7 pasos para la implementación del teletrabajo en tu compañía de forma segura.

opencloud factory

opennac enterprise

Índice

Contexto:

Situación actual y postura de las compañías ante el teletrabajo

Si bien la modalidad de **Teletrabajo** ha sido una iniciativa que llevan adoptando algunas empresas en los últimos años como parte de su forma de trabajar, hasta el momento no se ha tratado ni mucho menos de una tendencia generalizada para el grueso de compañías: hasta el momento, en la mayoría de los casos, el teletrabajo ha sido abordado como una opción para mitigar algunos asuntos propios de la vida común de los empleados como bien pueden ser la movilidad, la falta de espacio en las oficinas, la mejora de la calidad de vida o una estrategia de atracción de talento por parte de la compañía mediante la flexibilización de la jornada laboral entre otros.

De acuerdo con la Encuesta a la Población Activa desarrollada por el Instituto Nacional de Estadística (INE) español, durante 2019, el **7'5%** de los empleados trabajaba en alguna ocasión en remoto. Tan sólo el **4'2%** de la población activa teletrabajaba de forma habitual, situándose así España a la cola de los países europeos en materia de teletrabajo. Por el contrario, los países escandinavos se sitúan a la cabeza en cuanto a teletrabajo, con un **37%** de sus trabajadores realizando tareas laborales desde sus hogares ocasionalmente.

No obstante, el año 2020 ha traído consigo desafíos para las empresas y la sociedad que, si bien algunas corporaciones no están completamente preparadas para abordar, sin duda van a marcar una tendencia al alza en los próximos meses y años: se producirá un interesante cambio de paradigma que posibilitará mantener el ritmo de producción de las compañías de forma remota a través del teletrabajo, siendo una opción común en las compañías y perfectamente compatible tanto con la continuidad del negocio como con la infraestructura tecnológica de las empresas.

ESPAÑA

7'5% Teletrabaja ocasionalmente

4,2% Teletrabajaba habitualmente

PAÍSES ESCANDINAVOS

37% Teletrabaja ocasionalmente

Esta nueva tendencia y forma de entender el día a día de las empresas traerá consigo un número considerable de desafíos a nivel de productividad, coordinación de tiempos y actividad entre los diferentes equipos, metodología de trabajo, entre otros. Desde Open Cloud Factory, nuestro objetivo para ayudar a las empresas a abordar este nuevo paradigma es el siguiente:

En un contexto en el que la superficie de exposición aumenta, es imprescindible gestionar el nivel de ciber riesgo de las compañías sin que la implementación del teletrabajo impacte en la seguridad de las mismas.

Pero, ¿cómo se logra esto?

Las compañías cuentan con unas medidas de ciberseguridad aplicadas dentro del perímetro de las redes corporativas, estas medidas tienen como objetivo mantener los niveles de riesgo en los niveles de aceptación definidos. El teletrabajo introduce un escenario que impacta los niveles de riesgo habituales, y es por ello por lo que las medidas de ciberseguridad deben ser trasladadas a las conexiones remotas, de manera que el teletrabajo no incremente los niveles de riesgo. Los empleados que ejerzan teletrabajo deben procurar no agregar factores de riesgo adicionales. La ejecución de las tareas laborales de forma remota debe alinearse con las directrices de ciberseguridad de las compañías, las cuales deben poner a disposición de los empleados las bases tecnológicas que les permita a los mismos realizar teletrabajo de manera segura, sin incrementar los niveles ciber-riesgo en el momento de ejecutar sus tareas en remoto. Todas las medidas e iniciativas de control de acceso al interior de las oficinas de las compañías deberán trasladarse y adaptase a un escenario de trabajo remoto, buscando gestionar el riesgo adicional generado por el incremento de la superficie de exposición.

7 pasos para implementar teletrabajo de forma segura

La mayoría de las medidas e iniciativas de seguridad para control de acceso aplicadas en las empresas aplican para la modalidad de teletrabajo. Sin embargo, algunos controles habituales se ven impactados por el teletrabajo, como es el caso por ejemplo del control de acceso físico. En la modalidad de teletrabajo no existe control de acceso físico a la compañía, la desaparición de este control impacta los valores de riesgo asociados a la validación de identidad de los empleados; por ello, la ausencia de este control debe compensarse con la implementación de un control adicional.

