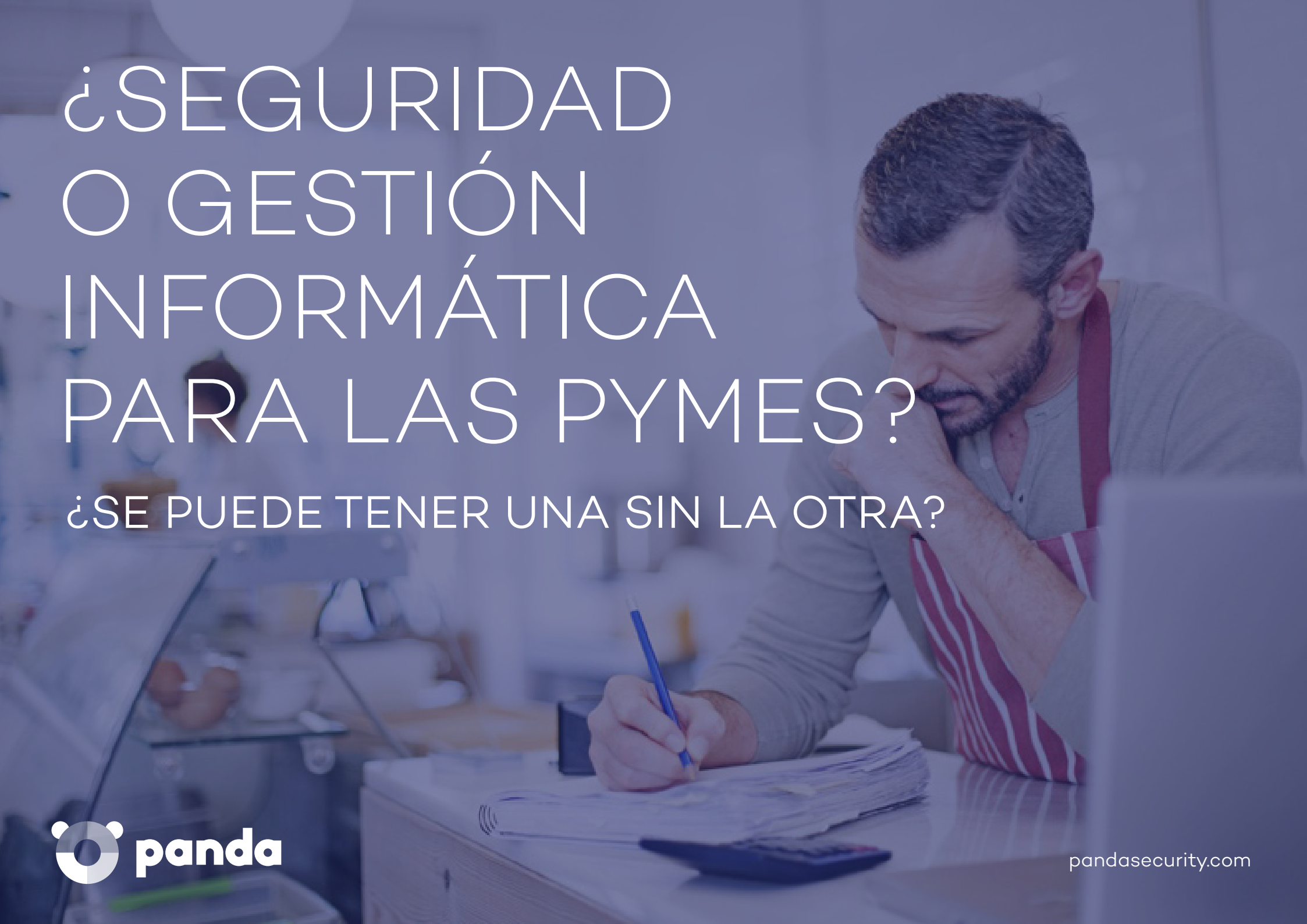


¿SEGURIDAD O GESTIÓN INFORMÁTICA PARA LAS PYMES?

¿SE PUEDE TENER UNA SIN LA OTRA?

panda

pandasecurity.com

El malware actual no tiene como objetivo provocar el caos sino obtener beneficios económicos.

