empleados para mejorar la seguridad

Contenido

Empoderar a los empleados para mejorar la seguridad

La seguridad informática ha ascendido en la agenda corporativa, dado que numerosas empresas han sido afectadas por devastadores ciberataques y vulneraciones de datos. Estos ataques han mostrado poca consideración por regiones, sectores o tamaños de compañía, y como resultado los profesionales de TI de todas las organizaciones han tenido que concentrarse de manera creciente en mejorar la seguridad.

Para combatir estas amenazas crecientes, muchos se han enfocado en la implementación y gestión de soluciones de alto nivel como los firewalls corporativos, programas de detección de amenazas y software antivirus. Si bien estas soluciones son sin lugar a dudas una parte esencial del marco de seguridad de cualquier empresa, están lejos de ser el único factor de su estructura de seguridad. Los profesionales de TI enfocados en estas soluciones, en muchos casos no se ocupan de las mayores debilidades de sus defensas: sus empleados. Al ser los empleados los responsables del 70 % de las vulneraciones de datos,[1] las organizaciones no pueden permitirse descuidar este problema por más tiempo.

Sin embargo, hacer cumplir las medidas de seguridad de los empleados sin ganarse su antipatía ni perjudicar la productividad no es una tarea simple. Las resoluciones excesivamente estrictas, en el mejor de los casos frustran a los empleados y en el peor dan como resultado el uso de soluciones alternativas que socavan completamente su seguridad. Para que los procedimientos de seguridad sean verdaderamente efectivos, se debe educar a los empleados en relación con sus beneficios, comprometerlos con su éxito y empoderarlos para trabajar con ellos.

En este artículo se examina la manera de combinar políticas de seguridad efectivas y razonables, programas de capacitación completos y las ultraseguras laptops EliteBook x360 de HP a fin de construir un entorno seguro y productivo para sus empleados. Siga estos pasos y podrá hacer de sus empleados, en lugar de una debilidad, un pilar vital de su marco de seguridad.

[1] Shred-it, 'State of the Industry: Information Security', (2018)

Las vulnerabilidades de sus empleados

Existen numerosas maneras en que los empleados pueden causar directamente una vulneración de datos, por lo que la mayor parte de la actividad criminal cibernética está orientada a explotar el error humano en lugar de una falla técnica de sus defensas.

Malware

El 30 % de las vulneraciones de datos de 2018 implicaban malware y el 39 % de esos ataques eran de ransomware

La mayoría de las amenazas que enfrentarán las organizaciones consistirán en alguna forma de malware, ya sea un virus, troyano, spyware, rootkit o ransomware. En efecto, el 30 % de las vulneraciones de datos de 2018 implicaban malware y el 39 % de esos ataques eran de ransomware.[2] Para las organizaciones de América Latina el problema no hace sino agravarse: los informes muestran que la cantidad de ataques de malware a las empresas de la región ha crecido bruscamente en el último año.[3]

Una vez que un malware se ha abierto camino en su sistema, probablemente intentará ocultar su presencia mientras se disemina por su red. Los firewalls y el software antivirus pueden prevenir o erradicar la mayor parte del malware, pero muchas veces no son capaces de reaccionar ante amenazas que no se identificaron previamente. Por otra parte, los hackers se esfuerzan cada vez más por burlar las defensas tradicionales. Es alarmante que el 68 % de las vulneraciones de datos necesite meses o más para descubrirse,[4] lo que indica que las organizaciones se esfuerzan por erradicar el malware que ha violado exitosamente sus sistemas. Existen múltiples formas en las que el malware puede abrirse camino en su sistema, pero la más común implica errores de empleados, como el acceso a un sitio comprometido, la apertura de un correo electrónico sospechoso o la descarga de un archivo desconocido.

