

 EDITORIAL

SUMARIO

CHECK POINT

CITRIX

ESET

KASPERSKY

SAMSUNG

SONICWALL

WATCHGUARD

Información de valor para la toma de decisiones *director* TIC

Tar
editorial

ESPECIAL DIRECTOR TIC

2020



Claves para hacer frente al gran desafío de la seguridad en la era covid-19

Información de valor para la toma de decisiones
director TIC

La ciberseguridad marcada por la era covid-19

2019 dejaba a una España marcada por una tendencia al alza en ciberataques en la empresa española, con una media de 436 ciberataques a la semana. Y con la seguridad en la nube como una asignatura pendiente y una parte importante de las infraestructuras críticas en peligro, según Check Point. Lo que nadie imaginaba era el gran cambio que iba a representar la covid-19.

Los ciberdelincuentes no se hicieron esperar. Ávidos por hacer negocio decidieron atacar a los más vulnerables, poniendo sus miras en las infraestructuras críticas del sector sanitario o entidades como la Organización Mundial de la Salud, por poner algunos ejemplos.



Las empresas tuvieron que desplegar un teletrabajo al que se habían resistido durante años,

llevando a cabo una prueba piloto a gran escala, que ha obligado a reforzar la ciberseguri-

EDITORIAL

dad empresarial ante el perfeccionamiento de los ataques por parte de los cibertacantes y unas redes domésticas con seguridad básica; contraseñas inseguras; vulnerabilidades en las conexiones...

Esto ha hecho que las preocupaciones principales por parte de las empresas sean, según Check Point el acceso remoto seguro, y la escalabilidad de las soluciones.

En el punto de mira

Marzo y abril han estado marcados intensamente por las consecuencias de la pandemia, el confinamiento y el aumento exponencial del teletrabajo, que han hecho que los ciberdelincuentes se hayan cebado con nuestro país, según un informe de la firma de seguridad eslovaca Eset.



"Falta madurez para garantizar la fiabilidad de las comunicaciones por correo electrónico"

Uno de los mayores vectores de ataque ha sido el correo electrónico, si bien los ciberdelincuentes habían reactivado esta tendencia antes de la covid-19. Estos han llevado a cabo campañas

protagonizadas por la herramienta de control remoto Netwire con la que, mediante el uso de supuestas facturas enviadas por *email* y suplantando a Correos Express, intentan que los usuarios

descarguen un fichero malicioso desde un enlace alojado en algún servicio gratuito. Otras campañas de *malware*, *phishing* y *ransomware* también han causado preocupación.

El aumento del teletrabajo ha hecho que los ciberdelincuentes también pongan sus objetivos en algunas de las herramientas usadas como Zoom y Microsoft Teams.

Kaspersky pone el foco de atención en el aumento masivo del número de ataques de fuerza bruta al protocolo de escritorio remoto (RDP), una de las herramientas de acceso remoto más habituales en los equipos informáticos y servidores. Un tipo de ataques que busca identifi-

EDITORIAL

car el nombre de usuario y contraseña del RDP mediante un proceso de prueba y error, hasta dar con la combinación correcta. Cuando lo consigue, el cibercriminal dispone del acceso remoto al equipo objetivo, por lo que puede hacer cualquier cosa con el ordenador.

Desde Proofpoint llaman la atención sobre la falta de madurez necesaria para garantizar la fiabilidad de las comunicaciones por correo

electrónico y de la adopción de sistemas de autenticación por parte de empresas e instituciones. En un análisis llevado a cabo por la compañía han detectado más de 200 estafas relacionadas con la pandemia, que contienen más de 500.000 mensajes, 300.000 enlaces y 200.000 archivos adjuntos maliciosos en todo el mundo, con tácticas tan convincentes



que resultan casi imposible a un usuario medio diferenciar un correo electrónico falso de uno real. Para verificar la identidad de los remitentes recomiendan desplegar el protocolo DMARC (Autenticación de Mensajes, Informes y Conformidad basada en Dominios).

Por otro lado, el teletrabajo ha supuesto un gran desafío para los equipos TI y de seguri-

dad a la hora de asegurar la migración masiva a la conectividad en remoto. Según Cybonet, el 95 % de los profesionales de seguridad destacan la gran dependencia de las redes por parte de las empresas para llevar a cabo todas sus operaciones, por lo que es fundamental su vigilancia. Para comprobar posibles vulnerabilidades en la seguridad de los sistemas informáticos, redes y otros elementos críticos, desde

Cybonet recomiendan hacer pruebas de penetración y *hacking* ético.

¿Cómo pueden hacer frente las empresas a los nuevos desafíos que se les presentan en materia de seguridad? Citrix, Check Point, Eset, Kaspersky, Samsung, SonicWall y WatchGuard nos dan las claves en esta guía.

EDITORIAL

SUMARIO

CHECK POINT

CITRIX

ESET

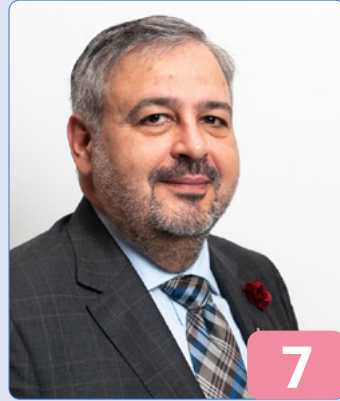
KASPERSKY

SAMSUNG

SONICWALL

WATCHGUARD

SUMARIO



7

Check Point: centrados en la seguridad de los dispositivos móviles



11

Citrix Workspace permite el acceso seguro a todos los recursos de una compañía



15

Eset: una de las compañías de mayor rendimiento en el entorno *endpoint*



19

Kaspersky: soluciones imbatibles ante diferentes pruebas de seguridad



23

La amplia estrategia de **Samsung** para garantizar la seguridad de sus dispositivos



27

El objetivo de **SonicWall** en 2020: la seguridad de la gran empresa



31

WatchGuard: un paso por delante en la gestión unificada de amenazas (UTM)

Directora: Marilés de Pedro
mariles@taieditorial.es

Redactora jefe: Inma Elizalde
inma@taieditorial.es

Redactora: Rosa Martín
rmartin@taieditorial.es

Redactora: Olga Romero
olga@taieditorial.es

Publicidad: David Rico
david@taieditorial.es

Publicidad: Nuria Díaz
nuria@taieditorial.es

Producción: Marta Arias
marta@taieditorial.es

Depósito legal: M-38033-2015
ISSN: 2341-1511

Edita:

T.A.I. Editorial, S.A.

(Técnicos Asesores

Informáticos Editorial, S.A.)

www.taieditorial.es

Avda. Fuencarral, 68

28108 Alcobendas (Madrid)

Tel. 91 661 61 02 - Fax: 91 661 29 28

e-mail: correo@taieditorial.es



Queda prohibida la reproducción total o parcial de los originales de esta publicación sin autorización por escrito.

No nos hacemos responsables de las opiniones emitidas por nuestros colaboradores y anunciantes.

