it Digital Security

Webinar Arquitecturas

#ITWebinars

Arquitecturas de Seguridad,

¿qué ventajas ofrecen?

it Digital Security

CIPHER IS NOW ENTRUST

Check Point SOFTWARE TECHNOLOGIES LTD.

SONICWALL

Diciembre 2020

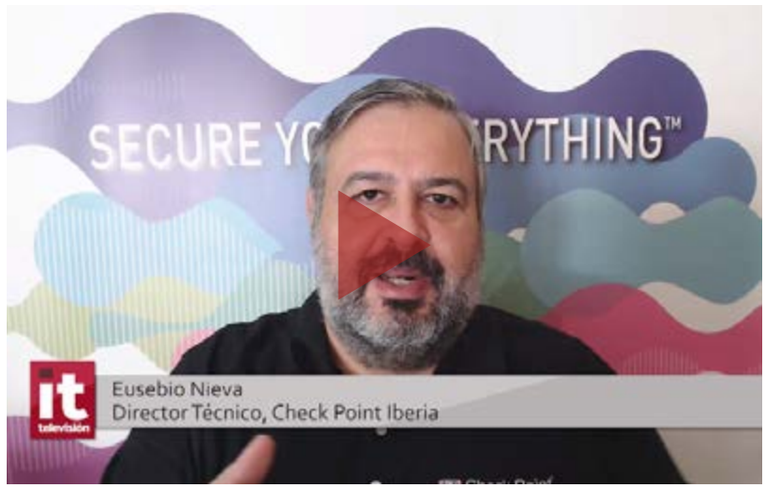
Arquitecturas de seguridad, ¿qué ventajas ofrecen?

Ataques cada vez más sofisticados, aumento del número de vectores de ataque, cientos de herramientas de seguridad, y diferentes entornos que proteger hacen que las arquitecturas de seguridad se hayan vuelto imprescindibles para dar cohesión a la seguridad empresarial.

Arquitecturas integradas, colaborativas y adaptativas diseñadas para ofrecer seguridad distribuida para empresas ofreciendo protección frente a amenazas, desde IoT a dispositivos remotos, y a través de las redes, nube o dispositivos móviles.

Acompáñanos en este IT Webinar en el que diferentes expertos de seguridad explicarán las ventajas de contar con una plataforma unificada de seguridad capaz de orquestar diferentes elementos y automatizar las operaciones para conseguir una seguridad más coherente y flexible.

A continuación, puedes leer un resumen de sus intervenciones, con los puntos más destacados. También puedes pinchar en cada una de las imágenes de sus portavoces para acceder a su intervención en el webinar o ver la sesión completa aquí.



Eusebio Nieva, Director Técnico, Check Point

"La seguridad tiene que estar automatizada"

"No debemos confiar por principio en nadie, ni siquiera aunque sea de dentro de nuestra compañía", asegura Eusebio Nieva, Director técnico de Check Point en la sesión online Arquitecturas de Seguridad, ¿qué ventajas ofrecen?. Se trata del modelo Zero Trust, que se antepone a un modelo anterior que confiaba en lo que ocurría en las redes internas, un modelo que propone verificar "absolutamente todo porque en ocasiones la amenaza está dentro".

Para Eusebio Nieva verificar y contrastar todos y cada uno de los accesos con respecto a los permisos que se deben y pueden tener es fundamental no solamente desde el punto de vista de aplicar ese Zero Trust, sino que es fundamental tener en cuenta que todas estas arquitecturas de seguridad, cualquiera que queramos implementar, tiene que estar automatizada, "porque la nube es uno de los mayores condicionantes que van a venir".

Explica que además de tender hacia arquitecturas híbridas, hay cambios importantes en el desarrollo de aplicaciones, "especialmente cuando hablamos de nube". Dice Eusebio Nieva que cuando hablamos de nube "estamos pasando de un modo de entender las aplicaciones a otro completamente diferente, basado en mucha mayor resiliencia y mucha mayor escalabilidad, y si no somos capaces de escalar y de automatizar la seguridad tal y como hacemos con las aplicaciones, olvídate. Es la hora de DevSecOps", de acercar lo más posible la seguridad y los controles de seguridad al propio desarrollo.