La naturaleza de los sistemas de seguridad está en permanente evolución para poder responder al siempre cambiante mundo de las amenazas informáticas. Mientras la mayor parte de sectores industriales se enfrentan a una transformación tecnológica impulsada por fenómenos como la nube, la movilidad y, hasta cierto punto, Big Data, el mundo de la seguridad informática no está al margen y debe afrontar también cambios profundos.

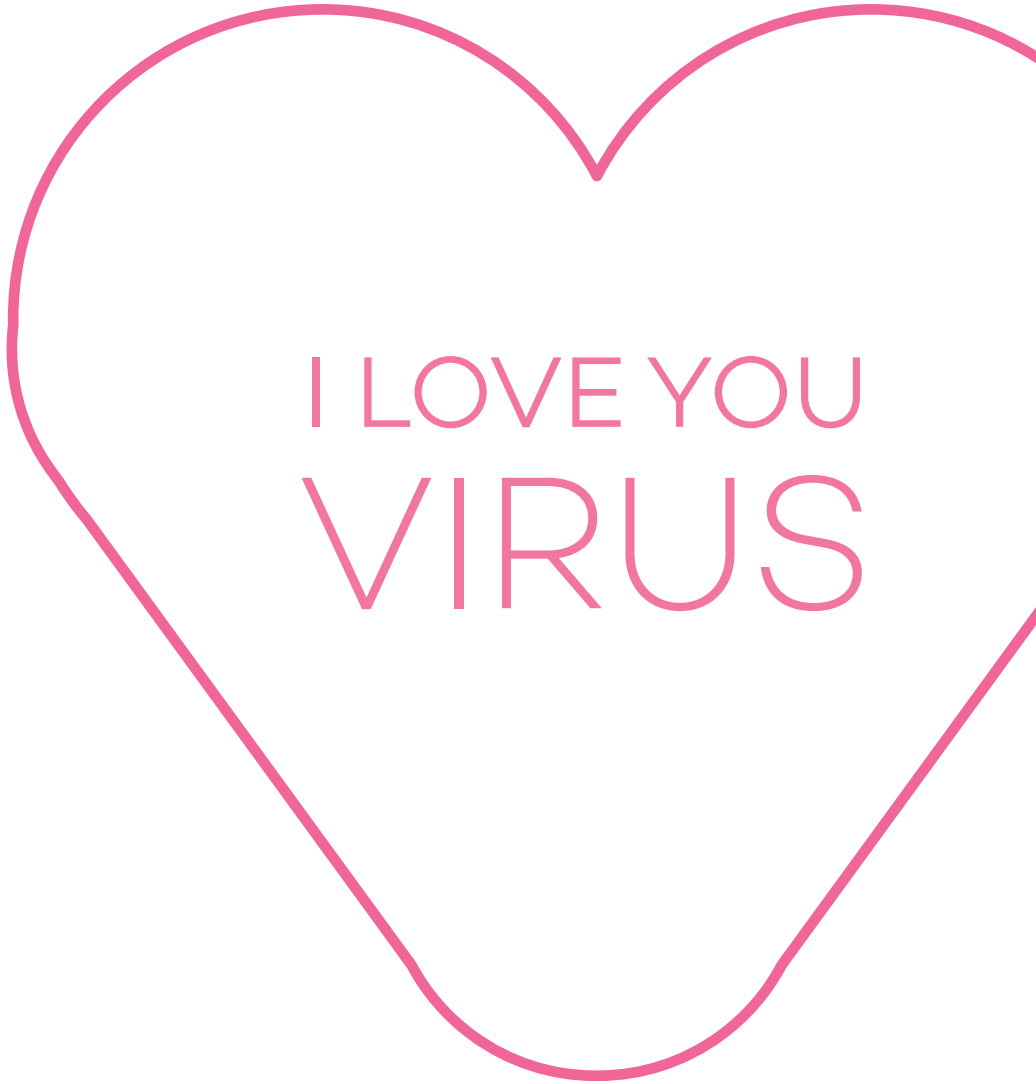
Hace tiempo que la industria del malware tiene como objetivo la obtención de beneficios económicos y ha dejado de girar en torno al ego personal de programadores, hackers, etc., tal y cómo sucedía en sus primeros tiempos en los que malware como **I Love You* y Anna Kournikova atraían la atención del público y los medios.**

Como en cualquier otra industria, en cuanto surgió la posibilidad de ganar dinero, empezaron a aparecer individuos interesadas en aprovechar la oportunidad.