No está permitida su reproducción o distribución sin la autorización expresa de Técnicos y Asociados Informáticos Editorial, S.A. Le informamos que sus datos personales y dirección de correo electrónico serán tratados por Técnicos y Asociados Informáticos Editorial, S.A., como responsables del tratamiento, con la finalidad de llevar a cabo una gestión de carácter comercial, y para el envío de nuestra publicación y también de comunicaciones comerciales sobre nuestros productos y servicios, así como de terceros que consideramos puedan resultar de su interés. Los datos serán cedidos a Tu web soluciones compañía de posicionamiento y análisis, S.L.V y Cia para la Empresa Servixmedia S.L empresas colaboradoras del responsable que tratan los datos con las mismas finalidades. Siendo conservados mientras no manifieste su oposición a seguir recibiendo el servicio solicitado. Puede usted ejercer los derechos de acceso, rectificación o supresión de sus datos, dirigiéndose a arco@taieditorial.es para más información al respecto, puede consultar nuestra Política de Privacidad en <https://taieditorial.es/politica/>

CHECK POINT

“La **digitalización** está **incompleta** si no viene acompañada de una **transformación** en términos de **ciberseguridad**”

Las previsiones de Check Point para 2020 auguraban, a principios de año, que el *phishing* se mantendría como una de las principales ciberamenazas, junto al *ransomware* dirigido. Con lo que la firma de seguridad no contaba era con un “enemigo inesperado”, que iba a incrementar el número de vulnerabilidades exponencialmente. La covid-19 ha arrasado con nuestra salud, al tiempo que pretende hacerlo con nuestra economía. Pero de toda crisis siempre surge una oportunidad, que los cibercriminales han aprovechado en beneficio propio. Eusebio Nieva, director técnico de Check Point para España y Portugal, confirma que desde la firma de seguridad israelí han detectado un crecimiento exponencial de los ataques, casi 10 veces más que la media de las últimas semanas, camuflados bajo esta temática.

Ante el confinamiento y un mayor consumo de contenidos en las plataformas digitales, los intentos de *phishing* utilizando Netflix como gancho se han duplicado. El *ransomware* dirigido ha puesto en jaque la seguridad de algunos hospitales. Y se han creado más de 16.000 nuevos dominios relacionados con el coronavi-

rus. Sin olvidar que el aumento del teletrabajo ha puesto el foco en la protección de los datos y dispositivos móviles corporativos. Esto, unido a la incertidumbre sobre cuanto se alargará esta situación, generará un cambio de paradigma de cara al futuro, asegura Eusebio Nieva.



Eusebio Nieva,
director técnico de **Check Point** para España y Portugal

CHECK POINT

La problemática del *malware*

Los piratas informáticos utilizan cada vez más la distribución automatizada de *malware*. Con el coronavirus los ataques de *malware* están suponiendo una gran amenaza para las empresas españolas, tal y como apunta el directivo. Entre los principales peligros destaca el hecho de que, con un menor esfuerzo, son capaces de infectar un mayor número de dispositivos, incrementando el número de potenciales víctimas y su tasa de efectividad. Entre sus principales objetivos figuran infectar los equipos de los usuarios o el robo de datos.

Un tipo de *malware*, el evasivo, está convirtiéndose en la regla. Uno de los principales riesgos que conlleva reside en que, al ser evasivo, este tipo de ataques pueden permanecer más tiempo dentro de dispositivos o redes corporativas, aumentando los daños, haciendo que las medidas tradicionales de seguridad no sean eficaces.

Para evitar estas vulnerabilidades Eusebio Nieva aconseja aplicar un enfoque centrado en la prevención y contar con las herramientas de ciberseguridad adecuadas para protegerse frente a archivos infectados, acceso a páginas web



maliciosas, etc. Así como garantizar la movilidad de dispositivos y datos en un momento en el que los empleados están teletrabajando desde ubicaciones y redes que no son las habituales. Entre las herramientas con las que Check Point cuenta para ello destaca ZoneAlarm Extreme Security, cuya extensión gratuita Anti-Phishing

Chrome Extensión escanea y elimina sitios web antes de que el usuario llegue a insertar su información personal, alertándole de si es un lugar seguro para usar o un sitio de *phishing*, independientemente del dispositivo desde el que se intente acceder.

Por otro lado, aconseja actualizar todos los sistemas y dispositivos de las empresas con los últimos parches y actualizaciones instalados, ya que el *malware* evasivo aprovecha las brechas existentes en nuestros equipos.

Análisis DAFO empresarial

A la hora de hacer un análisis sobre las fortalezas, debilidades, oportunidades y amenazas de las empresas, sería necesario ir viendo cada caso, pero en términos generales Nieva resalta que entre las principales debilidades se encuentran los dispositivos móviles que, en su mayoría, no están securizados y son un blanco fácil para los cibercriminales, sobre todo en el ámbito del teletrabajo. Sin olvidar la falta

CHECK POINT

de formación en nociones básicas de ciberseguridad. En cuanto a las amenazas, advierte sobre las nuevas generaciones de ciberataques, que son cada vez más sofisticados, sin olvidarnos de clásicos como el *phishing* o el *ransomware*.

Entre las fortalezas apunta a la cada vez mayor cultura en ciberseguridad que van adquiriendo nuestras organizaciones. Algo que también redundará en el apartado de las oportunidades, entre las que también menciona la adopción de un cambio de enfoque, pasando de defender ante un ataque a evitar las amenazas.

Hoja de ruta para CIO y CISO

Consejos todo ellos que también son extrapolables al CIO y al CISO de las empresas, aunque para ellos Eusebio Nieva añade otros, con el fin de ayudarles a mantener la

seguridad en sus compañías. Entre ellos la prevención y protección de entornos y dispositivos IoT. Y la movilidad, tanto de datos, como de elementos físicos como *smartphones*, ordenadores portátiles... ya que cada vez es mayor el número de puntos de conexión dentro de una misma red corporativa, por lo que considera necesario contar con herramientas de seguridad escalables que se adapten a las necesidades de las empre-

sas en todo momento. Y más en plena transformación digital, ya que tal y como Eusebio Nieva recuerda, "la digitalización está incompleta si no viene acompañada de una transformación en términos de ciberseguridad".

En este sentido, el enfoque de Check Point pasa por la escalabilidad y su lema "seguridad para todo", con el fin de concienciar sobre la necesidad de proteger todo lo que nos rodea ya

que, tal y como sostiene, "la protección debe expandirse a todos los puntos de conexión a la red corporativa, sobre todo teniendo en cuenta el auge del IoT o de tendencias como el *Bring Your Own Device*". En este sentido, desde Check Point están especialmente concienciados con la protección de los dispositivos móviles, un área que centra la estrategia de seguridad de la compañía para este año.



CHECK POINT

La limpieza de documentos, fundamental

Prevenir. Esa es la clave de Check Point para evitar que los usuarios sean atacados por los ciberdelincuentes. Una prevención que debe ir acompañada por medidas adicionales como la segmentación de todas las redes o las medidas higiénicas que los usuarios deben tener. Eusebio Nieva, director técnico de Check Point para España y Portugal, afirma que la limpieza del correo electrónico es fundamental porque ahí es donde se originan los ataques de *phishing* y por donde llega el *malware*.



