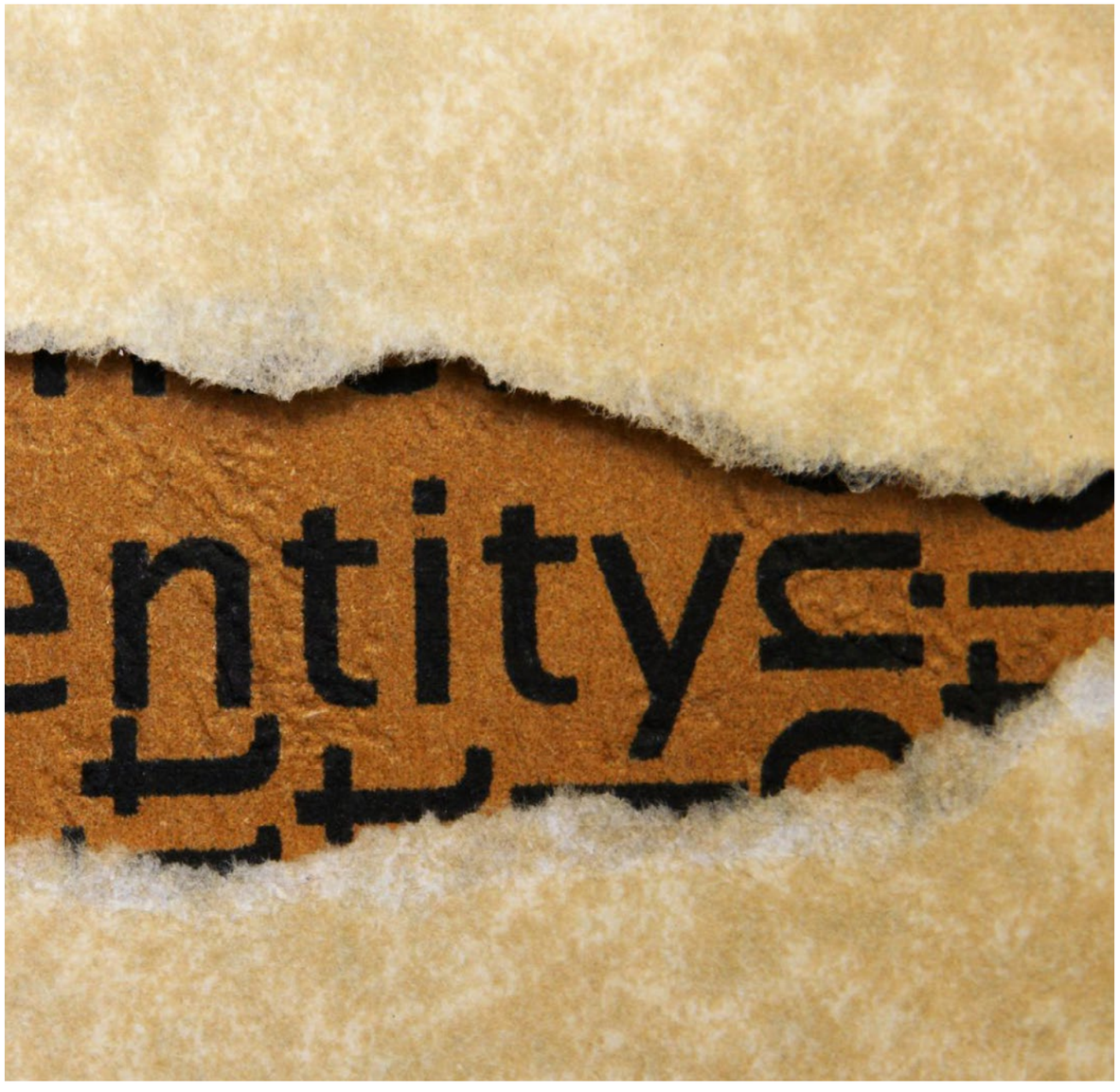
La identidad es el nuevo perímetro

La transformación digital, el trabajo remoto, la automatización y las actividades de migración a la nube de los últimos años... Todo ello y alguna cosa más han acelerado la cantidad de identidades que buscan acceso a datos y sistemas comerciales críticos. La consecuencia es un aumento de identidades, y con ello más y más ataques.