Suplantación de identidad (Phishing)

El phishing es la causa principal del 48 % de los casos de vulneración

La suplantación de identidad (phishing) es una amenaza absolutamente más complicada de combatir a través de los medios tradicionales. Este método de ingeniería social implica correos electrónicos o mensajes instantáneos que utilizan medios fraudulentos para convencer al destinatario de que entregue información crítica de la empresa, personal o confidencial. Los filtros anti-phishing pueden bloquear ejemplos evidentes de phishing, pero muchos ataques ahora son altamente personalizados y simulan contactos o instituciones conocidas, lo que los hace increíblemente difíciles de detectar. Como resultado, se ha informado que el phishing es la causa principal del 48 % de los casos de vulneración.[5]

Robo físico

Las vulneraciones físicas siguen siendo un problema importante, en especial en empresas pequeñas que pueden carecer de la infraestructura física de las organizaciones grandes. La prevención del acceso no autorizado a sus instalaciones será siempre importante, pero cada vez más las empresas necesitan prestar atención a las amenazas situadas fuera de la oficina. Gracias a las mejoras de movilidad, acceso a Internet y computación en la nube, los empleados pueden trabajar desde cualquier lugar en cualquier momento. Proteger los dispositivos en caso de robo es, por consiguiente, vital, pero existen otras amenazas detrás de esta. El malware puede tener acceso a los dispositivos a través de sus puertos USB, y los actores de las amenazas pueden obtener información confidencial mediante hackeo visual, en el que una persona visualiza datos importantes desde la periferia.

[2] Verizon, '2018 Data Breach Investigations Report', (2018)
[3] Malwarebytes, '2019 State of Malware', (2019)
[4] Verizon, '2018 Data Breach Investigations Report', (2018)
[5] F5 Labs, 'Lessons Learn From A Decade Of Data Breaches', (2017)

Más de 70 % de los empleados reutiliza las contraseñas en el trabajo

Contraseñas débiles
El simple hecho de tener una contraseña no suele ser suficiente para proteger el acceso cuando el 81 % de las vulneraciones relacionadas con hackeo se valen de contraseñas robadas o débiles.[6] Sin conciencia de los peligros, los empleados a menudo permanecen con una contraseña predeterminada o utilizan en su lugar una contraseña simple o común. Además de esto, más de 70 % de los empleados reutiliza las contraseñas en el trabajo;[7] esto significa que una vez que un hacker ha tenido acceso a una contraseña individual, tiene acceso a múltiples áreas de la empresa. Si sus empleados redistribuyen contraseñas personales en el trabajo, esto complica más el problema. Si otra organización que tiene la contraseña personal de uno de sus empleados sufre una vulneración, como las conocidas vulneraciones de Yahoo! informadas en 2016, entonces su empresa está también en riesgo.

Falta de actualización
A pesar de sus mejores esfuerzos, los proveedores de software están continuamente descubriendo vulnerabilidades e implementando revisiones y actualizaciones para solucionarlas. Sin embargo, dado que las empresas utilizan cada año una cantidad mayor de soluciones de software, asegurar que las soluciones se mantengan actualizadas se ha hecho más arduo que nunca. Cuando esa responsabilidad se les deja a los empleados mismos, normalmente queda relegada. Un informe determinó que el 57 % de las vulneraciones involucran una vulnerabilidad conocida que no fue sometida a revisión.[8]

Uso de dispositivos personales
Las políticas del tipo Traiga su propio dispositivo (Bring Your Own Device, BYOD) han cobrado impulso en épocas recientes; el mercado relativo a BYOD en América Latina creció hasta 15 500 millones de dólares en 2019. Los empleados han impulsado en gran medida esta tendencia, ya que prefieren la tecnología con la que están familiarizados y a menudo descubren que sus propios dispositivos son superiores a los proporcionados por el trabajo. Sin embargo, el uso incontrolado de dispositivos personales en el trabajo puede presentar un colosal riesgo para la seguridad: un 33 % de las empresas de todo el mundo dicen que se preocupan por ello.[9]

El uso incontrolado de dispositivos personales en el trabajo puede presentar un colosal riesgo para la seguridad: un 33 % de las empresas de todo el mundo dicen que se preocupan por ello

Los dispositivos personales están fuera del control de TI, y si se les permite el acceso a la red se convierten a menudo en un punto de entrada no protegido. En estas instancias, muchas de las medidas de seguridad implementadas por TI resultan socavadas y dejan el dispositivo dependiente de soluciones de seguridad de nivel de consumidor, las que raramente ofrecen la protección de sus homólogas empresariales. Asimismo, TI pierde el control de los datos tomados de los sistemas corporativos. Si un empleado deja la empresa, resulta difícil asegurar que no lleve consigo datos confidenciales.

