FORO it Digital Security

CAMINANDO HACIA ZERO TRUST

EL MODELO DE SEGURIDAD QUE SE IMPONE EN LA EMPRESA

fibratel | Cisco Partner | Forcepoint | SONICWALL

Akamai | aruba a Hewlett Packard Enterprise company | Barracuda | BlackBerry | f5 | netwrix

ONE IDENTITY | SOPHOS | THALES Building a future we can all trust | WatchGuard | CYTOMIC | zscaler

Caminando hacia Zero Trust, el modelo de seguridad que se impone en la empresa

El concepto Zero Trust fue acuñado en 2010 por John Kindervag, analista de Forrester. Supuso un avance frente al modelo Trust but Verify, en el que todo lo que se encontraba dentro del perímetro era considerado seguro por defecto. Una década después Zero Trust, que promueve la eliminación de la confianza como mecanismo para establecer políticas de seguridad adecuadas, se ha convertido en un modelo a seguir y en el foco de este I Foro ITDS.

Se ha organizado este evento en torno a tres ejes que necesitan ser validados constantemente dentro de este modelo de Zero Trust: los accesos, las identidades y los dispositivos. Cada uno de estos bloques ha contado con un patrocinador Platinum que ha estado presente en una mesa redonda en la que han participado diferentes CISOs. Además, cada temática ha sido desgranada tecnológicamente a través de diferentes ponencias, de gran nivel, en las que se ha hablado de Zero Trust Network Access como el complemento, o sustituto de las redes VPV; de la necesaria gestión de identidades o de la protección del endpoint bajo un modelo Zero Trust en el que la inteligencia artificial o el análisis de comportamiento cobran todo el sentido.

Como decíamos, en cada uno de estos bloques se ha celebrado una mesa redonda con diferentes responsables de ciberseguridad que no sólo han hablado de retos, sino de cómo están adaptando el modelo Zero Trust en sus empresas; cómo se aborda la protección de un endpoint heterogéneo y siempre conectado o la necesidad de conectar a los empleados en un entorno híbrido; cómo se implantan tendencias como XDR bajo un modelo de confianza cero o se adopta un múltiple factor de autenticación que garantice la identidad sin que impacte en la experiencia de usuario.

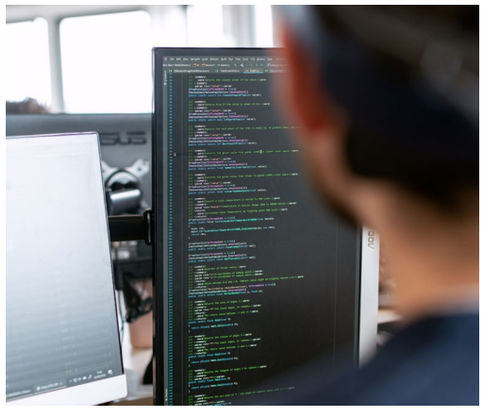
Muchas gracias a todos los participantes, tanto patrocinadores como expertos y responsables de seguridad por hacer posible el I Foro ITDS “Caminando hacia Zero Trust, el modelo de seguridad que se impone en la empresa”.

FORO it Digital Security

Sumario

Entrevistas

Esther Mateo Rodriguez, D.G Seguridad, Procesos y Sistemas Corporativos, ADIF



Mesa redonda. Nuevos modelos de seguridad para la empresa española

Mesa redonda

ZTNA, poniendo en práctica un modelo Zero Trust

La necesidad de gestionar las identidades y accesos

La importancia de mantener el endpoint seguro en un modelo Zero Trust

Impulso tecnológico

Forcepoint. **'Modelo de seguridad centrado en el dato: Zero Trust'**

Aruba Networks. **'Ciberseguridad en la nueva era del Extremo Inteligente'**

Sophos. **'Zero Trust. Modelo y filosofía de ciberseguridad'**

Barracuda. **'Barracuda CloudGen Access'**

Zscaler. **'Zero Trust Network Security madura y escalable'**

Akamai **'SASE/Zero Trust'**

F5 Networks. **'Zero Trust'**

SonicWall Iberia. **'Caminando hacia Zero trust'**

One Identity. **'La identidad de los usuarios en un modelo Zero Trust'**

Netwrix. **'Zero trust. Un mundo a salvo de las amenazas'**

Thales. **'Access Management Solutions'**

Fibratel. **'Transformación digital. Clouds. Puesto y trabajo. SASE'**

Sophos. **'Nuevos tiempos. XDR'**

Cytomic. **'La seguridad Endpoint en un mundo Zero Trust'**

Blackberry. **'Zero Trust Security. Zero Touch Experience'**

Tribuna de opinión

'Retos y cambios de paradigma' (Lucas Rey, Forcepoint)

'Ventajas de ZTNA con respecto a las soluciones VPN' (Alberto R. Rodas Sophos)

'Proteja sus activos compartidos con Seguridad Zero-Trust' (Sergio Martínez, SonicWall)

'Protegiendo la Transformación con un modelo Zero Trust' (Juan Francisco Moreda, Fibtratel)

Índice de anunciantes

Forcepoint	Zscaler
Fibratel	One Identity
SonicWall	Thales
Aruba	Blackberry
Sophos	Akamai
Barracuda	F5
Netwrix	Cytomic

FORO it Digital Security

Entrevista

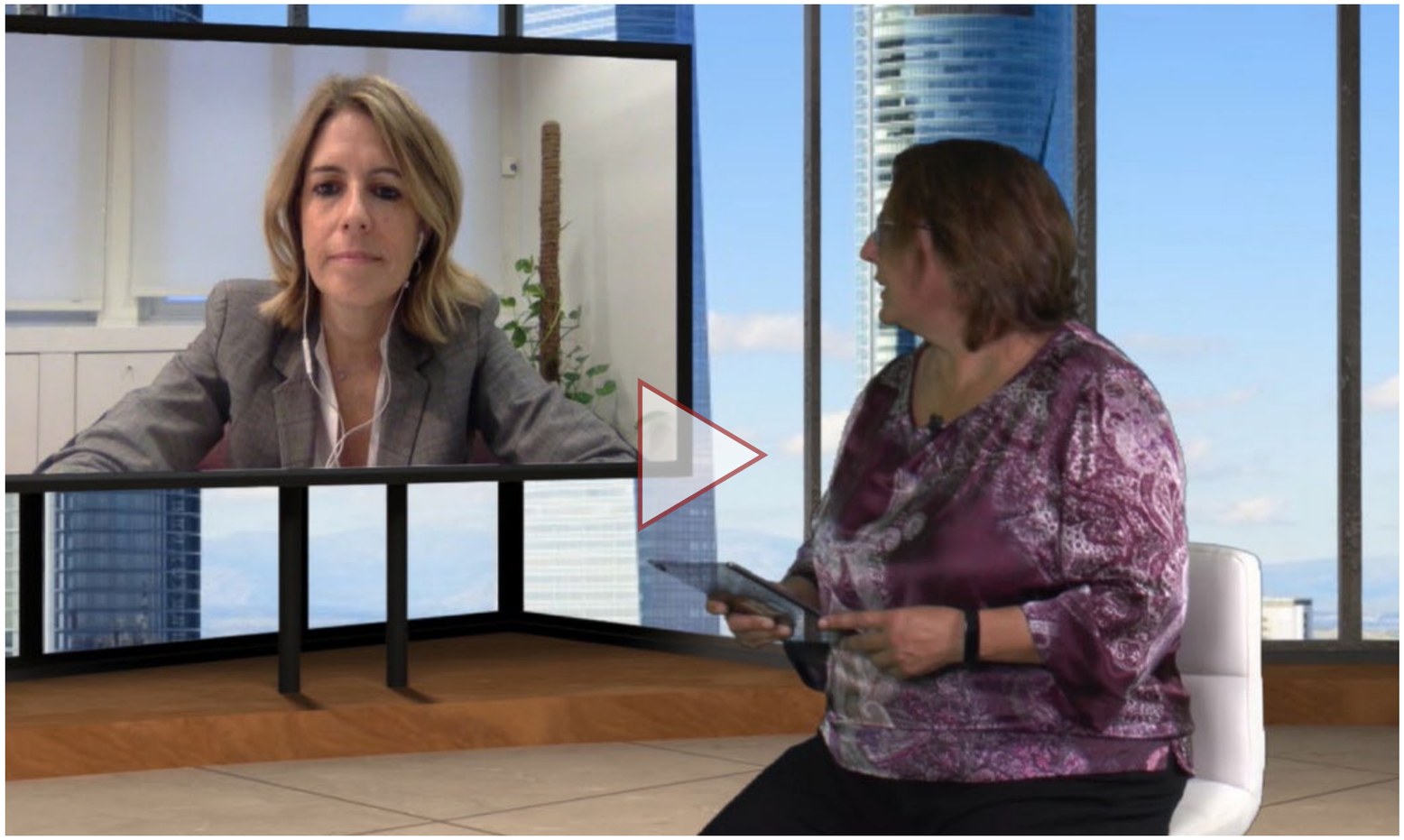
Hace unos años la presidenta de Adif, Isabel Pardo de Vera, impulsaba el nombramiento de cinco nuevos directores generales en el marco de la estructura organizativa que destacaba las áreas estratégicas de actividad de la compañía. Y una de esas áreas estratégicas es la seguridad, a cuyo cargo está María Esther Mateo Rodríguez, a quien pudimos entrevistar en el marco del I Foro ITDS centrado en Zero Trust.

“En Adif hemos apostado claramente por un modelo Zero Trust”

(Esther Mateos)

Lo primero que preguntamos a la directora general de Seguridad, Procesos y Sistemas Corporativos de Adif es si cree que la empresa española está concienciada en ciberseguridad. La respuesta es tan compleja como la propia situación del mercado. Asegura no desvelar nada cuando dice que existe un alto nivel de riesgo, un perímetro inmenso que proteger y una necesidad de hacer una gran inversión, y que los ciberdelincuentes no hacen sino esperar el momento, el vector de ataque y el objetivo, “con lo cual la situación es compleja, pero mirándola conozco con optimismo porque tenemos por delante un reto grande”.

Asegura al mismo tiempo Esther Mateos que las empresas sí que están concienciadas pero que



"Hace falta un cambio cultural para que el problema de la ciberseguridad no sea exclusivamente del CISO y su equipo, sino de toda la compañía"

"EN ADIF HEMOS APOSTADO CLARAMENTE POR UN MODELO ZERO TRUST" (ESTHER MATEOS)

CLICAR PARA VER EL VÍDEO

"hace falta un cambio cultural para que el problema no sea exclusivamente del CISO y su equipo, sino de toda la compañía".

El aumento que ha habido de ataques de ransomware, phishing o ataque al CEO son algunos de los retos a los que se enfrenta el CISO postpandemia. Además, asegura la directiva de Adif, con el COVID "hemos sido todos conscientes de que el trabajador es el eslabón más débil, junto con la cadena de suministro". Finalmente menciona un tercer aspecto que debe contemplarte como reto: la fiebre por implantar tecnología.

Zero Trust, el modelo de seguridad que se impone en la empresa y que es el motor que ha impulsado este primer Foro ITDS es también una apuesta dentro de Adif donde "no concebimos ya otra forma de protegernos frente a modelos previos". Añade Esther Materos que además del ámbito IT "tenemos un ámbito OT que requieres de un modelo diferente. En eses sentido hemos apostado claramente por el modelo Zero Trust". Menciona la directiva la capacidad del modelo de promover una visibilidad total sobre lo que hay conectado a la red; la doble autenticación; el control de acceso en función a los roles; una tecnología que además encuentre patrones extraños; monitorización continua del estado de seguridad de la red, así como la capacidad de

"El gran reto de la compañía es alcanzar el nivel de madurez en OT que ya se tiene en IT"

respuesta hacia el ataque; “con lo cual, para nosotros Zero trust es una apuesta firme, junto con la securización del cloud”.

Preguntamos a Esther Mateos por la madurez de Adif en los diferentes pilares que deben tenerse en cuenta en el modelo Zero Trust. Menciona la directora general de seguridad de Adif que el gran reto de la compañía es alcanzar el nivel de madurez en OT que ya se tiene en IT y que uno de los grandes retos tiene que ver con los endpoints de la parte OT, “y en donde más tenemos que centrarnos en Adif”, sin que eso signifique que no haya “margen de mejora” en otros pilares de Zero Trust.

La falta de talento es, desde hace tiempo, un problema en el mercado tecnológico, más en el seguridad, y mucho más cuando además se tienen que tener en cuenta aspectos como el OT o el cloud. ¿Crees que se están dando los pasos necesarios para para abordar esta problemática? Comenta que el problema parte desde la inexistencia de una formación reglara que permita conocer los pasos que a priori tiene que dar una persona para tener las competencias necesarias; “creo en eso hay que mejorar” porque “todavía creo que no tenemos claro lo que debe estudiar alguien que se quiera hacer especialista en ciberseguridad en el ámbito OT”, por ejemplo.

“Apasionante”, así prevé Esther Mateos el futuro de la ciberseguridad en un momento de cambio tecnológico hacia el 5G, la inteligencia artificial o el IoT.

Compartir en RRSS

Forcepoint

Modelo de seguridad SASE y Zero Trust

Las soluciones de ciberseguridad de SASE permiten a sus usuarios que accedan de forma segura y sin importar donde estén, a la web, las aplicaciones en la nube y las aplicaciones internas.

forcepoint.com

FORO it Digital Security

Mesa Redonda

Nuevos modelos de seguridad para la empresa española

Tras la entrevista con Esther Mateos, arrancamos la primera mesa redonda del I Foro ITDS sobre Zero Trust reuniendo a algunos expertos del mercado, representantes de organizaciones que pueden dar una visión de cuál es la situación de la empresa española, cómo impacta la falta de talento y cómo se hace frente a la problemática, así como aportar unas reflexiones de lo que ha ocurrido este año.

Participan en este encuentro Eduvigis Ortiz, presidenta de Women4Cyber Spain y Strategic Alliances Leader en SAS; Miguel Rego, Vocal del Cluster CiberMadrid y director general de Funditec; y Rubén Fuentes, CEO de TicJob. Durante su participación asegura Eduvigis que las empresas se enfrentan a cada vez más retos, pero que están haciendo los deberes, están invirtiendo en ciberseguridad, aunque hay que tener confianza cero y "hacer muchísimo trabajo de concienciación". Respecto a la situación de la empresa española en seguridad, dice Miguel Rego que hay que diferenciar a la gran empresa, la pyme, e incluso la micropyme; mientras que la gran cuenta es madura en seguridad, "cosa distinta sería el hablar de la pyme y especialmente la micro pyme"; como ejemplo un dato interesante: sólo el 4% de las pymes un utiliza algún servicio relacionado con la con la ciberseguridad, lo que significa que "en el campo de la pyme y la micro pyme queda muchísimo por hacer".

Como portal de empleo especializado en el sector tecnológico "hemos notado un aumento bastante notable de las ofertas de trabajo que

"La gente no sabe qué hace un ingeniero, o un científico de datos, o alguien que trabaja en vigilancia digital"

Eduvigis Ortiz, presidenta de Women4Cyber Spain y Strategic Alliances Leader en SAS

se publican relacionadas con la ciberseguridad", asegura Rubén Fuentes, así como también el de otro tipo de perfiles "que a priori parecen menos importante, como el perfil de ciberinteligencia, que es menos técnico pero muy importante en el proceso de rastreo de un ciberataque para saber qué ha pasado y por qué ha pasado y poder prevenir futuros ataques".

Cuando ponemos sobre la mesa uno de los grandes problemas del mercado de la seguridad, que no es otro que la falta de profesionales de ciberseguridad, dice Migue Rego que en España hay una sobreoferta de formación en ciberseguridad, y con gran calidad, "pero no estamos siendo capaces de atraer el suficiente número de profesionales que se demandan", lo que debe llevar a hacer una "profunda reflexión de la situación en todos los estamentos y un esfuerzo a nivel nacional".

Dice Rubén Fuentes que el 10% de las ofertas de trabajo que hay en el TicJob están relacionadas con las redes y la seguridad, pero que no hay tanta oferta formativa para toda la demanda que hay; "a pesar de que haya másters, no hay grados

NUEVOS MODELOS DE SEGURIDAD PARA LA EMPRESA ESPAÑOLA **CLICAR PARA VER EL VÍDEO**

"Estamos abocados a ir a un modelo Zero Trust porque la propia digitalización nos lleva hacia él"

Miguel Rego, Vocal del Cluster CiberMadrid y director general de Funditec

universitarios", dice el CEO de TicJob.

"Comunicar, visibilizar, inspirar, informar y finalmente acompañar" son las cinco líneas de trabajo de Women4Cyber Spain, asegura Eduvigis Ortiz, añadiendo que hace falta mucha comunicación en la sociedad en todos los niveles, porque "la gente no sabe qué hace un ingeniero, o un científico de datos, o alguien que trabaja en vigilancia digital". Afirmando que "necesitamos todas las miradas", dice también Eduvigis Ortiz que la asociación que preside busca promover esa incorporación de talento femenino en el mundo de la ciberseguridad.

En 2022 esperamos que "todas las partes de la empresa sean conscientes de la importancia de controlar este tipo de posibles brechas o de fugas de seguridad que pueda haber", dice el CEO de TicJoc, añadiendo que en las empresas se piensa que solamente son los profesionales técnicos o

aquellos que manejan datos críticos son los que tienen que tener esta confianza cero, pero las empresas deben reflexionar y empezar a implantar planes formativos para para todos los niveles, desde el personal de administración hasta el hasta el directivo de más alto nivel.

Para el próximo año espera Eduvigis Ortiz que la ciberseguridad se ponga encima de cada proyecto, que las empresas también sean conscientes de que el dato tiene más relevancia “y es el que tenemos que proteger porque es el que está transformándose”. Además, se seguirá apostando por la comunicación y hacer que las personas y las empresas sean cada vez más conscientes de los riesgos a los que se enfrentan.

Asegurando que el concepto de confianza cero tardará un poquito en calar, dice Miguel Rego que al final “todos estamos abocados a ir a un modelo Zero Trust porque la propia digitalización nos lleva hacia él”.

> "Las empresas deben reflexionar y empezar a implantar planes formativos de ciberseguridad para todos los niveles"
>
> Rubén Fuentes, CEO, TicJob

Compartir en RRSS

Fibratel es un integrador global de soluciones IT que acompaña a las empresas en su transformación digital

La ciberseguridad ha dejado de ser una opción para convertirse en una necesidad

CISCO Partner
Premier Certified

Soluciones

- Next Generation Firewall
- E-mail Security
- SD-WAN
- Secure Web Gateway
- CASB
- Backup-Resiliency
- Antivirus Endpoints
- MFA

Servicios

- Security Posture and Road Mapping

Servicios Gestionados

- Managed Security
  - -Managed Firewall
  - -Managed EDR
  - -Managed Proxy
  - -Cybersecurity Monitoring
- Security & Vulnerability Management (/fsafe)
- Breach & Attack Simulation
- Security Awareness

ZTNA, poniendo en práctica un modelo Zero Trust

Las VPN, o redes privadas virtuales, se diseñaron hace varias décadas para extender el alcance de las redes corporativas. La movilidad y el teletrabajo han llevado al límite esta tecnología, que se verá desplazada por Zero Trust Network Acess, o ZTNA, diseñada específicamente para resolver los muchos problemas que se pueden encontrar al cambiar los modelos operativos y pasar a formas de trabajo remotas.