Las iniciativas de seguridad más conocidas en lo que se refiere al control de acceso en las redes corporativas modernas son las siguientes:

1. Principio del mínimo privilegio
2. Reducción la superficie de ataque
3. Zero trust
4. Posturing

Sumado a esto, cuando se habla de teletrabajo los desafíos a considerar con el objetivo de mantener los valores riesgo en sus rangos de aceptación, se sugieren las siguientes medidas:

5. Conexiones VPN
6. Doble factor de autenticación
7. Prohibición de usuarios genéricos

A continuación se detallara cada iniciativa de seguridad y su variación y adaptación de cara al teletrabajo.

1 Principio del Mínimo Privilegio

Cuando se aborda el principio del mínimo privilegio tenemos dos preguntas que resolver:

¿Quién accede? ¿A qué accede?

En primer lugar, se debe resolver de quién estamos hablando cuando queremos establecer los privilegios mínimos, es decir, validar su identidad. A continuación de acuerdo con su rol en la compañía, se definirán los permisos y a qué servicios se deberá otorgar el acceso a la persona en cuestión para el desempeño óptimo de sus funciones al interior de la compañía. De esta forma, las compañías darán a sus empleados únicamente los accesos imprescindibles para cada rol, ni uno mas ni uno menos. El principio del mínimo privilegio debe mantenerse con el teletrabajo.

El hecho de que los empleados realicen sus tareas laborales de forma remota no debería modificar sus accesos habituales: cada usuario deberá mantener sus permisos sin importar su ubicación y sin añadir o reducir permisos, esto se logra mediante una validad estricta de la identidad y la articulación de diferentes plataformas tecnológicas, cuyo propósito será la gestión de accesos asociado a las identidades, mas adelante se revisaran algunos controles que permiten un endurecimiento de los procesos de validación de identidades.

2 Reducción de la Superficie de ataque

La reducción de la superficie de ataque es una iniciativa de seguridad bien conocida y altamente difundida en las organizaciones modernas. La superficie de ataque considera 5 elementos principales:

- **End-point**
- **Aplicaciones y software**
- **Network**
- **Fisica**
- **Políticas y concienciación.**

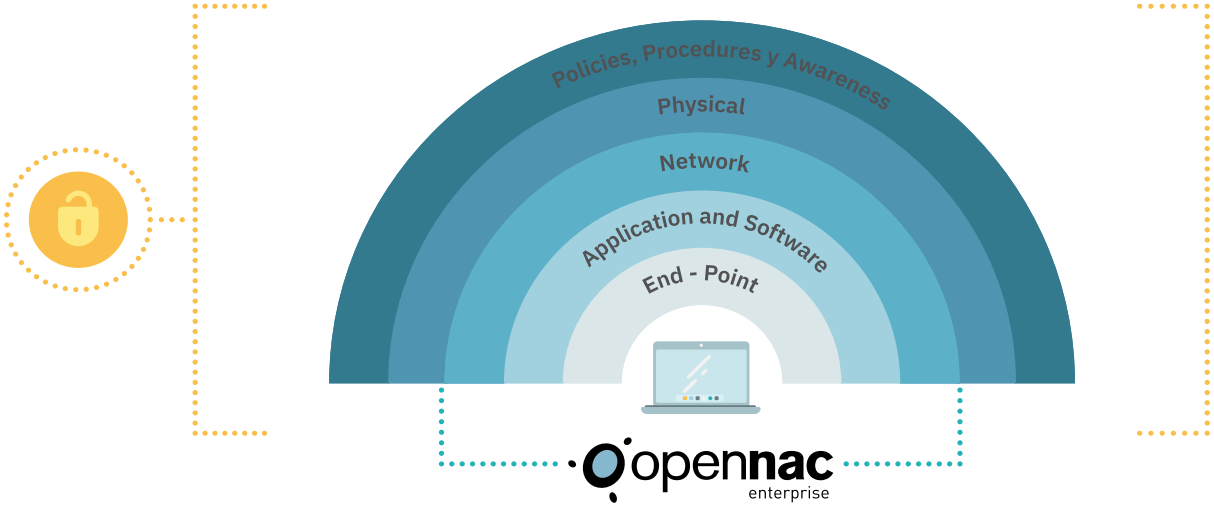
Cuando abordamos el tema de superficie de ataque en el teletrabajo tenemos que considerar el incremento de los niveles de riesgo en todos los elementos de la superficie de ataque. Por ello, las empresas tienen que dar respuesta e incrementar controles para cada caso. El nivel de riesgo agregado a los dos primeros elementos de la superficie de ataque (End-point y software) se encuentran direccionados bajo las iniciativas de principio del mínimo privilegio, Zero-trust y Posturing. El incremento de niveles de riesgo correspondientes al elemento físico de la superficie de ataque lo direccionamos por medio del control de doble factor de autenticación. El factor de riesgo impactado por el teletrabajo, asociado al elemento de políticas y concienciación, se debe gestionar por medio de los equipos de SI encargados de la definición y difusión de las políticas y concienciación de riesgo de cada compañía.
Para este caso, trataremos el incremento en el nivel de riesgo vinculado con el elemento red, para dar respuesta y gestionar oportunamente esta variación de nivel de riesgo en la superficie de red introducimos la segmentación de red y la implementación de conexiones tipo VPN que abordaremos mas adelante.