La propuesta CloudGuard de Check Point es el paraguas bajo el cual estamos implementando todos los controles que tenemos que poner para que la seguridad en la nube sea de facto "como la arquitectura de la nube nos está exigiendo", una nube

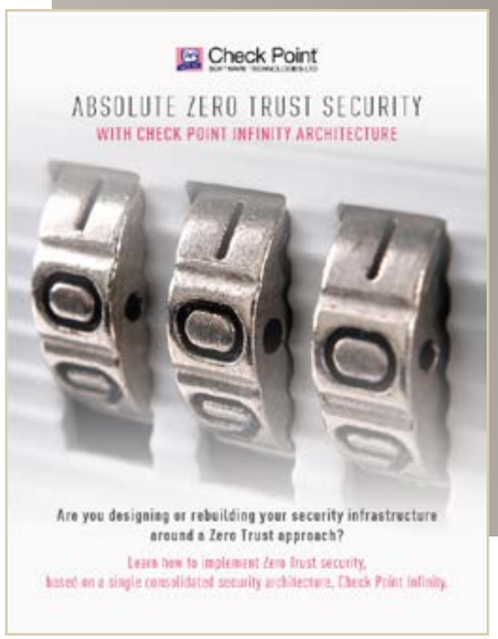
**EUSEBIO NIEVA,
DIRECTOR TÉCNICO, CHECK POINT**

**CLICAR PARA
VER EL VÍDEO**

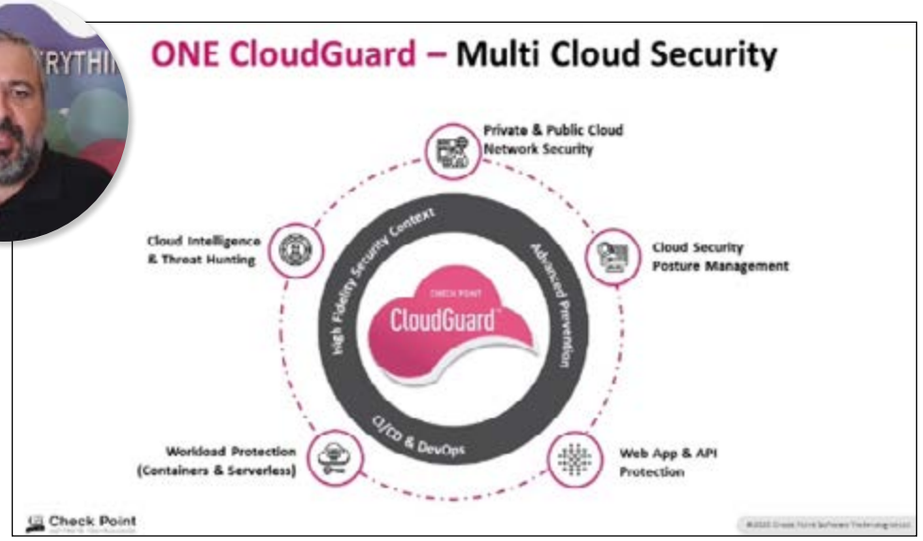
it whitepapers

SEGURIDAD ZERO TRUST ABSOLUTA CON CHECK POINT INFINITY

La reconstrucción de su infraestructura de seguridad en torno a un enfoque de Confianza Cero utilizando tecnologías dispares puede generar complejidades y brechas de seguridad inherentes. La arquitectura de seguridad de Check Point Infinity permite a las organizaciones implementar completamente todos los principios Zero Trust.