Una de las grandes ventajas de ZTNA es que puede funcionar en paralelo con las tecnologías de acceso remoto existentes mientras se eliminan gradualmente. Para hablar de la situación a la que se enfrentan los responsables de ciberseguridad de las empresas, así como la manera en que se está abordando la necesidad de conectar a los empleados en un entorno híbrido reunimos un grupo de expertos en una debate patrocinado por Forcepoint y titulado “ZTNA, poniendo en práctica un modelo Zero Trust” en el que estuvieron presentes Fanny Perez, CISO de Codere; José Luis Paramio, CISO de Userlytics Corporation; Joan Massanet, CISO de Maximice Events Group; Javier Sánchez Salas, CISO de HAYA Real Estate y Lucas Rey, director de canal para la región de Iberia de Forcepoint.

La reunión arrancó pidiendo a los responsables de ciberseguridad invitados qué retos creen que tendrán que afrontar el próximo año. Asegurando que el incremento de los ciberataques va a más, aseguraba Fanny Pérez, CISO de Codere, que los responsables de ciberseguridad deben optimizar

ZTNA, PONIENDO EN PRÁCTICA UN MODELO ZERO TRUST

CLICAR PARA VER EL VÍDEO

los procesos para aumentar tanto las capacidades de ciberresiliencia como de protección, y que “Zero Trust será sin duda un pilar fundamental para todos los responsables de seguridad el próximo año”.

Mencionaba durante su intervención José Luis Paramio cómo la consolidación del mercado de TI y de ciberseguridad afectará a la prestación de algunos servicios, sin que prevea grandes cambios a nivel tecnológico. Advertía Joan Massanet por su parte que en los próximos años la ciberdelincuencia equivaldrá a la tercera economía más potente del mundo, y que tanto la resiliencia como el plan de continuidad de negocio son dos elementos fundamentales que “todos los que nos dedicamos a la gestión de la ciberseguridad deberíamos tener más en cuenta”.

Para Javier Sánchez Salas, CISO de Haya Real Estate, “el mayor problema que vamos a tener en los próximos dos o tres años es la falta de talento”. Decía que ya no hay que hablar tanto de nuevos ataques o de la utilización de la inteligencia artificial en los mismos, sino de “cómo defendernos”.

Los retos planteados por los responsables de ciberseguridad coinciden con las demandas que llegan a Forcepoint. Aseguraba su director de canal que los clientes demandan talento para desarrollar proyectos, y se muestran preocupados por la protección de

"Zero Trust será sin duda un pilar fundamental para todos los responsables de seguridad el próximo año"

Fanny Pérez, CISO, Codere

"El mayor problema que vamos a tener en los próximos dos o tres años es la falta de talento"

Javier Sánchez Salas, CISO, Haya Real Estate

datos y la necesidad de adaptar su arquitectura a los diferentes entornos que se han ido generando antes, durante y después de la pandemia.

Y uno de los elementos que han tenido que afrontarse es el teletrabajo, la necesidad de conectar a los empleados a los recursos empresariales desde cualquier lugar y con cualquier dispositivo. A la hora de hacer frente a este nuevo modelo híbrido, explicaba Joan Massanet que se "están estableciendo todos los accesos condicionales que podemos" porque no se pueden poner barreras al trabajo diario, y que se debe enseñar a la gente a cómo manejar los datos. Explicaba José Luis Paramio que su compañía ya contaba con un modelo híbrido antes de la pandemia "y no hemos tenido que adaptar sobre la marcha nuestra forma de trabajar".

"El modelo híbrido viene en nuestro ADN", dice el CISO de Haya Real Estate, explicando que la apuesta de la compañía ha sido el convertir el Zero Trust en una 'commodity' para el usuario gracias a una única plataforma a través de la cual se acceden a todos los servicios IT de Haya Real Estate "con la comodidad de que sea un único punto de acceso".

Codere se enfrenta a esta nueva situación de acceso híbrido con una estructura y servicios definidos con anterioridad a la pandemia. En ese 'antes y después de la pandemia' la diferencia es que "muchas empresas estamos pensando en ser más ágiles y competitivas", asegura Fanny Pérez, añadiendo que la pérdida de perímetro lleva a una adopción del Zero Trust que obliga a adoptar nuevas soluciones de seguridad que no son las tradicionales. Reflexiona la CISO de Codere en que Zero Trust no es una solución ni un fabricante sino "una arquitectura que tenemos que construir".

Preguntamos a Lucas Rey cómo está ayudando Forcepoint a la empresas a conectar a los empleados en este nuevo entorno híbrido. Aseguraba el directivo durante su intervención que la compañía busca ayudar a las empresas en la transformación

del modo de trabajar con tecnología que te permite establecer un acceso explícito y confiable y donde tienes un control de esa información, dándole un contexto a quién se conecta, por qué se conecta y a qué información accede.

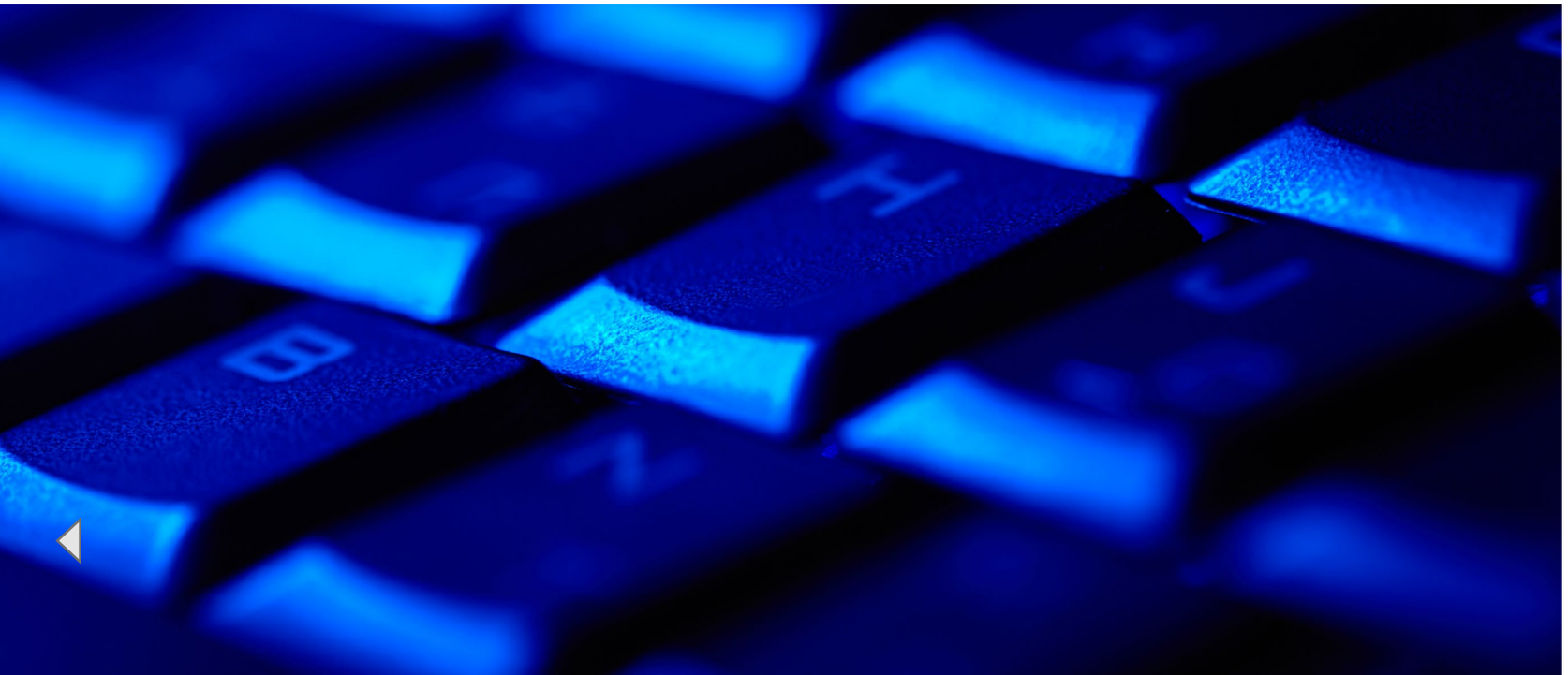
Protección del dato

Planteamos cómo se afronta la protección del dato en estos entornos híbridos, con multitud de soluciones y multitud de aplicaciones. Para Javier Sánchez Salas es importante acompañar al negocio, así como poder identificar cuáles son los datos críticos de la empresa. A partir de ahí es “hay que ir poniendo controles y ver cuáles son los flujos de datos de la empresa”.

“Si no sabemos lo que tenemos que proteger, las protecciones que vayamos a incorporar no van a ser muy efectivas”, decía Fanny Pérez, añadiendo que más que tecnología esto es una disciplina, y que en un modelo Zero Trust es fundamental adaptar los accesos en función de dónde se esté conectando el empleado para resguardar la protección del dato.

Con una base de datos de más de un millón de testers repartidos por todo el mundo, Userlytics Corporation tiene que hacer frente a diferentes regulaciones de diferentes países, por lo que la seguridad del dato “depende fundamentalmente de dónde hayamos recopilado ese dato, y definiendo los roles en las empresas” para saber quién puede acceder a qué datos, explica José Luis Paramio.

A lo dicho por sus compañeros añade Joan Massanet que hay que establecer un control del dispositivo que se conecta, teniendo en cuenta si está actualizado o la versión del sistema operativo. También apunta a que, en lo que a protección de



"El plan de continuidad de negocio es uno de los elementos fundamentales que todos los que nos dedicamos a la gestión de la ciberseguridad deberíamos tener más en cuenta"

Joan Massanet, CISO, Maximice Events Group

"La seguridad del dato depende fundamentalmente de dónde hayamos recopilado ese dato"

José Luis Paramio, Userlytics Corporation

datos se refiere, las empresas se ven a menudo condicionadas por una cadena de suministro con la que deben compartirse los datos y que en ocasiones "nos genera mucho trabajo porque tenemos que estar no sólo pendientes de lo nuestro, sino de lo de los demás.

Preguntamos también a Lucas Rey cómo ayuda Forcepoint a proteger el dato en estos entornos híbridos y bajo un modelo Zero Trust. Asegura el responsable de canal que lo que se busca desde la compañía es entender cómo es el comportamiento del usuario y, dependiendo de ese comportamiento, "permitirles unos accesos o no en función de un scoring de riesgo". En cuanto al dato, no sólo se le busca, sino que se le clasifica y protege por los cuatro vectores por los que el dato se mueve: endpoint, correo, firewall o proxy, y entorno colaborativo de aplicaciones en nube. "Mezclando los dos conceptos de monitorización de usuario y la protección del dato somos capaces de ayudar a las compañías a evitar una exfiltración del dato, sea intencionada o malintencionada".

Conclusiones

Tras finalizar el encuentro con los CISOs pedimos a Lucas Rey unas conclusiones, entre las que destaca la preocupante falta de talento en el sector; la necesidad de proteger los accesos y la información en un modelo de trabajo híbrido y que entre los retos de 2022 veremos cómo los atacantes siguen ingeniándoselas para intentar generar brechas de seguridad y poder acceder al dato.

Sobre si la empresa española está madura para adoptar el modelo Zero Trust, dice Lucas rey que en España se ha hecho un buen trabajo en ciberseguridad y que la empresa en España está preparada para dar ese salto.

"Ofrecemos tecnología que permite establecer un acceso explícito y confiable y donde se tiene un control de la información"

Lucas Rey, Channel Manager Spain + Portugal, Forcepoint

Compartir en RRSS

2021

SONICWALL®

INFORME DE CIBERAMENAZAS

SONICWALL.COM | @SONICWALLSPAIN

A medida que las situaciones de trabajo evolucionaron en 2021, también lo hicieron los **métodos de los actores de las amenazas y los perpetradores motivados**.

En la **actualización semestral del Informe de Ciberamenazas 2021 de SonicWall**, se analiza cómo los actores de las amenazas utilizan cualquier medio necesario (**controles de seguridad laxos, vulnerabilidades sin parches, ataques de día cero y debilidades en la cadena de suministro**) para obtener beneficios maliciosos y provocar disturbios a nivel mundial.

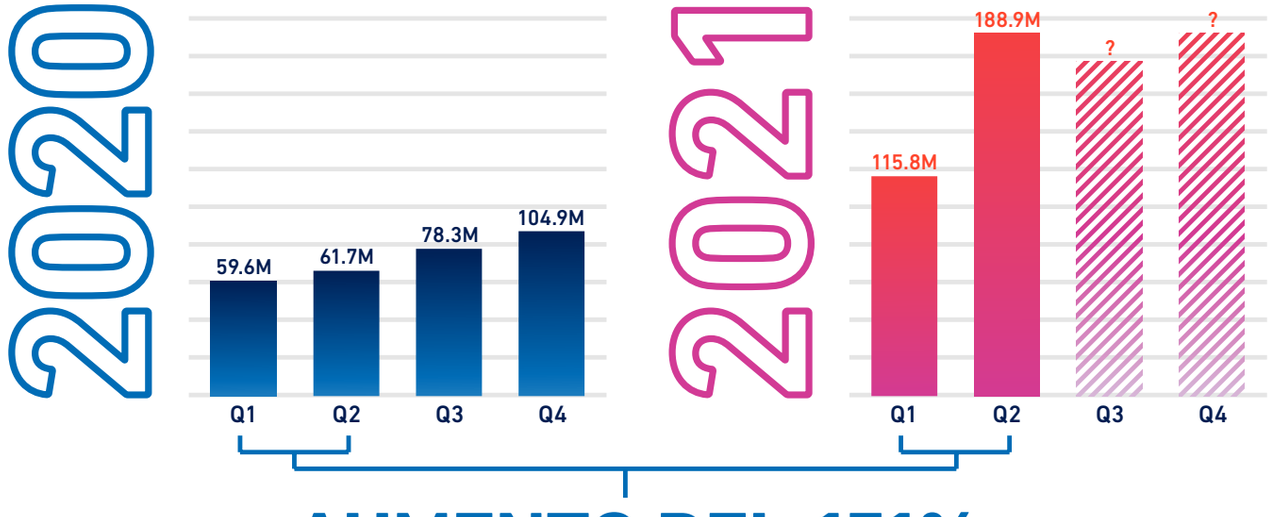
OBTENGA EL INFORME COMPLETO

sonicwall.com/threatreport

EL RANSOMWARE ALCANZA SU MÁXIMO HISTÓRICO

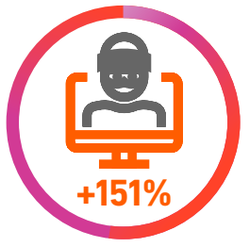
Los ataques de ransomware en el primer semestre de 2021 ya han eclipsado todo el volumen total de 2020: **un aumento del 151% en lo que va de año.**

En los primeros seis meses de 2021, el volumen mundial de ransomware alcanzó la cifra sin precedentes de **304,7 millones** de intentos de ataque.

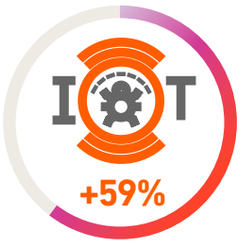


TENDENCIAS MUNDIALES DE LOS CIBERATAQUES

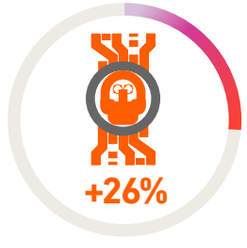
2.5 billones
ATAQUES DE MALWARE



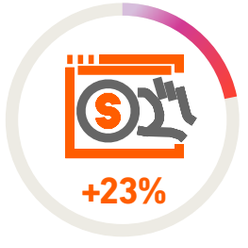
304.7 millones
ATAQUES DE RANSOMWARE



32.2 millones
ATAQUES DE IoT



2.1 millones
AMENAZAS CIFRADAS



51.1 millones
ATAQUES DE CRYPTOJACKING

2.5 trillones
INTENTOS DE INTRUSIÓN

Forcepoint. Lucas Rey, Channel Manager Spain & Portugal

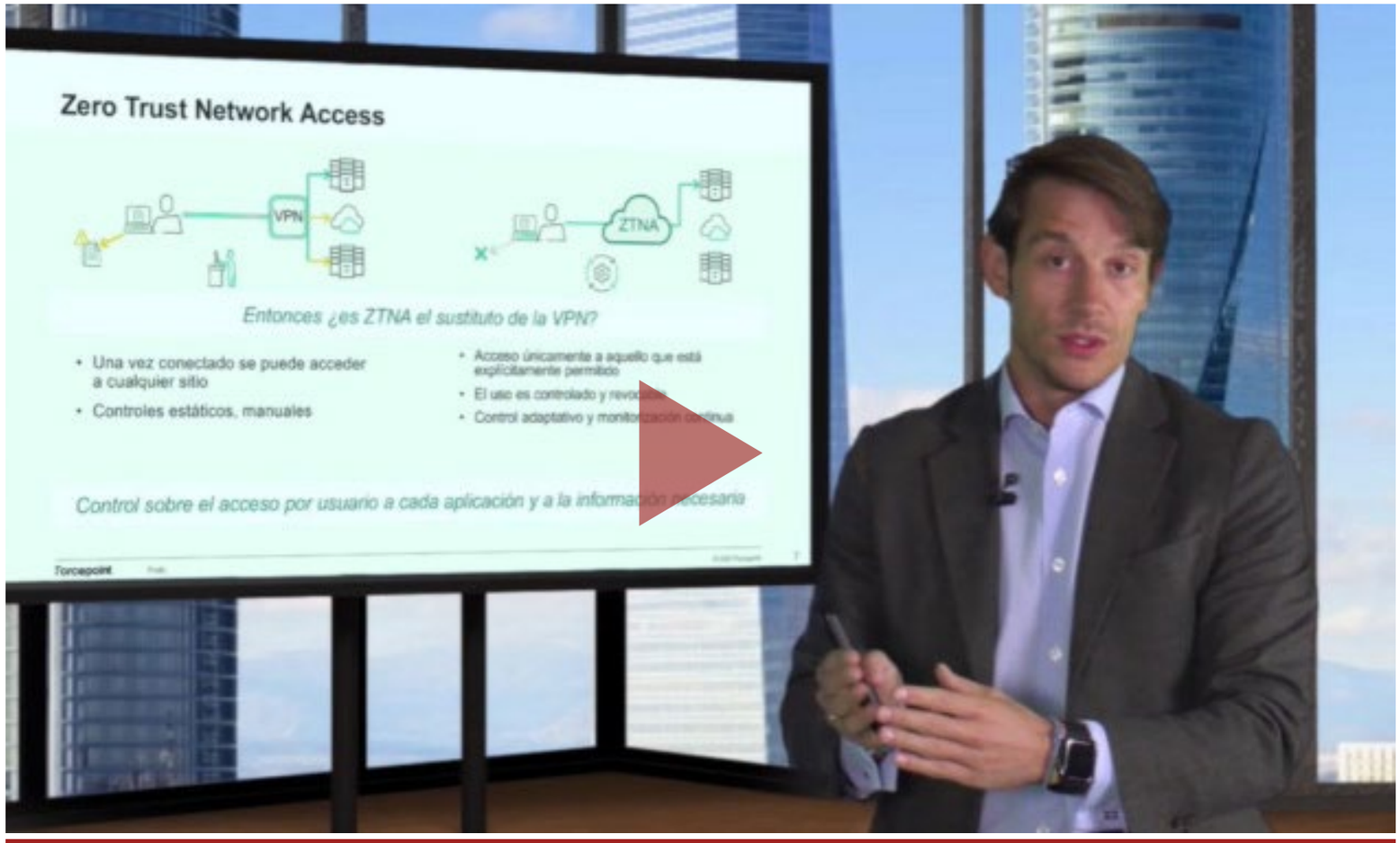
“Zero Trust Network Access es un complemento de las VPNs”

Lucas Rey, Forcepopint

Zero trust Network Access es una tecnología que se ha convertido en algo indispensable para muchísimas empresas. Su adopción se disparó en tiempos de pandemia, cuando muchísimas empresas se vieron en la necesidad de apostar por el cloud y el teletrabajo.