En la actualidad, el objetivo es puramente económico, y cuanto más tiempo logra permanecer el malware en nuestros sistemas sin ser detectado, más beneficios reporta a su creador.

Se calcula que el virus I Love You afectó a 45 millones de PCs en todo el mundo, provocando daños equivalentes a 5.500-8.700 millones de dólares y pérdidas de 15.000 millones de dólares en su erradicación.

Sin embargo, no produjo ningún tipo de beneficio económico para sus creadores (Wikipedia).



la inversión en malware está alcanzando cifras históricas

El flujo de inversión en el desarrollo de malware esta rompiendo todos los records de creación de amenazas. El malware creado en el año 2013 supuso un 20% de todo el malware aparecido en la historia, con 84.000 nuevas amenazas creadas cada DÍA.

En el primer puesto de las listas de amenazas siguen estando los troyanos, un tipo de malware diseñado para aprovechar las vulnerabilidades existentes en los sistemas y aplicaciones informáticas. Dichas vulnerabilidades representan en sí mismas una parte importante del problema de la seguridad, y plantean la necesidad de futuros cambios en las estrategias encaminada a asegurar los sistemas.

31,53%
ORDENADORES INFECTADOS EN EL MUNDO

3.800
CADA HORA

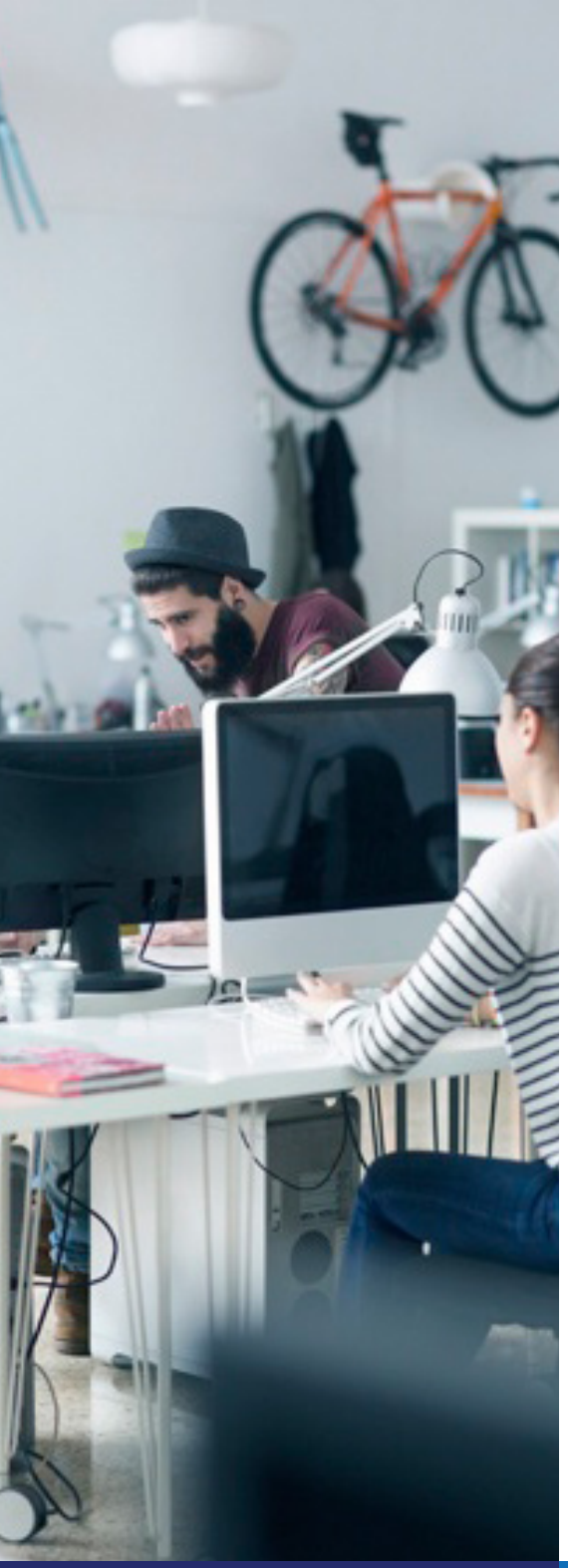
84.000
POR DÍA

30
MILLONES
2013

PANDALABS
HA REGISTRADO HASTA HOY

145
milliones
DE EJEMPLARES DE MALWARE

28,96%	USA
24,84%	España
54,03%	Brasil
38,01%	Argentina
22,68%	UK
20,28%	Suecia
22,14%	Alemania
38,18%	Rusia
34,99%	China
32,72%	Japón



La movilidad, heterogeneidad y dispersión de los entornos actuales añaden nuevas dificultades a la hora de administrar y proteger las redes corporativas.