La segmentación de red consiste básicamente en dividir la superficie total de la red en segmentos de red aislados para mitigar tanto probabilidad como el impacto cuando se contempla la materialización de un riesgo cibernético. No obstante, para dividir una superficie en segmentos menores, se debe definir previamente una estrategia de segmentación de red que, además de ser sostenible, esté alineada con la operación y el día a día de las compañías. La estrategia de segmentación deberá considerar varios inputs, como por ejemplo:

- **El rol de las personas**
- **La tipología de los dispositivos**
- **El perfil de riesgo**
- **La localización de la conexión, entre otros.**

Como mínimo, la estrategia de segmentación, base del establecimiento de la iniciativa conocida como reducción de superficie de ataque, tiene un requisito fundamental que es validar la identidad de cada conexión que se realiza al interior de la red corporativa. Validando la identidad de las conexiones, se asignarán estratégicamente los segmentos de red pertinentes que agrupen activos con propósitos y características similares. Por ejemplo, un segmento que agrupe a todas los empleados del área financiera o todas las impresoras de la red. El hecho que los empleados de las compañías se conecten de forma remota, por definición, incrementa el elemento Red en la superficie de ataque, pero no debe variar el nivel de ciber-riesgo.

Los permisos de acceso asociados a los segmentos de red de los usuarios dentro de las oficinas de las empresas deben heredarse y ser iguales a los segmentos de red asignados a través de las conexiones remotas, en su defecto deben mantenerse los permisos de acceso otorgados y replicarse para el segmento de red usado por cada empleado durante el establecimiento de una conexión remota, es decir, cuando los empleados se encuentren en modalidad de teletrabajo. Este control junto con el uso de conexiones seguras, permitirá mantener el nivel de riesgo asociado a la red en la superficie de ataque y gestionar sus variaciones de manera segura.



3 Zero Trust

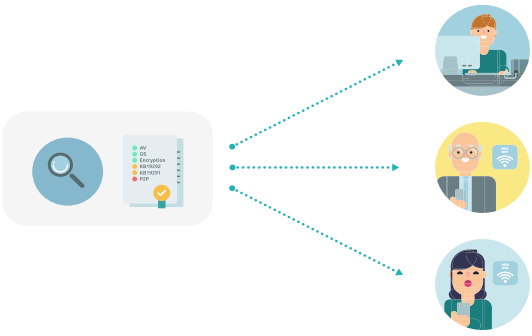
En la actualidad, la tendencia de la que se habla mayoritariamente en lo que se refiere a seguridad cibernética es el enfoque Zero Trust. Consiste principalmente en la validación indiscriminada de todos los accesos a todos los recursos y servicios de las redes corporativas, TODOS, incluidos los accesos provenientes de fuentes internas o "confiables". Se trata de desconfiar de todo, así que todo será sometido a procesos de validación y chequeo. Nuevamente, existe entonces bajo este enfoque una necesidad imperativa por validar la identidad de todas las conexiones realizadas en la red. Los procesos de validación de identidades tienen un nivel de rigurosidad que debe ajustarse para cada caso. Por ejemplo, las compañías bancarias en su mayoría implementan dos factores de autenticación para algunos procedimientos, como bien puede ser las transferencias, el segundo factor aplica generalmente para un usuario ya autenticado en la plataforma antes de confirmar una transacción; es decir, se desconfía incluso de los usuarios ya autenticados. Esto es una iniciativa Zero Trust.