Las tres grandes claves del ZTNA son los usuarios, las aplicaciones y la información. Con esta tecnología se promueve una confianza explícita, permitiendo que el usuario solo acceda a aquello a lo que ha de acceder, a lo que tiene permitido. El uso de esa aplicación está controlado y por lo tanto es revocable, el control es adaptativo y se monitoriza continuamente.

Para Lucas Rey, Channel Manager Spain & Portugal de Forcepoint, ZTNA no es un sustituto de las VPNs, sino que se trata de una tecnología



“ZERO TRUST NETWORK ACCESS ES UN COMPLEMENTO DE LAS VPNS” **CLICAR PARA VER EL VÍDEO**

Contenido relacionado

Foro ITDS. Caminando hacia Zero Trust

Tu camino a Zero Trust

Seguridad Zero Trust Continua

Zero Trust lo que acaba representando es el cambio de una confianza implícita a una confianza explícita

complementaria, ya que siguen existiendo en los data centers de muchas aplicaciones que se han tardado años en desarrollar y en validar con la arquitectura y los sistemas que tienen actualmente y que no es viable a nivel económico migrar a un entorno IaaS. El valor que aporta ZTNA es ofrecer el acceso a aplicaciones para los usuarios, estén donde estén, protegiendo tanto a usuarios como a aplicaciones de una forma transparente.

Desde Forcepoint se trabaja de una manera estratégica. La compañía entiende las áreas de trabajo y de mejora que demandan las empresas, con desafíos como procesos de transformación digital, de migraciones a nube, entornos multifabricante… Además ofrecen mejoras de rentabilidad y de ROIs, y una predictibilidad del gasto cubriendo todas las áreas necesarias bajo un acuerdo global y con gran flexibilidad ante posibles cambios estratégicos.

Aruba Networks. Pedro Martínez Busto, Business Development Manager Southern Europe

“Aruba da un paso más a través del Advanced Zero Trust”

Pedro Martínez, Aruba

“ARUBA DA UN PASO MÁS A TRAVÉS DEL ADVANCED ZERO TRUST” CLICAR PARA VER EL VÍDEO

Zero Trust es un concepto muy conocido en el mundo de la ciberseguridad. Aplicado al ámbito del networking quiere decir no permitir la entrada de ningún usuario a la red si previamente no se ha identificado, autorizar el acceso a servidores y aplicaciones en base a ello. Aruba da un paso más a través del Advanced Zero Trust.

Las dos preguntas más importantes que se hace un responsable de ciberseguridad son cómo puede securizar todo el entorno corporativo más tradicional y cómo proteger ese acceso a los servicios que están fuera del entorno corporativo.

Para responder a estas preguntas, Pedro Martínez Busto, Business Development Manager Southern Europe de Aruba Networks, se apoya en el concepto de Advanced Zero Trust, que parte del concepto básico del Zero Trust de identificar y autorizar a los usuarios, pero añade dos elementos

nuevos: microsegmentación y capacidades de seguridad UTM a localizaciones remotas.

En el centro de la propuesta de Aruba está la solución ClearPass Policy Manager, para identificar, autorizar y aplicar controles de acceso a los diferentes usuarios y dispositivos que se conectan a la red. Junto a los siwtches, puntos de acceso wifi o gateways de la compañía, permite aplicar esa microsegmentación o funciones de UTM.

Para garantizar el acceso seguro a esos otros servicios que están fuera del entorno corporativo, Aruba apuesta por una combinación de dos tecnologías: SDWAN y seguridad en la nube, concepto que ya acuñó Gartner en el 2019 con el famoso SASE, a partir de las soluciones SDWAN de la compañía que permiten integrar las mejores soluciones de seguridad en la nube para garantizar siempre la libertad de elección al cliente.

Contenido relacionado

Foro ITDS. Caminando hacia Zero Trust

El panorama de las arquitecturas de seguridad de confianza cero, SD-WAN y SASE

Aruba ESP con seguridad Zero Trust

La propuesta global de Aruba es securizar todas las comunicaciones desde el extremo a la nube sin perjudicar en ningún caso la experiencia del usuario y asegurándonos de que aplicamos la seguridad allí donde tiene más sentido

Compartir en RRSS

aruba
a Hewlett Packard Enterprise company

LLEVE LA SEGURIDAD AL EDGE

Proteja su entorno de trabajo híbrido

Sophos Iberia. Sergio Mendoza Martín, Territory Account Manager

“La tecnología ZTNA viene a solucionar los accesos en un modelo híbrido”

Sergio Mendoza, Sophos

Tras cerca de dos décadas trabajando con un sistema de VPNs, aunque son un buen sistema de acceso, se ha quedado un poco obsoleto, en concreto a nivel de seguridad. Sobre todo debido a los últimos tiempos en los que el enfoque ha cambiado y las empresas han necesitado de alternativas como el ZTNA.

“LA TECNOLOGÍA ZTNA VIENE A SOLUCIONAR LOS ACCESOS EN UN MODELO HÍBRIDO”

CLICAR PARA VER EL VÍDEO

En los últimos meses se ha observado un aumento de ataques a través de VPN y sobre todo de ransmoware, por lo que las empresas han decidido por apostar por el modelo de ZTNA. Se trata de un acceso a redes desde confianza cero que consiste en microsegmentar cada usuario a nivel de aplicación o a nivel de datos para que cada uno tenga acceso solo a sus propias necesidades y no a toda la red.

Según Sergio Mendoza Martín, Territory Account Manager de Sophos, los principios básicos del Zero Trust indican que ya no hay un “dentro” de la red,

no se debe confiar en nada y se debe verificar todo, y la seguridad debe adaptarse en tiempo real. La confianza se la tiene que ganar el usuario, tiene que verificar bien su identidad.

Por ello en su propuesta Sophos ha desarrollado una nueva funcionalidad con un agente que proporciona más visibilidad con una validación continua de credenciales, para que en el caso de que algún usuario tenga un malware o esté realizando un proceso que no sea legítimo este acceso sea restringido. Los beneficios que aporta este modelo son una mayor facilidad de despliegue, gestión mucho más sencilla y reducción drástica del tiempo de latencia.

Contenido relacionado

Foro ITDS. Caminando hacia Zero Trust

La confianza cero desmitificada

Sophos Adaptive Cybersecurity Ecosystem

Intercept X

La confianza se gana, no se da. Tenemos que hacer que ese usuario verifique bien su identidad

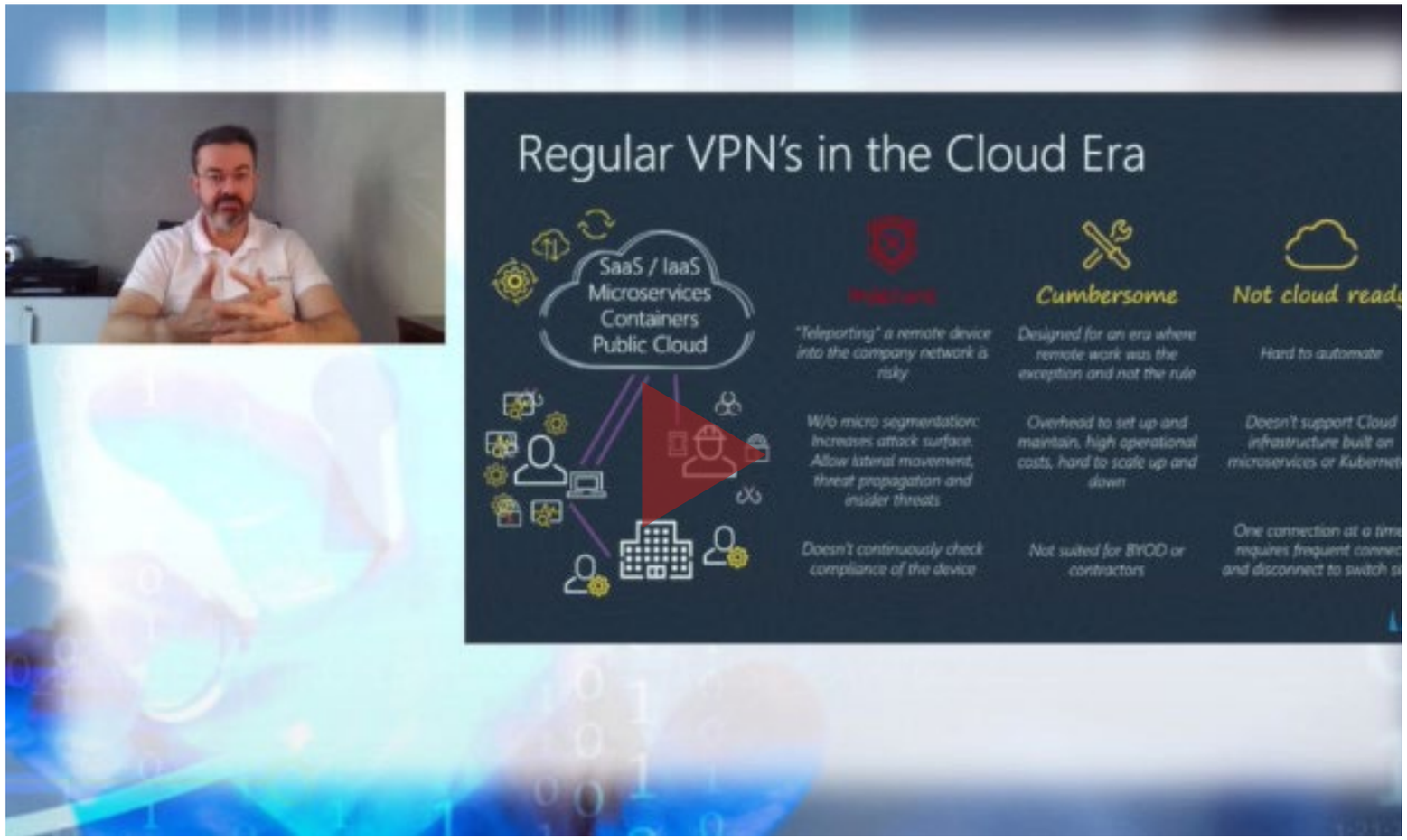
Compartir en RRSS

Barracuda Networks. Miguel López, Senior Regional Sales Manager

“Hace tiempo que las VPN se han vuelto insostenibles”

Miguel López, Barracuda

Las VPNs o redes privadas virtuales se desarrollaron hace unas décadas para extender el alcance de las redes corporativas. La movilidad y el teletrabajo han llevado al límite a esta tecnología. En la actualidad, el modelo Zero Trust Network Access es necesario para garantizar conexiones seguras.



“HACE TIEMPO QUE LAS VPN SE HAN VUELTO INSOSTENIBLES” CLICAR PARA VER EL VÍDEO

Si algo ha dejado claro la pandemia es que las VPN han dado todo lo de sí que podían dar. La llegada del teletrabajo ha hecho que todos aquellos problemas que se venían viendo desde hace tiempo en las VPN se hayan vuelto ya insostenibles.

Para Miguel López, Senior Regional Sales Manager de Barracuda Networks Iberia, la tecnología Zero Trust es lo que viene a marcar un antes y un después, lo que viene a sustituir a las VPN en la nueva normalidad.

Barracuda se apoya en el concepto Zero Trust Network Access a través de su solución CloudGen Access, que ofrece seguridad extremo a extremo y la posibilidad de gestionar las políticas de acceso de forma centralizada. Además, ofrece una conectividad remota muy superior a lo que sería una VPN, con beneficios como mayor seguridad, visibilidad, control de accesos y la posibilidad de dotar a los usuarios de una forma de acceder a todos los recursos información que necesiten de la empresa de forma muy inmediata, de forma perfectamente compatible con las herramientas de seguridad y firewalls ya instalados.

No teletransportamos al usuario remoto a nuestra red, sino que definimos una serie de permisos, que pueden ser flexibles en función del entorno, el dispositivo o las circunstancias en las que esté accediendo este usuario

Contenido relacionado

Foro ITDS. Caminando hacia Zero Trust

Barracuda CloudGen Access

Estado de la seguridad de la red en 2021

Cinco pasos que a seguir para proteger los dispositivos domésticos y mejorar la productividad en el teletrabajo

Compartir en RRSS

Securizando organizaciones en cualquier lugar

cualquier localización,
cualquier dispositivo,
cualquier recurso

Más información en **sophos.com/es-es/**

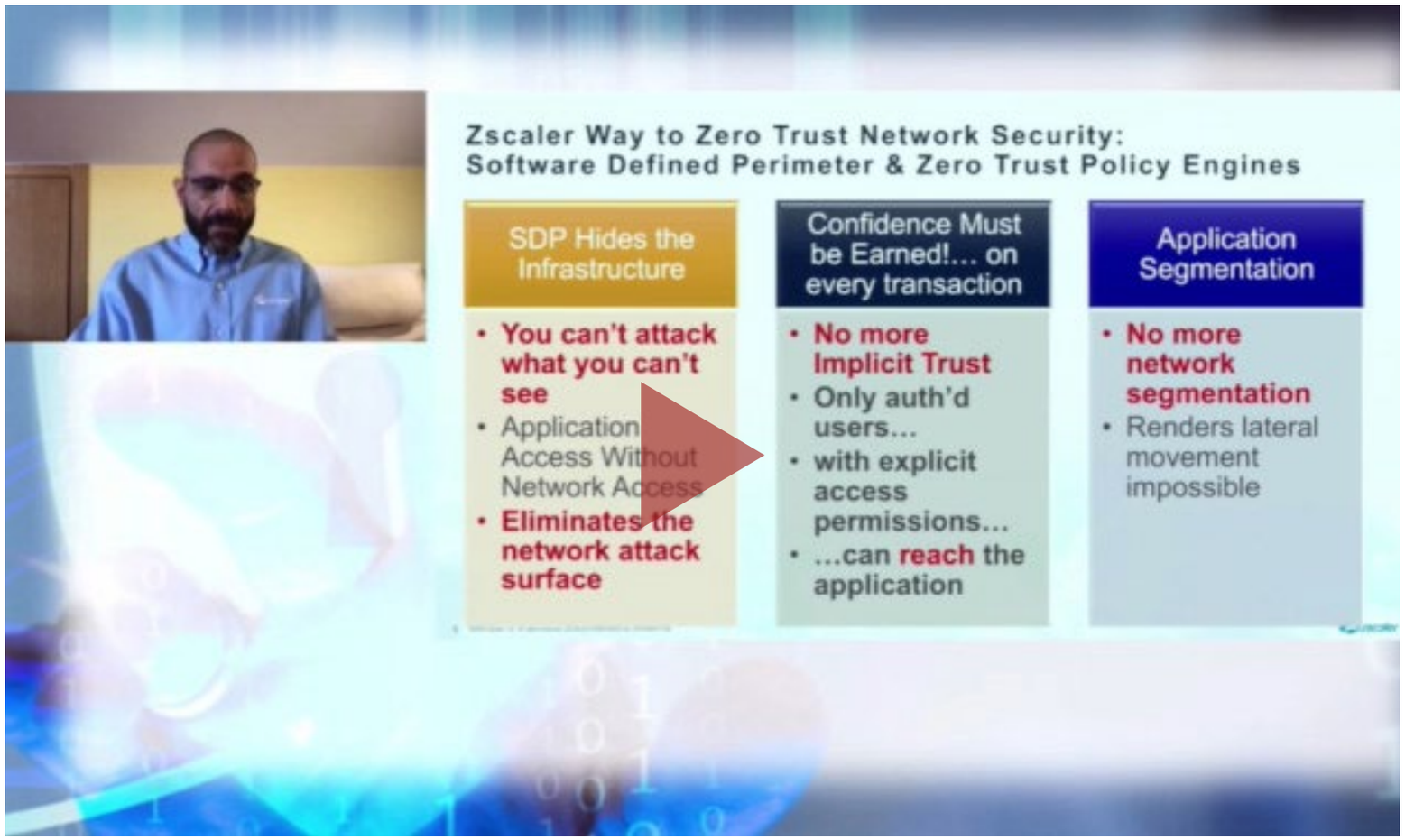
© Copyright 2021. Sophos Ltd. All rights reserved.

SOPHOS
Cybersecurity evolved.

Zscaler. Alberto Cita, Sales Engineering Manager Iberia & Italy

“La microsegmentación es clave en entornos Zero Trust”

Alberto Cita, Zscaler



“LA MICROSEGMENTACIÓN ES CLAVE EN ENTORNOS ZERO TRUST” CLICAR PARA VER EL VÍDEO

Las soluciones de seguridad de red tradicionales, centradas en securizar el acceso a la red establecen una confianza implícita. A su vez se están produciendo diferentes cambios desde el punto de vista de las arquitecturas de las redes de comunicaciones de datos de las empresas, que están suponiendo un desafío todavía más importante para este modelo de seguridad implícito.

Las arquitecturas de seguridad perimetral tradicionales a día de hoy se han quedado obsoletas debido fundamentalmente a que con la adopción del cloud por un lado y con el incremento drástico en la movilidad de los usuarios que se ha producido durante el último año y medio por otro, la mayor parte del tráfico del negocio ocurre fuera del perímetro corporativo, con lo cual, cualquier tipo de control que se ejerza sobre

Contenido relacionado

Foro ITDS. Caminando hacia Zero Trust

El IoT en la empresa: edición “oficina vacía“

Exposed

Tres estrategias para acelerar la transformación empresarial

el perímetro es un control al que va a escapar la mayor parte del tráfico corporativo.

