it Digital Security

Webinar Autenticación

Autenticación y gestión de identidades, el nuevo perímetro de seguridad

#ITWebinars #ITTrends

it TRENDS

Check Point SOFTWARE TECHNOLOGIES LTD.

FORTINET

CYBERARK

MICRO FOCUS

ONE IDENTITY

f5

SONICWALL

Akamai

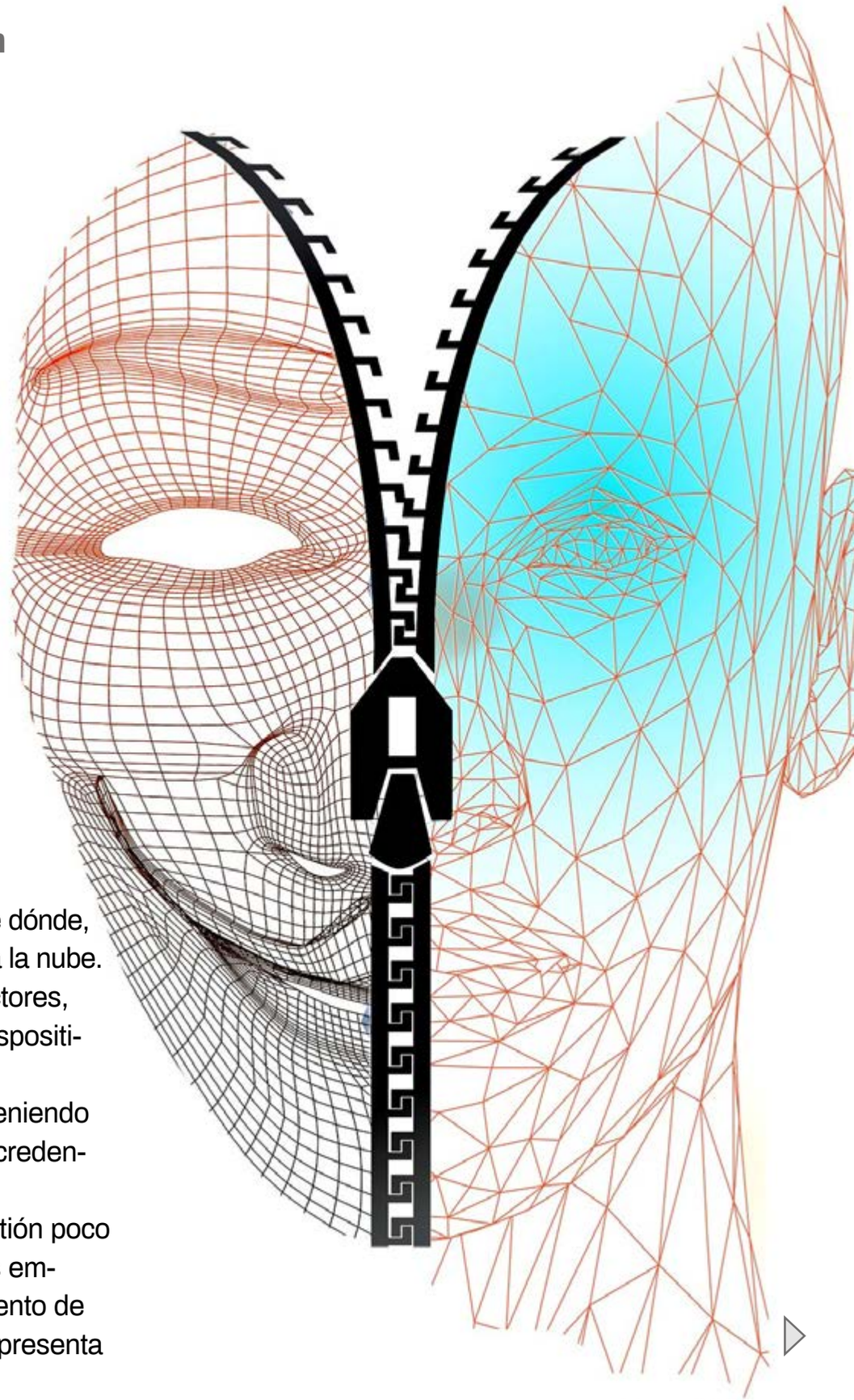
THALES

Mayo 2020

itds

Webinar Autenticación

Autenticación y gestión de identidades, el nuevo perímetro de seguridad



La identidad se ha convertido en el nuevo perímetro de seguridad. Saber quién accede, desde dónde, con qué dispositivo y a qué recursos es uno de los pasos más complicados de la migración a la nube.

La manera de afrontarlo pasa por la autenticación basada en contexto y de múltiples factores, una autenticación no sólo de las personas, sino también de las aplicaciones y dispositivos, y de una manera centralizada.

No nos olvidemos de la gestión de cuentas privilegiadas, un aspecto muy importante teniendo en cuenta que, según Forrester, el 80% de las violaciones de datos tienen una conexión con credenciales privilegiadas comprometidas, como contraseñas, tokens, claves y certificados.

Las empresas necesitan mejorar la protección de las identidades, amenazadas por una gestión poco hábil de las contraseñas, un panorama digital en constante cambio o una gran rotación de los empleados, lo que genera la necesidad de gestionar el aprovisionamiento y el desaprovisionamiento de credenciales. Desde una perspectiva de capacidad de administración y cumplimiento, esto representa

Mayo 2020

itds

Webinar Autenticación

Carlos Luaces de Santiago,
Sales Engineer, Iberia, CyberArk

Ramsés Gallego,
Security International Director, Micro Focus

Raúl Tejeda,
System Engineer, Fortinet

Guillermo Martín Soto, Regional Sales Manager IAM, Thales Iberia y Magreb

Eusebio Nieva,
Director Técnico, Check Point

Daniel Varela, Solutions Engineer Security, F5 Networks

Raúl D'Opazo, Solution Architect, EMEA Sales Consultant

Enric Mañez,
Enterprise Security Sales, Akamai

Sergio Martínez,
Director General, SonicWall Iberia

una gran amenaza para proteger los datos de su empresa

En este IT Webinars hemos reunido un grupo de expertos para hablar de gestión de accesos y cuentas privilegiadas. Contamos con CyberArk, Micro Focus, Fortinet. Thales, Check Point, F5 Networks, One Identity, Akamai y SonicWall. A continuación, puedes leer un resumen de sus intervenciones, con los puntos más destacados.También puedes pinchar en cada una de las imágenes de sus portavoces para acceder a su intervención en el webinar o ver la sesión completa aquí.

