



ACCESO REMOTO EN LA MANUFACTURA:

**Preocupaciones, Retos,
y Orientación en 2024**

El sector de Manufactura es una bestia única desde el punto de vista tecnológico; los entornos de tecnología de la información (TI) y de tecnología operativa (TO), igualmente importantes, por sí solos la diferencian enormemente de casi cualquier otra industria. Y luego está la necesidad de dar soporte, seguridad y acceso a esos entornos, lo que aumenta la complejidad; la disparidad de dispositivos, sistemas operativos y protocolos de comunicación sólo hace que mantener operativa una empresa de Manufactura sea mucho más difícil.

Las soluciones de Acceso Remoto han facilitado enormemente la labor de los equipos de TI, TO y seguridad en casi todos los aspectos de su trabajo, desde la asistencia a los empleados hasta el acceso a servidores y dispositivos de red dentro del entorno de TI, pasando por el acceso a dispositivos TO. El usuario habitual también se beneficia del Acceso Remoto, ya que le permite ser productivo, ya sea accediendo al sistema interno a trabajadores remotos o realizando tareas de proceso como transferir archivos de forma segura.

Dado el entorno único de TI/TO en las organizaciones de Manufactura, la solución de Acceso Remoto elegida tiene la capacidad única de afectar materialmente al estado de seguridad y productividad de una organización -positiva o negativamente-, a la vez que repercute en los resultados finales.

En este documento, analizaremos si el Acceso Remoto satisface las necesidades de la industria manufacturera, dónde se encuentran los desafíos y qué pueden hacer las organizaciones manufactureras para mejorar su estado actual de seguridad y productividad mediante el uso de soluciones de Acceso Remoto.

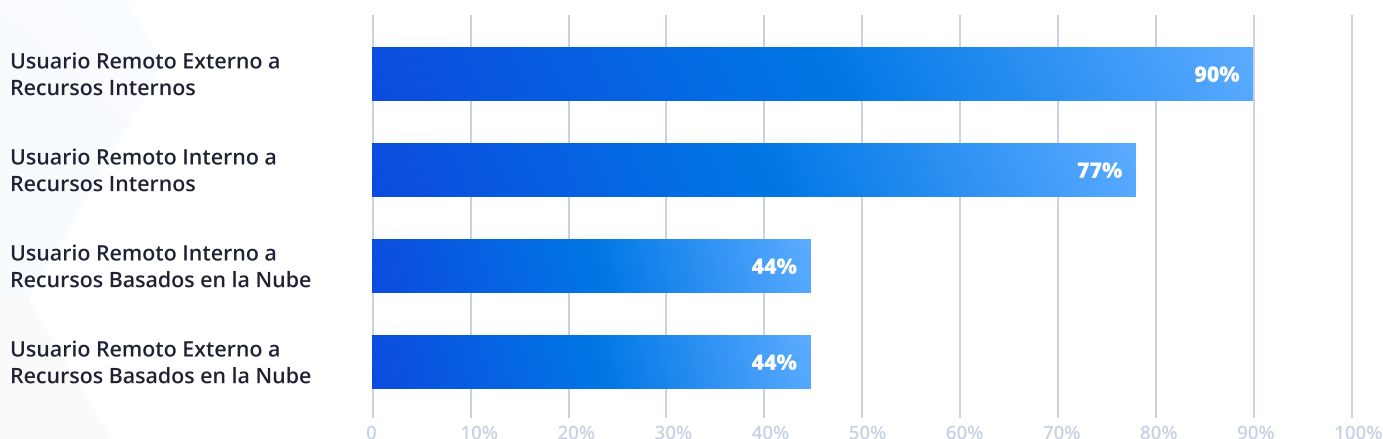
Para proporcionar contexto, hemos encuestado a más de 450 miembros de TI, desde analistas de asistencia técnica hasta ejecutivos de TI, del sector de la Manufactura para comprender mejor cómo utilizan las organizaciones el Acceso Remoto, cuáles son las principales preocupaciones generales y cómo se puede mejorar el uso del Acceso Remoto para superar los retos actuales. Comencemos con una breve descripción de cómo la industria utiliza el Acceso Remoto.