Según Alberto Cita, Sales Engineering Manager Iberia & Italy de Zscaler, la seguridad Zero Trust va a permitir un modelo centrado en la identidad de los usuarios y en la definición de políticas que permitan restringir el acceso a las aplicaciones.

La forma en la que Zscaler implementa la tecnología Zero Trust para la seguridad de red tiene dos componentes fundamentales: la definición de perímetros mediante software, que se implementan además sobre una solución en nube, y la definición de políticas Zero Trust. Esta arquitectura permite proteger los tráficos este-oeste, implementando microsegmentación automatizada basada en identidades digitales generadas automáticamente para cada uno de los procesos que componen una aplicación.

Solamente aquellos usuarios que estén correctamente autenticados y que tengan permisos explícitos para poder acceder a una aplicación van a poder hacerlo

Compartir en RRSS

Akamai Technologies. María Ramírez Fernández, Solutions Engineer

“Las VPN son una tecnología obsoleta”

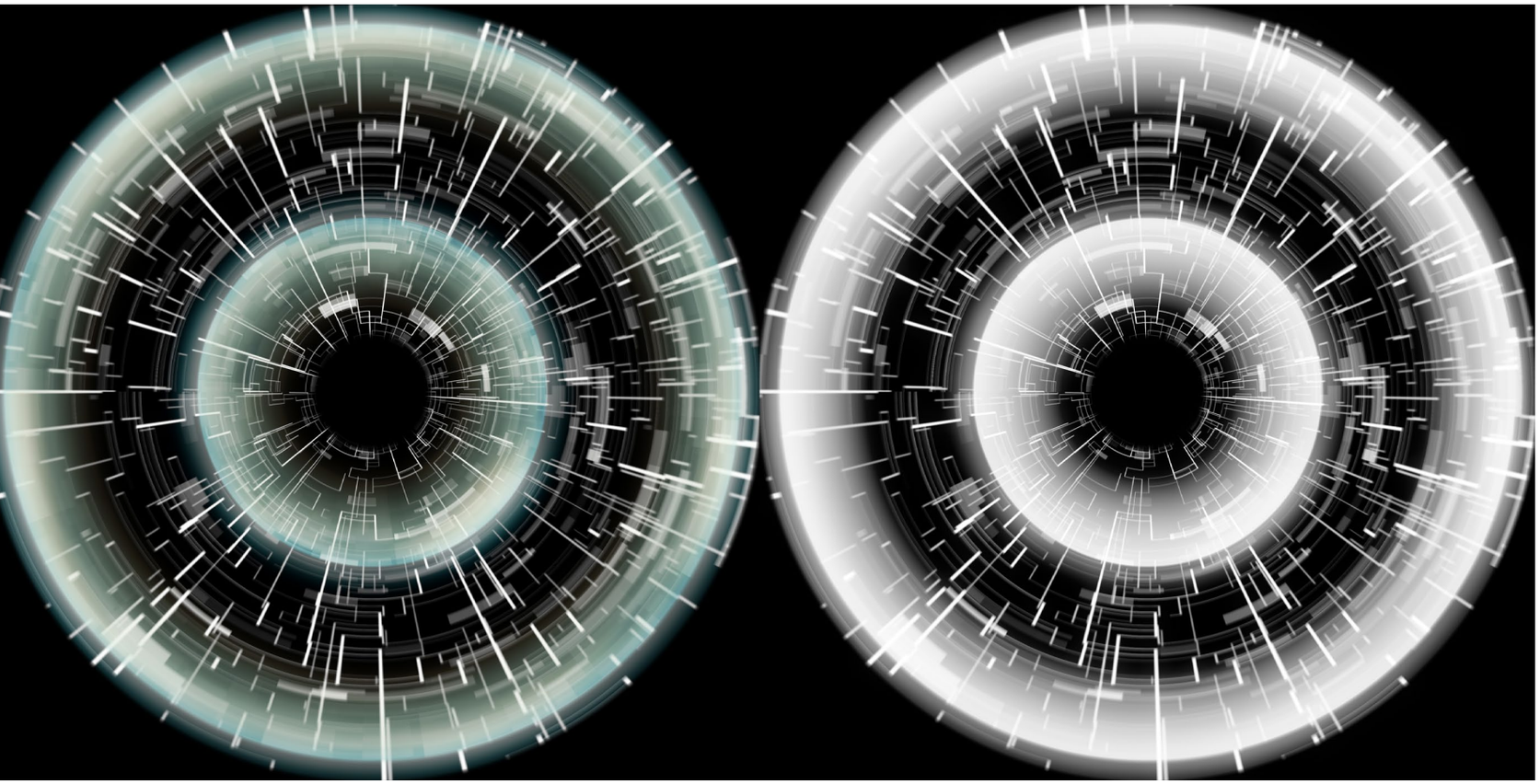
María Ramírez, Akamai

Cada vez se observan más ataques relacionados con la autenticación y el acceso remoto de usuarios a aplicaciones dentro y fuera del data center. La superficie de ataque ha aumentado y con ella las posibilidades de sufrir un problema de seguridad. Es necesario contar con soluciones robustas que ofrezcan una buena experiencia al usuario.

“LAS VPN SON UNA TECNOLOGÍA OBSOLETA”

CLICAR PARA VER EL VÍDEO

Hace tiempo que el perímetro de seguridad, tan cuidadosamente delimitado por los primeros firewalls, desapareció. María Ramírez Fernández, Solutions Engineer de Akamai Technologies, señala que esto ha creado nuevos vectores de ataque, lo que plantea otros retos, sobre todo relacionados con la autenticación, el acceso remoto y el IoT.



Contenido relacionado

Foro ITDS. Caminando hacia Zero Trust

Akamai MFA

Akamai MFA: ¿Dónde está la diferencia?

Para María, las VPN son una tecnología obsoleta, no solamente en términos de seguridad, sino también a la hora de hablar de performance, sobre todo a medida que las empresas van creciendo y sus aplicaciones van aumentando en número y en complejidad.

El concepto de Akamai se basa en una plataforma inteligente formada por servidores Edge en el borde que actúan como Identity Aware Proxys, proporcionando autenticación, autorización, protección y rendimiento. Como marca el framework de SASE, Akamai divide su modelo en dos áreas: la capa de red y la de seguridad. Su punto fuerte es la aceleración. Además tienen la visibilidad de aproximadamente un 30-35% de todo el tráfico que circula por Internet, lo que les permite tener una solución Zero Trust muy robusta, con la máxima seguridad y lo más eficaz posible para usuarios y empresas.

Protegemos a todos los usuarios, independientemente de desde dónde se estén conectando

Compartir en RRSS

F5 Networks. José Manuel Flores, Solution Engineer

“Apostamos por no confiar, verificar y monitorizar continuamente”

José Manuel Flores, F5

“NO CONFIAR, VERIFICAR Y MONITORIZAR CONTINUAMENTE”

CLICAR PARA VER EL VÍDEO

Cuando llegó la pandemia de repente las empresas se vieron en la necesidad de tener a toda su plantilla teletrabajando para poder seguir operando, por ello tuvieron que adaptarse a pasos agigantados. Este teletrabajo se está haciendo de tres formas: tunelización, portales de acceso y acceso remoto.

Dado que las circunstancias de cada compañía pueden ser muy diferentes, hay que escoger la mejor solución de acceso remoto para cada uno de los casos de uso. La filosofía Zero Trust implica dar al usuario los mínimos privilegios posibles y según vaya confiando en su arquitectura y en su entorno y cuál es el tipo de conexión que está realizando, ir

Contenido relacionado

Foro ITDS. Caminando hacia Zero Trust

F5 BIG-IP Access Policy Manager (APM)

Hay que entender las amenazas en el entorno de Zero Trust como si ya estuvieran dentro

otorgándole más permisos en función de esas variables.

Para José Manuel Flores, Solution Engineer de F5 Networks, los principios de Zero Trust son nunca confiar, siempre verificar y monitorizar continuamente. Para ello establece cuatro puntos de control: la identidad del servicio, el entorno de red en el que se realiza la conexión, el tipo de dispositivo y las aplicaciones a las que se quiere conectar.

Lo que hace la solución APM de F5 Networks es contextualizar ese tipo de acceso. Crea una política que contextualiza la conexión, el usuario, su grupo de pertenencia y los permisos que puede tener en función del entorno, ya sea una conexión VPN, un acceso remoto a través de un portal, o un escritorio remoto. Se trata de una plataforma de alto rendimiento con gran escalabilidad y muy sencilla de gestionar.

Compartir en RRSS

Implemente un Acceso Zero Trust a cualquier recurso.

Descubra una alternativa más segura y rápida a las VPNs.

Más información:
iberia_team@barracuda.com | barracuda.com

Barracuda®
Your journey, secured.

RETOS Y CAMBIOS DE PARADIGMA:

empezando el on-prem, pasando por el Cloud y terminando en Híbrido

LUCAS REY

CHANNEL MANAGER, FORCEPOINT IBERIA

Radicado en Madrid, Lucas Rey está graduado en la Escuela de Negocios y Marketing de ESIC. Antes de Forcepoint, Lucas Rey estuvo en Symantec durante más de diez años, realizando funciones que van desde la gestión de productos hasta la certificación de socios y el desarrollo de alianzas.

Compartir en RRSS

Desde Forcepoint se ha apreciado que muchas organizaciones han estado considerando y planificando su transformación digital durante años. Pero en marzo de 2020, la pandemia y el éxodo resultante de la oficina aceleraron la migración de todos a la nube casi de la noche a la mañana. Por necesidad, el enfoque de muchos departamentos de TI en 2020 fue permitir que las personas trabajen desde casa. En 2021, en un escenario aún en definición aparecen múltiples posibilidades. Muchas organizaciones buscan reemplazar las soluciones a corto plazo que implementaron apresuradamente con más soluciones sostenibles.

Los enfoques tradicionales, basados en segmentos de red y productos de seguridad para proteger un perímetro definido, no encajan en este nuevo modelo. Muchas aplicaciones y datos ahora están en la nube, y los usuarios remotos superan en número a los usuarios en el sitio. Los enfoques tradicionales obligan a hacer que el tráfico de usuarios y aplicaciones pasen por un punto central, utilizando tecnologías que limitan la flexibilidad y pueden tener un impacto negativo en el rendimiento.

La industria ya comenzaba a reconocer estos problemas y avanzar en una nueva dirección.

Uno de los principales atractivos de SASE es la capacidad de utilizar una única plataforma basada en la nube para abordar una amplia gama de necesidades

Contenido relacionado

Forcepoint Zero Trust

Forcepoint SASE

Gartner diseñó la arquitectura Secure Access Service Edge (SASE) específicamente para abordar las necesidades de organizaciones cada vez más distribuidas. Uno de los principales atractivos de SASE es la capacidad de utilizar una única plataforma basada en la nube para abordar una amplia gama de necesidades. Desde Forcepoint creemos de gran importancia que a la hora de escoger esta plataforma se tengan en cuenta los siguientes puntos:

- Protección de usuarios remotos en cualquier lugar frente a contenido web malicioso y el uso indebido de aplicaciones en la nube.
- Acceso a aplicaciones privadas sin necesidad de utilizar VPN, simplemente a través del acceso a esta plataforma cloud.
- Protección del uso de la información en cualquier lugar: defina políticas precisas de protección de la información y aplíquelas de manera uniforme en el puesto, en la red y en la nube.
- Adopción progresiva, con la capacidad de comenzar con necesidades inmediatas y adoptar capacidades SASE adicionales a su propio ritmo.
- Plataforma completa, nativa en cloud, que permita evolucionar para adoptar todas las capacidades requeridas ahora y a futuro.
- Acceso de forma directa a esos servicios cloud de modo flexible como con el uso de tecnología SD-WAN que permite fácilmente conectar las oficinas con la plataforma de seguridad en nube.” it

Compartir en RRSS

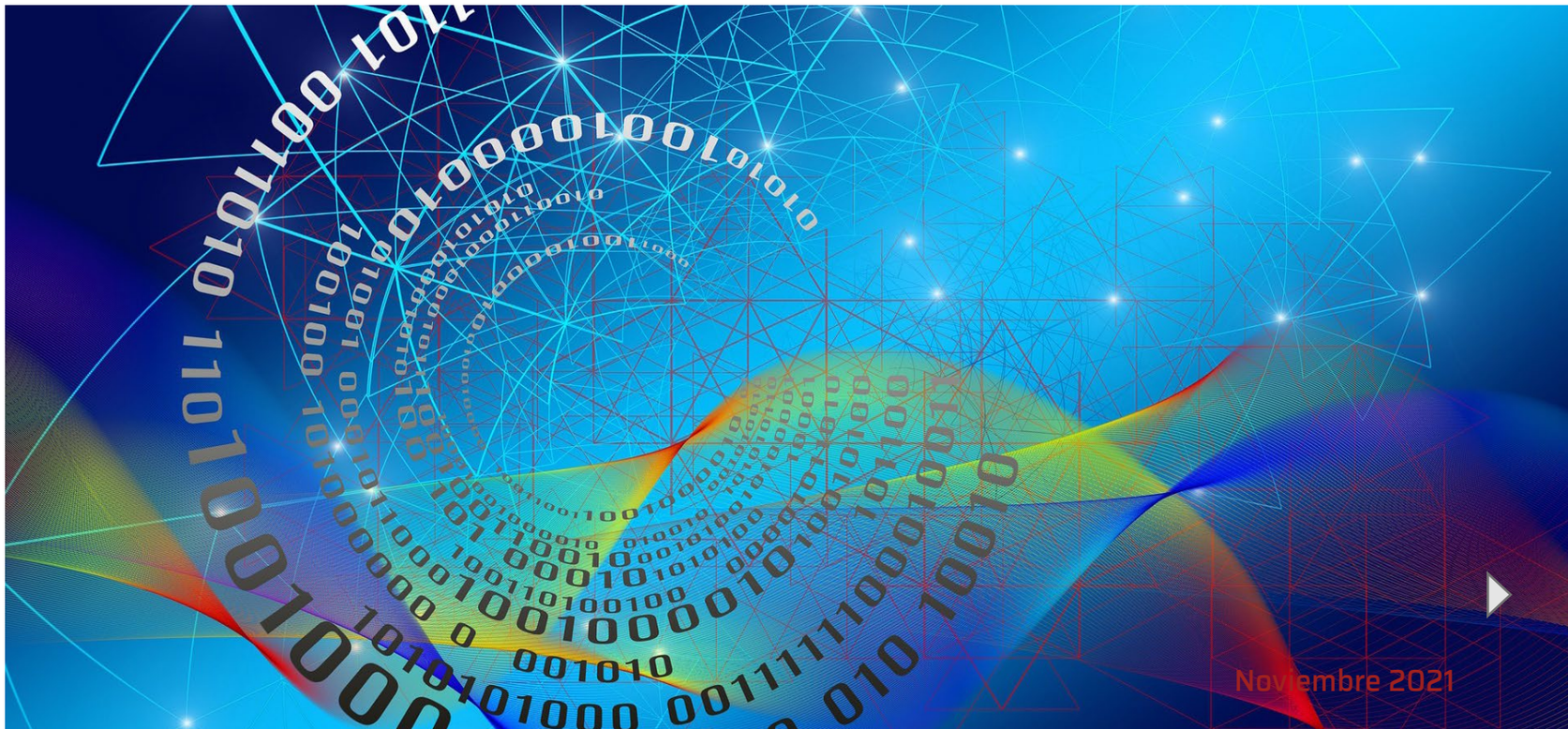
ALBERTO R. RODAS

SALES ENGINEER MANAGER, SOPHOS IBERIA

Alberto Ruiz Rodas es responsable del apoyo técnico y comercial de los proyectos de seguridad de Sophos Iberia. Ingeniero de Telecomunicaciones por la Universidad de Alcalá de Henares, Alberto cuenta con más de 14 años de experiencia en seguridad TIC. Ha sido invitado como ponente en varias conferencias, como Qurtuba, Navaja Negra, Mundo Hacker o el Foro asLAN, y realizado varias demostraciones sobre hacking ético.

Ventajas de ZTNA con respecto a las soluciones VPN

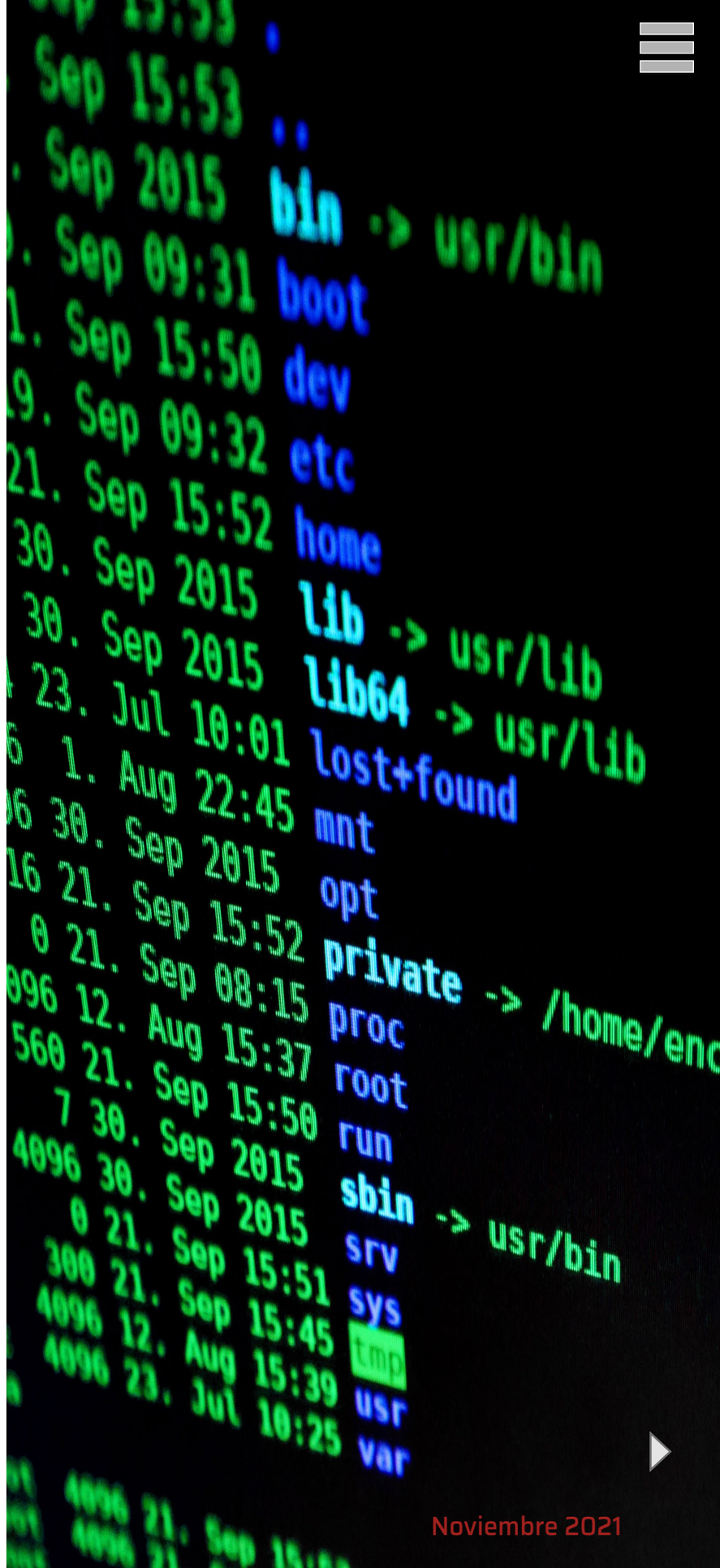
La VPN de acceso remoto nos ha hecho un buen servicio durante mucho tiempo, pero el reciente aumento del teletrabajo ha puesto de manifiesto las limitaciones de esta tecnología anticuada. Mientras que algunas organizaciones siguen exprimiendo al máximo las posibilidades de la VPN, muchas buscan una alternativa mejor, algo que resuelva los problemas de la VPN de acceso remoto. Varias organizaciones ya han empezado a adoptar plenamente la nueva generación de tecnología de acceso remoto: ZTNA o acceso a la red de confianza cero. ZTNA ofrece una mejor seguridad, un control más granular, una mayor visibilidad y una experiencia de usuario transparente en comparación con la VPN de acceso remoto tradicional.