A medida que aumentan los gastos y la dependencia con respecto al hardware y software **(ver el informe «State of SMB IT»de Spiceworks),** los sistemas informáticos se vuelven más heterogéneos, dispersos y complicados de administrar. Desde el punto de vista del volumen, por ejemplo, los profesionales informáticos se enfrentan al reto de administrar múltiples sitios, varios sistemas operativos y múltiples dispositivos por usuario. Cada dispositivo adicional mejora la eficacia de la empresa, pero también supone un nuevo punto vulnerable.

En cuanto a la movilidad, el problema se acentúa en el caso

de las PYMES tal y como señala la consultora Gartner en un informe reciente*; Las PYMES se enfrentan a los mismos desafíos que las grandes empresas a la hora de mantener sus dispositivos móviles bajo control y protegidos. Sin embargo,

las PYMES no disponen del conocimiento ni de los recursos necesarios para responder a este problema de la misma forma que una gran empresa.

La movilidad, heterogeneidad y dispersión de los entornos actuales añaden nuevas dificultades a la hora de administrar y proteger las redes corporativas.

Por ejemplo, uno de los problemas existentes a la hora de proteger este nuevo conglomerado tecnológico es la existencia de una falsa sensación de seguridad causada por la creencia de que algunos dispositivos no son vulnerables, como los dispositivos Mac o Linux.

«La mayor vulnerabilidad de Macintosh es la creencia existente entre sus usuarios de que el sistema operativo Apple es superior e inmune al malware»**.

Esta concepción errónea deja una puerta abierta para que el malware (incluyendo el malware para Windows) entre tranquilamente en los sistemas y se aproveche de sus puntos débiles.

*Gartner_Marzo 2014

The Six Pain Points of Managing Mobile Devices for Small or Midsize Businesses.

** Whitepaper de mayo de 2014: Should I be worried about viruses in my MAC?

• Según AMI, los gastos por cuestiones de movilidad a los que tendrán que enfrentarse las PYMES de Estados Unidos y Canadá alcanzarán los 71.500 millones de dólares en el año 2018. La tasa de crecimiento anual de los planes de datos para tablets en Estados Unidos y Canadá es del 21%.

http://www.ami-partners.com/ index.php?target=news&mode=details&news_id=323

• Predicciones de Gartner sobre el fenómeno BYOD para el año 2017 http://www.gartner.com/newsroom/id/2466615

• Gartner predice que para el año 2017 la mitad de las empresas exigirán que sus empleados utilicen sus propios dispositivos para realizar tareas laborales.

El primer paso en la dirección correcta:

La nube, de opción para pioneros a necesidad de la industria.

En un panorama en el que las cifras de malware crecen sin parar, las empresas de seguridad no pueden seguir confiando únicamente en soluciones on-premise basadas en ficheros de firmas para proteger los sistemas informáticos de sus clientes. Además de disponer de menor capacidad de detección, como el volumen de malware en circulación aumenta, dichas soluciones son cada vez más «pesadas» y tienen un mayor impacto en el rendimiento de las redes.

En la actualidad, las empresas de seguridad miran a la nube y a la inmensa capacidad de procesamiento de los sistemas Big Data para responder a esta gran y creciente amenaza, trasfiriendo su carga de trabajo desde la red y sus dispositivos a la nube. Esto ha permitido, en parte, que algunas empresas de seguridad hayan podido responder con firmeza al nuevo panorama de malware, permitiendo a la vez que sus clientes puedan centrarse en su negocio sin tener que preocuparse de la gestión de su protección. Esto supone un gran paso en la dirección adecuada pero, como hemos mencionado anteriormente, sólo soluciona parte del problema.

En la actualidad, las vulnerabilidades presentes en el software y los sistemas operativos son la principal causa de infección, hasta el punto de que los responsables de IT más expertos saben que centrarse únicamente en los mejores antivirus y firewalls, incluso aquellos alojados en la nube, no es suficiente para responder con total garantía a un problema creciente.