Carlos Luaces de Santiago, Sales Engineer, CyberArk Iberia

"El primer paso para minimizar los riesgos es tener una visibilidad de las cuentas privilegiadas"

Desde hace años, la gestión de cuentas privilegiadas va ganando posiciones, siendo cada vez más importante dentro de las iniciativas de ciberseguridad de las organizaciones. A este respecto, Carlos Luaces de Santiago, Sales Engineer de CiberArk, confirma durante la sesión online Autenticación y Gestión de Identidades, el nuevo perímetro de la seguridad que dichas cuentas, esenciales para que ciertas aplicaciones, servicios o usuarios realicen su operativa normal, pueden resultar especialmente atractivas para posibles atacantes. Se hace necesario, por tanto, instaurar diferentes controles que minimicen los riesgos que llevan asociados tanto su gestión como el uso que se ha de hacer de este tipo de credenciales. El primer paso para minimizar los riesgos es tener una visibilidad de dónde se encuentran estas cuentas privilegiadas.

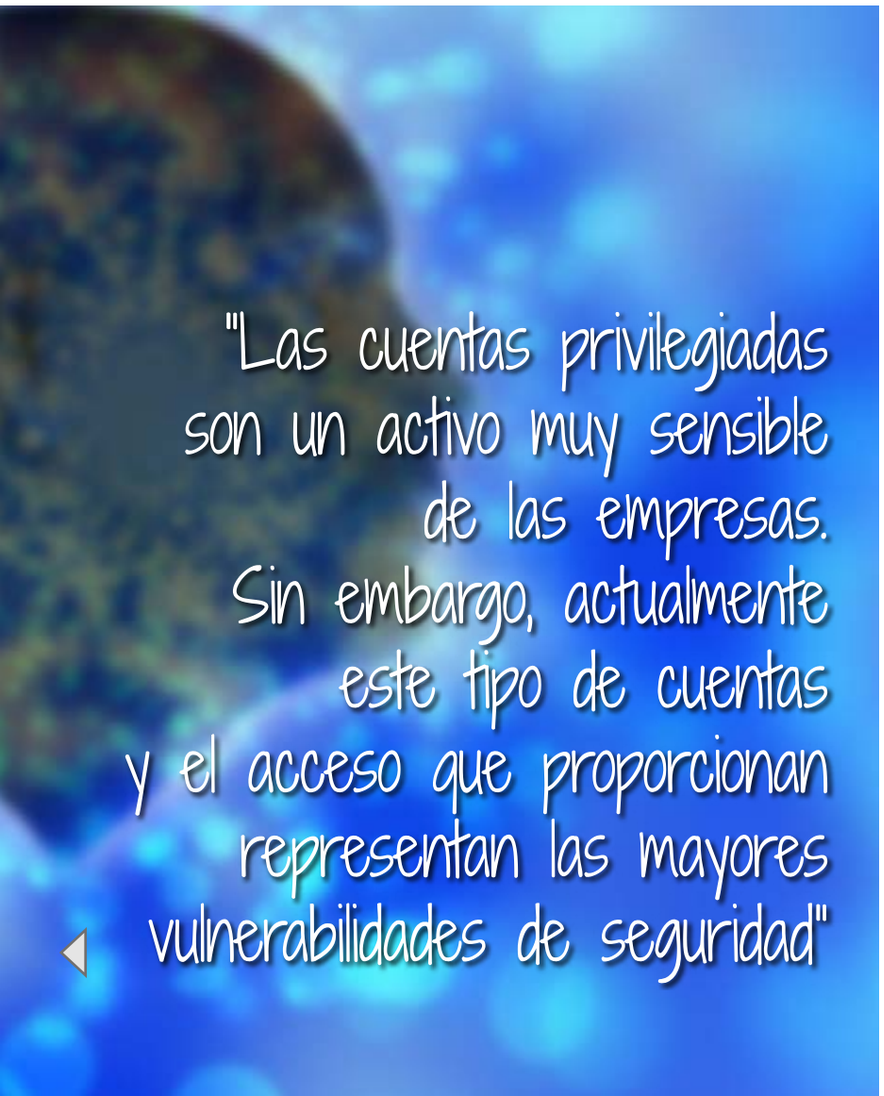
Las cuentas con privilegios y el acceso que proporcionan representan las mayores vulnerabilida-

CARLOS LUACES DE SANTIAGO, SALES ENGINEER, CYBERARK IBERIA

CLICAR PARA VER EL VÍDEO

des de seguridad a las que se enfrenta una empresa en la actualidad. Según diferentes estudios, el nivel de criticidad de este tipo de cuentas es muy alto, y entre el 75 y el 85% de las brechas de seguridad suponen un acceso privilegiado.

No obstante, hay otros escenarios como el elemento humano que pueden suponer un alto riesgo. Un usuario interno puede llevar a cabo diferentes acciones (intencionadas o no) que abran las puertas de la organización a los ciberdelincuentes.



Para hacer frente a esta situación, y proteger las organizaciones, Carlos Luaces recomienda a las empresas "pensar" como lo haría un atacante. En este sentido, es primordial entender que estos se mueven lateral o verticalmente por la red, buscando credenciales que les permitan acceder a los recursos más críticos. Por ello, y para mitigar al máximo los riesgos asociados y cerrar cualquier puerta de entrada, la clave es romper la cadena de ataque, y hacerlo cuanto antes.

CyberArk cuenta con un programa prescriptivo (Blueprint) para aplicar eficazmente la gestión del acceso con privilegios, el cual alberga recomendaciones encaminadas a prevenir el robo de credenciales, detener el movimiento lateral y vertical de los ciberdelincuentes y limitar el uso de privilegios y el abuso de los mismos. Blueprint también aborda las iniciativas de transformación digital, como la adopción de la nube, DevOps, RPA y SaaS, así como entornos locales, cloud o híbridos.