[6] https://www.tracesecurity.com/blog/articles/81-of-company-data-breaches-due-to-poor-passwords
[7] ibid
[8] ServiceNow, 'Today's State of Vulnerability Response: Patch Work Demands Attention', (2018)
[9] https://www.kaspersky.com/blog/the-human-factor-in-it-security/

Seguridad y productividad: alcanzar un equilibrio

Frente a tantas vulnerabilidades potenciales, puede ser tentador limitar drásticamente los derechos de acceso de los empleados e introducir múltiples medidas de seguridad. Sin embargo, las medidas de seguridad severas pueden entorpecer drásticamente la productividad y reducir la satisfacción de los empleados: el 91 % de las compañías estiman que las medidas de seguridad impactan de manera negativa sobre la productividad.[10] Los empleados que constantemente se encuentran con obstáculos que requieren la asistencia de TI, muy pronto se sentirán frustrados.

Usted podría argumentar que la frustración de los empleados es un precio que merece la pena pagar en procura de una seguridad robusta, pero desafortunadamente un empleado frustrado puede muchas veces terminar debilitando sus defensas. Los empleados, si pueden hacerlo, pueden elegir ignorar las políticas: 44 % de las compañías dicen que los empleados no siguen correctamente sus políticas de seguridad informática.[11] Alternativamente, ante las exigentes reglas muchos empleados encontrarán a menudo soluciones alternativas como el uso de contraseñas débiles, VPNs o sus propios dispositivos. No hay problema pequeño: casi 70 % de los profesionales de TI dicen que las soluciones alternativas que utilizan los empleados para evitar las medidas de seguridad impuestas por TI conllevan el mayor riesgo para su organización.[12]

Casi 70 % de los profesionales de TI dicen que las soluciones alternativas que utilizan los empleados para evitar las medidas de seguridad impuestas por TI conllevan el mayor riesgo para su organización

Las medidas rigurosas también pueden dañar la relación entre TI y el personal. Los empleados pueden estar menos inclinados a pedir ayuda o pueden tener miedo de admitir un error si piensan que esto puede llevar a recriminaciones. De hecho, en el 40 % de las empresas de todo el mundo los empleados ocultan un incidente cuando se produce.[13] Cuando ocurre una vulneración, las organizaciones deben actuar rápidamente para limitar el daño que puede haberse infligido, por lo que es esencial que los empleados se sientan cómodos al informar todos y cada uno de los errores que podrían causar una vulneración.

El panorama de amenazas actual puede entrañar muchos peligros para los empleados desprevenidos, pero aplicarles restricciones no es ningún modo seguro de garantizar la seguridad de su empresa. Sin embargo, si a los empleados se les proporcionan las apropiadas destrezas, herramientas y entorno, usted puede tener la garantía de que ni su seguridad ni su productividad sufrirán.

En el 40 % de las empresas de todo el mundo los empleados ocultan un incidente cuando se produce

[10] https://businessinsights.bitdefender.com/security-impacts-productivity
[11] https://www.kaspersky.com/blog/the-human-factor-in-it-security/
[12] https://businessinsights.bitdefender.com/security-impacts-productivity
[13] https://www.kaspersky.com/blog/the-human-factor-in-it-security/

Crear un personal más seguro

Cada empresa debe tratar de crear un entorno en el que sus empleados puedan trabajar de manera segura y efectiva; sin embargo, pocos saben por dónde empezar. En esta sección examinaremos tres áreas en las que usted deberá enfocarse para alcanzar su objetivo. En primer término, necesitará elaborar políticas claras, controlables y comprensibles que sus empleados puedan seguir sin entorpecer su vida laboral. En segundo término, necesitará brindar capacitación que no solo empodere a los empleados para trabajar de manera segura sino que también esclarezca los beneficios de observar las mejores prácticas de seguridad. Por último, al proporcionar a los empleados dispositivos de avanzada que superen a las alternativas de consumo masivo y cuenten con elementos de seguridad, usted puede garantizar que se evitan los trastornos de BYOD y que muchas de sus inquietudes respecto a la seguridad están consideradas.