El nuevo tal, el nuevo cual Y lo que nos gustan estas cosas, ¿eh? Más que a un gorrino revolcarse en un lodazal. Lo nuevo, la querencia por la inmediatez. Claro que hay querencias y querencias lo mismo que hay novedades y novedades. Un disco, un libro, etcétera. Pero cuando son novedades que ponen la carne de gallina -que *no panda el cúnico*, que decía el Chapulín Colorado. Aquí no toca hablar del *Negreiragate* y parecidos, sino de cosas serias- y afectan a la seguridad de las empresas, entonces sí que sí. Y una de esas novedades es la identidad, digital que se ha convertido en el nuevo perímetro. Tantos y tantos dispositivos e identidades para acceder a ellos tienen esta consecuencia.

Pasen y lean, pues les va a interesar.

Lo primero, definamos identidad

Como siempre, las cosas claras y el chocolate, a poder ser, espeso. Lo primero que se impone es definir identidad para eso, tener las cosas claras -el chocolate aún no lo hemos visto.

"Definimos la identidad como la parte de un todo. Para las grandes empresas, la identidad forma un parte esencial de su estrategia de ciberseguridad. Estas estrategias suelen ser bastante complejas e incluir muchos verticales y productos, lo que conlleva una gran complejidad a la hora de integrarlos todos juntos. En las empresas grandes, poseedores de

Víctor Manuel Fernández

recursos materiales y humanos, el mayor problema es la complejidad", dice Alberto Carrillo, *manager, Iberia Sales engineering* de Hillstone Networks.

El estado de cuestión

Con el acceso a los recursos desde cualquier ubicación y momento, y con el 5G subiendo como la espuma, gestionar accesos se ha vuelto tan vital como el comer, dado que la superficie potencial de ataques va camino de la espuma del 5G. En suma, un panorama escalofriante, más si el perímetro se diluye como un azucarillo en agua. Bien lo dice José Luis Paletti, *senior security sales engineer* de WatchGuard: "Sin duda, controlar un entorno vivo como es el de las identidades hace que a priori no sea fácil la protección de los distritos dispositivos móviles, terminales, equipos ofimáticos, servidores... Todo esto, aderezado con distintos sistemas operativos, entornos *Cloud*, híbridos, aplicaciones en nube, etc. Sin embargo, la realidad es que existen herramientas que permiten de una forma sencilla y a un coste muy asequible, poder proporcionar seguridad a todo este entorno tan poco homogéneo".

Alberto Carrillo, Iberia *Sales engineering* de Hillstone Networks.

Y no hay que olvidar una cosa: "Los empleados pueden trabajar desde cualquier lugar sin ningún tipo de problemas, mientras que la gestión centralizada se asegura de que sólo accedan a los recursos específicos que necesitan para sus trabajos, garantizando así la productividad. Pero esta situación incrementa sustancialmente el riesgo, generando una hiperexposición. Por ello, vamos a peor, y hay que prestar mucha más atención a la ciberseguridad. Las credenciales son las joyas de la corona a proteger", reconoce Sergio Martínez, *country manager* de SonicWall en Iberia.

Así llegamos a lo que tenemos hoy en día: un perímetro de la empresa tan difuminado que es casi inexistente porque trabajamos en remoto, porque están las distintas modalidades de nubes, o por lo que sea. "Con este escenario, la gestión de identidades se hace muy necesaria en las empresas, de ahí que sea crítico tener sistemas de autenticación multifactor (MFA) y tener distintos recursos que garanticen la identidad de la persona y que está autorizada para acceder a determinados datos", apunta Sergio Cabrera, director comercial del área de Ciberseguridad de ITE.