En definitiva, CiberArk considera la gestión de cuentas privilegiadas como ese último reducto sobre el que instaurar controles de seguridad adicionales para frenar cualquier acción que vaya contra los servicios operativos. En el caso de España, donde aún queda camino por recorrer, las empresas avanzan convenientemente, estableciendo la gestión de cuentas privilegiadas en un lugar cada vez más alto dentro de sus estrategias de seguridad.

Vea aquí la intervención de CyberArk en Autenticación y Gestión de Identidades, el nuevo perímetro de la seguridad.

LAS CINCO GRANDES RAZONES PARA DAR PRIORIDAD A LOS PRIVILEGIOS

El acceso privilegiado es una puerta de entrada a los activos más valiosos de una organización y la base de casi todas las filtraciones graves de seguridad. Las organizaciones deben contar con una estrategia tanto para gestionar y supervisar el acceso privilegiado como para detectar y responder a amenazas si quieren reducir el riesgo de convertirse en el blanco de los ataques avanzados que existen en la actualidad.

Ramsés Gallego, Security International Director, Micro Focus

"Afrontamos la gestión de identidad sin silos, de una manera coherente"

La gestión de identidades y accesos es un elemento cada vez más imprescindible para mantener la seguridad de las empresas. Bajo este punto de vista, Ramsés Gallego, Security International director de Micro Focus, confirma durante la sesión online Autenticación y Gestión de Identidades, el nuevo perímetro de la seguridad que la apreciación de una seguridad centrada en la identidad, junto a los datos y a las aplicaciones, crece cada día. Desde esta consideración, la identidad se está convirtiendo en un pilar fundamental para cualquier organización, al permitir conocer quién consume qué, en qué momento, con qué aplicación y con qué datos. Es más, el sector está jugando una triple partida de ajedrez, con distintos tableros: identidad, datos y aplicaciones, y es en este triángulo dónde hay que brillar, ya que, si el cliente es el rey, la gestión de identidades es la reina, y sin la reina no se puede ganar.

Al respecto de esta triple partida, Micro Focus enfrenta este juego de una manera holística, asumiendo que tanto la gestión de identidades como el gobierno de los accesos y la administración de esa identidad, de los datos y de las aplicaciones

**RAMSÉS GALLEGO,
SECURITY INTERNATIONAL DIRECTOR, MICRO FOCUS**

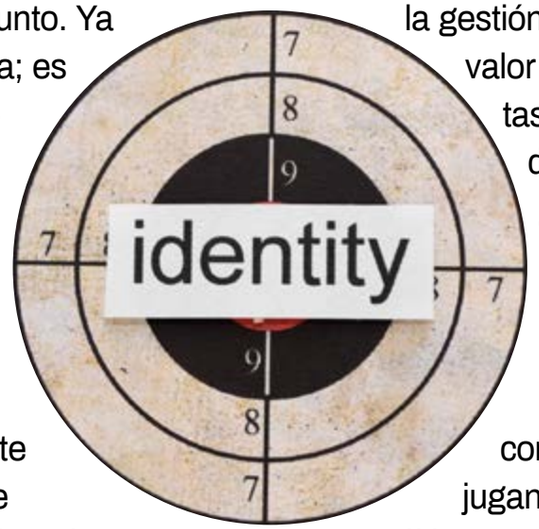
**CLICAR PARA
VER EL VÍDEO**

Compartir en RRSS

CASO DE ÉXITO MICRO FOCUS: MEDICA FOUNDATION

Medica Foundation realiza revisiones de acceso periódicas en todas sus aplicaciones para garantizar que sus 2.000 usuarios tengan los derechos de acceso correctos. La tarea se realizaba anualmente, pero al tomarse la decisión de pasar a revisiones trimestrales, en línea con las mejores prácticas de la industria, esto planteó un desafío para el equipo de seguridad de TI, que se enfrentó a un proceso manual, lento, laborioso y con el riesgo de que se produjesen errores.

requieren de una visión en su conjunto. Ya no basta con utilizar una plataforma; es necesario apostar por un ecosistema, sistemático, sistémico y orientado al valor, a la confianza y a la confiabilidad. Es fundamental. Es más, ahora tanto la seguridad como la gestión de identidades deben estar centradas en las personas y en su comportamiento. Este fundamento es en el que se mueve Micro Focus, con un porfolio completo donde no se deja ningún sistema atrás (ecosistema, sistemático y sistémico), y que, además, comprende todas las cuestiones que tienen que ver con la identidad, la confiabilidad y el uso intensivo del machine learning, y donde el análisis del comportamiento y la previsión del próximo movimiento del ciberatacante o del empleado resultan decisivos.



Partiendo de esta realidad, Ramsés Gallego no duda en afirmar que 2020 será el año de la gestión de identidad, máxime cuando se trata de un mercado que crece al ritmo del 30% anual. Ciertamente, la gestión de identidad es capaz de aportar valor al negocio, pero también respuestas, control y visibilidad. La identidad debe ser el centro de una estrategia de seguridad robusta y sólida: identidad, datos y aplicaciones precisan de ese ecosistema completo para un entorno complejo.

Por último, es importante reseñar como la gestión de identidad está jugando un papel protagonista en las últimas semanas, con el auge del teletrabajo a consecuencia del COVID 19. Pocas empresas estaban preparadas para una situación así. Ante ello, algunas organizaciones como Micro Focus han movido ficha, ofreciendo parte de sus soluciones de manera gratuita, a fin de permitir a los clientes que tengan que autenticar, dar fe, que alguien en remoto es quién dice ser, más allá de una contraseña o de unas credenciales.

Vea aquí la intervención de MicroFocus en Autenticación y Gestión de Identidades, el nuevo perímetro de la seguridad.

"Tanto la seguridad como la gestión de identidades deben centrarse en las personas y en su comportamiento. Este fundamento es en el que se mueve Micro Focus, con un porfolio completo donde no se deja ningún sistema atrás"

Raúl Tejeda, System Engineer, Fortinet

“Las empresas necesitan estar preparadas para que sus usuarios puedan trabajar desde casa de manera segura y autenticada”

La gestión de identidades y accesos (IAM) es crucial hoy en día para la implementación de una política de seguridad efectiva. Partiendo de esta realidad, Raúl Tejeda, System Engineer de Fortinet, asegura en la sesión online Autenticación y Gestión de Identidades, el nuevo perímetro de la seguridad que la integración es un elemento clave, entendiéndola como la capacidad para unir distintas funcionalidades de autenticación avanzadas en una única solución que simplifica la administración y la experiencia del usuario final. Esta piedra angular en Fortinet se llama FortiAuthenticator y su misión es la de asegurar que la gestión de identidades dentro de la Security Fabric de la compañía sea lo más sencilla y poderosa posible.