Fortalezas en ciberseguridad de Check Point

Una de las fortalezas de Check Point es su amplio abanico de soluciones. Soluciones de seguridad que cubren todo el espectro de amenazas del usuario: desde la nube, las aplicaciones a través de un servicio en la nube, en la infraestructura en la nube, en las infraestructuras internas y estableciendo políticas *Zero Trust* dentro de las compañías. En definitiva, abarcan todas las soluciones con una única gestión. Así lo explica Eusebio Nieva, director técnico de Check Point para España y Portugal, en este vídeo.



Citrix protege al usuario al asegurar el espacio de trabajo"

Nuno Silveiro, *sales networking specialist* de Citrix, reconoce que 2020 ha empezado de un modo totalmente inesperado, mostrando la importancia de tener un espacio de trabajo digital seguro. Por ello, considera que para las empresas es fundamental contar con un ecosistema como el Workspace de Citrix, en el que se engloban herramientas de autenticación, seguridad, alta disponibilidad y balanceo de Citrix ADC, junto a su tecnología SD-WAN para conectar oficinas y hogares al entorno multinube híbrida.

"Históricamente la ciberseguridad ha utilizado un principio de castillo y foso, donde el acceso a la información corporativa por parte de los usuarios y de los dispositivos fuera de la red estaba protegido por una combinación de *firewall*, autenticación y VPN, con la premisa de que todos los que estaban dentro de la red corporativa eran confiables", explica el directivo. Pero el mundo ha cambiado y hoy los usuarios consumen un conjunto de aplicaciones desde la nube, web y su CPD por lo que este modelo de seguridad ya no aplica. Por ello, asegura que en un momento en el que las amenazas llegan a las empresas de diferentes maneras, es



Nuno Silveiro, *sales networking specialist* de Citrix

muy importante enfocarse en la seguridad de la aplicación y en el usuario a través de políticas de "confianza base zero" o "zero trust" ya que los usuarios se conectan desde distintos dispositivos, ubicaciones, redes

CITRIX

y aplicaciones que pueden estar en diferentes nubes, en el CPD o en el SaaS, ampliando el perímetro.

Silverio considera como elemento fundamental transmitir las políticas de seguridad a los usuarios para que sospechen de un *email* que puede ser un "*phishing*", comprender lo importante que es tener una contraseña segura o no dejar el ordenador desbloqueado mientras toman un café.

Citrix garantiza una productividad segura, analizando las diferentes dimensiones del usuario dentro de la perspectiva de "*zero trust*" entre el dispositivo corporativo o personal. En la parte del usuario evalúan, en función del contexto, realizando un acceso granular, permitiendo a ese usuario tener acceso a más o menos funcionalidades. Y desde la dimensión de la aplicación, definen qué puede hacer el usuario con ella para evitar determinados riesgos. Dentro del paraguas de



"Citrix Workspace permite el acceso seguro a todos los recursos de una compañía"

estas dimensiones, añaden una capa de visibilidad que permite tomar decisiones con datos,

en tiempo real y con la ayuda de inteligencia artificial, siempre que exista una sospecha de la violación de la seguridad.

Seguridad a demanda

Citrix Workspace permite el acceso seguro a todos los recursos de una compañía, desde aplicaciones SaaS como aplicaciones web internas, aplicaciones nativas, aplicaciones virtuales y escritorios, y archivos en cualquier dispositivo desde cualquier lugar.

Nuno Silverio destaca que, "a diferencia de otras soluciones de gestión de acceso, no solo proporciona SSO a SaaS y aplicaciones web, también proporciona controles de seguridad adicionales para proteger los datos dentro de estas aplicaciones. Los administradores pueden insertar marcas de agua en páginas SaaS que tienen información crítica y altamente confidencial. Pueden evitar copiar datos de estas

CITRIX

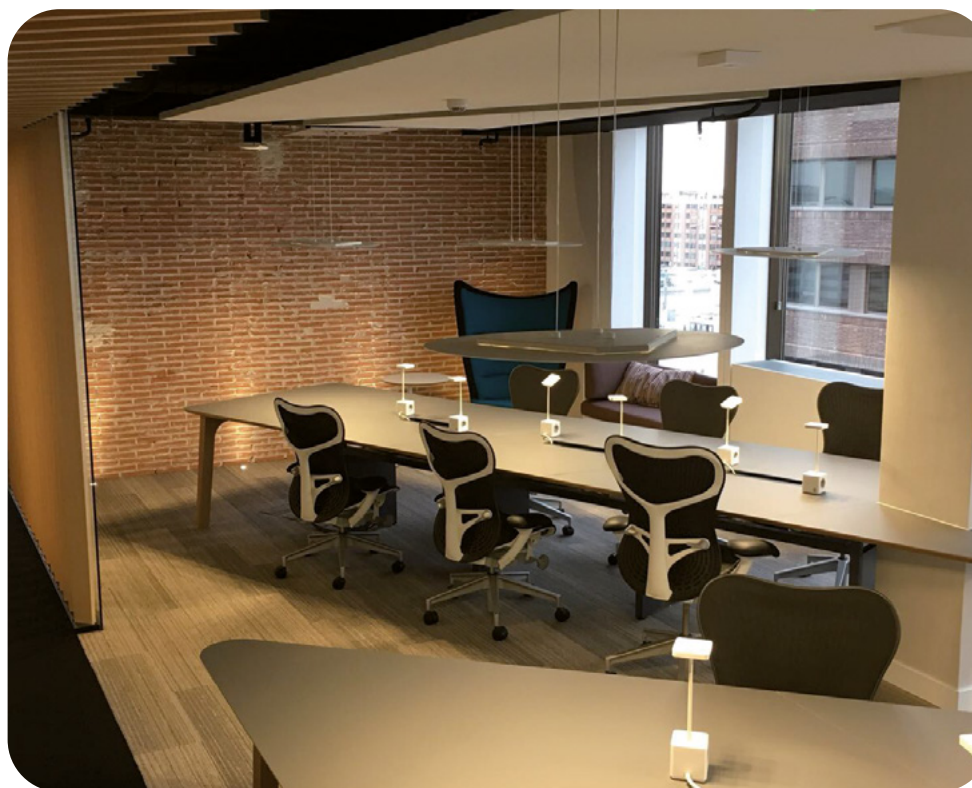
aplicaciones y pueden evitar el robo de datos corporativos y de usuarios al impedir el acceso a enlaces maliciosos integrados en estas aplicaciones”.

La tecnología *anti-keylogger* del Citrix Workspace proporciona protección transparente contra *keyloggers* maliciosos y *malware* de captura de pantalla. Y las soluciones de filtrado de URL

y aislamiento remoto del navegador protegen al usuario de ataques de *malware* como *phishing* y *ransomware*. Estas capacidades pueden activarse en función de factores contextuales en el momento del inicio de sesión. “En conjunto, con Citrix Analytics for Security, proporcionamos un entorno seguro para el usuario al monitorear continuamente los eventos e indicadores de riesgo de los servicios de Citrix y las soluciones de seguridad de terceros”, añade.

CISO y CIO

Nuno Silverio considera que una gran mayoría de los CISO hacen, en muchos casos, “verdaderas obras épicas con los recursos que las compañías les destinan, ya que existe una sobrevaloración de la confianza en el factor humano interno y una subvaloración de las amenazas cibernéticas reales”.