EL USO DEL ACCESO REMOTO EN EL SECTOR DE MANUFACTURA

Una parte del funcionamiento de cada organización de Manufactura no es diferente de las organizaciones de cualquier otra industria vertical en la que se utilizan regularmente soluciones de Acceso Remoto. Según nuestro informe State of Remote Access Security (Estado de la seguridad del Acceso Remoto), publicado recientemente, en el 73% de las empresas manufactureras, las soluciones de Acceso Remoto son utilizadas por el departamento de TI y, en el 68% de ellas, también las utilizan usuarios normales ajenos al departamento de TI.

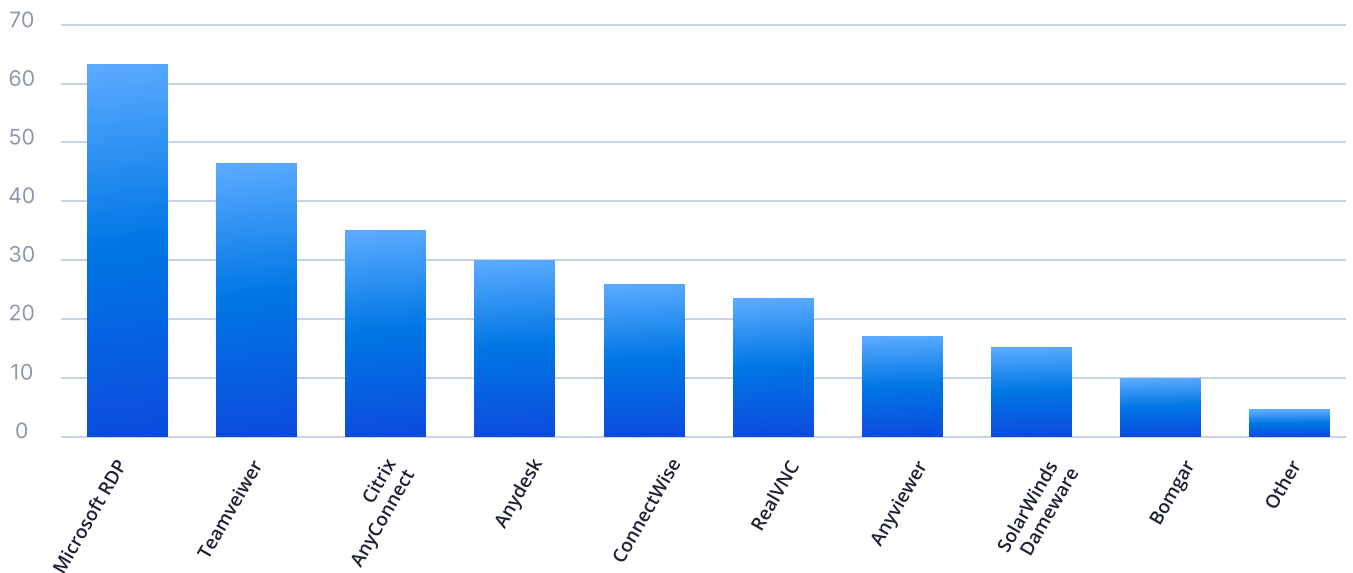
Cuando se profundiza un poco más en los datos del mismo informe (como se muestra a continuación), el 90% de las organizaciones de Manufactura

utilizan el Acceso Remoto para proporcionar a los usuarios remotos externos acceso a los recursos internos -esto es muy superior a la media del 74% en todos los sectores. Algo más de tres cuartas partes (77%) de ellas también utilizan el Acceso Remoto para proporcionar a los usuarios remotos internos acceso a los recursos internos, lo que coincide con la media general. El uso del Acceso Remoto en la industria manufacturera para conectar usuarios a la nube es mucho menor (44% de las organizaciones) que la media (un 57% de las organizaciones). Una explicación podría ser el uso de acceso directo para conectarse a varios equipos, permitiendo que los datos permanezcan en la red de la organización.



¿QUÉ SOLUCIONES SE UTILIZAN?