RAÚL TEJEDA,
SYSTEM ENGINEER, FORTINET

CLICAR PARA
VER EL VÍDEO

Ahora bien, ¿por qué es tan importante esta integración?

FortiAuthenticator ofrece una respuesta segura a los desafíos que enfrentan las empresas actuales con respecto a la verificación de la identidad del

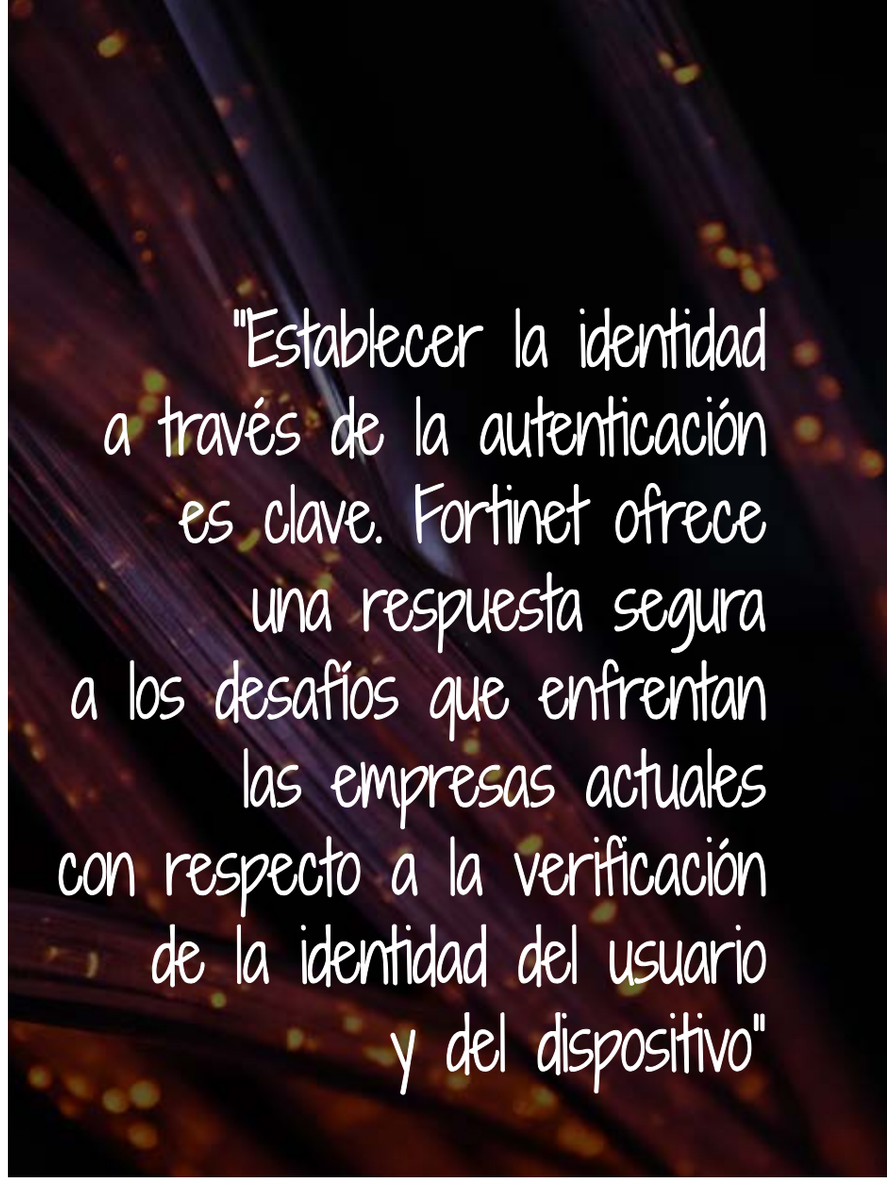
usuario y del dispositivo. De este modo, asegura una identificación transparente de todos los servicios en la red a través de una amplia gama de conectores que proveen distintas funcionalidades, siendo la principal la de ser una base de datos de autenticación global y transversal para toda la red.

FortiAuthenticator también asegura la autenticación fuerte, con doble factor de autenticación de diferentes formas: Con FortiToken (físico o Mobile), mediante SMS o vía correo electrónico.

En lo que respecta a la parte de certificados y HSM, esta es esencial, igual que SAML. SAML genera una autenticación federada, consiguiendo crear un token, una SAML assertion. Fortinet permite hacer esta integración tanto en modo servidor como en modo cliente, en IDP SP.

No obstante, dentro de las funciones de FortiAuthenticator, la más conocida y potente es Single Sign On de Integración Total; la posibilidad de integrar con un Single Sign On cualquier tipo de autenticación, o, dicho de otro modo, que en el día a día la autenticación sea segura pero también útil y sencilla para el usuario.

Explicadas estas funcionalidades lo más importante es integrarlas para ofrecer distintos casos de uso de gestión de identidades. En este sentido, Raúl Tejeda señala cuatro: aprovisionamiento automático de usuarios y tokens en la red; portal de autoservicio de autenticación y token; política basada en roles, tanto en los sistemas como en los equipos de seguridad; y administración de estos sistemas basada en roles.



Por último, Raúl Tejeda no puede dejar de referirse a la importancia que están tomando las soluciones de gestión de identidades, sobre todo ahora, desde que se ha disparado el teletrabajo. Bajo su entender, las empresas necesitan estar preparadas para que sus usuarios puedan trabajar desde casa de manera segura y autenticada, pero sin perder el control de quién se conecta a las aplicaciones y de cómo lo hace.

Vea aquí la intervención de Fortinet en Autenticación y Gestión de Identidades, el nuevo perímetro de la seguridad.