Por ello, les aconseja pensar en la seguridad desde una perspectiva contextual, analizando quién es el usuario, qué está realizando, dónde está, cuándo se está conectando y porqué se está conectando y con todo ello determinar qué grado de permiso va a tener. Al tiempo que advierte que tener como base de la seguridad los modelos de seguridad de *firewall* de nueva

generación, con acceso remoto por VPN y doble factor de autenticación ya no basta para las amenazas actuales. “Si el usuario tiene un dispositivo infectado con un *keylogger* o con un troyano que haga grabación de pantalla, estos mecanismos de seguridad ya no van a ser suficientes”, señala.

Las compañías que no cuentan con un CISO confían en la experiencia de Citrix. 30 años garantizando la seguridad de las aplicaciones y dando a las empresas una visión holística del estado de seguridad de sus organizaciones de 360 grados, es su mayor aval.

ESET

Eset proporciona un alto rendimiento en seguridad al usuario final

La implantación masiva del teletrabajo, impuesta por las circunstancias de la pandemia, en marzo, ha dejado al descubierto la falta de planes de contingencia por parte de un elevado número de compañías para poder desarrollar su actividad por medio del mismo. Así lo reconoce Carlos Tortosa, director de canal y grandes cuentas de Eset España.

En este sentido admite que desde Eset han encontrado empresas con empleados que comenzaron a utilizar dispositivos con una seguridad obsoleta o inexistente. Se ha generado la necesidad de reconocer a la persona que accedía a la información de la compañía por medio de herramientas que identifican, de manera fehaciente, quien está accediendo a la misma. Y monitorizar quien accede a cada activo para evitar las fugas de información.

Medidas de prevención

Tortosa pide no relajar las medidas que adoptamos en la sede de la empresa porque, tal y como recuerda, teletrabajar supone ampliar los riesgos que corremos. Por ello aconseja utilizar herramientas de protección más robustas,



Carlos Tortosa, director de canal y grandes cuentas de Eset España

en caso de ser posible; identificar al usuario, asegurar qué herramientas utiliza el usuario para proteger sus dispositivos y reforzar la formación

ESET



"Eset protege prácticamente cualquier sistema operativo en el entorno endpoint"

que reciben los empleados para que aumente su atención ante ciertas amenazas.

Y, aunque la situación parece no revertir en breve, el teletrabajo permanecerá cuando la pandemia quede atrás ya que hay compañías que están valorando seguir teletrabajando por deci-

sión propia, por lo que será necesario mantener vigente el plan de contingencia y las medidas de seguridad adoptadas, asegura. "Una vez se regularice la situación e iniciemos esa nueva realidad anunciada, será necesario tener visibilidad de los activos a los que se ha accedido, utilizando herramientas como un DLP", apunta.

Fortalezas

En su lucha contra un cibercrimen que ha aprovechado esta situación para lanzar nuevos ataques y diseñar nuevas campañas malignas, Eset ha trabajado analizando todo ello para dar a los usuarios la información necesaria que les mantuviera alerta. Una labor que llevan haciendo desde sus inicios y que les ha valido para que analistas independientes como Kuppinger Cole les haya reconocido como una de las compañías de mayor rendimiento en el entorno *endpoint*.

Entre las fortalezas que presentan en este sentido, Carlos Tortosa destaca el alto rendimiento que proporcionan al usuario final. "El motor de análisis de Eset desde sus inicios fue una he-

EDITORIAL

SUMARIO

CHECK POINT

CITRIX

ESET

KASPERSKY

SAMSUNG

SONICWALL

WATCHGUARD

ESET

Kuppinger Cole ha reconocido a Eset como una de las compañías de mayor rendimiento en el entorno endpoint

“Herramienta que cargaba muy poco los sistemas y esta característica se ha aplicado a cualquier nuevo desarrollo que se ha llevado a término”, comenta. “Aparte, disponemos de una serie de características altamente demandadas como la protección *antiransomware*”.

Además, protegen prácticamente cualquier sistema operativo en entorno *endpoint*, cubriendo incluso SO obsoletos como XP, o SO Linux cuya solución han lanzado recientemente en una nueva versión actualizada. “Independiente de todo ello facilitamos una consola de administración



centralizada en entorno *onpremise* o *cloud*, muy accesible y de fácil uso que permite una gestión integral de todas las soluciones de seguridad que Eset proporciona a sus clientes”, recuerda. En cuanto a la privacidad de los datos que se recopilan en los dispositivos, opina que es primordial centrarse primero en la seguridad de los dispositivos que utilizamos, y de las aplicaciones que

vamos añadiendo. Sin olvidar estar informados de cualquier noticia que surja respecto a nuevas vulnerabilidades o ataques por parte de los ciberdelincuentes. En el caso de Eset esta información está actualizada en su *blog* “blogs.protegerse.com” en la que la compañía de seguridad intenta mostrar, de manera sencilla, las investigaciones que sus equipos de analistas realizan.

ESET

Eset ayuda a ver los flancos abiertos en ciberseguridad

El teletrabajo tiene que llevar consigo una serie de medidas de seguridad que, en muchos casos, las empresas no han tenido en cuenta por la velocidad a la que han implantado el mismo.

Carlos Tortosa, director de grandes cuentas y canal en Eset, manifiesta en este vídeo que desde esta compañía de ciberseguridad están ayudando a las organizaciones a ver los flancos que podrían tener abiertos, en temas tan importantes como la protección de sus dispositivos.



VÍDEO



Eset y sus herramientas contra amenazas avanzadas persistentes

Recientemente Eset ha sido nombrado "Top Player" en el cuadrante de Radicati, sobre protección contra amenazas avanzadas persistentes. Carlos Tortosa, director de grandes cuentas y canal en Eset, destaca en este vídeo que las herramientas de última generación por las que han sido premiados permiten, por un lado, la protección de la información por medio de la herramienta instalada en cada uno de los equipos de cada *endpoint* y, por otro lado, una gestión centralizada que le hace la vida muy fácil al administrador de sistemas o al responsable de seguridad de la empresa.



VÍDEO



Kaspersky: invencible ante las pruebas de seguridad

Las empresas pueden ser más vulnerables que nunca ante la actual situación de pandemia y el uso masivo del teletrabajo, sobre todo si tenemos en cuenta el último estudio de Kaspersky que indica que el 73 % de los empleados españoles no ha recibido formación en ciberseguridad para teletrabajar. Por ello, recomiendan tanto que las organizaciones formen a su personal en ciberseguridad como contar con soluciones de seguridad robustas.

En un mundo en el que los ciberdelincuentes no descansan, las empresas españolas están en el punto de mira. Según el informe *IT Security Economics 2019* de Kaspersky, el coste medio de una brecha de datos, a nivel empresarial, en 2019, en España podía oscilar entre los 82.000 dólares de una pyme a los 442.000 dólares de una gran empresa. Las de mayor coste siguen siendo las infecciones de *malware* en los dispositivos corporativos, que afectan a la infraestructura de los proveedores con los que se comparte información, o las que afectan a los dispositivos del IoT. Aunque también crecen, en gran medida, los ataques dirigidos a la vulneración de los datos empresariales y personales.

Por ello, Alfonso Ramírez, director general de Kaspersky Iberia, advierte a las organizaciones de que, independientemente de su tamaño, tie-



Alfonso Ramírez, director general de Kaspersky Iberia

nen que mejorar su seguridad constantemente. Un enfoque, el de la seguridad adaptativa, que consiste en prevenir, detectar, responder y predecir, sobre el que la multinacional de ciberseguridad asesora a sus clientes.