Todas las iniciativas de autenticación y autorización deben mantenerse cuando los empleados de las compañías realizan teletrabajo; la validación de la identidad debe ser más rigurosa y los controles habituales que se encuentren ausentes cuando los usuarios realizan sus tareas de forma remota deberán reemplazarse por otros, todo ello con el objetivo de que los niveles de ciber-riesgo se mantengan.

4 Posturing

La masificación de dispositivos IoT es el argumento de mayor peso para que en la actualidad se considere imperativo que las conexiones de red permitan que los usuarios usen cualquier dispositivo para hacer uso de los servicios corporativos. Usar cualquier dispositivo no debería incrementar el riesgo de la conexión ligado al dispositivo. Esto se logra mediante una iniciativa conocida como posturing, en ocasiones compliance: consiste en la definición y aplicación de unos requerimientos mínimos de conexión tales como antivirus, antispyware, parches de sistema operativo o versiones mínimas de software, entre otros. Cada empresa deberá definir los requerimientos minimos de conexión para los usuarios, lo cual constituirá la postura de los dispositivos usados en la conexión. Una vez la conexión se intenta establecer, cada dispositivo será consultado por los requerimientos mínimos de conexión definidos y en caso de cumplimiento se otorgará el acceso, en caso contrario, será denegado y enviado a remediación.

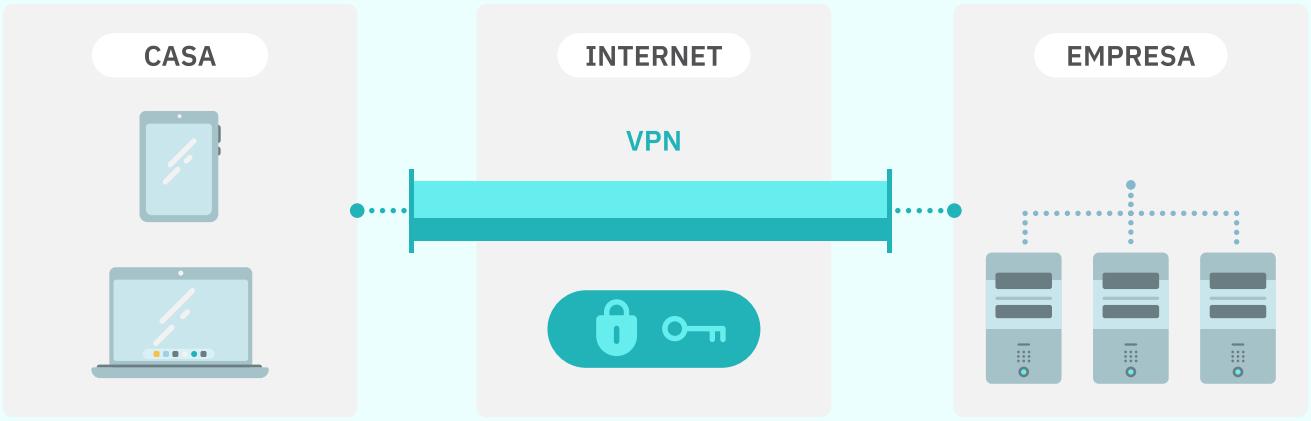
Cuando hablamos de teletrabajo existe un hecho muy recurrente, a menudo las empresas cuentan con equipos de mesa o laptops que los usuarios no llevan a casa para trabajar; generalmente, cuando se realiza teletrabajo, los empleados usan dispositivos propios, diferentes a los asignados por la organización para acceder a los recursos corporativos. Este hecho agrega un riesgo y es que el dispositivo personal usado en la conexión, no se encuentra configurado y podría no cumplir con los requerimientos minimos de conexión, la postura que se ha definido para los dispositivos corporativos.. Por esta razón, tras realizar la **validación de identidad,** se debe asegurar que el dispositivo usado para teletrabajo cumple con los requerimientos mínimos de conexión definidos por la organización, es decir se ajusta la postura definida para dispositivos corporativos. De este modo, sin importar desde qué dispositivo se realice la conexión de teletrabajo, se asegurará en primer lugar la identidad del usuario, para posteriormente asegurar el cumplimiento del dispositivo usado en la conexión.