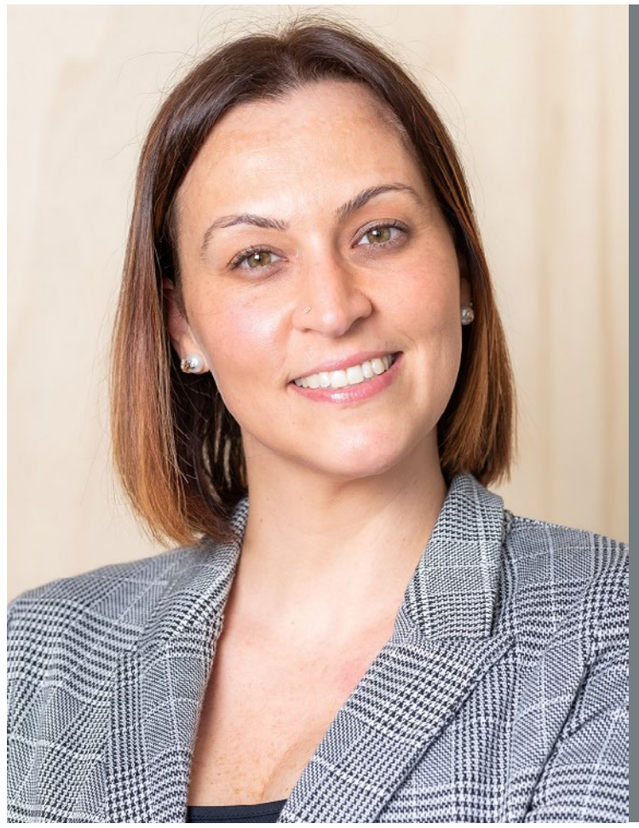
Ahora, ¿cuál es el perímetro actual de la empresa? Porque hay que tener en cuenta que se puede trabajar desde cualquier sitio: la oficina, en casa con una ADSL doméstica, en remoto utilizando una conexión 5G o un aeropuerto con una red Wifi pública... Y si preguntáramos a Rutger Hauer de estar vivo, seguro que nos saldría con aquello de que él ha visto cosas que nosotros no creeríamos.

José Luis Paletti, *Senior Security Sales engineer* de WatchGuard-Cytomic.

"El perímetro tradicional como lo conocíamos y protegíamos ha desaparecido. En esta situación, el nuevo perímetro, reside en los dispositivos empleados por los usuarios; los servicios *Cloud* corporativos, distribuidos entre distintos proveedores, donde residen los datos y servicios que consumen los usuarios; y las identidades empleadas por los usuarios para autenticarse en estos servicios desde sus

dispositivos", acuerda José de la Cruz, director técnico de Trend Micro Iberia.

Por lo tanto, sí es una preocupación para las empresas el poder garantizar la seguridad de la identidad digital de los trabajadores, pues de ello depende la propia seguridad de la empresa. Por un lado, "es imprescindible ser consciente de la gran importancia que supone contar con recursos que garanticen una experiencia digital más segura, tanto para empresas como para usuarios", regresa Sergio Cabrera para completar el otro lado: "Debemos tomar el control sobre nuestra identidad digital, decidir quiénes acceden a nuestros datos, e incluso cuándo y cómo. Y para ello hay que gestionarlos".



Credenciales: el objetivo número uno de los atacantes

"Las credenciales son el objetivo número uno para los atacantes. Una afirmación que podemos comprobar al leer el informe de Verizon en el que se indica que las credenciales destacan como el principal objetivo de los ciberdelincuentes para atacar el patrimonio de la empresa, seguidas del *phishing*, la explotación de vulnerabilidades y los *botnets*. De hecho, ninguna organización está segura sin un plan para gestionarlos todos.

La identidad se ha convertido en el último objetivo de alto valor en el campo de batalla de la ciberseguridad. Sin embargo, la proliferación de identidades ha dificultado que los profesionales de la seguridad logren el equilibrio adecuado entre las medidas de seguridad y la velocidad para hacer lo necesario para proteger la compleja red de terminales y soluciones SaaS. Y eso sin dificultar demasiado las cosas para la empresa ni dejar lagunas que los ciberdelincuentes puedan explotar fácilmente".

Karina Rojas, *Channel Sales manager* de CyberArk para Iberia.

Proliferación de identidades, ¿ese problema?

Con cada vez más dispositivos y personas que se conectan a la red de la empresa desde el exterior, y con la creciente digitalización de las administraciones y de los servicios públicos, la proliferación de identidades se ha convertido en un problema añadido para los responsables de seguridad corporativos. Más de uno y de dos están dando palmas con las orejas de la alegría que les embarga, por concretar. "Esto les está obligando a elevar sus niveles de protección en relación con su arquitectura y sistemas, pero también con su información y empleados", dice Jordi Hidalgo, *Chief Product Officer* de Redtrust. Pues eso.

Así que, aquí es cuando hace acto de presencia el certificado digital, santo y seña, luz de Oriente y todo lo que queremos, aunque si es por resumir en que se trata de mecanismo de autenticación válido que verifica la identidad del trabajador o usuario que quiere acceder a los sistemas de información de la empresa. "Almacenar y custodiar estos certificados en un repositorio único, controlado, seguro e independiente es una ayuda para los profesionales de la seguridad", añade Jordi Hidalgo.