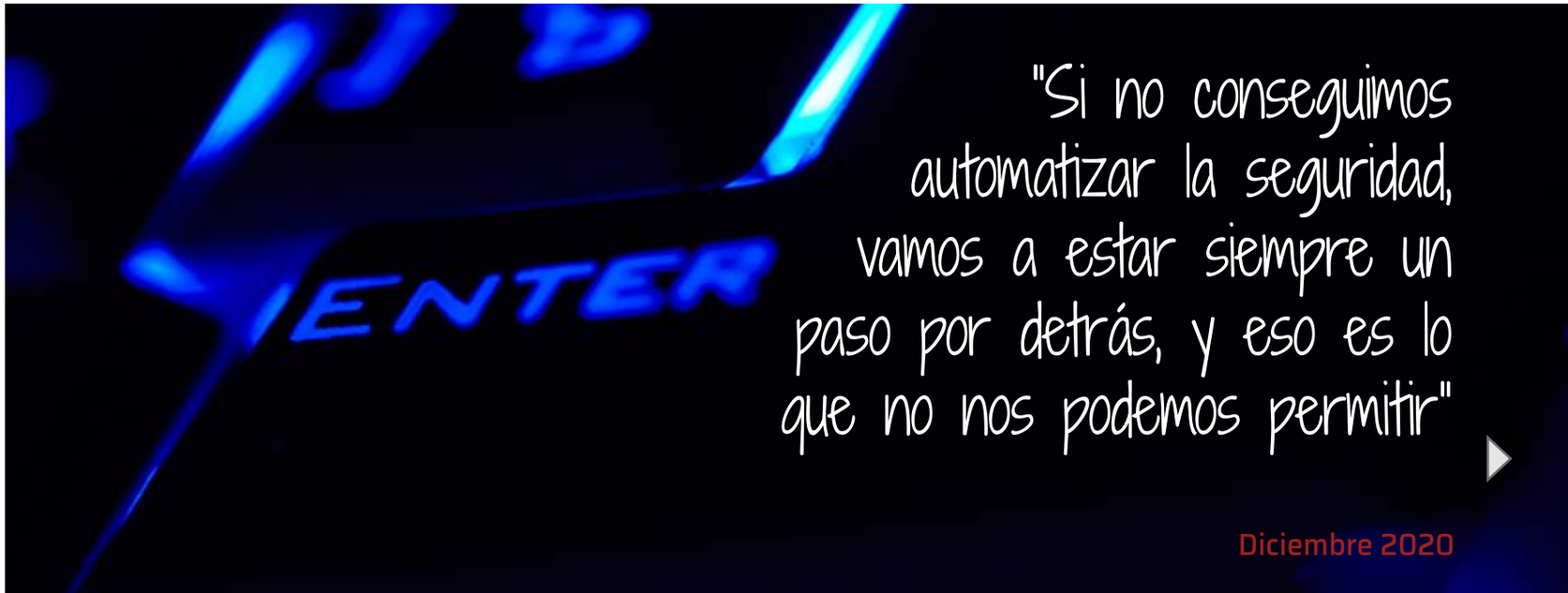
que exige escalabilidad, ir a la misma velocidad que los cambios que se producen y aplicar múltiples controles.



CloudGuard establece una serie de protecciones que ayudan a implementar esos cambios en la nube. No sólo se protege el tráfico, norte-sur y este-oeste, sino la gestión automatizada de la postura de seguridad, aplicaciones en la nube, cargas de trabajo y todo ello con la inteligencia necesaria para responder a una amenaza mediante técnicas de threat hunting. Añade Eusebio Nieva que el elemento común, importantísimo, de todas estas protecciones es la automatización; “si no conseguimos automatizar todo esto, vamos a tener un problema muy grave a la hora de ser capaces de adaptarnos desde el punto de vista de seguridad a lo que implementan nuestros departamentos de desarrollo. No vamos a ser capaces de poner una seguridad efectiva en la nube”.

Explica el directivo que la arquitectura de Check Point automatiza la seguridad mediante una gestión única que simplifica la forma de aplicar la seguridad mediante políticas dinámicas.

Vea aquí la intervención de Check Point en Arquitecturas de Seguridad, ¿qué ventajas ofrecen?



Sergio Martínez, Regional Manage, SonicWall Iberia

"Hay que cambiar de arquitectura"

Al mismo ritmo que COVID-19 se expandía por todo el mundo, la digitalización se aceleraba y lo que debería haber ocurrido en años, ocurrió en semanas. Lo dice Sergio Martínez, director general de SonicWall Iberia, en la sesión online Arquitecturas de Seguridad, ¿qué ventajas ofrecen?, añadiendo que esto suponía un reto para la supervivencia de las empresas, "para los ciberdelincuentes ha sido una bendición".

La superficie de exposición ha crecido muchísimo como consecuencia del teletrabajo, rompiendo definitivamente el perímetro de seguridad, incrementando el uso de aplicaciones cloud. Toda esta situación ha creado lo que SonicWall denomina un "Business Gap" entre lo que tienen las compañías y lo que efectivamente necesitan, explica Sergio Martínez.