Luego está la cuestión de qué soluciones de Acceso Remoto se están utilizando. Según la encuesta, las empresas manufactureras utilizan una media de algo menos de tres soluciones diferentes. El siguiente gráfico resume el porcentaje de organizaciones que utilizan una solución específica de Acceso Remoto:



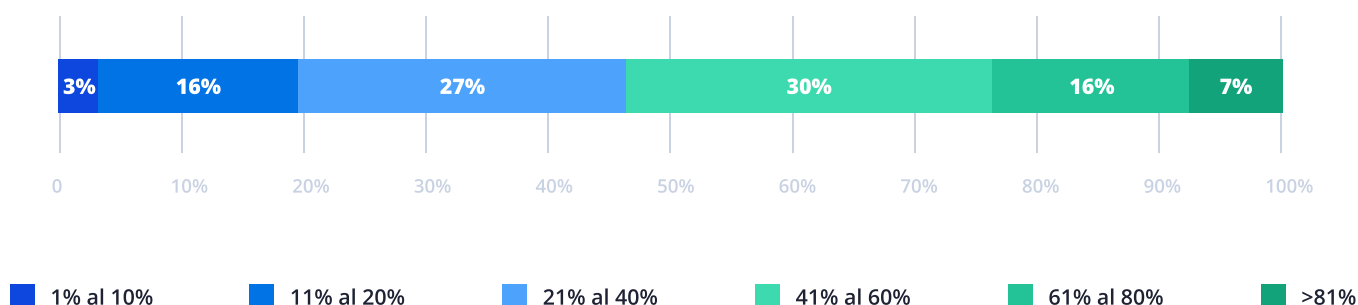
"...Las empresas manufactureras utilizan una media de algo menos de tres soluciones diferentes."



EL USO DEL ACCESO REMOTO POR PARTE DE TI

Centrémonos momentáneamente en el uso del Acceso Remoto por parte de TI en la Manufacturación. Según nuestra encuesta más reciente sobre TI en el sector de Manufactura, el departamento de TI utiliza el Acceso Remoto una media del 42% del tiempo para realizar su trabajo, con el desglose de uso que se muestra a continuación.

¿Con qué frecuencia utilizan usted y sus compañeros de TI la tecnología de Acceso Remoto como parte de las tareas y responsabilidades generales de su trabajo?



Y según los encuestados, esta dependencia del Acceso Remoto aumentará una media del 26% en 2024. Descubrimos que TI utiliza el Acceso Remoto para cuatro casos de uso principales:

- Acceso Remoto a servidores y dispositivos de red
- Acceso Remoto al escritorio de los dispositivos de los empleados
- Supervisión remota del mantenimiento de los equipos de Manufactura
- Acceso Remoto a dispositivos y equipos de Manufactura

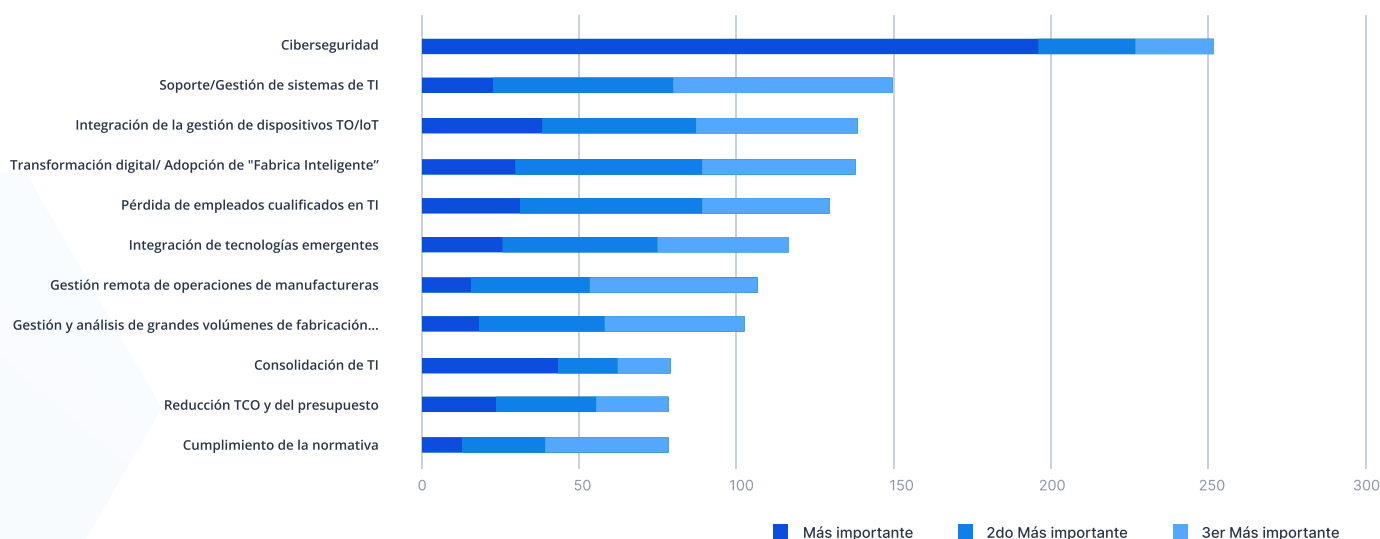
Con el Acceso Remoto desempeñando un papel tan crítico en lo que resultará siendo más de la mitad del tiempo que los informáticos dediquen a realizar su trabajo en 2024, las organizaciones deberían plantearse cómo el Acceso Remoto debería ser algo más que una herramienta utilizada para acceder a los servidores remotos, en lugar de una herramienta que desempeñe un papel clave en la forma en que las organizaciones resuelven sus principales retos informáticos.