Más del 90% de todas la infecciones están provocadas por vulnerabilidades no parcheadas, normalmente en software Java, Adobe, Flash, etc.

PandaLabs 2013

La mayoría de soluciones on- premise dependen de ficheros de firmas que se actualizan una vez cada 24 horas, o menos en algunos casos, pero que aun así resultan insuficientes para los 82.000 nuevos ejemplares de malware que aparecen cada día en Internet, según el informe: 2013 de PandaLabs.

Las soluciones en la nube garantizan que todo esté actualizado en todo momento, lo que elimina una tarea de administración y la necesidad de implementar hardware o software adicional en la red.

The convergence of security and management.

A medida que las vulnerabilidades de los sistemas y aplicaciones informáticas se vuelven más importantes, se está produciendo una convergencia lógica entre **la seguridad y la gestión de los dispositivos.** La seguridad va más allá del enfoque tradicional basado en el antivirus y el firewall, y alcanza un ámbito mucho mayor que empieza con la visibilidad y termina con la aplicación de políticas de seguridad en la empresa. Este nuevo enfoque debe contemplar también medidas para solucionar los problemas causados por el malware para ser considerado completo, y debe poder aplicarse en la totalidad de la red informática sin excepciones.

Hasta hace algún tiempo (en la era del PC), en redes LAN dominadas por equipos y servidores Windows salvo raras excepciones, era posible gestionar todos los aspectos relacionados con la actualización de los sistemas y del software, aunque llevase mucho tiempo. Ahora, sin embargo, la excepción se ha convertido en la regla, pero el desafío sigue siendo el mismo: los responsables de IT deben de ser capaces de gestionar todos y cada uno de sus dispositivos, independientemente de su ubicación, para proteger su seguridad. Expresado de una forma más tangible: Deben tener una visibilidad permanente de sus dispositivos, y deben asegurarse de que estén siempre actualizados, completamente parcheados y optimizados. Y si algo va mal, debe haber mecanismos para responder de forma rápida y efectiva.

Desgraciadamente, las empresas actuales suelen tener problemas hasta para disponer simplemente de visibilidad total de unos entornos cada vez más dispersos y heterogéneos.

Según estimaciones de Microsoft, sólo un 40% de las empresas disponen de un sistema creíble de gestión de sus dispositivos.

Reducir la complejidad y la fragmentación

Dispersión

La existencia de entornos dispersos y fragmentados con dispositivos de diversos tipos puede llevar

a la implementación de arreglos rápidos y soluciones fragmentadas: una solución para las actualizaciones de software, otra para la segu- ridad, una para el soporte remoto, otra para la gestión de los disposi- tivos móviles, etc.

Para poder controlar el problema y aumentar la eficiencia manteniendo el mismo número de personas en cada equipo es necesario disponer

de una solución centralizada que permita controlar todos los disposi- tivos y todas las tareas desde una única consola para todo el equipo de IT, disponible en cualquier momento y desde cualquier lugar.

Complejidad

La complejidad es un aspecto inherente al problema, sobre todo por la existencia de múltiples dispositivos por usuario, varias ubicaciones, el fenómeno BYOD, etc.

Sin embargo, responder al problema con soluciones fragmentadas sólo sirve para crear un círculo vicioso en el que la complejidad aumentará con cada solución adicional que se implemente. La solución elegida debe de aportar valor de forma rápida, ser fácil de implementar y administrar, y carecer de curva de aprendizaje. En definitiva, una solución que simplifique la complejidad de los sistemas informáticos actuales.

To summarize

El malware creado con fines económicos está creciendo de forma exponencial. Las PYMES se enfrentan al desafío de gestionar sistemas informáticos cada vez más heterogéneos, dispersos y complejos, lo que dificulta aún más el problema de la seguridad. Esto crea dificultades adicionales y exprime los recursos humanos hasta el límite de su capa- cidad y más allá.