5 VPN Client to Site

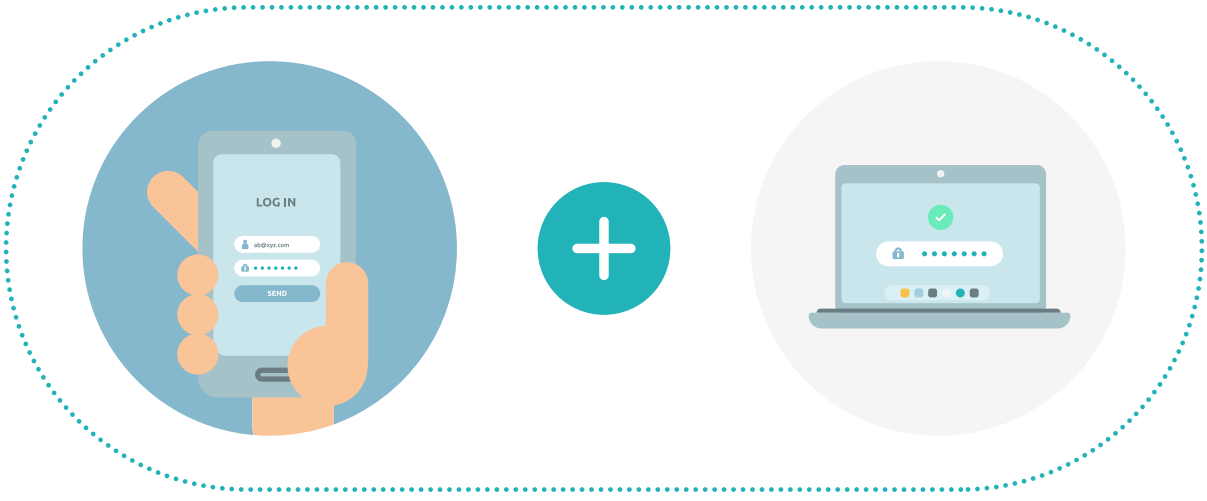
La infraestructura tecnológica base del teletrabajo son las VPN. Se basan en el establecimiento de una red privada de forma virtual; la conexión se establece desde la ubicación remota sobre infraestructura publica (un proveedor regular de internet en el hogar) y termina en un concentrador VPN corporativo. El tráfico intercambiado se asegura por medio de algoritmos de cifrado. De esta manera por más que la conexión se establezca remotamente, a través del cifrado, se logra una red privada virtual sobre una infraestructura publica que blinda la conexión, brindando confidencialidad, integridad y disponibilidad de la información intercambiada.

Todas las medidas de seguridad tomadas para mantener bajos los niveles de riesgo en teletrabajo y en general en conexiones remotas se logran a partir del establecimiento de conexiones de tipo VPN.



6 Doble Factor de Autenticación

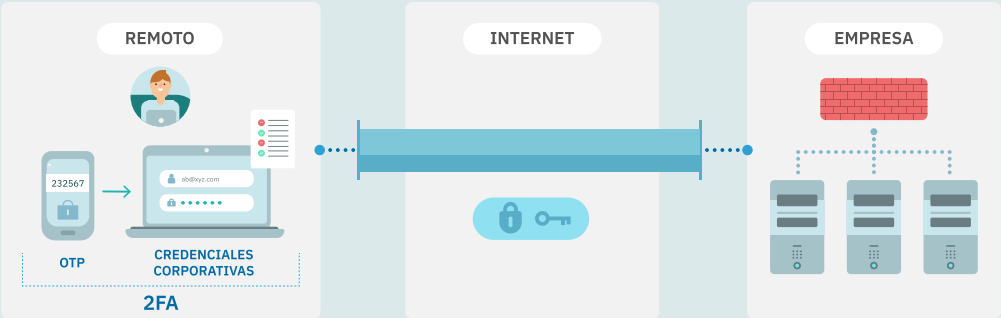
Cuando se habla de conexiones remotas existe un control tradicional que desaparece, el control de acceso físico, este hecho incrementa los niveles de riesgo, es por eso que debemos agregar un control adicional en aras de compensar y mantener los niveles de riesgo habituales. Cuando los empleados se desplazan a su lugar de trabajo, estos tienen en su mayoría que superar un control de acceso físico a las instalaciones de la compañía, esto se logra mediante una tarjeta, una llave, huella, etc. En el teletrabajo es imperativo validar la identidad de quién esta detrás del dispositivo a través del cual se quiere lograr el acceso, si bien las compañías confían en métodos tradicionales de autenticación como lo son, por ejemplo, las credenciales de usuario. Esta situación, ha generado un escenario de debilidad y amenaza para las empresas, ya que el conocimiento de unas credenciales no siempre demuestra la identidad de un usuario, este hecho sumado a la desaparición del control de acceso físico presente un escenario de vulnerabilidad. Se debe entonces implementar un control que permita la **validación de identidades** no solo a través de lo que se sabe (usuario y contraseña), sino también a través de algo que se tiene, por ejemplo, un teléfono móvil. El segundo factor podría ser entonces la validación del numero de móvil asociado a la identidad del usuario, eb consecuencia estamos hablado de la implementación de un segundo factor de autenticación. Este hecho incrementa de manera sustancial la seguridad de una conexión remota, como las que se realizan para el teletrabajo a través de conexiones VPN.