Las ventajas de ZTNA con respecto a las soluciones VPN de acceso remoto tradicionales incluyen:

- **1. Confianza cero:** ZTNA se basa en el principio de confianza cero, es decir, no confiar en nada y verificarlo todo. Al tratar en la práctica a cada usuario y dispositivo como su propio perímetro y al evaluar y verificar constantemente la identidad y el estado de seguridad para obtener acceso a las aplicaciones y los datos corporativos, se mejora considerablemente la seguridad y la microsegmentación. Los usuarios solo tienen acceso a las aplicaciones y los datos definidos explícitamente por sus políticas, lo que reduce el movimiento lateral y los riesgos que conlleva.
- **2. Estado de seguridad del dispositivo:** ZTNA integra el cumplimiento y el estado de los dispositivos en las políticas de acceso, lo que le da la opción de excluir los sistemas no conformes, infectados o comprometidos del acceso a las aplicaciones y los datos corporativos, eliminando así un importante vector de amenazas y reduciendo el riesgo de robo o fuga de datos.
- **3. Funciona en cualquier lugar:** ZTNA no está vinculado a redes específicas, por lo que puede funcionar con la misma eficacia y seguridad desde cualquier red, ya sea en casa, en un hotel, en una cafetería o en la oficina. La gestión de la conexión es segura y transparente, independientemente de dónde se encuentren el usuario y el dispositivo, lo que hace que la experiencia sea ágil sin importar dónde esté trabajando el usuario.
- **4. Más transparente:** ZTNA ofrece una experiencia de usuario final fluida y sin fricciones, ya que establece automáticamente conexiones seguras bajo demanda en segundo plano a medida que se

> ZTNA ofrece una mejor seguridad, un control más granular, una mayor visibilidad y una experiencia de usuario transparente en comparación con la VPN de acceso remoto tradicional



necesitan. La mayoría de los usuarios ni siquiera serán conscientes de la solución ZTNA que está ayudando a proteger sus datos.

- **5. Mayor visibilidad:** ZTNA puede ofrecer una mayor visibilidad de la actividad de las aplicaciones que puede ser importante para el seguimiento del estado de las mismas, la planificación de la capacidad y la gestión y auditoría de las licencias.
- **6. Administración más sencilla:** las soluciones ZTNA suelen ser mucho más eficientes y limpias y, por tanto, más fáciles de desplegar y gestionar. También pueden ser más ágiles en entornos que cambian rápidamente, con usuarios que entran y salen, lo que hace que la administración diaria sea una tarea rápida y sencilla y no un trabajo a tiempo complete.

Sophos ZTNA se ha diseñado desde el principio para que el acceso a la red de confianza cero sea fácil, integrado y seguro. Sophos ZTNA se distribuye y gestiona en la nube y se integra en Sophos Central, la plataforma de generación de informes y gestión de ciberseguridad en la nube en la que más confía el mundo. Desde Sophos Central, no solo puede gestionar ZTNA, sino también sus dispositivos Sophos Firewall, endpoints, protección de servidores, dispositivos móviles, seguridad en la nube, protección del correo electrónico y mucho más.

Sophos ZTNA también es único porque se integra perfectamente con Sophos Firewall y los endpoints de Sophos Intercept X. Esto permite sacar partido de la Seguridad Sincronizada y Security Heartbeat para compartir el estado de los dispositivos entre el firewall, el dispositivo, ZTNA y Sophos Central a fin de responder automáticamente a las amenazas o a los dispositivos no conformes. Limite automáticamente el acceso y contenga los sistemas comprometidos hasta que se limpien.

Los clientes de Sophos coinciden en que las ventajas de ahorro de tiempo con una solución de ciberseguridad de Sophos totalmente integrada son enormes. Afirman que utilizar el conjunto de productos de Sophos, gestionados desde Sophos Central, y servirse de la Seguridad Sincronizada para la identificación y respuesta automáticas a amenazas es como duplicar el tamaño de su equipo de TI. Por supuesto, Sophos ZTNA funcionará con los productos de seguridad de cualquier otro proveedor, pero es único al trabajar mejor junto al resto del ecosistema de Sophos para ofrecer ventajas tangibles en el mundo real en cuanto a visibilidad, protección y respuesta.

Contenido relacionado

Sophos ZTNA

netwrix

UN MUNDO PROTEGIDO CONTRA LAS CIBERAMENAZAS

En una era de ciberamenazas constantes, ¿cómo puede hacer que su organización sea más segura de lo que es actualmente?

Netwrix ayuda a más de 10.000 organizaciones en todo el mundo:

- Supere la seguridad en silos eliminando los puntos ciegos
- Siga las mejores recomendaciones para identificar, gestionar y reducir el riesgo de ciberseguridad

Potente seguridad de datos, identidades e infraestructura con sencillez

www.netwrix.es

La necesidad de gestionar las identidades y accesos en un mundo híbrido

En un mundo basado en la nube y en los modelos as a service, no podemos confiar en las estructuras de seguridad centradas en el perímetro de la red. La seguridad de la identidad se ha convertido en el nuevo perímetro que hay que proteger porque las empresas necesitan permitir el acceso seguro a su ecosistema de usuarios (empleados, contratistas, partners, etc.) independientemente de la ubicación, la red o el dispositivo.

De esta forma, la gestión de la identidad se ha convertido en uno de los pilares básicos del modelo de Confianza Cero que gana cada vez más adeptos. Para hablar de todo ello y de cómo las empresas afrontan este reto reunimos un grupo de expertos en un debate patrocinado por SonicWall bajo el Título “No confíes en nadie” en el que estuvieron presentes Angel Gálvez, CISO de Dufry; Javier Allende, CISO de Konecta; Pablo Perancho, CTO, CIO y CISO del Centro Universitario U-tad; Iván Sánchez, CISO de Sanitas y Sergio Martínez, Country Manager de SonicWall.

Iniciamos el debate preguntando a nuestros invitados sobre los retos a los que creen que tendrán

"Hay que tener en cuenta que aún hay mucha gente que no tiene móvil y el doble factor de autenticación se complica"

Angel Gálvez, CISO, Dufry

que enfrentarse. Comentando que el modelo de trabajo híbrido que se ha establecido tras la pandemia ya se ha estandarizado, dice Ángel Gálvez que "hay que potenciar la seguridad en toda la cadena de suministro". También es foco la protección del dato así como "los modelos de big data e inteligencia artificial que se están aplicando a los nuevos modelos de negocio". No se olvida el CISO de Dufry de la identidad de los usuarios y cuentas privilegiadas, que forman parte "de un proceso de seguridad clave que envuelve a cualquier iniciativa que tengamos".

Explica Javier Allende que en Konecta se está trabajando en "unificar la identidad en un único sistema para garantizar la trazabilidad y tener controlado qué hace el usuario y cuándo lo hace". Asegura que más que trabajar alrededor del centro de datos, ahora se pone foco en el usuario, que es quien va a hacer la acción.

Coincidiendo con sus compañeros respecto a los retos a los que se enfrentarán los CISOS, añade Iván Sánchez, CISO de Sanitas, que hay que "estabilizar todos los controles de seguridad que se han desplegado en un momento récord en tiempos de pandemia". Menciona también como retos la seguridad de los entornos Agile, la regulación y la falta de talento.

Como centro especializado en formación digital, "nuestro reto es asegurar el acceso a la información, tanto de la del alumno presencial como del alumno online", asegura Pablo Perancho, CTO, CIO y CISO del Centro Universitario U-tad. Añade que sólo tienen que garantizar los datos de la Universidad como empresa, sino también que los alumnos puedan acceder y recibir la formación que están cursando, manteniendo la independencia entre los entornos.

Preguntamos a Sergio Martínez, director general de SonicWall en Iberia, si los retos planteados por los CISOs asistentes a la mesa coindicen con sus previsiones y con lo que observan en el mercado. Se muestra de acuerdo y asegura que se observa "un movimiento muy rápido de racionalización de todo lo que se acometió el año pasado a toda velocidad".

Apostando por IAM

¿Cómo se están afrontando esa seguridad de los accesos y de las identidades en un mundo cloud? Explica Iván Sánchez que en el mundo pre-pandemia “estábamos acostumbrados a gestionar la identidad de una manera muy particular”. En el mundo cloud los empleados se conectan desde orígenes

"La parte biométrica no termina de arrancar porque es un poco intrusiva para las personas"

Javier Allende, CISO, Konecta

“NO TE FÍES DE NADIE” **CLICAR PARA VER EL VÍDEO**

no conocidos, desde redes no seguras, con comportamientos que en el mundo anterior podían ser potencialmente maliciosos, “porque antes no era normal que un usuario de oficina se conectase a las doce de la noche”, lo que lleva a las empresas a adoptar modelos basados en comportamiento con un enfoque de Zero Trust.

Antes los sistemas se basaban en la información a la que se quería acceder, y sobre eso se permitía, o no, el acceso. Ahora, asegura el CISO de Dufry, “estamos fomentando que cualquier usuario, interno o externo, pueda acceder en cualquier momento y desde cualquier lugar, con lo cual el foco cambia y se centraliza en esa identidad”. Añade Gálvez que debe tenerse en cuenta cómo enlazar esa gestión de la identidad con el resto de servicios de seguridad que están alrededor de una compañía, como es la protección del endpoint así como “todos los

sistemas y herramientas de monitorización que van alimentando a esos modelos de comportamiento para, de forma dinámica, poder permitir a qué se accede, cuándo, etc.”.

La manera de afrontar la gestión de identidades pasa por tener en cuenta el comportamiento

"La enseñanza online obliga a abrir nuevas líneas de investigación y pruebas de control de identidad"

Pablo Perancho, CTO, CIO y CISO, Centro Universitario U-tad

a través de soluciones que te digan “qué hace el usuario en cada momento”, asegura Javier Allende, CISO de Konecta, añadiendo que el teletrabajo ha provocado un cambio en las alertas y hay que unificar qué puede hacer el usuario, a dónde puede acceder y qué tipo de parámetros se quieren monitorizar.

“Estamos arrancando esa línea”, dice Pablo Perancho cuando le preguntamos cómo se está haciendo frente a la gestión de identidades en U-tad, que afronta una nueva línea de negocio de formación online “que nos obliga a explorar nuevas vías” en el que el control de la identidad es fundamental. La universidad no sólo está activando el múltiple factor de autenticación (MFA), sino control de accesos biométricos y explorando nuevas líneas, como herramientas de acceso por blockchain.

“Proporcionamos diferentes estrategias, servicios y productos que permitan conocer los ataques de corte desconocido, así como un control y una visibilidad de lo que está sucediendo en la red en tiempo real. Y con un TCO asumible en todo tipo de empresas”, asegura Sergio Martínez cuando le preguntamos cómo está ayudando su compañía a las empresas. La pérdida de perímetro de seguridad, añade, empuja al mercado hacia un modelo Zero Trust.

MFA y experiencia de usuario

Con demasiada frecuencia, la seguridad y la experiencia del usuario están en desacuerdo. La seguridad adicional puede significar obstáculos

"Hace tiempo que el MFA es obligatorio en Sanitas"

Iván Sánchez, CISO, Sanitas

adicionales en el viaje digital del cliente. ¿Cómo están gestionando las empresas los procesos de autenticación con la experiencia del usuario? “Por ahora nos estamos quedando en el segundo factor de autenticación (2FA)”, dice Javier Allende, CISO de Konecta, añadiendo que la parte biométrica, “no termina de arrancar porque es un poco intrusiva para las personas”.

Dependiendo de la plataforma y de los usuarios, la aplicación de la tecnología multifactor se hace de forma diferente en Dufry, según explica su CISO, añadiendo que hay que tener en cuenta que

"El nuevo perímetro de seguridad es la identidad, por eso securizarla es más necesario que nunca"

Sergio Martínez, Country Manager, SonicWall

todavía hay gente que no tiene teléfono móvil, y entonces se habilitan diferentes métodos de autenticación, "con diferentes grados de protección y complejidad".

Para Pablo Perancho, de U-tad el MFA se acabará implementando "porque tiene todo el sentido para garantizar la seguridad".

Asegura Iván Sánchez, que "el MFA es obligatorio desde hace bastante tiempo en todos los métodos de trabajo remoto", bien sea en el uso de una VPN o de un entorno colaborativo como Office 365. La existencia de personal sin teléfono corporativo ha hecho que la adopción de este MFA haya sido "más lenta de lo que nos hubiera costado", pero en Sanitas decidieron no correr riesgos. Respecto a la experiencia de usuario asegura el CISO de Santitas que ha sido fácil porque las herramientas permiten todo tipo de opciones.

En su intervención asegura Sergio Martínez que desde SonicWall se lleva tiempo impulsando la adopción de buenas prácticas. Asegura además que el nuevo perímetro de seguridad es la identidad y que, por tanto, "es más necesario que nunca poner en marcha este tipo de soluciones" de autenticación multifactor.

Conclusiones

Tras finalizar el encuentro con los CISOs pedimos a Sergio Martínez unas conclusiones de lo dicho en el encuentro, que no hace sino poner de manifiesto que el robo de identidades se ha convertido en una gran preocupación "que fuerza a la implementación de estrategias de autenticación". Destaca también el directivo de Sonicwall la referencia al despliegue de estrategias de accesos remotos para terceras partes, la retención del talento y el cambio de CAPX a OPEX para hacer más eficaz la inversión en ciberseguridad.

Sobre si la empresa española está madura para adoptar el modelo Zero Trust, dice Sergio Martínez que "estamos empezando". Recuerda que el pasado fue un año complejo de entornos de acceso remoto a toda velocidad y que, estando en unos entornos de confianza implícita, "hay que dar el salto a entornos de Zero trust o confianza explícita".

LA TRANSFORMACIÓN CLOUD COMIENZA CON ZERO TRUST

Pase a la nube de forma segura y transforme su negocio con la plataforma Zscaler Zero Trust Exchange.

©2021 Zscaler, Inc. All rights reserved. Zscaler™and Zero Trust Exchange™are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.

SonicWall. Sergio Martínez, Iberia Regional Manager

“La transformación digital ha redefinido un modelo de seguridad, que no es otro que Zero Trust”

Sergio Martínez, SonicWall

“LA TRANSFORMACIÓN DIGITAL HA REDEFINIDO UN MODELO DE SEGURIDAD” CLICAR PARA VER EL VÍDEO

Las empresas se han sumergido de forma muy rápida en los últimos meses en una situación de IT distribuida en la que se ha generado una explosión de la superficie de exposición, dirigiéndose en la actualidad hacia un entorno más híbrido. Además se está produciendo una escasez tanto de recursos, como de profesionales.

La transformación digital ha redefinido un nuevo perímetro. Las empresas se han movido desde un data center privado a uno público, están realizando accesos corporativos desde cualquier sitio y se utilizan más aplicaciones Saas que nunca.

En opinión de Sergio Martínez, Iberia Regional Manager de SonicWall, ese acceso remoto conlleva una serie de retos en las VPNs: los escalados

Contenido relacionado

Foro ITDS. Caminando hacia Zero Trust

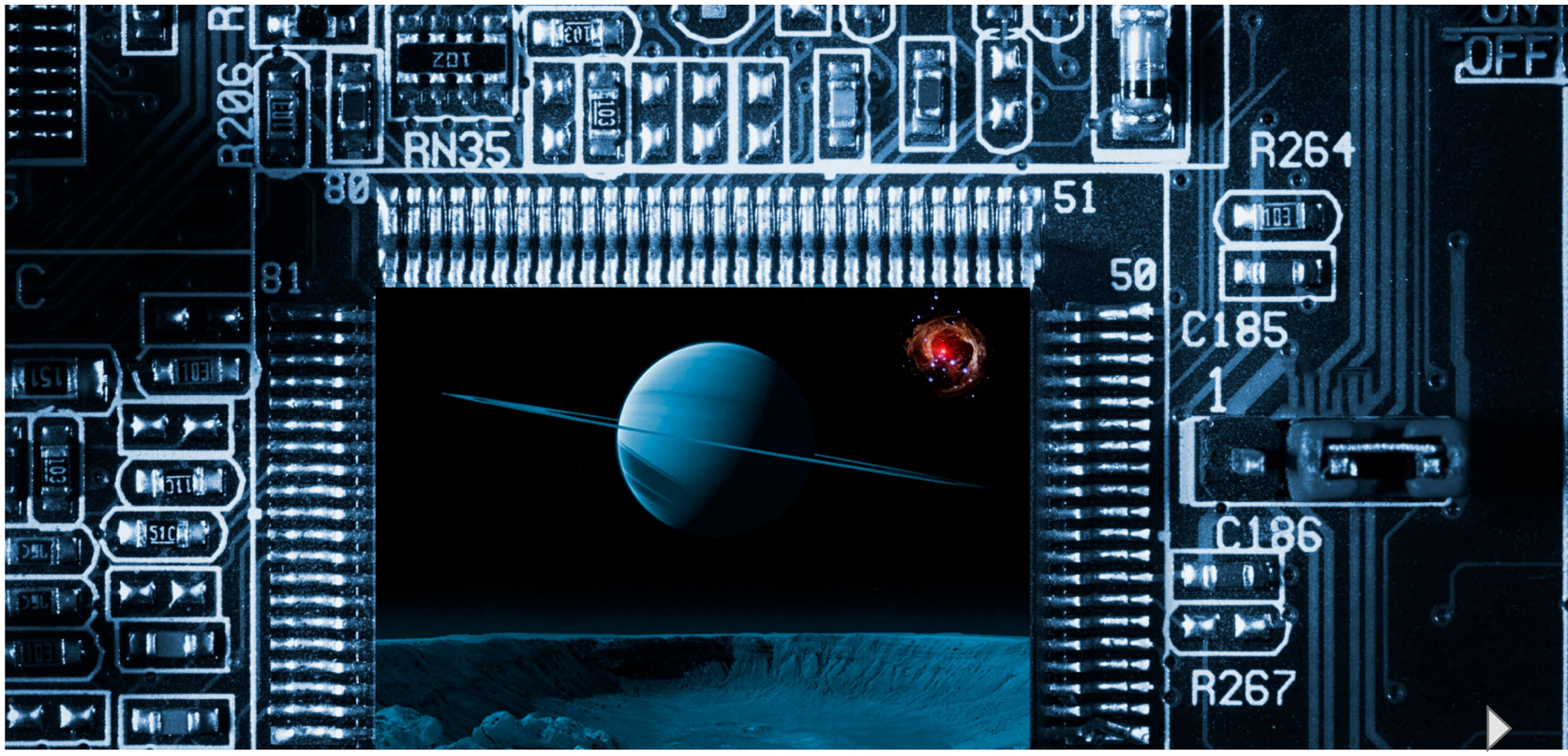
SonicWall Zero Trust Security

SonicWall Cloud Edge Secure Access

No es que haya pocos profesionales, sino que se necesitan más que nunca

y los despliegues son lentos y muy complejos, las amenazas se mueven ahora de forma lateral y la experiencia de usuario no es positiva por la alta latencia que introducen estas tecnologías. De ahí la necesidad de una seguridad Zero Trust con lo que se llaman microperímetros definidos por software, en los que el modelo empieza en el dispositivo del usuario y acaba en las localizaciones en las que están los recursos.