Estar preparados para afrontar un ciberataque, con soluciones de seguridad fiables que protejan los diferentes puntos de la infraestructu-

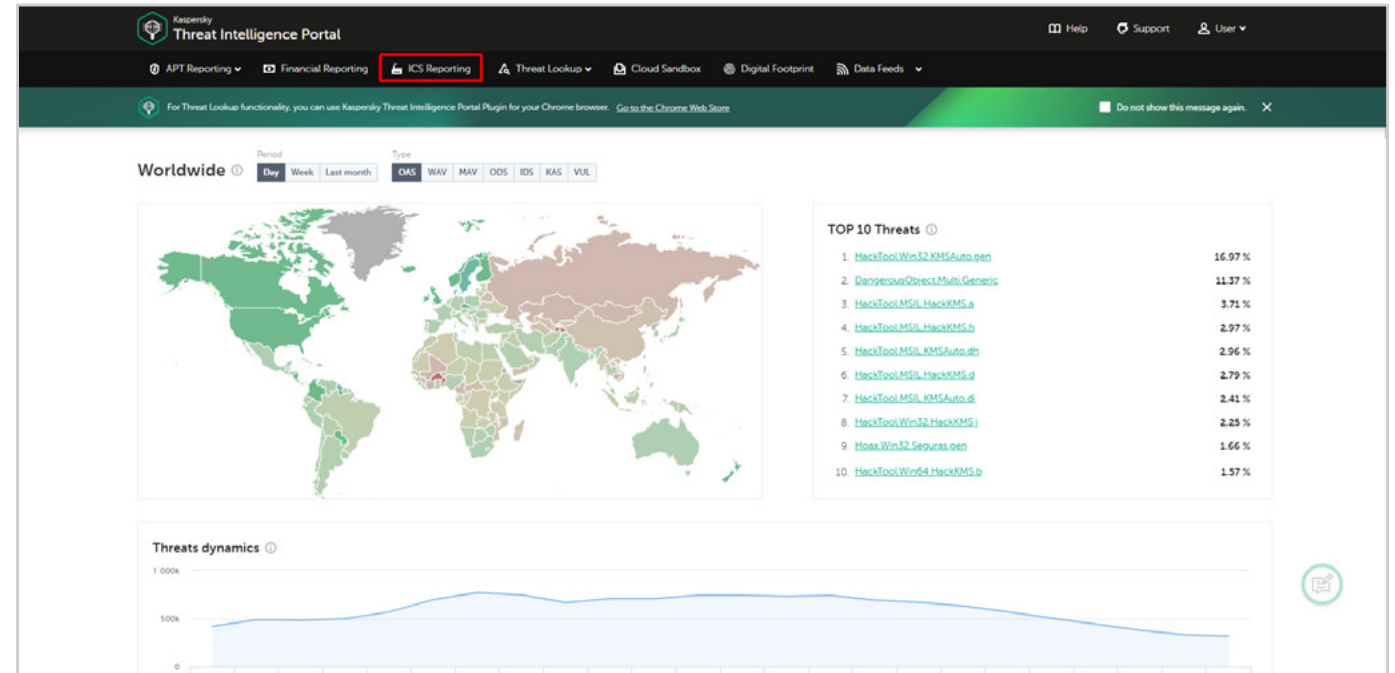
KASPERSKY

ra corporativa, es fundamental. Y contar con trabajadores que estén alerta imprescindible porque, según estudios de Kaspersky, solo un 12 % de los empleados encuestados son conscientes de las políticas y normas de seguridad de TI establecidas en sus organizaciones. Y en un 46 % de los incidentes se vieron involucrados empleados que comprometieron la seguridad de forma involuntaria o inconsciente.

Ramírez recuerda que un gran número de campañas de *phishing* y otro tipo de ataques se dirigen a los empleados, con el fin de conseguir información personal identificable o comprometer las infraestructuras corporativas. El desenlace para las empresas en las que sus datos se han visto violados suele pasar por problemas a la hora de atraer nuevos clientes.

Crecimiento y fortalezas

Según Alfonso Ramírez, en los próximos tres años la seguridad seguirá creciendo un 9 % en Europa. En este sentido Kaspersky, en el mercado español, apuesta por las soluciones



En 2019 consiguieron el podio en 70 de las 86 pruebas independientes en las que participaron

y los servicios de inteligencia, por soluciones que van más allá del *endpoint* como el EDR y

la ciberseguridad industrial, segmentos donde esperan registrar mayor crecimiento.

Su intención, reconoce, es "seguir incrementando su presencia tanto en los mercados B2C como B2B -en *non-endpoint* y en servicios de inteligencia de ciberseguridad-, desarrollando soluciones y servicios innovadores para proteger de las ciberamenazas más sofisticadas a las infraestructuras críticas, las ciudades, las empresas y las personas".

KASPERSKY

*El concepto de inteligencia
HuMachine, fundamental
para la efectividad de sus
productos*

Las perspectivas para la multinacional de ciberseguridad son buenas. En 2019, los productos de Kaspersky consiguieron el podio en 70 de las 86 pruebas independientes en las que participaron, de ellos 64 fueron primeros puestos, algo que para Alfonso Ramírez indica que sus tecnologías mantienen altos niveles de calidad y ayudan a proteger a millones de sus clientes contra las ciberamenazas más complejas. En esto también influye su enfoque de ciberinmunidad, basado en la integración de la ciberseguridad desde el diseño de la arquitectura del sistema. Con ello, tratan de desarrollar un ecosistema donde todo dispositivo conectado



esté protegido. Lanzar al mercado productos inmunes.

Otro elemento fundamental es la importancia de la inteligencia artificial en sus soluciones porque, tal y como reconoce Alfonso Ramírez, la efectividad de sus productos se debe igualmente al concepto de inteligencia HuMachine, “la base de la verdadera ciberseguridad”, dice. La esencia de la inteligencia HuMachine

pasa por la fusión de tres elementos: *big data*, aprendizaje automático y la experiencia de sus analistas.

Sin olvidar que Kaspersky también se está adentrando con fuerza en la protección de aplicaciones *blockchain*, con una nueva oferta de servicios con la que pretenden ayudar a las organizaciones a proteger las aplicaciones basadas en *blockchain* que desarrollan internamente.

Soluciones destacables

La seguridad en el *endpoint* es la base de cualquier estrategia de seguridad corporativa. Kaspersky cuenta con soluciones para su protección que se adaptan a todos los tamaños de empresa. La compañía ha presentado recientemente **Kaspersky Endpoint Security Cloud** que incorpora ahora Kaspersky Security para Microsoft Office 365 y protege todas las aplicaciones de Microsoft Office 365, incluyendo Exchange Online, OneDrive y SharePoint Online y garantiza el intercambio seguro de archivos a través de Microsoft Teams.

En el ámbito del *blockchain* la compañía cuenta con **Kaspersky Enterprise Blockchain Security**, que incluye los servicios Smart Contract / Chain Code Audit y Application Security Assessment. Esta solución lleva a cabo una evaluación de las aplicaciones que trabajan sobre la infraestructura *blockchain* y una auditoría inteligente del código del contrato, ayudando a las empresas a descubrir y solucionar problemas de seguridad y discrepancias en la lógica de negocio de los contratos inteligentes.