"Estamos en una ciberguerra", dice el directivo de SonicWall cuando le preguntamos por lo que está sucediendo en el mercado. A destacar también un fuerte incremento de los ataques de intrusión y de ransomware, "el gran caballo de batalla del cibercrimen", que se ha disparado desde el pasado mes de junio. La necesidad de más ancho de banda, un mayor número de dispositivos inalámbricos, la necesidad de integrar todas las soluciones o tener que añadir nuevas capacidades está añadiendo más complejidad al mercado de ciberseguridad.

SERGIO MARTÍNEZ, REGIONAL MANAGE, SONICWALL IBERIA

CLICAR PARA VER EL VÍDEO

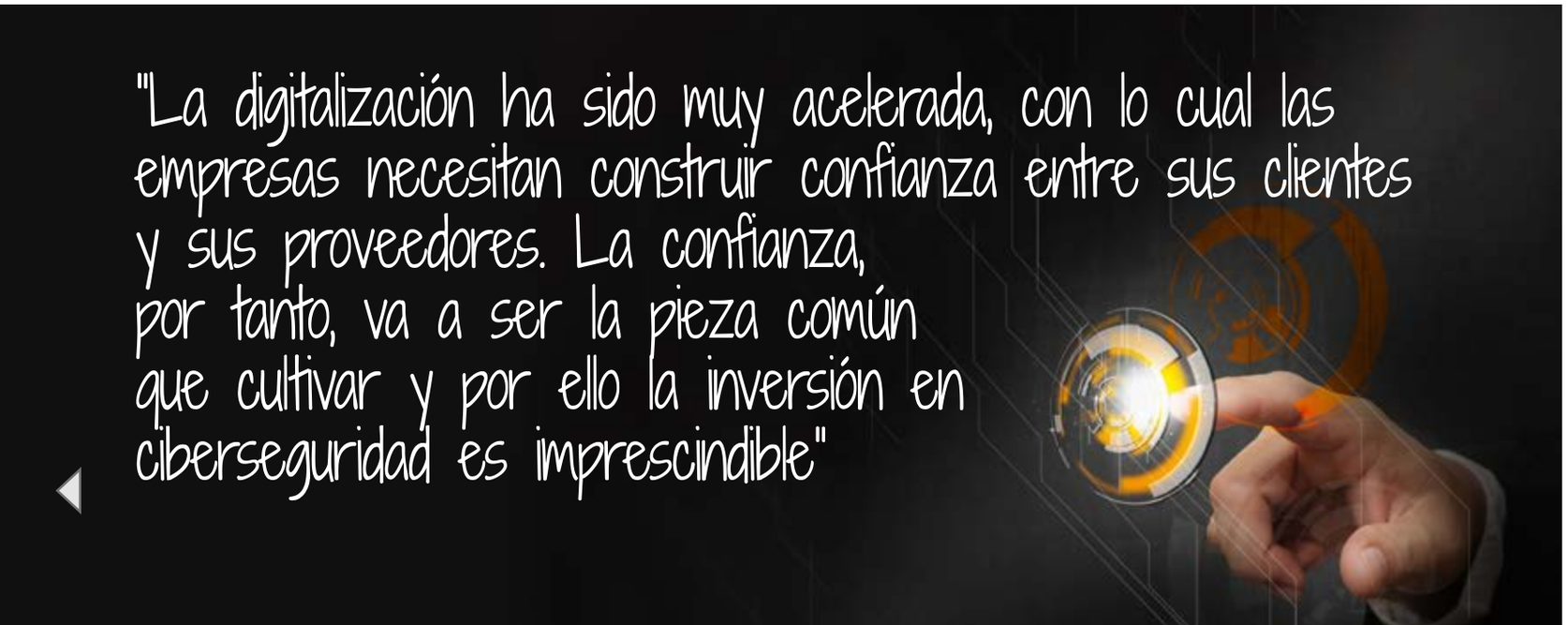
Asegurando que hay que cambiar de arquitectura, menciona Sergio Martínez la estrategia Boundless Cybersecuity lanza a primeros de año y que propone una plataforma que "proporciona seguridad en cualquier momento, en cualquier lugar e independientemente de los dispositivos con una serie de pilares", dice el directivo de SonicWall. El primer pilar es poder conocer lo desconocido, y

le siguen el poder establecer una defensa por capas, con una visión unificada Para saber lo que está ocurriendo en tu red, un TCO disruptivo, con una inteligencia artificial que va a aprendiendo y una adaptación continua ante cualquier tipo de amenaza.