La propuesta tecnológica de SonicWall destaca tres soluciones: la tecnología ZTNA Cloud Edge Secure Access para proporcionar un modelo SASE; sus firewalls virtuales, muy conocidos por su efectividad y su alto performance; y su tecnología para securizar aplicaciones SaaS en la nube Cloud Application Security, servicio cloud de protección de email, datos y credenciales de aplicaciones SaaS, a través de una API.



Compartir en RRSS

One Identity. Javier Gómez, Account Manager

“La identidad es clave en la aplicación de un modelo ZeroTust”

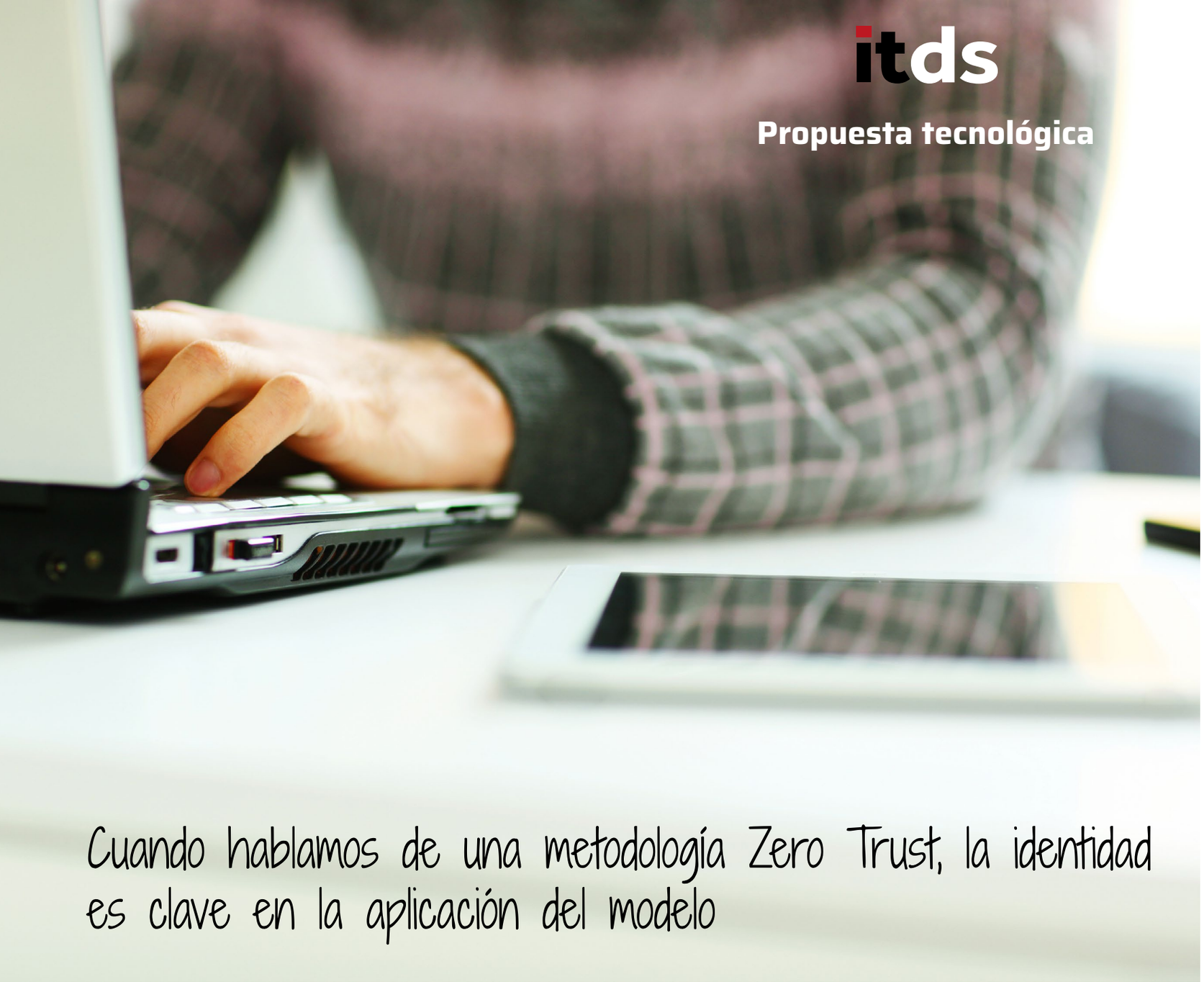
Javier Gómez, One Identity

En un mundo basado en el cloud y el as a service, el acceso a los recursos empresariales se realiza desde cualquier lugar y en cualquier momento, lo que ha convertido a la identidad de los usuarios en el nuevo perímetro de seguridad. El lema del modelo Zero Trust es nunca confíes, siempre verifica. Esto es fundamental para aplicar este nuevo paradigma de seguridad.

El perímetro de seguridad se ha diluido por varias tendencias del mercado, sobre todo por la hiperdispersión de las empresas, que en los últimos 24 meses se ha visto acelerada; la adopción del cloud, por razones de eficiencia y de reducción de costes; y las aplicaciones as a service. Se ha pasado de un modelo en el que la infraestructura estaba en el centro a un modelo en el que la identidad se ha convertido en la clave.

“LA IDENTIDAD ES CLAVE EN LA APLICACIÓN DE UN MODELO #ZEROTUST”

CLICAR PARA VER EL VÍDEO



Cuando hablamos de una metodología Zero Trust, la identidad es clave en la aplicación del modelo

Javier Gómez, Account Manager de One Identity, señala que es necesario tener un acceso en el momento oportuno a los privilegios y a las aplicaciones que necesita el usuario para desempeñar su labor en la compañía. Forrester, cuando hablaba de Zero Trust marcaba tres capas claves: la identidad y el gobierno de la identidad, la identidad privilegiada y el multifactor de autenticación.

Para aplicar el modelo Zero Trust One Identity plantea diferentes vías: la primera, más estratégica, centrada en la identidad y el gobierno de la identidad. La segunda sería más táctica y comenzaría por los accesos, por ejemplo a través del directorio activo. La tercera comenzaría por los usuarios privilegiados, que son los principales vectores de ataque de los ciberdelincuentes.

Contenido relacionado

Foro ITDS. Caminando hacia Zero Trust

Confianza cero y seguridad con privilegios para entornos híbridos

Compartir en RRSS

www.oneidentity.com/solutions/zerotrust/

CONFIANZA CERO

ACCESO PRIVILEGIADO AL MOMENTO

#Zero trust #JiT #Pam

Producto recomendado por el CCN

Certificación Nacional Esencial de Seguridad CCN

ONE IDENTITY by Quest

Netwrix. Jesús Sáez, Country Manager Spain & Portugal

“Vivimos en la era de las brechas de seguridad”

Jesús Sáez, Netwrix

Cualquier organización debería adaptarse al modelo de Zero Trust porque es básico en cuanto a cualquier perspectiva de políticas de ciberseguridad. El Zero Trust es un modelo en el que una organización se niega a confiar en cualquier entidad, dentro o fuera de su perímetro. En su lugar se debe autorizar cada solicitud antes de permitir una conexión de cualquier tipo a su red.

Es prácticamente seguro que cualquier empresa, independientemente de su tamaño, se va a enfrentar con algún problema de seguridad antes o después. Por eso es importante subsanar los silos de seguridad, para eliminar los puntos ciegos en cómo se aplican los distintos parámetros y procesos en la parte de datos, identidad e infraestructura.

“NETWRIX ARTICULA SU OFERTA EN TRES PILARES”

CLICAR PARA VER EL VÍDEO

Contenido relacionado

Foro ITDS. Caminando hacia Zero Trust

Netwrix Data Classification

Netwrix SbPAM

Vivimos en la era de las brechas de seguridad. Si no has sido atacado ahora, la cuestión es cuándo vas a ser atacado

Como comenta Jesús Sáez, Country Manager Spain & Portugal de Netwrix, la compañía de seguridad aporta una visión holística situándose en la parte central de estos tres vectores, ya que puede aplicar control en la parte de datos, visibilidad y control en la parte de identidad y vigilar todo lo que es la infraestructura. El objetivo es mitigar y remediar, de modo que la superficie de ataque sea la mínima posible en los tres planos.

Netwrix articula su posicionamiento de producto en tres pilares fundamentales: Data Access Governance, Active Directory Security y Privileged Access Management. Desde la compañía inciden en que con un enfoque de Zero Trust es importante apoyarse también en otros vendors, tener APIs de modo que puedan integrarse con otras tecnologías y obtener al final un ecosistema de ciberseguridad amplio, rico y automatizado.

Compartir en RRSS

Thales. Guillermo Martín Soto, Regional Sales Manager Spain & Portugal Cloud Protection & Licensing-Identity and Access Management

“Aportamos visibilidad a los responsables de seguridad de quién está haciendo qué”

Guillermo Martín Soto, Thales

Desde 2018 la Unión Europea ha recibido más de 40.000 notificaciones de fugas de datos. Dado que el 80% de las fugas de datos vienen de suplantaciones de identidad, más que nunca toma valor aquella frase que dice que una cadena es tan fuerte como lo sea su eslabón más débil. Y su eslabón más débil son los usuarios.

“APORTAMOS VISIBILIDAD A LOS RESPONSABLES DE SEGURIDAD DE QUIÉN ESTÁ HACIENDO QUÉ”

CLICAR PARA VER EL VÍDEO

El mundo ha cambiado en todos los ámbitos. Hasta ahora la infraestructura de las compañías solía seguir un modelo de perímetro único, con el firewall en el punto de entrada inspeccionando paquetes, lo que daba una sensación de falsa seguridad, ya que no tenía en cuenta que dentro de ese perímetro único se encontraba la mayor amenaza que una empresa tiene que hacer frente a diario, el usuario.

Guillermo Martín Soto, Regional Sales Manager Spain & Portugal Cloud Protection & Licensing-Identity and Access Management de Thales indica que la seguridad perimetral no consigue proteger entornos híbridos como los que existen en la actualidad, sobre todo a raíz de la aparición de la nube.

Por ello, el planteamiento de Thales es implementar estrategias de acceso, para señalar quién puede acceder y a qué dentro de los servicios y recursos de la empresa. Además, aporta un Smart Single Sign On, que solicita una autenticación fuerte, flexible y adaptativa en función del riesgo, que se realiza a través del móvil, basada en FIDO, SMS, email o incluso tokenless, según sean las necesidades de cada usuario. La solución SafeNet Trusted Access aporta visibilidad, seguridad, escalabilidad y comodidad.

Contenido relacionado

Foro ITDS. Caminando hacia Zero Trust

Cumplir las directrices del NIST para una seguridad Zero Trust

Índice de Gestión de Acceso de Thales de 2021

Compartir en RRSS

THALES

Building a future we can all trust

Implementa una **seguridad Zero trust** con la gestión de accesos de Thales

Proteja sus activos compartidos con seguridad Zero-Trust

SERGIO MARTÍNEZ

IBERIA REGIONAL MANAGER, SONICWALL

Country Manager de Sonicwall en Iberia. Tiene más de 25 años de experiencia en el sector, habiendo trabajado en diferentes puestos de responsabilidad en Techdata, Telefónica, Colt, Ricoh y en varios startups de ciberseguridad y Cloud. Es Ingeniero de telecomunicaciones por la Universidad politécnica de Cataluña y MBA por el IESE (universidad de Navarra). Ponente habitual en varios foros, ha ejercido también la docencia en varias universidades y centros educativos sobre tecnología y su uso en el mundo de la empresa.

Con la adopción de nubes públicas y privadas y el rápido aumento de los dispositivos móviles y teletrabajadores, el perímetro de la red corporativa actual se ha redefinido por completo. Estas fronteras ahora son fluidas, ya que los trabajadores móviles con teléfonos móviles personales, tablets, ordenadores portátiles, etc. requieren cada vez más acceso a los recursos y aplicaciones de TI corporativos. Dado que las TI no pueden monitorear o registrar estos dispositivos, lo conocido como "Bring Your Own Device" o BYOD, puede exponer a las empresas a malware y ataques muy dañinos si los dispositivos de los empleados no cumplen con las políticas de seguridad BYOD corporativas.

Compartir en RRSS

A medida que las organizaciones continúan alejándose del entorno local tradicional y avanzan hacia esta nueva realidad de TI, sus soluciones de ciberseguridad heredadas no han podido mantenerse al día, creando una complejidad inmanejable y una mayor oportunidad para los ciberdelincuentes. Esto ha llevado a un aumento en el uso de arquitecturas de seguridad Zero-Trust, que no extienden la confianza automáticamente independientemente de si un usuario está dentro o fuera del perímetro, lo que se conoce como “confianza implícita”.

Una arquitectura de Zero-Trust (“Confianza explícita”) también ayuda a mitigar los riesgos derivados del aumento de las necesidades de acceso. En las empresas actuales, el acceso no se limita normalmente a los empleados y socios comerciales, en muchos casos, también debe extenderse a consultores, clientes, proveedores y más. Todas estas personas necesitan acceso a aplicaciones comerciales y recursos de TI que residen en centros de datos privados globales y nubes públicas.

Deficiencias de las VPN tradicionales y la necesidad de perímetros definidos por software

Las redes privadas virtuales (VPN), brindan conectividad segura y privada a los empleados que necesitan acceso remoto o de “site-to-site” a las aplicaciones basadas en las redes corporativas internas.

Como conexiones virtuales punto a punto, las VPN se pueden crear a través de conexiones dedicadas, protocolos de túnel virtual o mediante el cifrado del tráfico de red. Si bien las VPN tradicionales brindan acceso remoto seguro, tienen inconvenientes, incluido el soporte limitado del cliente para situaciones de BYOD, la latencia, los servicios en la nube o restricciones de ancho de banda, así como soporte del servidor global de proveedores de VPN o recursos de TI corporativos.

Modelo de seguridad SDP centrado en el usuario

SDP (o Perímetro definido por Software) es un modelo de seguridad de red que crea dinámicamente conexiones de red uno a uno entre el usuario y los recursos a los que accede. Los componentes incluyen la verificación de la identidad de un usuario, sus dispositivos y su función antes de otorgar acceso a los recursos de la red.

Este modelo de seguridad de red, basado en la autenticación y autorización antes del acceso a la red, exige que cada servidor se oculte detrás de una puerta de enlace de acceso remoto en la que los usuarios deben autenticarse y obtener acceso antes de que cualquier servicio autorizado esté disponible.

Una arquitectura de Zero-Trust ("Confianza explícita") también ayuda a mitigar los riesgos derivados del aumento de las necesidades de acceso

Solución integral de ZTNA en la nube

Hoy en día, muchas empresas tienen empleados en diferentes oficinas globales que dependen de aplicaciones de productividad basadas en la nube (como Office 365, AWS o Salesforce CRM) a las que se accede a través de dispositivos Windows, iOS, macOS y Android corporativos o de propiedad de los empleados. La conectividad remota también se ha vuelto crítica ya que los empleados trabajan desde casa o viajan por negocios, accediendo a redes corporativas a través de puntos de acceso WiFi no seguros o redes públicas bloqueadas por restricciones geográficas o por la censura online.

Por lo tanto, los gerentes de TI deben mirar más allá de la VPN tradicional hacia el acceso a la red Zero-Trust (ZTNA) basado en la nube que se puede implementar y configurar rápidamente en una configuración SDP.

El perímetro de seguridad debe seguir dondequiera que trabajen los humanos y extenderse hasta donde residan los activos

El nuevo Cloud Edge Secure Access de SonicWall permite una red como servicio (NaaS) simple para la conectividad de sitio a sitio y de nube híbrida con seguridad integrada Zero-Trust y acceso basado en el mínimo-privilegio. Las organizaciones ahora pueden proporcionar acceso seguro a las fuerzas de trabajo remotas fuera del perímetro tradicional mientras protegen los activos comerciales de alto valor, independientemente de su ubicación.

Cloud Edge Secure Access proporciona eficazmente un “rail and fence” dedicado e invisible para cada dispositivo de los empleados y terceras partes. Ofrece acceso seguro a aplicaciones y datos en cualquier lugar de la nube, incluidos privados, AWS, Azure, Google y más. Y es un primer servicio de acceso remoto de nueva generación ZTNA de Sonicwall, al que se irán uniendo pronto otros de ciberseguridad en la nube, claves en el mundo sin perímetro al que nos dirigimos a toda velocidad.

BlackBerry

EVITA MALWARE Y RANSOMWARE

Puedes prevenir ataques de Darkside, Nobelium y Revil con los sistemas de Inteligencia Artificial de Cylance

VISITA WWW.BLACKBERRY.COM

BlackBerry® Intelligent Security. Everywhere.

FORO it Digital Security

Mesa Redonda

La importancia de mantener el endpoint seguro en un modelo Zero Trust

El concepto Zero-Trust no es nuevo. Es la complejidad de las estructuras de las empresas y el crecimiento de la transformación digital la que está inspirando su adopción, una adopción que plantea crear controles basados en políticas para permitir un acceso seguro independientemente de cuán diverso o disruptivo sea el panorama actual.

La evolución del malware ha hecho que los antivirus y sistemas de seguridad endpoint tradicionales se vayan quedando obsoletas casi al mismo tiempo en que la pérdida de perímetro hace que el endpoint recobre protagonismo en el ecosistema de seguridad. Las siglas de moda son XDR (Extended, Detection and Response).