En el ámbito de las soluciones más reconocidas por los proveedores podemos destacar **Kaspersky Anti Targeted Attack**, solución contra amenazas avanzadas. La única de su clase que demostró un 100 % de detección y cero falsos positivos en la prueba de Protección contra Amenazas Avanzadas realizada por **ICSA Labs en el tercer trimestre**

de 2019. También superó con éxito el **Test de Respuesta a Brechas de SE Labs**, en el que se emulan 85 ataques para comprobar si la solución puede prevenir y remediar cualquier daño real, no solo detectarlos.

Kaspersky EDR también es fundamental. Con ella las empresas están mejorando su estrategia de seguridad para responder a las amenazas avanzadas y a los ciberataques modernos.

Para evitar errores humanos: **Kaspersky Security Awareness**, una familia de productos de formación *online* que emplea lo último en técnicas de aprendizaje y aborda todos los niveles de la estructura empresarial.

También es destacable **Kaspersky Security Cloud**, una solución que ofrece antivirus, *antiransomware*, seguridad móvil, gestión de contraseñas, VPN y control parental, además de herramientas de privacidad, detección de fugas de datos, seguridad para redes Wi-Fi domésticas y protección de pagos. Existe la posibilidad de probarlo de forma gratuita durante 30 días.

Kaspersky también ha incorporado formación sobre GDPR y confidencialidad de los datos en su plataforma de concienciación sobre seguridad, **Kaspersky Automated Security Awareness**, así como nuevos temas de formación, para ayudar a las empresas a mejorar la capacitación de su personal. Y un curso sobre datos confidenciales.

Samsung o la seguridad en la movilidad

El mundo empresarial está sometido a un gran número de riesgos. Los ciberatacantes no descansan y la seguridad móvil se ha convertido en una preocupación. David Alonso, director del área B2B de Samsung, asegura que la misión de esta multinacional pasa por ayudar a las empresas a superar los desafíos provocados por una digitalización cada vez mayor, sobre todo en el ámbito de la movilidad, proporcionando nuevos servicios y dispositivos que les hagan mantener su actividad con los estándares de seguridad más altos.

Samsung Knox es una de las soluciones de seguridad de Samsung más conocidas, sin embargo la multinacional coreana cuenta con una amplia gama de soluciones de seguridad en la que se incluyen circuitos integrados para tarjetas inteligentes, procesadores IoT, semiconductores... Así lo reconoce David Alonso, al afirmar que "Samsung es el único fabricante de dispositivos que adopta una estrategia amplia e integral para garantizar la seguridad de sus dispositivos". Entre sus fortalezas figuran los estrictos estándares de seguridad de Gobiernos de todo el mundo, con los que cumple su plataforma Samsung Knox, como el de Estados Unidos, con la



David Alonso, director del área B2B de Samsung

Agencia de Sistemas de Información de Defensa (DISA), la Agencia Nacional de Seguridad de Sistemas de Información de Francia o el Centro Criptológico Nacional en España, por poner algunos ejemplos.

Para conseguir que sus dispositivos sean aprobados para su uso en redes gubernamentales seguras, la compañía los envía a organismos

SAMSUNG



de certificación gubernamentales de todo el mundo, donde pueden probar todas las novedades de seguridad. Esto les ha llevado a conseguir un mayor número de acreditaciones de seguridad, a nivel global, que cualquier otro dispositivo o plataforma en la historia de la industria, asegura Alonso.

Todo ello les ha llevado a obtener un gran número de reconocimientos. Samsung Knox ha sido clasificada como la plataforma de seguridad más sólida y robusta, obteniendo la máxima calificación en 27 de las 30 categorías de seguridad empresarial, posicionándoles como la plataforma de mayor confianza en el mer-

cado, con el mayor número de certificaciones de seguridad recibidas en todo el mundo.

La movilidad, fundamental

Cada día es mayor el número de profesionales que trabajan en movilidad. En este apartado Samsung apuesta por dispositivos seguros de principio a fin, que incluyen una solución de seguridad que permite la gestión de todo el ciclo de vida del equipo. "Para nosotros la protección de la información comienza en la etapa de producción, con la implementación de la seguridad en el hardware, y continúa con una serie de comprobaciones que se activan desde que se inicia el sistema e incluso cuando el dispositivo está apagado, por lo que se monitoriza la integridad del equipo, tanto si se utiliza como si no", sostiene el directivo.

Samsung Knox encripta los datos y los aísla

para evitar intromisiones en el caso de pérdida o robo del dispositivo. Actualmente, esta plataforma protege más de 1.000 millones de dispositivos, donde también se incluyen Administraciones Públicas de todo el mundo, por lo que se trata de un sistema muy robusto y de gran fiabilidad.

Por otro lado, la protección física de los dispositivos también es un aspecto clave para la multinacional coreana, con el fin de evitar el acceso de personas no autorizadas a la información sensible que se almacena en los



SAMSUNG

smartphones empresariales. Para ello cuentan con múltiples soluciones biométricas que protegen la información gracias a tecnologías de vanguardia, como el sensor de huella dactilar ultrasónico 3D, o el reconocimiento facial.

Samsung acaba de lanzar un *chip* de seguridad mejorado para dispositivos móviles, que protege completamente los datos privados en un almacenamiento de datos aislado. David Alonso lo define como “una caja fuerte a prueba de manipulaciones, que almacena

de forma segura los datos confidenciales y criptográficos de los usuarios, como los códigos PIN, las contraseñas o las credenciales de criptomonedas, separada de la memoria móvil típica. “Este *chip* agrega una serie de protecciones adicionales para defenderse de posibles ataques como la ingeniería inversa, la falta de potencia o ataques láser”, explica, lo que hace que sea extremadamente difícil para otros acceder o copiar los datos confidenciales almacenados. Además, gestiona los intentos fallidos y evita que se repitan los ataques al aceptar solo la última solicitud de autenticación como válida.

Otras fortalezas

David Alonso quiere poner el foco, además, en el resto de soluciones de seguridad como la herramienta Samsung Enterprise Firmware Over the Air (E-FOTA), con la que los departamentos de TI pueden tener control sobre el sistema operativo, actualizaciones y parches de seguridad. Gracias a la misma los admi-



nistradores pueden probar las actualizaciones antes de la implementación, con el fin de asegurar la compatibilidad entre el software interno y la nueva versión de *firmware*. Además, recuerda que Samsung Knox Configure permite la configuración de manera remota y automática de una gran cantidad de dispositivos, en función de los requisitos de cada perfil de usuario. También posibilita la incorporación de la marca de la empresa en el dispositivo, incluyendo las pantallas de arranque y las aplicaciones empresariales personalizadas.

Incrementa su seguridad en movilidad



Descubra en este enlace cómo Samsung, a través de su plataforma Knox, puede ayudarle a incrementar la seguridad de su empresa en movilidad.



SAMSUNG

Seguridad, uno de los mayores desafíos en el teletrabajo

El teletrabajo ha supuesto un gran reto para la mayor parte del sector empresarial ya que, tal y como reconoce David Alonso, director del área B2B de Samsung, en este vídeo, tan solo había un número muy reducido de compañías preparadas para llevarlo a cabo.