7 Prohibir usuarios genéricos

En redes corporativas es muy común la mala práctica de usuarios genéricos para algunas tareas. Por ejemplo, para pruebas, para agilizar una solicitud o para soporte, entre otros. Esta mala práctica si bien soluciona de manera momentánea un requerimiento de acceso, agrega nuevos riesgos e incrementa los valores de los riesgos ya identificados. El uso e implementación de usuarios genéricos en aplicaciones e infraestructura de red va en contra de todas las iniciativas enfocadas a la validación de identidades. Entendiendo la validación de identidades clave para establecimiento de: mínimo privilegio, zero trust, reducción de superficie de ataque. Los usuarios genéricos deben prohibirse y depurarse de toda la infraestructura de redes y servicios de las empresas.

La Solución: **Acceso remoto seguro con doble factor de autenticación. 2SRA Secure Remote Access**



Para el acceso remoto seguro, el módulo de 2SRA actúa como frontend para la finalización de túneles VPN con los clientes, mediante un agente (para dispositivos corporativos y no corporativos). **OpenNAC Enterprise** realiza la autenticación, autorización y auditoría contra el gestor de identidades corporativas del Organismo (Active Directory (AD), LDAP...) y permite añadir un segundo factor de autenticación (OTP), de esta forma mitiga el riesgo de suplantación de identidad (uso de credenciales robados por parte de un atacante para acceder a la red). Se recoge el inventario y perfilado completo del equipo. Este perfilado se podrá utilizar en las políticas de acceso a la conexión remota. Adicionalmente, permite definir y aplicar políticas de acceso en función de una postura de seguridad, además de otros factores (horario de la conexión, características del equipo, role de usuario etc.). Permite así una conexión segura y verificada de manera robusta entre el usuario y los sistemas corporativos.

Beneficios principales de 2SRA Secure Remote Access

1. **Favorece el principio del mínimo privilegio:** los usuarios sólo acceden a la información y recursos imprescindibles para el desempeño de su actividad.
2. **Favorece el enfoque Zero Trust:** establece un marco de seguridad corporativa en el que sólo usuarios y dispositivos autenticados y autorizados pueden acceder a la información corporativa.
3. **Ejerce controles de aseguramiento para superficie de ataque:** asegura la conexión remota mediante cifrado y los dispositivos de usuario.
4. **Reduce el riesgo asociado al dispositivo de usuario:** permite la evaluación de postura de dispositivos, estableciendo el cumplimiento de los requisitos mínimos de conexión a la hora de acceder a la red.
5. **Mitiga el riesgo de suplantación de identidad:** añade un nivel de seguridad extra mediante doble factor de autenticación.