Así, con la centralización se evita tener que ir equipo por equipo instalando los certificados y se asegura un uso de los mismos completamente transparente por parte del usuario. "Los administradores de TI tienen acceso a la consola de administración de certificados inmediatamente después de la configuración del servicio, lo que les facilita controlar su uso en todo momento", apostilla.

De todas formas, Santiago Méndez Colomo, *Senior director, Advanced Solutions*, TD SYNNEX Iberia, considera que

Clave para que el Canal obtenga un valor diferencial

"Para obtener un verdadero valor diferencial, el Canal debe apoyarse en un proveedor que les permita cubrir las tres áreas más importantes para la gestión centralizada del ciclo de vida de los certificados: centralización, control y seguridad. Y esta gestión de 360º se consigue custodiando los certificados digitales y creando políticas de uso no sólo por organismos o URL, sino también restringiendo el acceso a trámites concretos. Además de poder establecer alertas de caducidad y emitir y renovar los certificados directamente".

Jordi Hidalgo, *Chief Product Officer* de Redtrust.

"más que la proliferación de identidades, que al fin y al cabo están asociadas a las personas, lo que ha aumentado es el número de servicios disponibles para una tarea determinada (y por tanto las cuentas asociadas) y los roles de trabajo que agrupan varios subconjuntos de estos servicios para esas tareas. La combinación de cuentas y roles presenta una complejidad que crece de manera exponencial, y que hace muy difícil su gestión".

¿Resultado de la transformación digital de las empresas?

"Realmente tiene mucho que ver", admite Jordi Hidalgo. Porque otra cosa, pero digitalmente ya se han transformado unas pocas, y eso trae como consecuencia más dispositivos, más accesos... Un sindiós. "El creciente proceso de digitalización que han afrontado las empresas, sobre todo desde 2020, para impulsar prácticas como el trabajo a distancia o la realización de trámites telemáticos con la Administración Pública, ha obligado a ampliar el rango de protección. Sin duda, el robo o la suplantación de la identidad representan un problema en ciernes, por lo que proteger la identidad digital se ha vuelto una necesidad creciente", insiste aquel especialista.

"Obviamente, a más vectores de ataque y mayor número de identidades distintas haya, más difícil va a ser ponerles un índice de riesgo a sus usuarios y delimitar permisos", advierte Sergio Cabrera. Por tanto, en su opinión, si no se gestiona la identidad de forma correcta, es posible que en estos puntos no definidos del perímetro en la nube, todo se complique mucho más y por tanto, repercuta en la seguridad de la organización".

Por tanto, Cabrera cree que sí hay muchas soluciones que lo que hacen es dar permisos a la persona y no al sitio al que se conectan o desde el que se conectan. "Con el trabajo en la nube no solo hay que proteger el punto de conexión y el *Endpoint*, sino que también hay que proteger el camino, que es muy importante para que veamos desde dónde se conecta el usuario y quién se conecta. Es necesario contar con un factor de identidad digital bien marcado", apostilla.

Una nueva visión de la gestión de identidades

¿Recuerda aquel celebérrimo programa del gran Fernando Jiménez del Oso? *Millennials* y similares abstenerse de la pregunta. Sí, más allá. Pues eso es lo que hay que hacer con la gestión de las identidades visto lo visto.

Primero, las fronteras. Cada vez más difusas, ya que los trabajadores remotos con teléfonos móviles personales, tabletas, ordenadores portátiles etc., solicitan cada vez más acceso a los recursos y aplicaciones de TI corporativos desde este tipo de dispositivos móviles. Lo que conocemos como BYOD -*bring your own device*-, "que puede exponer a las empresas a *malware* y piratas informáticos si los dispositivos de los empleados no cumplen con las políticas de seguridad BYOD corporativas. Hemos visto este año ataques muy dirigidos y focalizados

en la obtención de réditos monetarios, con muchos secuestros de servidores, ordenadores corporativos, etc. El *ransomware* ha sido una auténtica plaga bíblica en 2022", reconoce Sergio Martínez.

No se vayan todavía, que aún hay más decía Superratón. Y lo hay, porque a medida que las organizaciones continúan alejándose del entorno local tradicional y acercándose a esta nueva realidad, sus soluciones de ciberseguridad heredadas no han podido mantenerse al día, creando una complejidad inmanejable y mayores oportunidades para los ciberdelincuentes. "Esto ha llevado a un aumento en el uso de arquitecturas de seguridad *Zero-Trust*, aumentando el perímetro de seguridad allá donde estén los trabajadores, independientemente de si un usuario está dentro o fuera del perímetro. Así, más que nunca es necesario redefinir quién puede acceder y a qué", prosigue Martínez.