Para hablar de todo ello y de cómo las empresas afrontan este reto reunimos un grupo de expertos en un debate patrocinado por Fibratel, un partner de Cisco, bajo el Título “La importancia de mantener el endpoint seguro en un modelo Zero Trust” en el que estuvieron presentes Toni García, CISO de Leti Pharma; Juan Carlos Castro Ortiz, CISO de Ayesa; Francisco Alonso Batuecas, Jefe AREA de infraestructura y seguridad TIC del Ministerio del Interior; Juan Carlos Valle, CISO de LiberbankIT y Juan

"Pensamos que es interesante la combinación de las dos tecnologías, antivirus y EDR, siempre que no penalicen en los puestos de trabajo"

Francisco Alonso Batuecas, Jefe AREA de infraestructura y seguridad TIC, Ministerio del Interior

LA IMPORTANCIA DE MANTENER EL ENDPOINT SEGURO EN UN MODELO ZERO TRUST

CLICAR PARA VER EL VÍDEO

Francisco Moreda, Head of Cybersecurity Unit de Fibratel.

Iniciamos el debate preguntando a nuestros invitados sobre los retos a los que creen que tendrán que enfrentarse. Dice Toni García que, dependiendo de la compañía, se han tenido que hacer cambios importantes "que aún tienen que asentarse y consolidarse". Sobre Zero Trust asegura que se lleva hablando desde hace tiempo, pero que "no es sencillo tenerla como base real" y que muchas empresas aún se están aprovisionando de las herramientas que permitan implementarlo de una manera adecuada.

Para Juan Carlos Castro aún existe "una cobertura inadecuada para este escenario post pandémico" pero existe una hoja de ruta clara: se sigue con la gestión de vulnerabilidades en todos los activos corporativos, con el correcto perfilado de usuarios

"No debemos luchar contra el Shadow IT ni contra el BYOD porque es una batalla perdida"

Juan Carlos Castro, CISO, LiberbankIT

dentro de la organización, y están surgiendo muchas normativas que están ayudando a implementar Zero Trust.

Afianzar y revisar todo lo que se ha hecho, en ocasiones de manera precipitada durante la pandemia, es uno de los retos de los CISOs apuntado por Francisco Alonso. Añade que hay que seguir apostando por la cultura de la ciberseguridad a través de una formación continua.

Mostrándose de acuerdo en retos como el consolidar las acciones realizadas en tiempo de pandemia y el seguir concienciando en ciberseguridad, dice también Juan Carlos Valle que hay que seguir trabajando la detección temprana así como en la limitación de accesos y permisos de los usuarios. Añade como retos importantes "la automatización de todas las respuestas y ataques, continuar con los planes de continuidad de negocio y analizar el comportamiento de usuarios y sistemas".

Lo que desde Fibratel se observa coincide con lo comentado por los responsables de ciberseguridad presentes en el encuentro. Añade Juan Francisco Moreda que el dato está distribuido, por lo que es importante "mantener el control de que tanto el usuario como el dispositivo que accede al dato es quien dice ser".

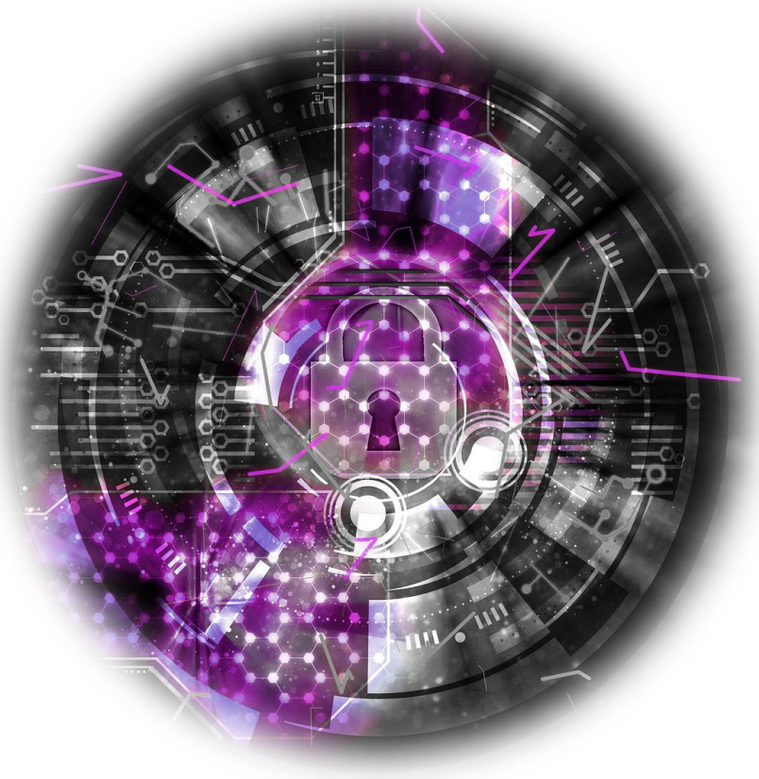
Protección del endpoint

Los responsables de seguridad deben afrontar el reto de proteger un endpoint heterogéneo y que siempre está conectado. Explica Francisco Alonso Batuecas que, "por la sensibilidad de la información que se maneja en el Misterio del Interior", la movilidad de los usuarios se afrontaba con mucha precaución. Sin embargo, COVID-19 impulsó el teletrabajo, lo que llevó a centrarse en "securizar la conexión y comprobar el estado del endpoint, que cada vez es más variopinto". La concienciación en el buen uso de los dispositivos "nos está costando", dice el directivo, añadiendo que se trabaja en un perfilado de usuarios para ver quién tiene acceso a qué y desde qué dispositivo.

Para Toni García la heterogeneidad de los endpoint supone un reto y se fija un objetivo: "me gustaría plantearme la opción de que alguien pudiese ir a comprarse un dispositivo cualquiera y en el momento en que accediera con su login se puedan

"Sobre Zero Trust se lleva hablando desde hace tiempo, pero no es sencillo tenerla como base real"

Toni García, CISO, Leti Pharma



aplicar las políticas necesarias". Añade que este sería "un estado idílico desde el punto de vista de control de acceso, control de la identidad y control del dato al que es difícil llegar" y que se trabaja en ello para ver cómo y con qué herramientas se puede llegar a ese punto.

La securización de un endpoint heterogéneo y siempre conectado se afronta con complejidad, dice Juan Carlos Valle, añadiendo que "el cambio de un antivirus tradicional a un EDR conlleva cambios que no son solo técnicos, sino culturales de la propia compañía" y que es fundamental la monitorización y la adaptación de los roles de los usuarios y procurar automatizar al máximo.

Juan Carlos Castro, CISO en LiberbankIT, asegura que "debemos aceptar y asumir la premisa de que no debemos luchar contra el Shadow IT ni contra el BYOD porque es una batalla perdida" y apostar "por enfoques más modernos gracias a tecnologías como con EDR, Zero Trust, controlando el acceso a los activos y haciendo análisis de comportamiento".

Desde Fibratel aseguran que aún hay muchos clientes que todavía utilizan antivirus basados en firmas, que están obsoletos frente a las nuevas amenazas. También se da el caso de clientes que adoptan un EDR/XDR, con lo que reciben mucha información pero que "no tienen personal para poder extraer valor de esos datos y poder actuar de una manera rápida"

EDR, XDR, NDR...

"Esto va a mucha velocidad", dice Juan Carlos Valle cuando le preguntamos por la evolución de los antivirus hacia las nuevas propuestas de detección y respuesta. La compañía que protege, LiberbankIT, ya cuenta con un EDR y está en proceso de implantación de un XDR, que según este CISO es "una tecnología muy potente".

En el caso del Ministerio del Interior explica Francisco Alonso Batuecas que la implantación del EDR se llevó a cabo hace unos dos años pero que se sigue manteniendo el antivirus; "pensamos que es interesante la combinación de las dos tecnologías, siempre que no penalicen en los puestos de trabajo y hemos encontrado ese equilibrio". Añade que se está trabajando en la transición hacia el XDR "buscando la automación".

> "El cambio de un antivirus tradicional a un EDR conlleva cambios que no son solo técnicos, sino culturales de la propia compañía"
>
> Juan Carlos Castro Ortiz, CISO, Ayesa

El principal impacto que supone el pasar de un antivirus tradicional a un XDR es "la cantidad de información que antes no tenías y que ahora tienes",

"Hay empresas que adoptan un EDR/XDR pero no tienen personal para poder extraer valor de los datos que generan y poder actuar de una manera rápida"

Juan Francisco Moreda, Head of Cybersecurity Unit, Fibratel

recuerda Toni García, añadiendo que hemos vivido mucho tiempo con los SIEMS y vamos a una tecnología llega con automatización y capacidad de respuesta pero que es complejo de gestionar. Señala que antes de adoptar las nuevas propuestas de detección y respuesta hay que tenerlo claro porque "podemos correr el riesgo de depender de una única solución o proveedor tecnológico y estar atados de pies y manos hasta el punto de que realmente no conozcas tu propia infraestructura".

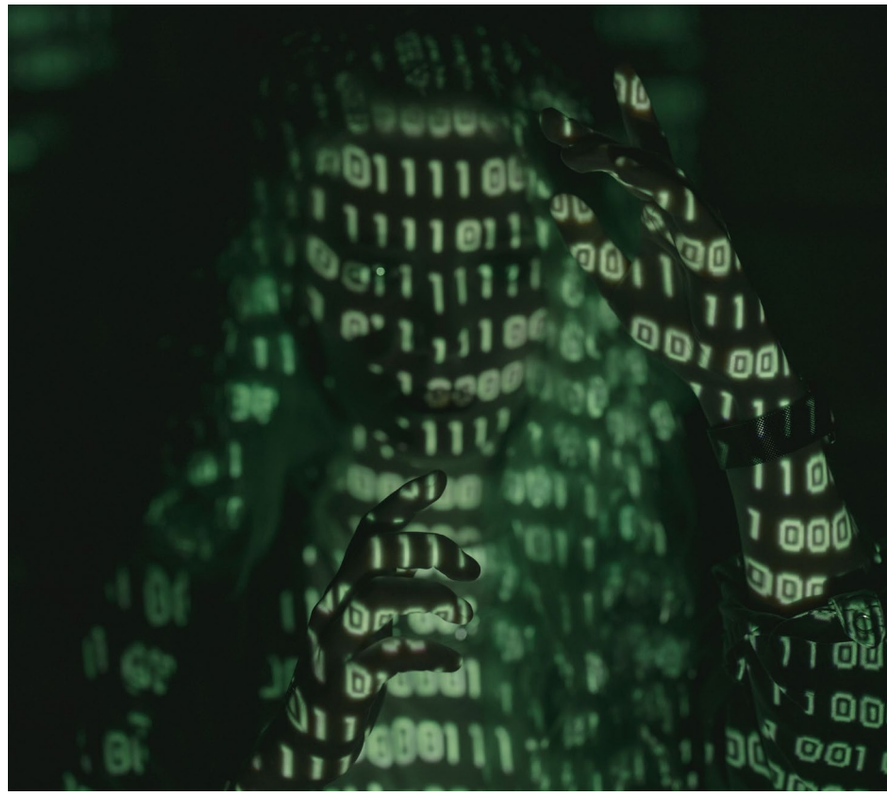
Explica Juan Carlos Castro que en Ayesa ya hay implementado un antivirus y un EDR. Mirando hacia el XDR, esta tecnología "podría echarse de menos por la comodidad de poder introducir inputs de diferentes sitios en un data lake para poder refinar todos esos eventos y para tomar acciones automáticas", y que durante el próximo año se verá cómo varía esta tecnología y cuán eficaz es.

En opinión de Juan Francisco Moreda las nuevas propuestas de detección y respuesta llegan con un reto: "los automatismos nos van a venir bien, pero al final hay que tener personas detrás que hagan ciertas revisiones".

Conclusiones

Tras finalizar el encuentro con los CISOs pedimos a Juan Francisco Moreda unas conclusiones, entre las que destaca que las empresas participantes en el encuentro "van unos pasos por delante de muchos de los clientes con los que normalmente trabajamos" añadiendo que la mayoría de los clientes con los lo que trabaja Fibratel no llegan a tener un SOC ni tanto personal como para poder gestionar toda la información que genera un EDR/XDR/NDR, lo que al final supone un incremento de ese tipo de servicios.

Sobre si la empresa española está madura para adoptar el modelo Zero Trust, dice el responsable de /fsafe, la unidad de ciberseguridad de Fibratel, que está un poco lejos, pero que, en todo caso, el camino hacia Zero Trust puede no tener fin.



235%

Akamai ha observado un aumento del 235% en los ataques de phishing.

¿Tú solución de MFA está a prueba de phishing?

Akamai MFA: Seguridad FIDO2 sin claves de seguridad físicas

Protege tu empresa contra el robo de cuentas de empleados, y filtración de datos con la tecnología MFA de última generación. Convertimos tu smartphone en una llave de seguridad, con una autenticación sencilla, y sin carga de trabajo para tu equipo de TI.

- **Máxima seguridad**
- **Push mobile a prueba de phishing**
- **Gestión de TI unificada y sencilla**

Akamai MFA – pruébalo gratis durante 60 días

Solicita una prueba gratuita en: contact-spain@akamai.com
o si lo prefieres, llámanos al Tel. 91 793 32 43

©2021 Akamai Technologies

Fibratel. Juan Francisco Moreda, Head of Cybersecurity Unit

“El dato es algo primordial y hay que protegerlo muy bien”

Juan Francisco Moreda, Fibratel

La transformación digital en la actualidad viene marcada por dos factores: la desaparición del perímetro y la adopción de la nube, ya sea en modo híbrido o 100% cloud. Para proteger el dato es necesario incidir en el modelo de ciberseguridad compartida y la visibilidad.

“DATO, EL PETRÓLEO DEL SIGLO XXI” **CLICAR PARA VER EL VÍDEO**

Tras la pandemia, el teletrabajo y el BYOD ya son una realidad completa, lo que implica que las empresas deben adaptarse a este nuevo paradigma. Además, la adopción de la nube ha traído muchas ventajas, como flexibilidad, capacidad de escalado o acceso global a aplicaciones y servicios de una manera rápida, sencilla y segura.

Estas clouds han permitido trabajar de una manera diferente. Había un puesto de trabajo tradicional en

En las empresas la ciberseguridad ha dejado de ser una opción para convertirse en una necesidad

el cual todos los usuarios trabajaban directamente dentro de la sede y rara vez salían. Ahora se utilizan equipos tanto corporativos como no corporativos y el acceso a la información o a las aplicaciones se da tanto desde dentro como desde fuera de la empresa.

Para Juan Francisco Moreda, Head of Cybersecurity Unit de Fibratel, “el dato es algo primordial, es el petróleo del siglo XXI, hay que protegerlo muy bien”. A la hora de hablar del cloud, es imprescindible recordar que la seguridad del dato siempre depende del cliente final, así como el acceso, qué usuarios pueden o no pueden acceder. También es necesario mantener una visibilidad total de todo lo que se encuentra dentro de esas clouds.

Para poder asegurar estos dos vectores existen distintas soluciones como el MFA, el Zero Trust, el EDR, las VPN, el CASB o el DLP. Aquí entra el concepto de arquitectura SASE, que recoge elementos de seguridad como el SWG, CASB, firewalls cloud y el Zero Trust Network Access y los traslada a una arquitectura nativa de cloud proporcionada as a service.

Contenido relacionado

Foro ITDS. Caminando hacia Zero Trust

/fase, Fibratel Cynersecurity Unit

Compartir en RRSS

Sophos Iberia. Javier Donoso, Senior Sales Engineer

“XDR provee las herramientas suficientes para tener una visibilidad completa de lo que ocurre en una infraestructura”

TENEMOS QUE ADOPTAR UN NUEVO ENFOQUE Y ZERO TRUST ES EL MODELO A SEGUIR

CLICAR PARA VER EL VÍDEO

Javier Donoso, Sophos

La mayor calidad del malware, así como los ataques avanzados y más dirigidos están haciendo que los antivirus y las soluciones de seguridad endpoint tradicionales se vayan quedando obsoletas. Ahora, las siglas de moda son XDR (Extended Detection and Response).

El mundo ha cambiado en todos los ámbitos. Hasta ahora la infraestructura de las compañías solía seguir un modelo de perímetro único, con el firewall en el punto de entrada inspeccionando paquetes, lo que daba una sensación de falsa seguridad, ya que no tenía en cuenta que dentro de ese perímetro único se encontraba la mayor amenaza que una empresa tiene que hacer frente a diario, el usuario.

La confianza es una palabra muy peligrosa cuando estamos hablando de la seguridad en las TICs

Para Javier Donoso, Senior Sales Engineer de Sophos, el perímetro ha muerto, ya que no protege al 100% los recursos de la compañía, por lo que es necesario adoptar un nuevo enfoque. Para esto, la metodología Zero Trust se ha convertido en el modelo a seguir. El XDR va a proporcionar las herramientas suficientes al administrador para tener una visibilidad completa de qué es lo que está pasando en su infraestructura.

Sophos ofrece un ecosistema de seguridad real, con capacidad de analizar la red, el email y otras fuentes de datos, además de los endpoints y los servidores, permitiendo así tener una visión holística del entorno de la seguridad de la organización. Se trata de un ecosistema de seguridad organizado en la interoperatividad, que para la compañía es lo que este nuevo mundo necesita.

Contenido relacionado

Foro ITDS. Caminando hacia Zero Trust

La confianza cero desmitificada

Sophos Adaptive Cybersecurity Ecosystem

Intercept X

Compartir en RRSS

WatchGuard-Cytomic. Miguel Carrero, Vice President Strategic Accounts & Security Service Providers

“El nuevo modelo de seguridad apuesta por la confianza cero y la verificación absoluta”

Miguel Carrero, WatchGuard-Cytomic

El concepto de Zero Trust vino como contraposición a otro concepto que ha marcado la filosofía de la ciberseguridad en los últimos años, Trust but verify, sobre todo debido a las limitaciones tecnológicas que teníamos en su momento. Ahora hay que darle la vuelta completamente a ese concepto.

“CONFIANZA CERO. VERIFICACIÓN ABSOLUTA”

CLICAR PARA VER EL VÍDEO

Antes de que se estableciera este modelo de confianza cero, en el sector de la ciberseguridad tradicional primero se confiaba en que los procesos eran beningnos y después se verificaban. El concepto de Zero Trust dio un vuelco a esta filosofía, basándose en esta máxima: yo no confío en nada, yo verifico todo por adelantado.

Miguel Carrero, Vice President Strategic Accounts & Security Service Providers, WatchGuard-Cytomic, señala que el Zero Trust Application Service es la aplicación letra por letra de esa filosofía Zero Trust, además de pieza esencial en la solución Zero Trust de Cytomic EDR y Cytomic EPDR. Quiere decir que todo lo que se ejecuta en el endpoint ha sido previamente determinado como benigno.

A esto WatchGuard-Cytomic le añade una capa más de verificación proactiva, los servicios de Threat Hunting. Además, hay un elemento más que no es endpoint en el sentido más tradicional pero que la compañía ve como esencial para lograr el Zero Trust: la gestión de identidad, necesaria para lograr una verificación absoluta en esos entornos de confianza cero.