Guillermo Martín Soto, Regional Sales Manager IAM, Thales Iberia y Magreb

"El nuevo perímetro de seguridad es el usuario y la contraseña"

**GUILLERMO MARTÍN SOTO,
REGIONAL SALES MANAGER IAM, THALES IBERIA Y MAGREB**

**CLICAR PARA
VER EL VÍDEO**

La situación actual del mercado nos lleva a confirmar que el perímetro, tal y como lo entendíamos ya no es lo que era. A este respecto, Guillermo Martín Soto, responsable del Negocio de Gestión de Identidades de Thales en la zona de Iberia y Magreb, explica en la sesión online Autenticación y Gestión de Identidades, el nuevo perímetro de la seguridad cómo a pesar de que las empresas invierten mucho dinero en tecnología perimetral, las brechas o fuga de información son mayores cada año.

Por ello, y sobre la base de que la seguridad tradicional ya no es suficiente, sobre todo según el número de aplicaciones cloud crece rápidamente, Thales propone una estrategia de gestión de acceso apoyada sobre SafeNet Trusted Access, construido sobre la base de su solución de autenticación fuerte SafeNet Autentication Service.

SafeNet Trusted Access permite a las organizaciones gestionar el acceso a las aplicaciones cloud mediante la validación de identificaciones, determinando el nivel de veracidad y aplicando los controles de acceso apropiados cada vez que el usuario accede a un servicio cloud. SafeNet Trusted Access evalúa qué política de acceso debe emplearse y luego aplica el nivel de autenticación apropiado con Smart Single Sign On (autenticación única inteligente). Con este nivel de autenticación, los usuarios no necesitan utilizar una contraseña diferente para cada aplicación, mientras que los responsables de TI pueden implementar o hacer

tantas excepciones en este Single Sign On como consideren oportunas.

Según Guillermo Martín, una de las ventajas y diferenciadores que integra Thales es la gran variedad de métodos de autenticación que posee (pasword, hardware, kerberos, OTP, etc.) alguno incluso sin token (basado en patrones) y otros aprovechando la autenticación basada en certificado, con tarjetas inteligentes de PKI o token USB con certificado, entre otras. Thales también sigue una de las corrientes del mercado, los modelos de autenticación sin contraseña, los cuales, se basan únicamente en el contexto. A estos modelos puede agregársele un factor, como un OTP, o un multifactor, pero sin contraseña, como un token físico, una tarjeta inteligente, un OTP más un pin, pero, de nuevo, sin tener que recordarlo.

Por último, y en lo que a la adopción de tecnologías de gestión de acceso en la empresa española se refiere, Guillermo Martín vislumbra un incremento que continuará en los próximos meses, en parte, por la necesidad de implantar prácticas de teletrabajo a causa del COVID-19. La exigencia de dar acceso externo a usuarios a los que antes no había que dárselo, ha supuesto una transformación. Las empresas se han dado cuenta de que es necesario monitorizar y securizar todos los accesos a aplicaciones y a la red interna que se producen desde el exterior.

Vea aquí la intervención de Thales en Autenticación y Gestión de Identidades, el nuevo perímetro de la seguridad.

La gestión de identidades y accesos se ha vuelto algo imprescindible en un mundo descentralizado y sin perímetro. Thales evalúa que políticas de acceso deben emplearse para luego aplica el nivel de autenticación apropiado

ACCESO REMOTO SEGURO PARA LOS EMPLEADOS

En el entorno empresarial actual, es esencial disponer de acceso constante a la información y los servicios con vistas a comunicarse y llevar a cabo las actividades. Por eso es importante garantizar que los empleados puedan no solo colaborar, sino también acceder de forma remota a las aplicaciones y la información corporativas con la misma seguridad que si se encontraran en la oficina.

Compartir en RRSS

Eusebio Nieva, Director Técnico, Check Point

"Aunque utilicemos un segundo factor de autenticación, podemos ser atacados"

Mucho se habla estos días de la movilidad y teletrabajo dos entornos en los que la gestión de identidades y de la información, asociada a los usuarios, es fundamental. Durante la sesión online Autenticación y Gestión de Identidades, el nuevo perímetro de la seguridad dice Eusebio Nieva, Director Técnico de Check Point, que a esta situación se suma además la importancia de la seguridad, como factor esencial para asegurar la continuidad del negocio en un momento en el que muchas empresas y usuarios se apoyan en el mundo digital para desarrollar su actividad.

Al respecto de esta seguridad, Check Point considera parte intrínseca de la misma la gestión y el control de las identidades de los usuarios, además de la utilización de esos datos para construir una adecuada estrategia de protección contra los principales peligros a los que se enfrentan los usuarios en estos días, como el phishing (con ataques de Spear Phishing y de Whaling). Además, avisa de que determinadas prácticas como la reutilización de contraseñas, el uso de claves débiles o el Doble Factor de Autenticación (2FA) en dispositivos no protegidos entrañan riesgos importantes.

Por otro lado, no hay duda de que la adopción de la nube por las empresas se está acelerando, igual que las amenazas de Software-as-a-Service (SaaS). Los entornos SaaS se están viendo acechados principalmente por el phishing de credenciales, por lo que desde Check Point se considera

**EUSEBIO NIEVA,
DIRECTOR TÉCNICO, CHECK POINT**

**CLICAR PARA
VER EL VÍDEO**

sustancial que ese phishing pueda ser controlado de manera multifactorial, no solo por el contenido o las palabras claves, sino integrando además una protección de la identidad, con mecanismos de autenticación fuerte que vayan más allá de la propia identidad del usuario (desde dónde accede, qué dispositivo utiliza, con qué fin, a qué aplicación…) a fin de poder efectuar un control mucho más preciso y crear un acceso condicional. Dicho acceso será crucial para averiguar no solo la identidad del individuo, sino también con qué objeto accede y desde qué entorno. A partir de ahí se podrá limitar, aprobar, inspeccionar o permitir ese acceso.

Toda esta protección de la identidad puede ser realizada con diferentes formas de controlar la identidad; con un despliegue más sencillo (sin agente) o menos (con agente) para los usuarios, pero aprovechando la inteligencia de seguridad para saber que los ataques no van a ser exitosos. No obstante, no hay que olvidar que el Segundo Factor de Autenticación a veces no es suficiente. Si un dispositivo no está securizado o no está controlado, es posible sufrir un ataque utilizando precisamente ese 2FA.