Políticas seguras

Al proporcionar a los empleados entornos seguros en los que trabajar y políticas de seguridad que no entorpezcan excesivamente su capacidad para operar, es mucho más probable que cumplan las reglas. Sin embargo, la administración de esas políticas flexibles puede parecer una tarea abrumadora para los equipos de TI. Afortunadamente, existen soluciones disponibles que pueden simplificar el proceso. Los derechos de acceso de los empleados deben administrarse como parte de su marco de seguridad, pero las reglas generales raramente son una solución adecuada. Al utilizar un sistema de administración de puntos finales, usted puede asignar y revocar derechos de acceso de manera remota para asegurar que cada usuario tenga los derechos correctos en base a sus necesidades. Describa un proceso claro y simple para solicitar nuevos derechos que asegure que los empleados siempre recurran a TI cuando lo necesiten.

Estos sistemas pueden extenderse del mismo modo para administrar la implementación de actualizaciones y revisiones. Si se depende de los empleados para la instalación de actualizaciones es posible que queden fallas en su seguridad, pero enviar al personal de TI para la instalación manual de actualizaciones constituye un drenaje de recursos inaceptable. En lugar de esto, el proceso puede implementarse de manera remota a intervalos establecidos previamente, para asegurar que cada dispositivo de su flota esté de acuerdo con el estándar. Todos los parámetros y actualizaciones para BIOS, hardware y software preinstalado en dispositivos HP pueden administrarse de manera remota a través del kit de integración de gestión de HP. Esta herramienta, diseñada específicamente para administradores de TI, puede integrarse con su sistema de administración de puntos finales elegido para optimizar este proceso en su totalidad.

Del mismo modo, hacer cumplir la autenticación multifactor puede contribuir en gran medida a mejorar la seguridad y a la vez reducir la mala práctica de la contraseña común. Mediante el uso de variados factores como tarjetas inteligentes, reconocimiento facial y escaneo de huellas digitales, además de sus contraseñas tradicionales, usted puede limitar la ocurrencia de códigos olvidados o débiles y a la vez mitigar los peligros de que una contraseña caiga en las manos equivocadas.

Del mismo modo, hacer cumplir la autenticación multifactor puede contribuir en gran medida a mejorar la seguridad y a la vez reducir la mala práctica de la contraseña común

[14] https://www.kaspersky.com/blog/the-human-factor-in-it-security/

Para quienes insisten en mantener una política del tipo Traiga su propio dispositivo (Bring Your Own Device, BYOD), existen medidas que pueden adoptarse para limitar la exposición de su organización al riesgo a causa de estos dispositivos. Al proporcionar una red separada o red perimetral (DMZ) para dispositivos personales y visitantes, usted puede asegurar que aquellos que eligen utilizar sus propios dispositivos no puedan acceder a la red más allá del acceso directo a Internet. Si uno de esos dispositivos resulta infectado por malware, usted puede tener la seguridad de que no podrá abrirse camino por su red privada.

Capacitación de los empleados

Las empresas consideran la capacitación del personal como el segundo método más efectivo de defensa, después de la inversión en software de seguridad más sofisticado

Por más completo que sea su marco de seguridad, la sensibilización y vigilancia de sus empleados es a menudo lo único que se interpone entre su empresa y un ataque exitoso. Por lo tanto, es vital que usted eduque a sus empleados acerca de los peligros que pueden enfrentar durante su día de trabajo, aliente su compromiso personal para mantener la empresa segura y cultive una relación cooperativa entre TI y su personal. De hecho, las empresas consideran la capacitación del personal como el segundo método más efectivo de defensa, después de la inversión en software de seguridad más sofisticado.[14]

Los cursos de capacitación se han convertido en un componente esencial de los marcos de seguridad corporativos, por lo que se espera que todos los empleados asistan a alguno. Es importante que tomen parte los empleados de todos los niveles, ya que incluso los miembros del personal que más saben de TI suelen desconocer muchos de los peligros que existen en el mundo corporativo y la manera en que sus acciones podrían poner la empresa en riesgo. Del mismo modo, no debe suponerse que los empleados tengan un gran conocimiento de las prácticas de seguridad. Todo programa de capacitación debe tratar incluso sobre las acciones más básicas.

Mientras que TI puede elaborar e implementar un programa de capacitación completamente personalizado para su empresa, algunas organizaciones pueden no contar con los recursos necesarios para emprender un proyecto como ese por sí solas. Afortunadamente, los servicios de terceros pueden ofrecer cursos de capacitación interactivos que abarcan muchas de las mejores prácticas y peligros comunes. Cualquiera sea el enfoque que elija tomar, debe ofrecer segmentos personalizados que traten sobre los riesgos especiales para su empresa y describan las políticas de seguridad que usted ha implementado.