Poner a disposición de los trabajadores todas las herramientas necesarias supone uno de los mayores desafíos, junto a la necesaria seguridad. Así lo afirma el directivo a continuación.



Soluciones de seguridad para el ciclo de vida de un dispositivo

Ante situaciones de crisis hay que actuar rápidamente y con seguridad. Samsung protege los dispositivos con Samsung Knox, una plataforma que nació en 2013, que ha evolucionado hacia un *portfolio* de soluciones y servicios que gestionan todo el ciclo de vida del dispositivo.

En este vídeo David Alonso, director del área B2B de la compañía, describe la evolución de Samsung Knox y cómo ayuda a mantener la seguridad desde que el dispositivo sale de la caja.



SonicWall: “Una nueva ciberseguridad es necesaria”

Tres décadas de vida han servido para que SonicWall haya protegido a más de un millón de redes, en más de 200 países y cuente con más de 200 patentes, entre ellas RTDMI (*Real Time Deep Memory Inspection*), su algoritmo de reconocimiento de *malware* en tiempo real, que hace que el software malicioso se manifieste para detectarlo y bloquearlo al instante.

Importante también su presencia en entornos distribuidos y pyme en todo el mundo, con una cuota de mercado superior al 30 %. Así lo reconocen Sergio Martínez, director regional de Iberia, y Luis Fisas, director del sur de Europa de SonicWall.

Esta larga andadura en el ámbito de la ciberseguridad les permite ser conscientes del gran cambio que va a experimentar el mundo tras la covid-19. Un cambio de paradigma que viene dado, en gran medida por el aumento exponencial de la superficie de exposición y la desaparición del perímetro, por el paso hacia el teletrabajo del 10 al 100 % de empresas y organizaciones, apunta Sergio Martínez. Esto les está llevando a proporcionar a sus usuarios una experiencia similar a la que tienen dentro de la oficina, pero en un entor-

no mucho más hostil. “Esta situación ha puesto en primer plano las soluciones de acceso remoto seguro a redes, datos y aplicaciones, la autenticación segura y un incremento muy sustancial de ataques sofisticados para robo de identidades o el secuestro de ordenadores, por poner algunos ejemplos”, comenta. En definitiva, “una nueva ciberseguridad es necesaria y ya nunca volveremos a la situación anterior”.

¿Qué lección podemos aprender de esta crisis en materia de seguridad? Por un lado, que en



Luis Fisas, director del sur de Europa de SonicWall

SONICWALL



Sergio Martínez, director regional de Iberia de SonicWall

dos semanas hemos avanzado lo que estaba planificado realizarse en seis o siete y que la capacidad de transformación de los equipos

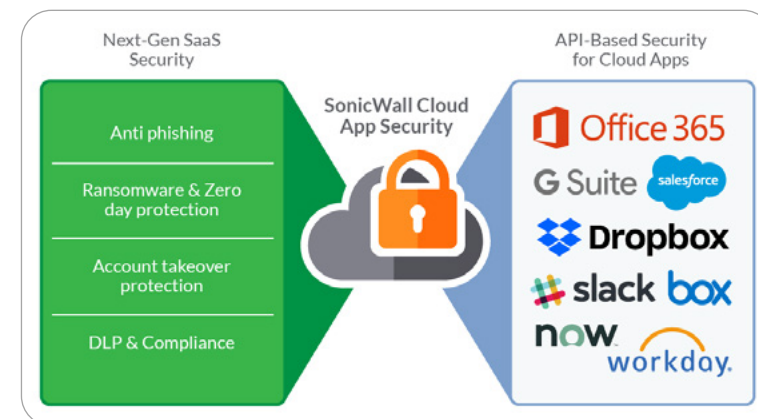
“Una nueva ciberseguridad es necesaria y ya nunca volveremos a la situación anterior”

de IT y ciberseguridad ha sido extraordinaria, responde Luis Fisas. “Pero también que el cibercrimen se ha adaptado y utilizado para su beneficio este cambio tan drástico, por lo que necesitamos más que nunca una seguridad por capas para enfrentarnos a lo desconocido, una capacidad de detección y respuesta en tiempo real a cualquier nivel: desde el *endpoint* hasta el *cloud*, el *firewall* o el *email*”, resalta.

Buenas perspectivas

Si 2019 fue un buen año para SonicWall, al suministrar miles de *firewalls* en España, 2020 se presenta mejor para la compañía, al experimentar un gran crecimiento de febrero a abril, por encima del 50 % con respecto al mismo trimestre del año pasado, sobre todo en su área de

negocio de acceso remoto, en la que cuentan con *appliances* físicos y virtuales y licencias SSL VPN o IPsec, así como la protección del *endpoint* y de las aplicaciones *cloud* (CAS-Cloud Application Security). Aunque Sergio Martínez reconoce que también han detectado una gran inquietud en el mercado para la autenticación en este nuevo mundo sin perímetro. Esto les ha llevado a establecer una colaboración con Perimeter 81, para construir una nue-



SONICWALL

va arquitectura de ciberseguridad en este entorno del que dice “nos hemos precipitado de forma súbita”. 2020 también será el año en el que se dirijan más a la gran empresa. Para ello cuentan con un nuevo producto en *portfolio*, avanza Luis Fisas: “muy sólido, integrado, con capacidades avanzadas de IA para la detección de *malware* sofisticado gracias a algoritmos propios como RTDMI. Todo ello lo hacen a través de su canal de distribución, del que afirman sentirse muy orgullosos.

Aspectos a reforzar

En el desafío que representa la seguridad hay eslabones que hay que reforzar, reconocen ambos directivos: el más débil, el factor humano, por lo que “cuantas más capas de ciberseguridad pongamos, más fácil nos resultará detectar y responder de



forma automática y en tiempo real todo tipo de amenazas”, apuntan.

Al CIO y al CISO les recuerdan que deben invertir en gran medida en soluciones seguras de



acceso remoto y autenticación, pero también en protección del *endpoint* con antivirus de nueva generación con capacidad de *rollback*. Así como en control y protección del *email* y de las aplicaciones en la nube.

En el apartado de la nube SonicWall cuenta con su Cloud Application Security (CAS), que permite monitorizar los *logins* de usuarios para proporcionar seguridad contra el robo de credenciales, inspección avanzada de *phishing* y *malware* (múltiples motores de *sandboxing*), prevención de fugas de información, integración con soluciones de correo en la nube vía API (Office 365, G-Suite), y protección de la aplicaciones *cloud* más comunes como Salesforce, Dropbox, Slack, Box, Office 365, G-Suite, etc. Y todo ello vía API, por lo que en pocos minutos y de manera no intrusiva, está funcionando y proporcionando una capa adicional de protección a la organización.

SONICWALL

Capas de seguridad para luchar contra el cibercrimen

La realidad se impone. La covid-19 nos ha llevado al mayor experimento del teletrabajo de la historia, creando una explosión de puntos de exposición sin precedentes. Por ello, Sergio Martínez, director regional de Iberia de SonicWall, reconoce que hemos pasado de un modelo de bastión con un parámetro bien definido a defender, a un modelo sin perímetro concreto.

¿Cómo hacer frente a los cibercriminales? La compañía dispone de un amplio porfolio de soluciones para ello.