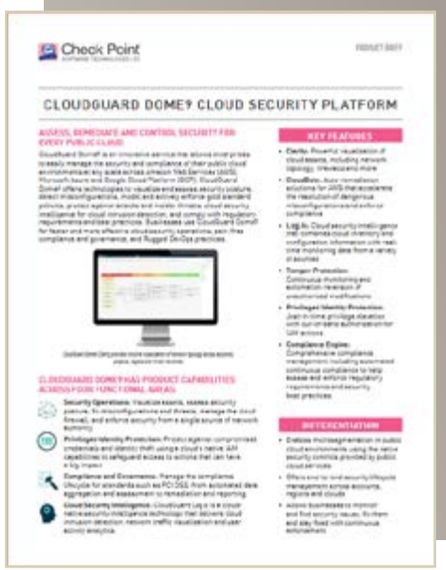
Check Point utiliza una infraestructura (Dome9) de control de la nube pública que permite tener una visibilidad completa en el entorno dinámico de la nube y los elementos implicados. También, ofrece una verificación de cumplimiento, gobierno y regulaciones, y remediación automática de fallos de configuración, sin olvidar la protección de las identidades para prevenir el acceso no autorizado y el secuestro de cuentas.

Vea aquí la intervención de Check Point en Autenticación y Gestión de Identidades, el nuevo perímetro de la seguridad.

> Check Point ofrece herramientas para la gestión de identidades que permiten seguir teniendo el control en la nube, pero sin perder la agilidad

CLOUDGUARD DOME9 CLOUD SECUITY PLATFORM

CloudGuard Dome9 ofrece tecnologías para visualizar y evaluar la postura de seguridad, detectar errores de configuración, modelar y hacer cumplir activamente las políticas del estándar de oro, proteger contra ataques y amenazas internas, inteligencia de seguridad en la nube para la detección de intrusiones en la nube y cumplir con los requisitos normativos y las mejores prácticas.


Check Point

CLOUDGUARD DOME9 CLOUD SECURITY PLATFORM

KEY FEATURES

DIFFERENTIATION

Compartir en RRSS

Daniel Varela, Solutions Engineer Security, F5 Networks

"Zero Trust es asumir que no se puede confiar en nadie y es el modelo más adecuado para proporcionar acceso remoto"

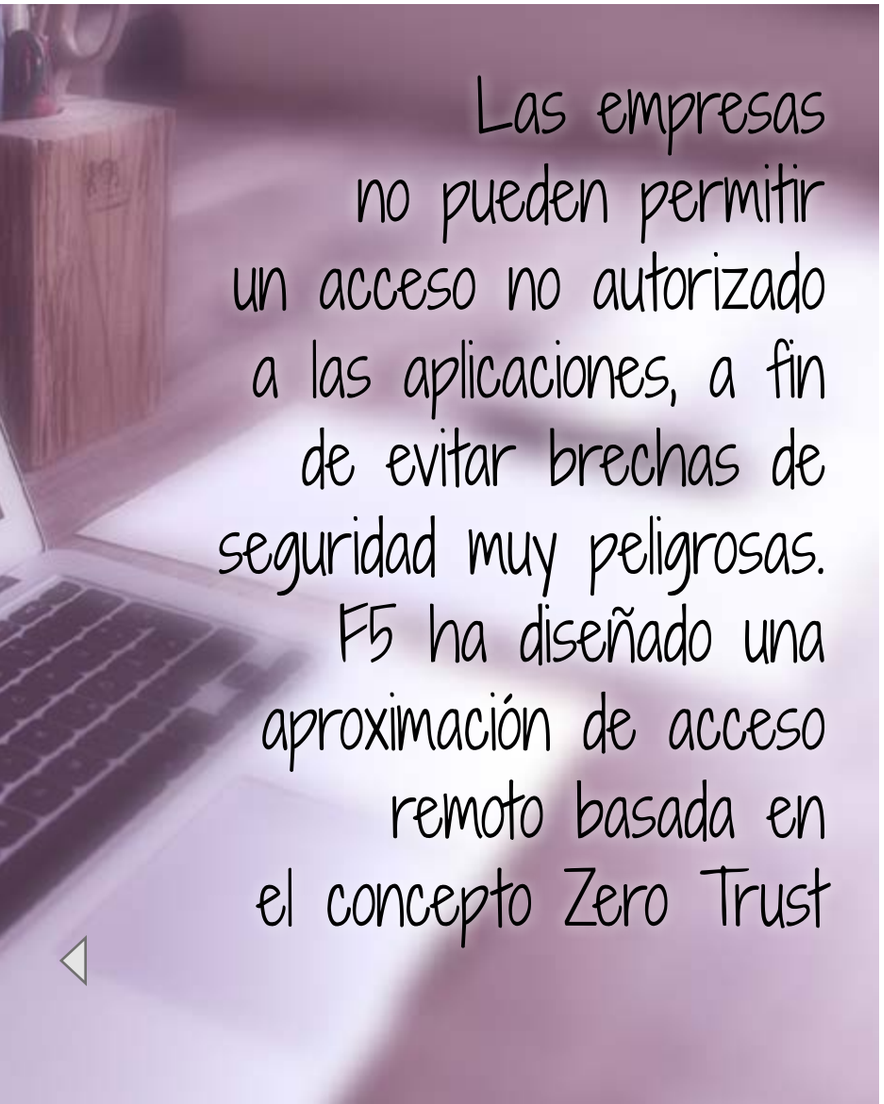
Los acontecimientos de las últimas semanas lo han cambiado todo. El acceso a las aplicaciones, el acceso remoto y el teletrabajo está siendo muy importantes. Sin embargo, y teniendo en cuenta este contexto en el que usuarios y equipos acceden continuamente a estas aplicaciones para desarrollar su trabajo, toca preguntarse si esto es confiable, seguro, y, sobre todo, cuál es la mejor manera de dar acceso a estas aplicaciones.