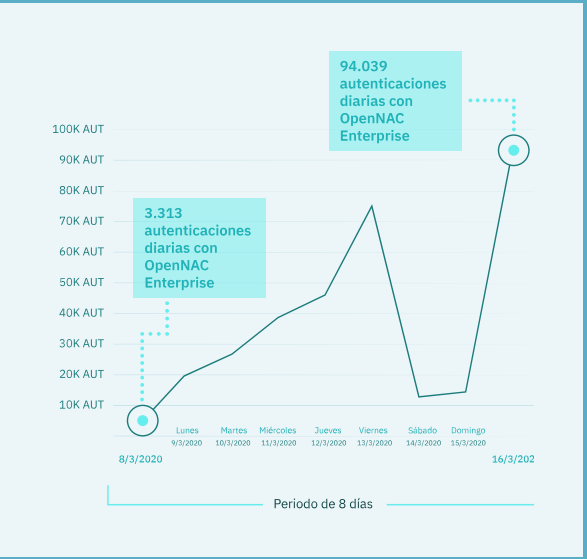
Caso de éxito real de teletrabajo en la situación actual por parte de uno de nuestros clientes con 2FA de OpenNAC Enterprise

Una de las multinacionales más importantes de España, que confía en Open Cloud Factory y en su solución **OpenNAC Enterprise** desde 2018, tiene implementado desde esa fecha un módulo de **OpenNAC Enterprise** para doble factor de autenticación (2FA) de usuarios VPN, el cual ha sido de extrema utilidad y de vital importancia para ellos en un contexto de crisis internacional y necesidad de habilitación por emergencia del teletrabajo como modalidad laboral para sus empleados. Nuestro cliente ha pasado de registrar un promedio de 3.500 autenticaciones diarias por medio del 2FA de **OpenNAC Enterprise**a un pico de 94.030 autenticaciones diarias por parte de los usuarios de la red interna en tan sólo 8 días. Esto presenta dos claras lecturas acerca del doble factor de autenticación de la solución: por parte del cliente, ha sido crucial a la hora de servir como medida de anticipación en su plan de continuidad del negocio (BCP) en una situación de crisis. Desde la perspectiva de la herramienta, se ha traducido en un caso de éxito a través de su excelente desempeño, superando pruebas de estrés y mostrando su característica de escalabilidad en esta situación de teletrabajo.

OpenNAC Enterprise ayuda a las empresas en el establecimiento de las 7 medidas de seguridad de esta Guía.

OpenNAC Enterprise es la única solución modular de visibilidad y control de acceso para redes corporativas ayuda a las empresas al establecimiento de las 7 medidas de seguridad propuestas anteriormente para mantener los niveles de riesgo en los umbrales de aceptación definidos previo a la implementación del teletrabajo.

El enfoque modular permite principalmente una reducción de costes de implementación, procesos de despliegue más rápidos y sencillos previniendo el impacto en entornos productivos durante la implantación.



Solución ante la problemática para organismos públicos: EMMA

EMMA es una solución del Centro Criptológico Nacional (CCN-CERT) encargada de la vigilancia de deficiencias en la capa de acceso y electrónica (cumplimiento), conectividad a la red (visibilidad), capacidad de respuesta ante eventos (respuesta) y acceso remoto seguro.Para más información acerca de Emma: **https://www.ccn-cert.cni.es/soluciones-seguridad/emma.html**

opencloud factory

Reconocimientos

Gartner

Único fabricante europeo de tecnología NAC incluido en Gartner Market Guide.

Common Criteria

Plataforma certificada en Common Criteria 3.1 release 5 por parte del Organismo de Certificación del Centro Criptológico Nacional OC-CCN de España.

CCN-CERT centro criptológico nacional

Incluido en el catálogo de productos de Seguridad de las Tecnologías de la información y la comunicación del Centro Criptológico Nacional, Ministerio de Defensa - Gobierno de España.

Contacta con nosotros

opencloudfactory.com

+34 91 614 53 22

Twitter
Linkedin
YouTube

Ubicaciones de Open Cloud Factory

SPAIN

MADRID.
Sede principal
Calle Segundo Mata,
6 Planta 1 Oficina 4B
Pozuelo de Alarcón, 28224

SPAIN

BILBAO.
OCF Industrial Cybersecurity
C/ Gran Vía Don Diego López
De Haro, 19-21 planta 2ª
48001

SPAIN

BARCELONA.
Centro de Desarrollo
Carrer Sant Leopold 101,
oficina 109, Terrassa,
08221

BRAZIL

SÃO PAULO.
Market Place Tower.
Av. Dr. Chucri Zaidan, 920
9º andar Cordeiro,
CEP: 04583-904

USA

BOSTON, MASSACHUSETTS.
Independence Wharf 470
Atlantic Avenue
02210

MEXICO

CIUDAD DE MÉXICO.
Presidente Masaryk 111
Piso 1, Miguel Hidalgo
Polanco V Sección
11560

opennac enterprise