Detrás de esta plataforma está la oferta de la compañía, compuesta por los firewalls de nueva generación, Secure WiFi, acceso remoto seguro, seguridad del email, firewalls virtuales, seguridad para Office 365 y Google Suite, y seguridad del IoT. “La integración de todas las soluciones es la clave”, asegura el directivo de SonicWall, mencionando el Capture Security Center

Con Cloud Edge Secure Access Sonicwall pone en marcha el paradigma Zero Trust. Se trata de un producto diseñado para proporcionar acceso remoto de todo tipo a las compañías, con un despliegue en minutos, con un control muy potente de los privilegios de acceso y un acceso directo a Cloud.

Vea aquí la intervención de SonicWall en Arquitecturas de Seguridad, ¿qué ventajas ofrecen?



it whitepapers

SONICWALL
CLOUD EDGE SECURE ACCESS

SonicWall Cloud Edge Secure Access es un potente servicio de red-as-a-service para conectividad de sitio a sitio y de nube híbrida a AWS, Azure, Google Cloud y más. En el proceso, combina enfoques de seguridad Zero-Trust y Least-Privilege en una oferta integrada.

El enfoque de acceso con privilegios mínimos restringe el acceso de un usuario en particular a solo lo que se necesita y nada más. Al limitar la exposición a otras áreas sensibles de la red, las organizaciones pueden asegurar sus recursos sin sacrificar su flexibilidad operativa.

José Perez, Sales Engineer, nCipher

"Security World es una arquitectura de protección de claves criptográficas"

Las soluciones criptográficas de nCipher Security, que a partir del 30 de noviembre de 2020 se convierte en Entrust, protegen las tecnologías y ayudan a cumplir con las nuevas exigencias en materia de cumplimiento. Dice José Pérez, Sales Engineer de nCipher, en la sesión online Arquitecturas de Seguridad, ¿qué ventajas ofrecen?, que en temas de cifrado su compañía trabaja con los HSM (Hardware Security Module) y que este tipo de dispositivos ofrecen muchas ventajas, "como el escalado, la flexibilidad y la resistencia a fallos que puedas ver en la operativa de diaria".

JOSÉ PEREZ
SALES ENGINEER, NCIPHER

CLICAR PARA VER EL VÍDEO

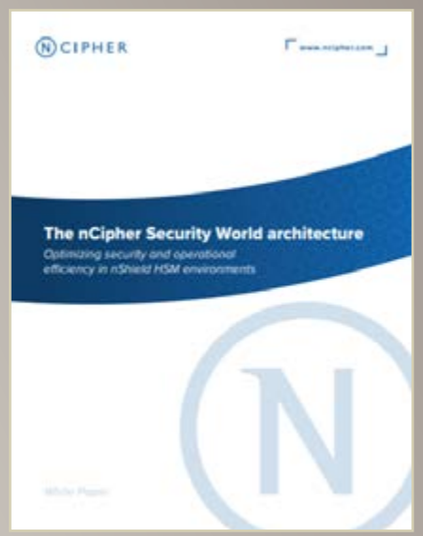
Explica este experto que cuando se habla de protección de claves de cifrado siempre hay un servidor de aplicación que le demanda criptografía al HSM; esa clave se genera dentro del HSM y, en teoría, nunca sale de ese HCM. "El problema que tiene esta aproximación es que si trabajas con un número de claves alto, la memoria del HSM muy probablemente se te acabe llenando", lo que lleve a comprar más HSM, y se termine ignorando la regla de que la clave nunca abandone el módulo, algo que también sucedería en el caso de que se quiera hacer un backup del material criptográfico.