LOS MAYORES RETOS DE TI/TO EN EL SECTOR DE MANUFACTURA

Si bien las TI dentro de una organización de Manufactura tienen muchas prioridades similares a las de otros sectores verticales de la industria, existe una dinámica completamente diferente para cada desafío que se enfrenta debido a la adición de entornos de TO (tecnología operativa). En nuestra reciente encuesta pedimos a las organizaciones que clasificaran los 3 problemas tecnológicos más

importantes a los que se enfrentan en la Manufactura. Como se muestra a continuación, la ciberseguridad fue la principal prioridad; el soporte y la gestión continua de los sistemas de TI ocuparon el segundo lugar; y la integración de la gestión de dispositivos especializados, dispositivos IoT y sensores que controlan los equipos de Manufactura ocupó el tercer lugar.

¿Cuáles son los problemas generales de TI, TO y tecnología más críticos a los que se enfrentará la industria manufacturera en 2024?



Dado que el Acceso Remoto puede tener un impacto material en el estado de la ciberseguridad de una organización y en la productividad de TI debido al amplio uso del Acceso Remoto en la Manufactura, es vital encontrar formas de garantizar que el Acceso Remoto mejore realmente

la seguridad y las operaciones de una organización. Así pues, echemos un vistazo a los 3 problemas generales de TI, TO y tecnología más críticos a los que se enfrentará la industria manufacturera en 2024 y veamos cómo el Acceso Remoto puede ayudar a formar parte de la solución.

CIBERSEGURIDAD

No cabe duda de que ésta debería ser la principal preocupación de la industria. Tomemos como ejemplo el ataque de ransomware dirigido al fabricante estadounidense Johnson Controls, con sede en EE. UU. y valorado en \$25 billones de dólares, que produce equipos contra incendios, de climatización (HVAC) y de seguridad para edificios. El ataque de 2023 pedía un rescate de \$51 millones de dólares y, una vez detectado, la empresa tardó casi dos meses en solucionarlo, lo que afectó a sus operaciones y a sus declaraciones públicas a los accionistas.

Debido a la combinación de TI y TO, ataques como el que sufrió Johnson Controls pueden dejar a las empresas manufactureras fuera del negocio o, como mínimo, en un mundo de perjuicios financieros. En nuestra encuesta, casi la mitad de las organizaciones respondieron con esta preocupación en el puesto número 1, eclipsando cualquier otra preocupación hasta en una proporción de 13:1. Y con razón, ya que la industria es un objetivo muy popular de los ciberataques:

El ataque de 2023 pedía un rescate de \$51 millones de dólares y, una vez detectado, la empresa tardó casi dos meses en solucionarlo, lo que afectó a sus operaciones y a sus declaraciones públicas a los accionistas.

- En Norteamérica y Europa, la industria manufacturera es la segunda más afectada¹.
- Dentro de los sectores que soportan TO, el sector manufacturero es el más atacado¹.
- De todos los ataques de ransomware en 2023, el sector manufacturero fue el más atacado².