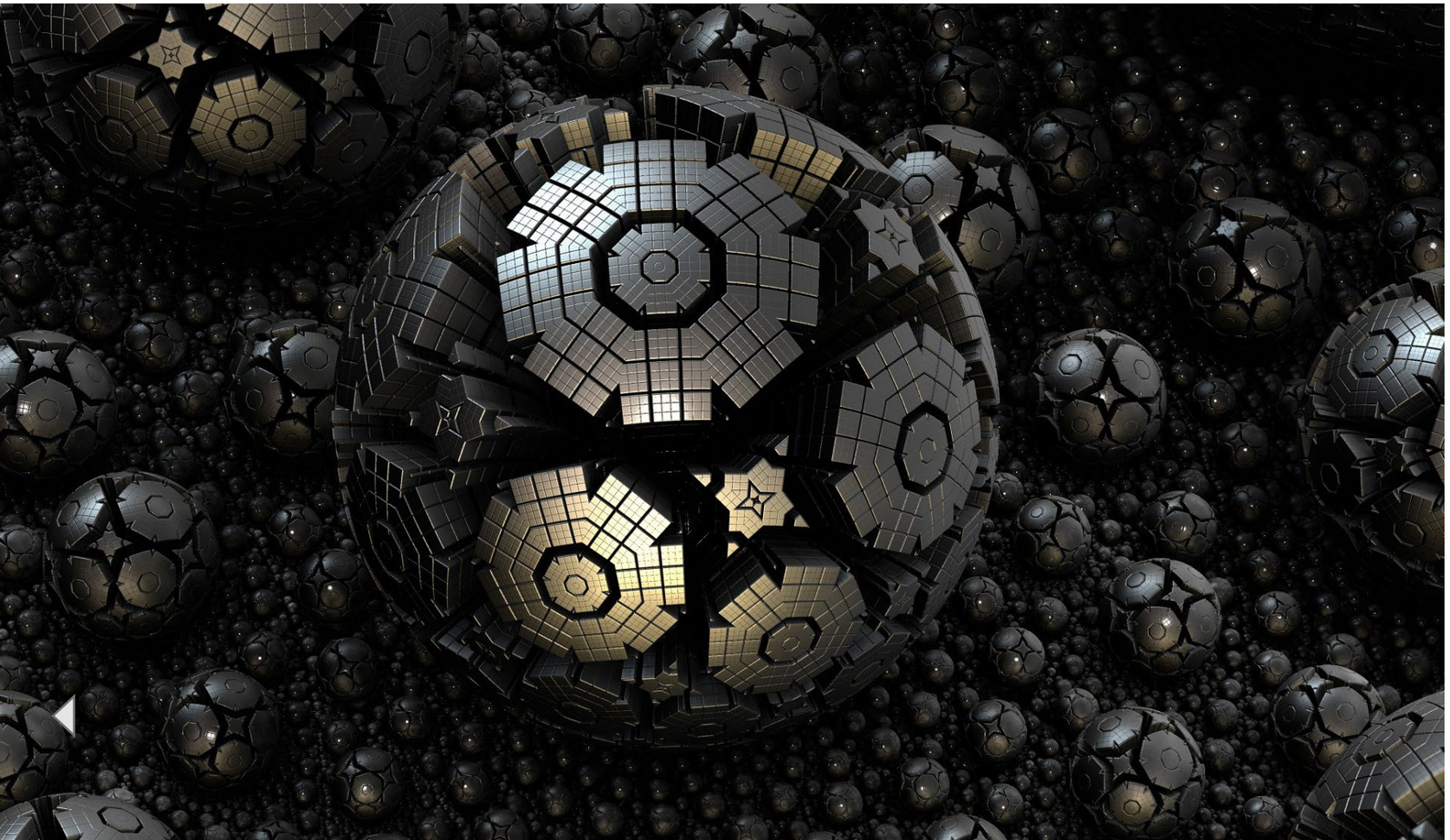
Contenido relacionado

Foro ITDS. Caminando hacia Zero Trust

Cytomic Portfolio

Cómo implementar un modelo de Zero Trust

Nosotros entendemos el concepto de Zero Trust en el mundo del endpoint como confianza cero y verificación absoluta



Compartir en RRSS

BlackBerry. Blas Simarro, Regional Sales Manager Iberia

“Ponemos la Inteligencia artificial al servicio de la validación de accesos”

Blas Simarro, Blackberry

La aplicación de la estrategia de Zero Trust puede ser muy compleja, en el sentido de que requiere de la adopción de controles muy diversos en multitud de fuentes y de accesos a los activos de información. La aplicación de inteligencia artificial nos permite que en los distintos casos de uso las políticas puedan ser adaptativas.

“PONEMOS LA INTELIGENCIA ARTIFICIAL AL SERVICIO DE LA VALIDACIÓN DE ACCESOS”

CLICAR PARA VER EL VÍDEO

Para aplicar correctamente una estrategia de Zero Trust hay que incorporar tanto aplicaciones, como personas, como todos los dispositivos que acceden a la red, como los propios dispositivos de acceso. Si alguna de esas áreas queda vulnerable, los accesos no autorizados sucederán a través del eslabón más débil.

Es por ello que Blas Simarro, Regional Sales Manager Iberia de BlackBerry, prefiere hablar del

concepto Zero Touch que han desarrollado en BlackBerry. Normalmente se suelen utilizar tres mecanismos de acceso: algo que el usuario conoce, como un password; algo que tiene, como una tarjeta de coordenadas; y algo que es. Este último mecanismo es en el que se basa esta premisa, estableciendo mecanismos de validación que sean transparentes tanto para la propia organización como para el usuario a través de características que le definan.

La validación puede ser contextual, pudiendo cambiar los niveles de validación en función de desde dónde, o cómo, o desde qué dispositivo se está validando el usuario. Lo más importante es que la validación es continua, permitiendo bloquear el acceso en caso de circunstancias anómalas durante la sesión.

Contenido relacionado

Foro ITDS. Caminando hacia Zero Trust

From Zero Trust to Zero Touch

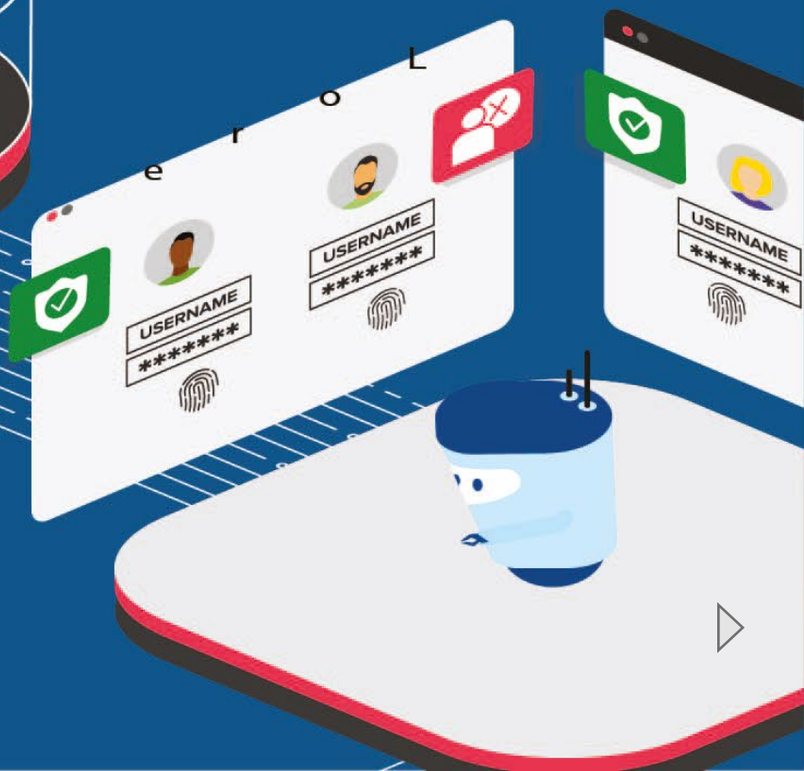
BlackBerry Zero Trust Architecture

Hay que tener en cuenta que en una estrategia de Zero Trust no podemos dejar a nada ni a nadie atrás

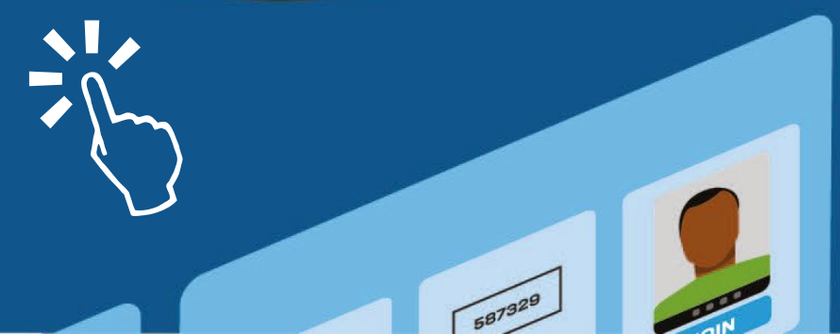
Compartir en RRSS

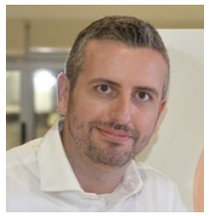
Implementar Zero Trust

Aumente la eficacia y la seguridad iniciando su viaje Zero Trust



Leer información general





JUAN FRANCISCO MOREDA

HEAD OF CYBERSECURITY UNIT, FIBRATEL

Tras pasar más de diez años en Sitel Ibérica, Juan Francisco Moreda se unió a Fibratel hace cinco como técnico de comunicaciones. Actualmente es el responsable de /fase, la unidad de negocio de ciberseguridad de Fibratel con vocación de ser una compañía diferenciadora por la amplitud e innovación de las tecnologías de seguridad que utiliza.

Protegiendo la Transformación con un modelo Zero Trust

Vivimos en la era de la transformación digital. Esta transformación de la manera de hacer negocios tiene múltiples implicaciones que van desde cambios en la estrategia de las empresas, su organización y, por supuesto, necesidades o retos tecnológicos.

Compartir en RRSS

Para empezar, podemos hablar de la adopción de las Clouds o mejor dicho de la utilización de las Clouds para incluir al surgimiento de las nuevas empresas 100% Cloud. Las Cloud son una herramienta tremendamente potente, es más, necesaria para ser competitivos en los modelos de negocio actuales.

Aportan, entre otras ventajas, flexibilidad, capacidad de escalado y acceso global a las aplicaciones y servicios; pero su adopción debe hacerse de forma segura.

Las nuevas metodologías de programación basadas en Contenedores, Kubernetes, DevOps, ha propiciado que el desarrollo de aplicaciones se multiplique exponencialmente. Las aplicaciones son parte fundamental de la nueva manera en la que se desarrolla la actividad de las empresas. Esta eclosión del software es un reto para la ciberseguridad, pues evoluciona a velocidad de vértigo y donde, a día de hoy, hay un hueco que cubrir.

Y, por supuesto, no debemos pasar por alto pues es el punto fundamental: LA PROTECCIÓN DEL DATO, el petróleo del siglo XXI, en los nuevos entornos.

Protección de los Datos Corporativos en las Clouds

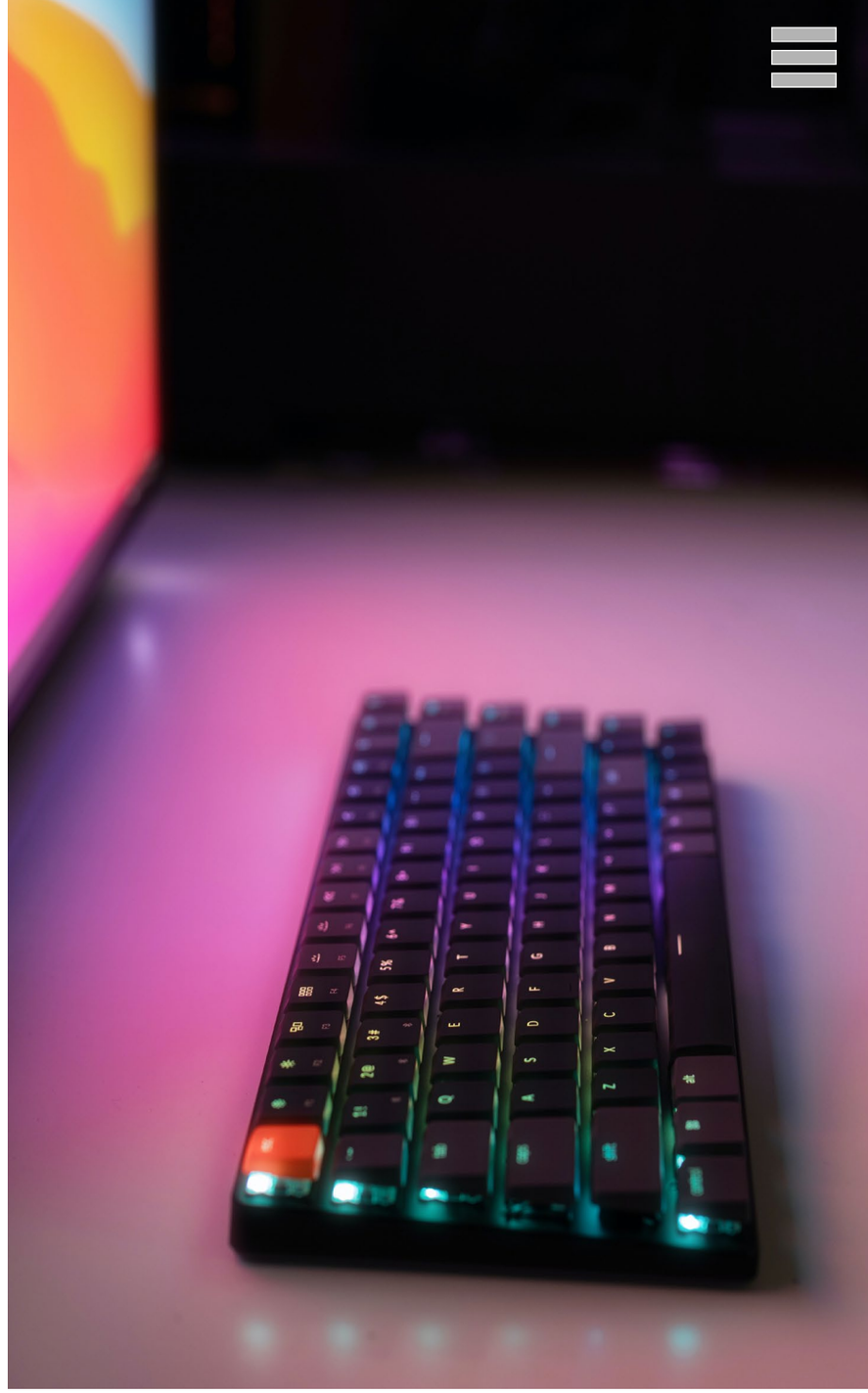
El nuevo entorno Cloud precisa de una gobernanza adecuada, para no incurrir en potenciales incidentes de ciberseguridad. El 75% de las mayores organizaciones de todo el mundo ya dispone de recursos, datos y aplicaciones en múltiples nubes, públicas y privadas, según la consultora Gartner. Se presenta un nuevo modelo de ciberseguridad compartida entre los proveedores Cloud, como Amazon, Google, Microsoft, etc. y las empresas que utilizan estos servicios Cloud, que no dejan de ser responsables de proteger la identidad y el dato.

También se plantea un problema respecto a la visibilidad en la Cloud, surgen preguntas sobre qué hacen los usuarios con los datos, quién accede a ellos, cómo se almacenan, etc... Soluciones como Cisco DUO o Cisco Umbrella, que poseen algunas tecnologías como MFA, Zero Trust, VPN SSL, CASB y DLP, deben de tenerse en cuenta cuando se trabaja en entornos Cloud.

El nuevo puesto de trabajo

En el nuevo puesto de trabajo, las personas trabajan desde cualquier lugar, utilizando indistintamente dispositivos corporativos y propios (BYOD) para el uso de aplicaciones corporativas (correo electrónico, ERP, gestor documental, etc..). Esta dispersión de usuarios, dispositivos, aplicaciones y datos trae consigo una evidente modificación de los modelos tradicionales de trabajo, generando nuevos riesgos de ciberseguridad y modificando las necesidades de securización.

Tenemos que prestar atención a los usuarios y a los dispositivos que utilizan para acceder a la información.



El nuevo entorno Cloud precisa de una gobernanza adecuada, para no incurrir en potenciales incidentes de ciberseguridad

Las nuevas metodologías de programación basadas en Contenedores, Kubernetes, DevOps, ha propiciado que el desarrollo de aplicaciones se multiplique exponencialmente

A las herramientas mencionadas anteriormente debemos añadir soluciones como Cisco Endpoint Security, es decir, antivirus de nueva generación (NGAV) y EDR, basados en análisis de comportamientos y machine learning para identificar las técnicas de ataque de los ciberatacantes y detener no solo los ataques basados en firmas y en ficheros, sino también los Zero Day y los fileless.

Los antivirus tienen que ser Cloud para para llegar a todos los usuarios y con capacidades de Threat Hunting y mitigación de incidente.

Contenido relacionado

Fibratel /fase

SASE

Esta dispersión de usuarios, aplicaciones y datos nos lleva a modificar los modelos tradicionales en los que los usuarios se concentraban en las oficinas con dispositivos corporativos, accedían a aplicación alojadas en el CPD y los datos permanecían en el mismo entorno.

Se impone la aplicación de arquitecturas SASE (Secure Access Service Edge), que combinan las capacidades de las VPN y la SD-WAN con funcionalidades de seguridad nativas cloud como los Secure Web Gateways, Cloud Access Security Brokers, firewalls y Zero Trust Network Access, donde nuevamente Cisco Umbrella con su versión SIG, puede ayudarnos.

En los nuevos modelos estas funciones de red y seguridad son ofrecidos “as a Service” desde la Cloud.

Desde fibratel estamos para acompañar a nuestros clientes en todo este camino de transformación hasta el Zero Trust.

WatchGuard Endpoint Security Solutions

Proteja sus dispositivos con confianza

Las soluciones nativas en la nube de WatchGuard Endpoint Security protegen a las empresas de cualquier tipo de ciberataques presentes y futuros mediante las soluciones Endpoint Protection Platform (EPP) y Endpoint Detection and Response (EDR). Nuestra plataforma WatchGuard Endpoint Security ofrece una protección completa de EPP y EDR, así como servicios de búsqueda de amenazas y aplicaciones de confianza cero, suministrados a través de un único agente ligero y gestionados desde una única plataforma basada en la nube.

WATCHGUARD EPP

Endpoint Protection Platform

WATCHGUARD EDR

Endpoint Detection and Response

WATCHGUARD EPDR

Endpoint Protection Detection and Response

Threat Hunting Service

Zero-Trust Application Service

+34 917 932 531

spain@watchguard.com

www.watchguard.com