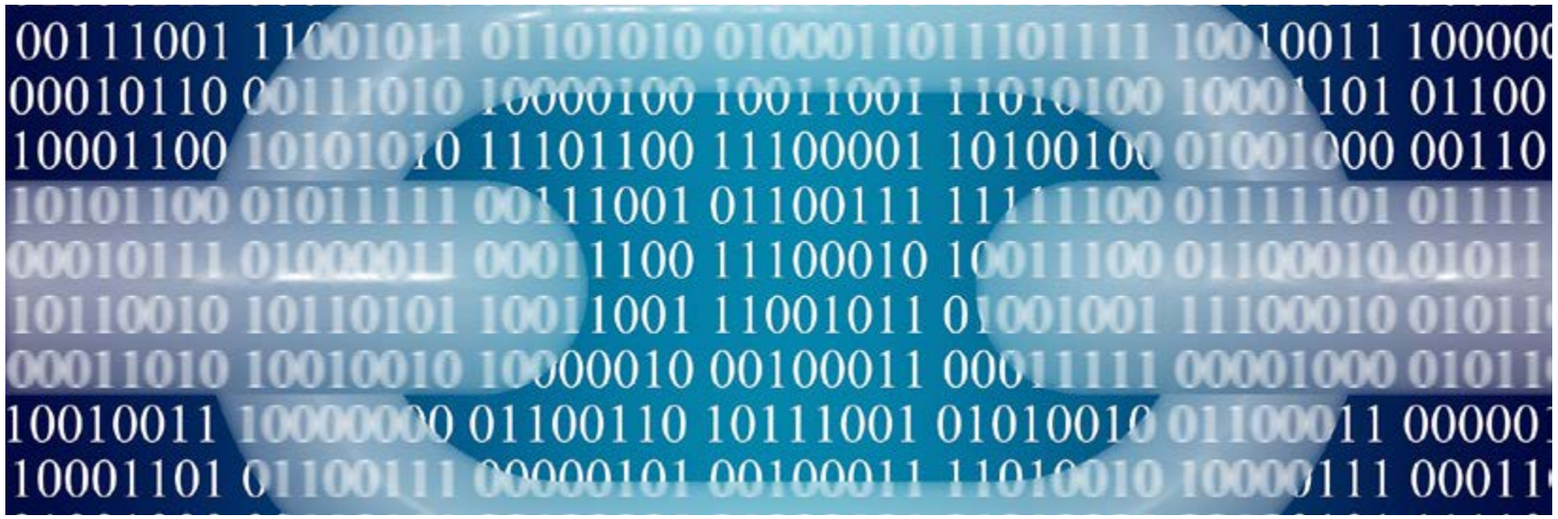
"Nosotros pensamos que esta no es la mejor aproximación a la hora de proteger tus claves y lo que proponemos es nuestra arquitectura Security World", donde al final se tiene lo mismo, un servidor de aplicación y un HSM. En este caso, explica

it whitepapers

THE NCIPHER SECURITY WORLD ARCHITECTURE

La arquitectura nCipher Security World admite un marco de gestión de claves especializado que abarca toda la familia nShield de HSM de propósito general. Esta arquitectura proporciona una experiencia unificada de administrador y usuario e interoperabilidad garantizada ya sea que el cliente implemente uno o cientos de dispositivos.





"Nuestra arquitectura Security World supone una ventaja en estos despliegues cloud en los que los HSM ya no son un appliance, sino que son un servicio"

José Pérez, el servidor de aplicaciones no va a empezar a generar claves sin más, "sino que va a generar una clave muy importante, la Clave Module, dentro del HSM", de forma que cuando se necesiten claves de aplicación, estas se crean dentro del HSM con su generador de números aleatorio, se cifran con la Module Key y se guarda fuera del HCM en el sistema de ficheros.

De esta manera "solo hay una clave dentro del HSM, lo que evita el peligro de quedarnos sin memoria" y que, en caso de tener que hacer un backup de las claves criptográficas, esas claves cifradas no son más que archivos de poco peso que si se abren están cifrados.

A la hora de utilizar esas claves cifradas "solo cuando están dentro de los límites seguros del HSM, se descifra con la Module Key se utilizan". El secreto, asegura el ejecutivo de nCipher, "es que la clave nunca está en claro fuera del HSM".

"El hecho de que sólo hagamos HSM no quiere decir que esos HSM no se puedan poner en el cloud", dice José Pérez apuntando a otra de las ventajas que tiene la arquitectura de la compañía, cuyos clientes pueden acceder a esos HSM en modo servicio.

Vea aquí la intervención de nCipher en Arquitecturas de Seguridad, ¿qué ventajas ofrecen?