Y el reintegro, que esto todavía no ha terminado: "No hay que olvidar el peligro que atisbamos en el horizonte de la computación cuántica, a la vuelta de la esquina, capaz de romper cualquier cifrado actual. Hay que empezar a poner los cimientos de una nueva ciberseguridad", insiste.

Las circunstancias que propician una mayor dificultad a la hora de proteger las identidades

José de la Cruz, director técnico de Trend Micro Iberia, considera las siguientes:

- "Heterogeneidad de servicios de autenticación disponibles: es perfectamente posible que un usuario disponga de una identidad independiente para acceder a cada servicio que consuma. Cada uno de ellos con sus particularidades, sistemas de almacenamiento y sistemas de seguridad independientes lo que complica la gestión de riesgos y políticas a aplicar.
- Descentralización de iDPs (Proveedores de servicios de identidad): en el caso de que el servicio consumido por el usuario, disponga de un iDP, existen infinidad de ellos. Esto nos devuelve a una situación, aunque más segura, comprometida en términos de consolidación de una política robusta de ciberseguridad.
- Ausencia de políticas de seguridad consolidadas: cada uno de estos servicios contarán, en el mejor de los casos, con políticas de seguridad independientes que dificultarán la aplicación de una política de seguridad robusta y consolidada".

José de la Cruz, director técnico de Trend Micro Iberia.

Dicho lo cual, "La seguridad debe ir más allá de la gestión de la identidad, haciendo mucho hincapié en su control, con una mayor influencia de los administradores en torno a las restricciones de accesos y privilegios. La IAM y las estrategias para proteger la identidad digital está camino de convertirse en una solución disruptiva para aumentar la seguridad de los accesos a los entornos empresariales, lo que hará que multitud de empresas planeen incorporarla a sus estrategias de ciberseguridad en el medio plazo. A esta exigencia por controlar la identidad y los accesos se une un mayor apoyo de la seguridad en remoto, ya que proteger la identidad de los empleados y asegurar su autenticación en cualquier parte será un verdadero desafío", recomienda Jordi Hidalgo.

Llegados a este punto, José de la Cruz, director técnico de Trend Micro Iberia, viene a estas páginas para ofrecer una solución a este hándicap. Léanla porque tiene fundamento, que diría un afamado cocinero vasco:

El papel del Canal

"En primer lugar, debe alertar de los riesgos que una deficiente estrategia puede conllevar no sólo de cara a la pérdida de competitividad, sino también de fallo como primera línea de defensa en cuanto a ciberseguridad. Y, en segundo lugar, ha de diseñar soluciones que afronten estos riesgos de forma efectiva, utilizando para ello las herramientas que los fabricantes de ciberseguridad desarrollan en este ámbito de IAM.

Estas herramientas son necesarias, pero en este tipo de proyectos hay un componente de adaptación y gestión muy importantes, que el canal puede cubrir perfectamente".

Santiago Méndez Colomo, *Senior director, Advanced Solutions*, TD SYNNEX Iberia.

"La solución consiste en abordar el problema acorde a las circunstancias actuales, teniendo en cuenta este nuevo perímetro e implementando medidas adecuadas para adaptar nuestra política de ciberseguridad. Simplificando el planteamiento, podríamos reducir esta solución a tres sencillos pasos:

- Gestión de identidades de manera centralizada. Una de las maneras más eficientes de mejorar la seguridad de las identidades es reducir el número de las mismas por usuario. Esto se puede conseguir implementando un iDP que pueda ser integrado de manera homogénea por los distintos servicios consumidos por parte del usuario. Es el caso del correo, navegación, acceso a servicios web corporativos, *VPN*, etc.). Este iDP deberá ir acompañado siempre de un sistema de autenticación de doble factor, limitando el posible impacto de una puntual fuga o robo de credenciales por parte del usuario.
- Aplicación de políticas consolidadas. Esta definirá cuestiones esenciales como uso obligatorio de un iDP definido por la compañía; requerimiento de utilización de un sistema de autenticación de doble factor definido por la compañía; y política de contraseñas robusta: longitud, complejidad y validez.
- Análisis de la postura de Seguridad. El nuevo perímetro, citado anteriormente, debe ser supervisado de manera continua para garantizar que no representa un riesgo para la organización. Los elementos que sería recomendable analizar son supervisión de posibles brechas de seguridad asociadas a las identidades, caso de su presencia en algún listado publicado en *Dark Web*; su utilización en dispositivos vulnerables (que dispongan de vulnerabilidades no parcheadas); análisis de comportamientos sospechosos, como es el caso de intentos de movimiento lateral, *logins* imposibles (un usuario accede ahora desde una dirección IP ubicada en Madrid y cinco minutos después desde una IP ubicada en USA); acceso a servicios *Cloud* inseguros o peligrosos, como puede ser el caso de servicios que hayan sido comprometidos recientemente, que hayan sufrido una fuga de información o cuyos controles de seguridad no cumplan con la normativa vigente; detecciones de *malware* asociadas al usuario, su cuenta de correo o dispositivo empleado; permisos de usuario, lo que implica identificar si el usuario dispone de demasiados privilegios dentro de la organización, caso de un usuario administrador trabajando desde un dispositivo; y cuentas inactivas, que son el principal objetivo de ataques de diccionario puesto que, dado que nadie las utiliza, comprometerlas será más fácil pasando desapercibido".

Asimismo, este especialista de Trend Micro considera que este análisis deberá efectuarse de manera continua, alertando de cualquier cambio relevante e

Javier Aguilar, Ciberseguridad en Ingram Micro.

identificando aquellas identidades que sean más vulnerables o representen un riesgo para la organización.

Cómo el Canal echa una mano

Hace años, eran pocos los *partners* que se enfocaron en vender y llevar a cabo proyectos de segurización y gestión de identidades. Como se suele decir, dos y el del tambor. Esto era así por ser un área menos conocida o demandada cuyo resultado eran toneladas de trabajo y proyectos cuya ejecución es tan larga como '*Amra Ekta Cinema Banabo*' -mire en Google, mire-. "Pero desde 2021 hemos visto un creciente interés por parte de los *partners* por especializarse en soluciones para asegurar las identidades, un área que habían dejado de lado por la poca demanda en sus clientes o la gran dedicación de tiempo y de recursos que requiere", confiesa Karina Rojas, *Channel sales manager* de CyberArk para Iberia.

Este interés está aumentando cada vez más, ya que los clientes demandan administración y protección de las identidades, en parte, motivados por la proliferación de ataques o por la labor de prevención y exigencia que hacen los seguros cibernéticos o seguros de responsabilidad civil cibernética (CLIC) en sus pólizas a la hora de ofrecerles una cobertura. "En este sentido, el Canal histórico sigue avanzando y sigue actualizándose en nuevas funcionalidades, pues están descubriendo que con especialización, certificaciones y experiencia podrán ayudar a sus clientes a recorrer este largo y cambiante camino", apostilla aquella especialista.

Sergio Martínez, *country manager* de SonicWall en Iberia.

Además, hay que tener en cuenta que la situación del control y la seguridad de la identidad digital está en plena expansión en España, especialmente desde 2020, cuando el trabajo remoto y los trámites *online* fueron imperativos. De hecho, la regulación europea 910/2014 eIDAS ha consolidado el uso del certificado digital y España es pionera en su utilización en formato software", apunta Jordi Hidalgo.

Por consiguiente, este especialista no tiene duda en reconocer que "los *partners* que deciden zambullirse en el mercado del certificado y la firma digital optan a grandes oportunidades para crecer, dada su mayor usabilidad, tanto para labores de autenticación y realización de trámites con la Administración Pública como para la firma de documentos de cualquier sector".

Pero, además de las propias soluciones software, servicios de valor añadido como asesoramiento y consultoría, el Canal también puede ayudar a sus clientes a evaluar sus necesidades específicas de seguridad y gestión de identidades acompañando en la elección de la soluciones más adecuadas para su entorno empresarial. A lo que hay que unir que "el Canal puede ayudar en la formación y capacitación de los empleados de la empresa, o bien o del propio *partner* que se encargará de implementarla, lo que permitirá aumentará la eficacia de las políticas de seguridad y garantizará la adopción adecuada de las soluciones propuestas", apunta Javier Aguilar, Ciberseguridad en Ingram Micro.

Ahí lo dejamos. Ahora, que lo recoja el Canal. **DW**