VÍDEO

IA propia para luchar contra el cibercrimen

Invertir en I+D es fundamental para luchar contra el cibercrimen. SonicWall lleva a cabo esta práctica, invirtiendo al año alrededor de 150 millones de euros al año en esta materia. El resultado son soluciones de seguridad con una eficiencia del 99,7 %, en la búsqueda de la perfección y de ese 100 % deseado.

Una de sus principales armas, resultado de esta inversión, es la inteligencia artificial, de origen propio, que aplican. En este vídeo Luis Fisas, director del sur de Europa de SonicWall, describe todo ello.



VÍDEO

WatchGuard espera que la **adopción de MFA** entre las **pymes** se generalice

WatchGuard se ha caracterizado, durante dos décadas, por proteger las redes empresariales. A principios de año esta multinacional compró a uno de los actores fundamentales de la seguridad española: Panda Security. Y en su visión de futuro se han adentrado en la seguridad del teletrabajo. Carlos Vieira, country manager de WatchGuard, nos da las claves de todo ello.

El resultado de la compra de Panda Security por parte de WatchGuard aporta una gran fortaleza: "Una potente plataforma de seguridad que conecta la red y el perímetro del usuario, ofreciendo una combinación de innovadoras funciones de seguridad y *packaging* simplificado, así como capacidades de despliegue y gestión por las que ambas organizaciones son conocidas", señala Carlos Vieira. "Esperamos construir una plataforma de seguridad que conecte la red y el perímetro del usuario, con capacidades inigualables en el mercado de ciberseguridad", avanza.

Además, va a dar respuesta a la problemática a la que se enfrentan las organizaciones: amenazas cada vez más sofisticadas, escasez de profesionales cualificados y un perímetro cada vez más poroso. La unión de ambas compañías también permitirá a clientes y *partners* consolidar sus servicios de seguridad esenciales bajo una sola marca.

Reforzando el endpoint

En el entorno del *endpoint* destaca que la adquisición de Panda Security hace que la me-



Carlos Vieira, country manager de WatchGuard

WATCHGUARD

jor detección y respuesta para el *endpoint*, la búsqueda de amenazas, el antivirus para el *endpoint*, la seguridad del correo electrónico, la aplicación de parches y el cumplimiento normativo y cifrado de datos hará que a corto plazo estén accesibles para la base de clientes de WatchGuard, a través de un fabricante de confianza y el proveedor de soluciones de TI que elijan.

A largo plazo, sus clientes y *partners* disfrutarán de beneficios adicionales que se derivan de que estas soluciones estén estrechamente integradas con el núcleo de la oferta de WatchGuard. Contarán con una solución que ofrecerá la máxima protección con una mínima complejidad, subraya.

Protegiendo la red

Tras dos décadas protegiendo las redes empresariales de todo tipo de organizaciones, una de sus máximas pasa por simplificar las soluciones, el despliegue y la gestión de estas, haciéndolas accesibles. Esto les ha hecho ser especialmente



atractivos para las pymes y empresas distribuidas, apunta.

WatchGuard, a lo largo de su trayectoria, ha logrado ofrecer 14 servicios de seguridad únicos en un solo dispositivo, facilitando servicios de seguridad de red: desde IPS tradicionales, *gateway* antivirus, control de aplicaciones, bloqueo de *spam* y filtrado web, hasta servicios más avanzados de protección contra el *malwa-*

re avanzado, el *ransomware* y la pérdida de datos confidenciales, correlación de riesgos desde la red hasta los *endpoints*, etc. Esto significa que están un paso por delante de la Gestión Unificada de Amenazas (UTM), explica Vieira.

En el ámbito del teletrabajo

Con el aumento del teletrabajo, y más tras la pandemia, señala que el perímetro de la red

WATCHGUARD

corporativa se difumina y las posibilidades de sufrir un ciberataque han aumentado drásticamente. "Sin la protección de la red de la empresa, un usuario remoto podría infectarse sin su conocimiento, e incluso introducir la infección en la red corporativa". Por ello, recomienda a las empresas dotar de medidas de seguridad a los teletrabajadores para que realicen sus tareas, sin exponer a la organización, garantizando la continuidad del negocio y la productividad de los empleados.

En la nueva realidad del teletrabajo aconseja concienciar a los empleados remotos sobre los riesgos de seguridad y educarles al respecto. Como punto de partida, considera necesario elaborar una lista de verificación basada en algunas de las mejores prácticas de seguridad básicas que los trabajadores remotos pueden llevar a cabo, como utilizar soluciones de autenticación multifactor (MFA) en *cloud*, contar con soluciones de seguridad Wi-Fi que permitan establecer un entorno inalámbrico de confianza,

emplear una conexión VPN segura para redirigir el tráfico de Internet a través de un servidor protegido, e implementar soluciones de filtrado web.

En definitiva, la estrategia a seguir debe contemplar una seguridad multicapa avanzada que abarque tanto el perímetro de la red como todo lo que está fuera de él.

Nuevas inversiones

La nueva realidad del teletrabajo y el aumento de la movilidad harán que las inversiones se deriven hacia herramientas de seguridad *cloud*, manifiesta, con soluciones MFA y el fil-

trado web. En este sentido, WatchGuard cuenta con su paquete de servicios de seguridad Passport, centrado en el usuario y diseñado para los trabajadores remotos que trabajan fuera de la red. Este *bundle* incluye su solución de autenticación multifactor (MFA) en *cloud* AuthPoint, que se caracteriza por permitir combatir el robo de credenciales.

Carlos Vieira confiesa que esperan que la adopción de MFA entre las pymes se generalice, ya que este tipo de soluciones se han vuelto más sencillas con opciones solo *cloud* y los teléfonos móviles han eliminado el costoso requisito del hardware de los *tokens*.

Pero lo que realmente esperan de las empresas es que, además de contar con las soluciones tecnológicas adecuadas, cuenten con un entorno confiable para sus redes, sobre todo las redes Wi-Fi. Y les recomiendan unirse al movimiento *WatchGuard Trusted Wireless Environment*, abogando por el estándar de seguridad global para Wi-Fi.



WATCHGUARD

WatchGuard, respuestas al mundo de la seguridad

WatchGuard ha ido dejando su huella en el mundo de la seguridad. Carlos Vieira, director general de WatchGuard de España y Portugal, recuerda en este vídeo que la compañía nació en el mundo de la seguridad perimetral. Se destacaron por contar con el primer *firewall* de mercado y tras ello vendrían sus UTM y otras soluciones. El *endpoint* es hoy una de sus prioridades, en una apuesta que han reforzado con la adquisición de Panda Security.



En seguridad no hay un servicio más importante que otro

Procedentes del mundo del perímetro, WatchGuard hace una aproximación cada vez mayor al mundo del *endpoint*. Carlos Vieira, director general de WatchGuard de España y Portugal, reconoce en este vídeo que "Panda va a llevar a WatchGuard a otra dimensión, a otro tipo de clientes, a otro tipo de protección". Aunque también asegura que dentro del mundo de la seguridad no hay un servicio más importante que otro. "Es fundamental la seguridad basada en capas, donde cuantas más tengamos, más problemas podremos mitigar y daremos una respuesta más adecuada", apunta.