Si los empleados desconocen sus políticas o los procesos que deben seguir (como procurar la aprobación de TI para la instalación de un nuevo software) es mucho más probable que las subviertan y que descubran posibles soluciones alternativas. Asimismo, explique la necesidad de esas políticas; si los empleados consideran que los procedimientos son innecesariamente burocráticos en lugar de vitalmente importantes, es más probable que se sientan frustrados y los eviten. Realice el seguimiento con documentación completa, de modo que los empleados puedan poner al día sus conocimientos en la forma y el momento en que lo necesiten.

Es importante recordar que la capacitación en seguridad no debe finalizar con un único curso. Continuarán surgiendo nuevas amenazas, las políticas requerirán adaptación ante el crecimiento de la empresa, y la memoria de los empleados flaqueará.

Es importante recordar que la capacitación en seguridad no debe finalizar con un único curso. Continuarán surgiendo nuevas amenazas, las políticas requerirán adaptación ante el crecimiento de la empresa, y la memoria de los empleados flaqueará. Planee cursos de repaso periódicos y mantenga a los empleados actualizados sobre las tendencias en seguridad. Por ejemplo, en 2018 el 71 % de los intentos de suplantación de identidad (phishing) se enfocaron en hacerse pasar por 10 prominentes organizaciones. Compartir actualizaciones como esta puede contribuir en gran medida a mantener seguros a los empleados.[15]

[15] F5 Labs, '2018 Phishing and Fraud Report', (2018)

La HP EliteBook x360 ofrece un excepcional diseño, desempeño y flexibilidad, a la vez que proporciona características de seguridad de grado empresarial sin precedentes

Puntos finales avanzados

Muchas de las dificultades mencionadas en este artículo pueden evitarse completamente, sin afectar la productividad, si se proporciona a los empleados los dispositivos correctos. El problema específico de BYOD puede eliminarse si usted puede ofrecer equipos mejores que las alternativas de consumo masivo. Sin embargo, los puntos finales raramente se construyen teniendo en cuenta la seguridad. HP ha intentado modificar eso con la laptop HP EliteBook x360, la PC más segura y manejable del mundo.[16] La HP EliteBook x360 ofrece un excepcional diseño, desempeño y flexibilidad, a la vez que proporciona características de seguridad de grado empresarial sin precedentes. Estas capacidades vienen incorporadas y son fáciles de dominar por los empleados y simples de administrar por TI.

A pesar de sus mejores esfuerzos para proteger a los empleados, ellos enfrentarán muchos peligros potenciales durante su día de trabajo. Afortunadamente, la HP EliteBook x360 puede respaldar sus políticas y capacitación con muchas características fáciles de usar. Como se mencionó anteriormente, la autenticación multifactor puede reducir drásticamente la probabilidad de una vulneración. Lamentablemente, las soluciones de terceros son un costo agregado que además puede requerir nuevas inversiones en equipos, mientras que la HP EliteBook x360 es compatible con el uso de la autenticación múltiple como estándar a través de su cámara IR, sensor de huellas digitales y lector de tarjetas inteligentes. Puede integrarse con su sistema operativo y aplicarse de manera remota a través del HP Client Security Manager.

HP Sure Click abre sus navegadores en un contenedor virtual aislado que impide el avance de cualquier malware detrás de la sesión del navegador

Si bien se debe educar a los empleados sobre los peligros del acceso a sitios web poco confiables, puede ser difícil identificar sitios comprometidos. Sin embargo, con HP Sure Click los empleados no deberán preocuparse nunca por ir a parar a una página potencialmente malintencionada. Sure Click abre sus navegadores en un contenedor virtual aislado que impide el avance de cualquier malware detrás de la sesión del navegador, liberando así a los equipos de TI de tener que elaborar una lista blanca de los sitios web a los que los empleados pueden tener acceso. Esta protección puede extenderse incluso a los archivos descargados, lo que permite a un empleado verificar la legitimidad de los archivos en modo de solo lectura antes de aceptarlos como dignos de confianza.