El 44% de las organizaciones del sector manufacturero se enfrentaron al menos a un ciberataque en los últimos 12 meses, y el 19% de las organizaciones sufrieron 10 o más³.

La presencia de soluciones de Acceso Remoto crea riesgos para la organización. Esto se debe a que el Acceso Remoto tiene el potencial de facilitar el acceso inicial de una amenaza remota al entorno de TI y también puede utilizarse para el movimiento lateral a los sistemas y dispositivos de TI y TO.

La preocupación por el estado de la ciberseguridad de la organización -y el papel que desempeña el Acceso Remoto- fue un tema que resonó en todas las respuestas a nuestra encuesta. La principal preocupación que tienen las organizaciones con su solución o soluciones de Acceso Remoto existentes es la solución de seguridad para el 59% de las organizaciones.

¹ IBM Security X-Force, Índice de inteligencia sobre amenazas (2023)

² Guidepoint Security, Informe sobre ransomware del tercer trimestre de 2023 (2023)

³ RealVNC, Informe sobre el estado de la seguridad del Acceso Remoto (2023)

CIBERSEGURIDAD CONTINUADO

En nuestro informe [State of Remote Access Security](#), preguntamos si se utilizaba alguno de los siguientes siete controles de seguridad:

- *Autenticación contra AD, vía RADIUS, TACACS, etc.*
- *Autenticación Multifactor (MFA)*
- *Control de acceso basado en políticas*
- *Mínimo privilegio / Confianza cero*
- *Cifrado de sesión*
- *Auditoría de sesión*
- *Inicio de sesión único*

Por término medio, las organizaciones de Manufactura utilizan entre dos y tres controles de seguridad, siendo los más populares la MFA (utilizada por el 67% de las organizaciones), el cifrado de sesiones (54%) y el inicio de sesión único (48%).

Entonces, ¿cómo puede el Acceso Remoto mejorar la ciberseguridad de la organización?



MEJORAR LA CIBERSEGURIDAD CON EL ACCESO REMOTO

Consideremos los dos usos indebidos más comunes del Acceso Remoto en los ciberataques que se han mencionado anteriormente: el acceso inicial y el movimiento lateral. Para ayudar a mitigar el riesgo de uso indebido para cualquiera de estas acciones de amenaza a través de sus soluciones de Acceso Remoto, considere las siguientes recomendaciones:

Haga de la seguridad una prioridad de las soluciones de Acceso Remoto

El 41% de las organizaciones de Manufactura ni siquiera eligieron la solución de seguridad como punto fuerte de su solución actual, centrándose más en la facilidad de uso y la velocidad/rendimiento. Si su organización se encuentra en ese 41 %, es hora de que se dé cuenta de que la solución de seguridad de Acceso Remoto es tan crítica (si no más) como su gran funcionalidad. De lo contrario, todo lo que tiene es una solución fantástica que probablemente proporcionará a los actores de amenazas un acceso relativamente fácil a su red.

Únase a la multitud de MFA

Si todavía se encuentra en ese tercio de organizaciones que no tienen implementada la autenticación multifactor para que todos los inicios

de sesión de Acceso Remoto requieran un segundo método de autenticación, es hora de que se una a él.

Implemente más controles de seguridad

A medida que la solución o soluciones de que disponga se lo permitan, considere la posibilidad de poner controles adicionales para garantizar una mejor autenticación inicial, controlar mejor el acceso y el uso de una sesión remota y proporcionar una mejor supervisión y responsabilidad en el uso de la sesión remota.

Preocúpese por RDP

Algo más de dos tercios de la industria manufacturera sigue utilizando RDP. ¡RDP! Ya sabes... ¡ese protocolo que a los ciberdelincuentes les ENCANTA aprovechar para el acceso inicial y el movimiento lateral! Debería considerar seriamente eliminarlo por completo en favor de otra solución de Acceso Remoto con sólidos controles de seguridad.