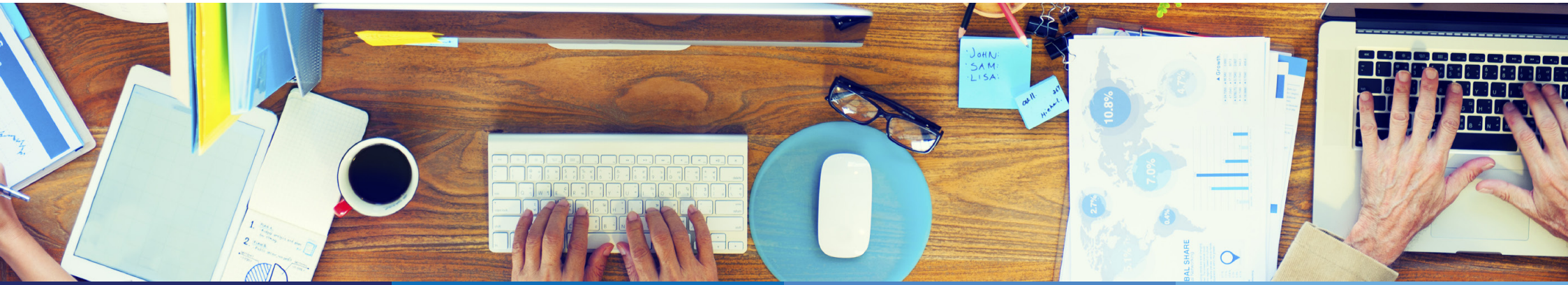
La nube, la movilidad y el Big Data no son solamente parte de esta nueva realidad informática, sino que son también parte intrínseca de su protección y administración.

La gestión y protección de los dispositivos están convergiendo, permitiendo a las empresas salvaguardar su seguridad desde una perspectiva más amplia y aumentar su eficiencia.

Dicha convergencia, para poder ser adoptada y aprovechada al máximo por las PYMES, debe ser centralizada y completa, pero NO compleja.

Las cuestiones subyacentes en este caso son la fragmentación y la complejidad.

La cuestión no es si una organización necesita gestionar y proteger todos sus dispositivos, sino cual es la mejor forma de hacerlo.



Panda Cloud Fusion

El objetivo de Panda Cloud Fusion consiste en simplificar y centralizar la seguridad, gestión y mantenimiento de los sistemas informáticos desde la nube. Panda Security propone una enfoque integral para la gestión de los sistemas en el que todos los dispositivos cuentan; No importa si se trata de un equipo con Windows XP, un servidor Linux, un MacBook, una tablet o un smartphone, o si se encuentra dentro o fuera de la LAN, con Panda Cloud Fusion podrás gestionar, proteger y mantener todos ellos desde una única consola centralizada.

Como Gartner señala en su Cuadrante Mágico sobre Plataformas de Protección Endpoint de enero de 2014, «Panda es el primer fabricante de plataformas para la protección endpoint en comprometerse plenamente con el desarrollo de servi- cios de seguridad basados en la nube.» Además de clasificarla como empresa visionaria en la protección de endpoints, Gartner destaca el poder de protección de Panda y su capacidad para «atrapar las últimas amenazas» gracias a sus tecnologías de detección por comportamiento y a la información almacenada en su plataforma de conocimiento en la nube, Inteligencia Colectiva.

En el mismo informe, Gartner menciona la fortaleza de «haber añadido recientemente una solución de gestión remota de sistemas y equipos, con funciones de auditoría, configuración, aplicación de parches y distribución de software, además de control remoto».

Las auditorías centralizadas dotan al administrador de una visibilidad permanente de todos sus sistemas informáticos desde una única consola, incluyendo dispositivos móviles y smartphones.

La inclusión de funcionalidades de aplicación de parches y distribución de software garantizan que todos los sistemas estén perfectamente parcheados y optimizados, reduciendo a su vez el riesgo de que se produzcan ataques a través de vulnerabilidades.

El soporte remoto no intrusivo completa la oferta y permite a los técnicos llevar a cabo diagnósticos exhaustivos en segundo plano sin molestar al usuario final.