A menudo se pasa por alto que el hardware de sus dispositivos corre riesgo de ataques tanto como su software. Desafortunadamente, son pocas las soluciones de seguridad que se extienden para incluirlo. En cambio, la EliteBook x360 cuenta con una serie de capacidades aplicadas por hardware que pueden resolver esta vulnerabilidad. Es posible que su BIOS resulte infectado por un malware como un rootkit, que puede residir sin que se lo detecte y abrirse camino en su red más amplia. HP Sure Start protege su BIOS mediante la detección automática de cualquier actividad anómala. En caso de descubrirla, inmediatamente restablece la versión de BIOS más reciente no afectada, con lo que elimina el malware.

Por otra parte, HP ha extendido esta protección al software que usted posee. Muchas de las amenazas avanzadas actuales están diseñadas para socavar y destruir las soluciones de seguridad como su firewall o agente antivirus. HP Sure Run protege estas aplicaciones y procesos críticos mediante el monitoreo de terminaciones o cambios inusuales y el reinicio automático de estos programas como respuesta. Tanto HP Sure Start como HP Sure Run están aplicadas por hardware; esto significa que son inmunes a los ataques en sí mismas y se ejecutan de manera predeterminada sin ninguna acción del usuario.

HP Sure Run protege aplicaciones y procesos críticos mediante el monitoreo de terminaciones o cambios inusuales y el reinicio automático de estos programas como respuesta

[16] https://www8.hp.com/co/es/elite-family/elitebook-x360-1030-1020.html?jumpid=sc_4ub-zd8e9pt

A menudo se pasa por alto que el hardware de sus dispositivos corre riesgo de ataques tanto como su software. Desafortunadamente, son pocas las soluciones de seguridad que se extienden para incluirlo. En cambio, la EliteBook x360 cuenta con una serie de capacidades aplicadas por hardware que pueden resolver esta vulnerabilidad. Es posible que su BIOS resulte infectado por un malware como un rootkit, que puede residir sin que se lo detecte y abrirse camino en su red más amplia. HP Sure Start protege su BIOS mediante la detección automática de cualquier actividad anómala. En caso de descubrirla, inmediatamente restablece la versión de BIOS más reciente no afectada, con lo que elimina el malware.

HP Sure Run protege aplicaciones y procesos críticos mediante el monitoreo de terminaciones o cambios inusuales y el reinicio automático de estos programas como respuesta

Por otra parte, HP ha extendido esta protección al software que usted posee. Muchas de las amenazas avanzadas actuales están diseñadas para socavar y destruir las soluciones de seguridad como su firewall o agente antivirus. HP Sure Run protege estas aplicaciones y procesos críticos mediante el monitoreo de terminaciones o cambios inusuales y el reinicio automático de estos programas como respuesta. Tanto HP Sure Start como HP Sure Run están aplicadas por hardware; esto significa que son inmunes a los ataques en sí mismas y se ejecutan de manera predeterminada sin ninguna acción del usuario.

La HP EliteBook x360 también cuenta con una serie de defensas físicas que reducen la interceptación, previenen la intrusión a través de los puertos físicos y protegen los datos en caso de robo del dispositivo. HP Sure View puede ayudar a prevenir el hackeo visual mediante el oscurecimiento de la pantalla para cualquiera que no la mire de frente. Por otro lado, HP Device Access Manager asegura sus puertos USB mediante el requerimiento de autenticación antes de aceptar cualquier almacenamiento extraíble. Finalmente, las unidades de disco duro con autocifrado de HP garantizan que si se roba un dispositivo los ladrones no podrán tener acceso a los datos de la unidad.

Todas estas medidas de seguridad vienen junto con características de calidad superior que mejoran la colaboración y la productividad

Todas estas medidas de seguridad vienen junto con características de calidad superior que mejoran la colaboración y la productividad. La HP EliteBook x360 es estilizada, liviana y durable. Su pantalla puede girar 360º, para permitir a los usuarios trabajar en cinco modos diferentes. Esto viene acompañado de un desempeño y potencia inigualables, que producen una laptop para todas las necesidades de sus empleados.

Conclusión

En el mundo actual de las empresas hay muchas amenazas al acecho para atrapar empleados desprevenidos y vulnerar las defensas de su organización. TI no puede permitirse ignorar estos peligros, pero tampoco puede optar por obstruir las actividades de sus empleados. En cambio, deben proporcionar a los empleados todo lo que necesiten para trabajar de manera segura y eficiente. La HP EliteBook x360 se fabricó pensando en este principio: proporcionar una incomparable protección de puntos finales que trabaja con sus empleados y no contra ellos.