Daniel Varela, Solution Engineer Security de F5 Networks, dice durante la sesión online Autenticación y Gestión de Identidades, el nuevo perímetro de la seguridad que cada vez existe un mayor número de aplicaciones, así como una mayor dispersión de las mismas (con aplicaciones que residen en la nube, en las instalaciones u ofrecidas en modo SaaS) lo que añade una mayor complejidad a la hora de ofrecer acceso remoto seguro. Las empresas no pueden permitir un acceso no autorizado a estas aplicaciones y, por supuesto, deben cuidar

DANIEL VARELA,
SOLUTIONS ENGINEER SECURITY, F5 NETWORKS

CLICAR PARA VER EL VÍDEO

las credenciales de los usuarios, a fin de evitar brechas de seguridad muy peligrosas. De igual modo, es importante que controlen qué usuarios están accediendo a qué tipo de aplicaciones y hacerlo de una manera activa y continúa, no solamente al inicio de una sesión. También es necesario simplificar el acceso a las aplicaciones para los usuarios, a fin de que este sea muy sencillo y, a la vez, muy seguro. En la última década los ataques a la capa de identidad han superado el 30% de los totales, lo que deja patente los beneficios que este tipo de acciones conllevan para los atacantes.



Poniendo todo esto en contexto, F5 ha diseñado una aproximación de acceso remoto basada en el concepto Zero Trust, esto es, de no confianza, asumiendo que la información ha sido comprometida, y que, por tanto, debe ser verificada y monitorizada continuamente, al igual que el usuario, el tipo de dispositivo, los elementos de seguridad, la red desde la que accede, etc. Se trata de integrar todos estos elementos para tenerlos en consideración a la hora de proporcionar acceso remoto. Esto va a simplificar mucho este acceso, pero sin sacrificar la seguridad.

En lo que respecta al grado de madurez de la empresa española para proteger la gestión de identidades y usuarios, Daniel Varela apunta a que, pese a que existe cierta conciencia de seguridad y de protección del acceso remoto en base a la identidad, lo cierto es que la adopción de tecnologías de Zero Trust aún está un poco por detrás, en el sentido de que las empresas, a día de hoy, siguen utilizando métodos de acceso más legacy, como es el VPN SSL. No obstante, es previsible que todo cambie, dado que empresas como Google, están recomendando el acceso a las aplicaciones usando tecnología Zero Trust. Lo ideal para un usuario sería que pudiese acceder a su aplicación corporativa igual que accede a su correo.

Vea aquí la intervención de F5 Networks en Autenticación y Gestión de Identidades, el nuevo perímetro de la seguridad.

it whitepapers

SEGURIDAD DE IDENTIDADES = SEGURIDAD PARA LA EMPRESA

Conforme las identidades pasan a ser el principal objetivo de los hackers, las empresas deben asumir que la seguridad de identidades y accesos es básica para garantizar la integridad de sus aplicaciones y datos. Combinando medidas como la formación de usuarios, protocolos de empresa sólidos y consistentes, WAFs robustos y un portal centralizado de autenticación y autorización, las empresas pueden prevenir, o al menos mitigar, los ataques de credential stuffing cada vez más temibles y potentes.

Raúl D'Opazo, Solution Architect, EMEA Sales Consultant, One Identity

"La seguridad empieza con la identidad"

**RAÚL D'OPAZO,
SOLUTION ARCHITECT, EMEA SALES CONSULTANT, ONE IDENTITY**

CLICAR PARA VER EL VÍDEO

En un momento en el que los datos de usuarios y trabajadores se enfrentan a continuos peligros externos e internos, además de a fuertes regulaciones que, como GDPR, exigen la implantación de medidas técnicas y organizativas para asegurarlos, su protección es más importante que nunca. Raúl D'Opazo, Arquitecto de Soluciones, Consultor de Ventas para EMEA de One Identity, explica en la sesión online Autenticación y Gestión de Identidades, el nuevo perímetro de la seguridad cómo las soluciones de gestión de identidades pueden mejorar la seguridad de los datos.

Las empresas destinan importantes presupuestos a la implementación de medidas técnicas que les permitan proteger sus datos. Sin embargo, existe también un componente humano, no solo sobre la persona, sino sobre cómo las organizaciones gestionan e imponen controles internos a estas personas, que debe ser tenido en cuenta.

Efectivamente, en las empresas son muchas las personas que acceden a aplicaciones, algunas, incluso, con privilegios, lo que eleva su control sobre ellas y el acceso a datos confidenciales. A esto, hay que sumarle errores y accidentes humanos y, por supuesto, la falta de visibilidad sobre todo lo anterior, lo que incrementa el riesgo de sufrir brechas

Mejorar la seguridad de los datos es una de las ventajas que aportan las soluciones de gestión de identidades. One Identity cuenta con un porfolio centrado en securizar y gestionar los accesos de cuentas normales y privilegiadas

de seguridad. No hay que olvidar además que la complejidad de gestionar todo esto es muy elevada y esto acrecienta los riesgos y los costes operativos de las compañías.

Ante esta situación, One Identity opta por un mensaje claro y que descansa sobre el hecho de que la seguridad empieza con la identidad. De esta manera, se asegura que, partiendo de una estrategia de seguridad en la que la compañía identifique o centralice esa seguridad como base en el empleado (o en la identidad) todo evolucione del modo correcto.

Para ayudar a las empresas en este camino, One Identity cuenta con un porfolio centrado en securizar y gestionar los accesos, tanto de cuentas normales como de cuentas privilegiadas, estas últimas mucho más expuestas a estos ciberdelincuentes porque tienen un mayor acceso a más información.

Los beneficios de esta política de seguridad centrada en la identidad son varios, desde un mejor acceso, las personas van a contar con los permisos de acceso en el momento correcto, y una mayor seguridad, hasta una mayor productividad de los empleados (acceso sin esperas) y una menor complejidad para los departamentos de IT y compliance. De igual modo, los costes de operación también se ven reducidos.

En España, aunque hay bastantes iniciativas de gobierno de identidad, lo cierto es aún se debe mejorar bastante. La mayoría son proyectos que van de la mano de la capa de negocio, muy acotados a nivel funcional, y relegados casi siempre al área de infraestructura.

Vea aquí la intervención de One Identity en Autenticación y Gestión de Identidades, el nuevo perímetro de la seguridad.

PROTECCIÓN DE ONE IDENTITY

En casi todas las infracciones recientes de alto perfil, las cuentas con privilegios se han visto afectadas para ganar acceso a los sistemas y datos críticos. Para los administradores del área de TI, estas cuentas con acceso ilimitado son un desafío para administrar por diversos motivos, entre ellos, la gran cantidad de cuentas con privilegios y la cantidad de personas que necesitan tener acceso a ellas. Además de estos problemas, las soluciones tradicionales de administración de acceso con privilegios (PAM) incluyen arquitecturas complejas, tiempos de implementación prolongados y requisitos de administración onerosos.