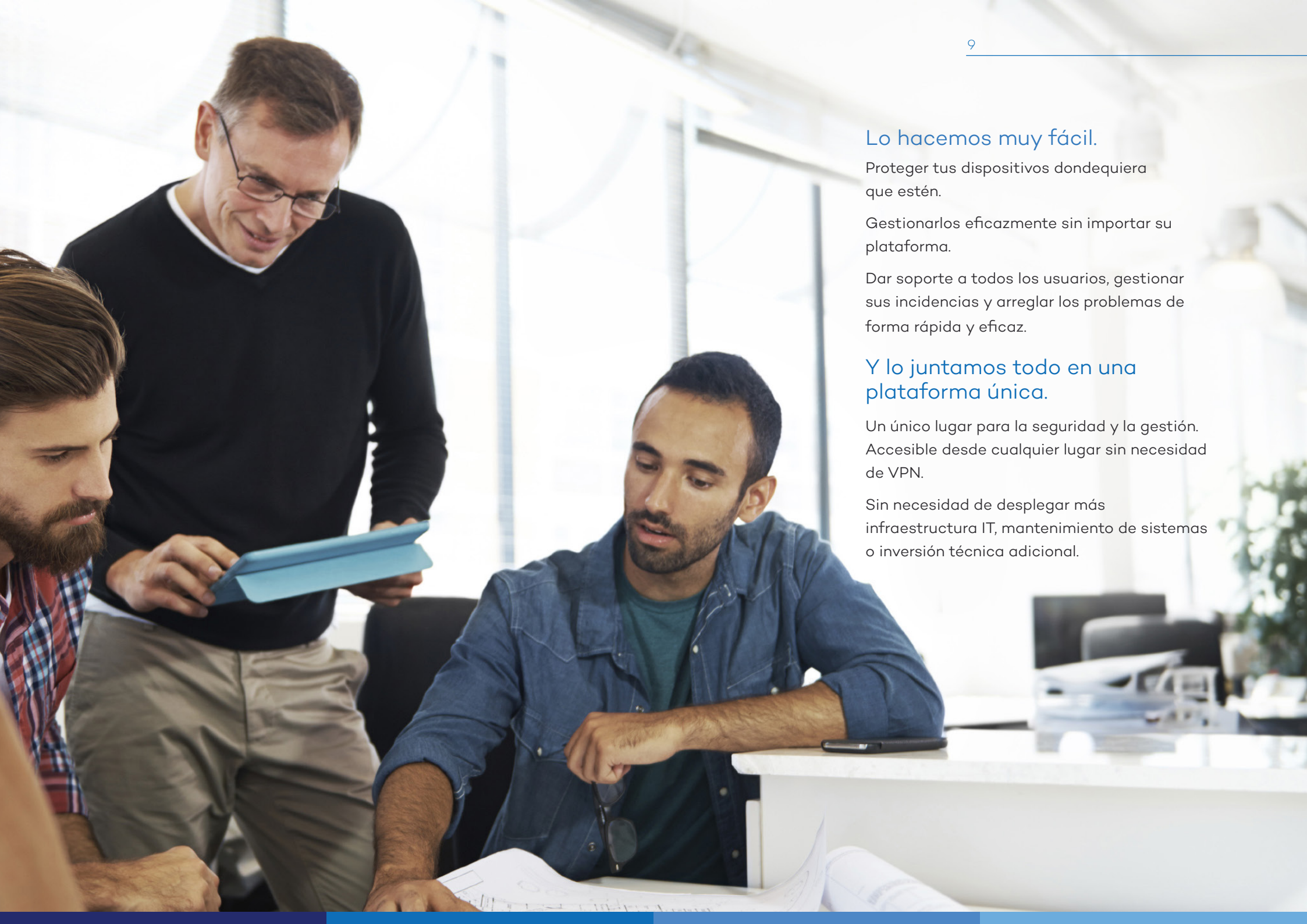
Además de optimizar y proteger todos los dispositivos, Panda Cloud Fusion ofrece a las organizaciones una gran cantidad de funcionalidades que les permitirán ser más eficientes mediante la automatización de las tareas más comunes.

Los sistemas automatizados de monitorización con respuestas predefinidas y el seguimiento de incidencias mediante tickets de soporte permiten a los profesionales centrarse en proyectos de valor añadido a la vez que garantizan una calidad de servicio consistente.

Más info sobre
Panda Cloud Solution

Pruébalo durante 30 días

Descarga aquí



Lo hacemos muy fácil.

Proteger tus dispositivos dondequiera que estén.

Gestionarlos eficazmente sin importar su plataforma.

Dar soporte a todos los usuarios, gestionar sus incidencias y arreglar los problemas de forma rápida y eficaz.

Y lo juntamos todo en una plataforma única.

Un único lugar para la seguridad y la gestión. Accesible desde cualquier lugar sin necesidad de VPN.

Sin necesidad de desplegar más infraestructura IT, mantenimiento de sistemas o inversión técnica adicional.


panda