Compartir en RRSS

Enric Mañez, Enterprise Security Sales, Akamai

"No tendremos una buena política de seguridad si la identidad de los usuarios no forma parte de ella"

En un mundo cada vez más cloud y descentralizado gestionar las identidades de los usuarios es crucial. Desde la perspectiva de que paradigmas como la nube, la movilidad o, más recientemente, el teletrabajo, han alterado la realidad TI, Enric Máñez, Enterprise Security Sales de Akamai, aboga, en esta sesión online Autenticación y Gestión de Identidades, el nuevo perímetro de la seguridad, por la necesidad de que estos cambios vengan acompañados por una transformación de la propia arquitectura de la seguridad. Se trata de avanzar en paralelo, a fin de poder responder ante el cambiante panorama de amenazas y superficies de ataque, pero también, como medida de adaptación a los diferentes escenarios que van surgiendo gradualmente. En este sentido, muchas empresas ya han experimentado esta transformación, desde la seguridad perimetral hasta la tan necesaria seguridad en el Edge.

ENRIC MAÑEZ,
ENTERPRISE SECURITY SALES, AKAMAI

CLICAR PARA VER EL VÍDEO

"Akamai plantea una estrategia de seguridad alejada de los arcaicos modelos tradicionales y asentada sobre un modelo Zero Trust alejado del perímetro y basado en la identidad"

Desde esta perspectiva, y entendiendo que tanto las aplicaciones como los usuarios operan en entornos cada vez más distribuidos, Akamai defiende una estrategia de seguridad alejada de los arcaicos patrones tradicionales, y asentada sobre un modelo Zero Trust, apartado del perímetro y basado en la identidad. Dicho modelo, además, se construye sobre tres pilares básicos: escalabilidad, visibilidad y sencillez, que son la base para implementar servicios centrados en el usuario. De este modo, la identidad se convierte en el nuevo perímetro virtual, un modelo lógico sobre el que construir la base de la seguridad corporativa.

Y es que, ¿de qué sirve tener una buena política de seguridad si la identidad de los clientes no forma parte de ella?

Conscientes de esta realidad, y a fin de proteger la identidad, Akamai quiere proporcionar un entorno altamente seguro y escalable, para registrar y almacenar información sensible de clientes a gran escala mientras se asegura la privacidad, la seguridad y, sobre todo, el cumplimiento con las regulaciones y normativas existentes. Para ello, cuenta con una solución cloud que permite a las empresas gestionar en modo servicio la identidad online de los clientes de forma eficiente, minimizando la complejidad operativa y los costes, y aumentando la visibilidad. Con este servicio, Akamai facilita la identificación y respuesta rápida ante eventos de seguridad, evitando falsos positivos y, en definitiva, acelerando la transformación digital.

Vea aquí la intervención de Akamai en Autenticación y Gestión de Identidades, el nuevo perímetro de la seguridad.

SERGIO MARTÍNEZ,
DIRECTOR GENERAL, SONICWALL IBERIA

CLICAR PARA VER EL VÍDEO

Sergio Martínez,
Director General, SonicWall Iberia

"La pregunta clave es cómo saber que quien se conecta es quien dice ser"

Los acontecimientos de las últimas semanas han propiciado una aceleración del trabajo digital sin precedentes. De hecho, se habla de todo esto, como el experimento más grande de trabajo nunca hecho en casa. En este sentido y en la sesión online Autenticación y Gestión de Identidades, el nuevo perímetro de la seguridad, Sergio Martínez, Director General de SonicWall para Iberia, se muestra convencido de que esta nueva realidad de informática distribuida acelerada por el COVID19 está creando una explosión de puntos de exposición inmensa, provocando la introducción de nuevas e inteligentes tácticas de ataque, a las que hay que hacer frente. Ante esto, Sergio Martínez defiende la importancia de dar una respuesta a los nuevos desafíos que este mundo sin perímetro está planteando: el acceso remoto, el acceso a aplicaciones cloud y el endpoint. SonicWall posee soluciones para estos tres problemas, empezando por el acceso remoto, que se puede corregir con autenticación segura, soluciones de endpoint y control, protección del acceso a aplicaciones cloud y Single Sign On federado.

Respecto al cloud y el correo electrónico, las empresas tienen que hacer frente ahora a un aumento en el número de vectores de ataques, a una mayor probabilidad de robo de datos y de credenciales y al incremento de los ataques de malware y phishing. SonicWall posee herramientas que

ACCESO MÓVIL SEGURO (SMA) DE SONICWALL

El SMA de SonicWall es un gateway de acceso seguro unificado que permite a las organizaciones proporcionar acceso en cualquier momento, en cualquier lugar y desde cualquier dispositivo a los recursos corporativos críticos.

Compartir en RRSS

permite monitorizar los logins de los usuarios para evitar el robo de credenciales, inspección avanzada de phishing y antimalware, DLP e integración con soluciones de correo mediante APIs.

En cuanto al endpoint, este merece una protección adicional. Estamos en un entorno hostil, lejos de la protección de la oficina, y esto presenta una serie de desafíos como el aumento de amenazas desconocidas, la necesidad de extremar las medidas de protección sobre los dispositivos personales (PCs) y los equipos remotos (redes tipo BYOD), así como medidas de desinfección, aislamiento o marcha atrás si fuera necesario.

Volviendo a la realidad del teletrabajo, Sergio Martínez detalla algunos de los errores que se están produciendo (publicar directamente servidores RDP, dar a todos los usuarios el mismo nivel de acceso, es necesario segmentar, o configurar políticas muy permisivas en las que prima el acceso a la seguridad, entre otras) y alude a que esta realidad estará muy presente en el futuro.

Así, y desde la perspectiva de que en estos días hemos pasado de un 20% de teletrabajo al 100%, Martínez manifiesta que el mundo ha cambiado para siempre: las oficinas ya no serán lo mismo. Teletrabajaremos muchos más. El teletrabajo ha venido para quedarse.

Vea aquí la intervención de SonicWall en Autenticación y Gestión de Identidades, el nuevo perímetro de la seguridad.