MEJORAR LA CIBERSEGURIDAD CON EL ACCESO REMOTO

Consolidar las soluciones de Acceso Remoto

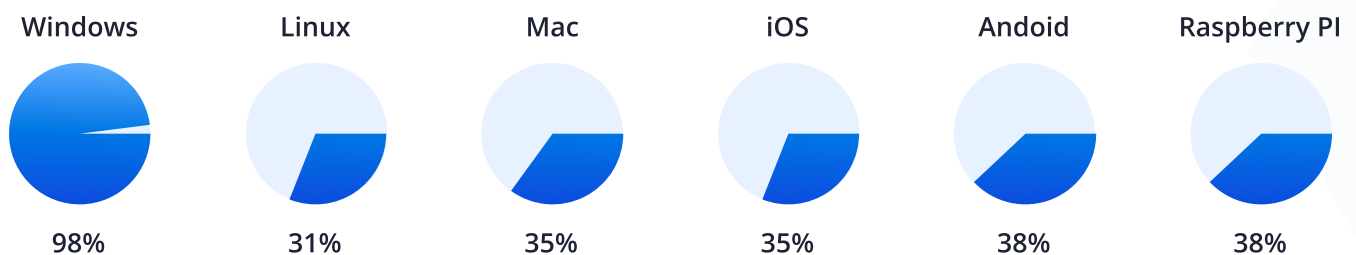
Ya es bastante difícil asegurar una única solución. Pero imagínese que quiere establecer una "Política de Seguridad de Acceso Remoto" en la que cada solución debe tener un conjunto mínimo de controles de seguridad. Es muy poco probable que las tres soluciones tengan las mismas características de seguridad y funcionalidad. Y luego está la implementación y la administración continua - ambas hechas tres veces. Hágale un favor a la organización - si se toma en serio la postura de soluciones de ciberseguridad de Acceso Remoto, encuentre la más segura y utilícela en toda la empresa. Esto permitirá una política coherente, una mayor visibilidad y un mejor control.



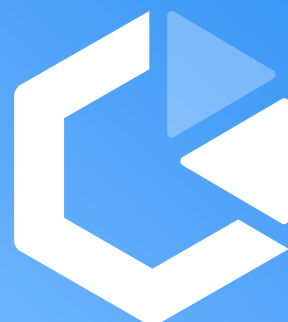
APOYO & GESTIÓN DE SISTEMAS DE TI

Los informáticos necesitan una solución de Acceso Remoto que les haga ser productivos, que les proporcione rápidamente una conexión fiable a un sistema remoto y les proporcione las herramientas necesarias para realizar el trabajo que tienen entre manos. Y, sin embargo, si tenemos en cuenta que la media de soluciones utilizadas es de tres, es un claro indicador de que cualquier solución de Acceso Remoto no satisface la necesidad.

Una de las razones más probables por las que se utilizan tantas soluciones es la mezcla dispareja de sistemas operativos que TI necesita conectar para realizar su trabajo. Según los datos de la encuesta, el principal uso del Acceso Remoto fue para acceder de forma remota a servidores y dispositivos de red, y el segundo uso más frecuente fue para acceder de forma remota a los escritorios de los dispositivos de los empleados. De nuestro informe State of Remote Access Security se desprende que, efectivamente, la industria necesita acceder a distancia a una amplia gama de sistemas operativos:



Uno de los principales puntos débiles de la solución de Acceso Remoto utilizada actualmente por las organizaciones de Manufactura que se planteó en repetidas ocasiones fue la falta de amplitud de plataformas y compatibilidad de dispositivos, lo que indica una necesidad continua de ampliar los sistemas operativos y dispositivos compatibles con las soluciones de Acceso Remoto.



MEJORA DE LOS SISTEMAS DE TI SOPORTE Y GESTIÓN CON EL ACCESO REMOTO

Para que las soluciones de Acceso Remoto mejoren la productividad de TI en el contexto del soporte y la gestión, tenga en cuenta las siguientes recomendaciones:

EMPEZAR CON LAS NECESIDADES DE TI Y TRABAJAR HACIA ATRÁS PARA ENCONTRAR UNA SOLUCIÓN

Muy a menudo, el departamento de TI empieza con una tecnología muy interesante y luego intenta simplemente "hacerla funcionar" con todas sus ineficiencias y defectos. Dado que tiene que dar soporte a unos sistemas de TI muy específicos, es fundamental empezar por las necesidades técnicas (por ejemplo, qué plataformas utiliza hoy y piensa utilizar mañana) y trabajar para encontrar una solución que satisfaga la necesidad.

DARSE CUENTA DE QUE HABRÁ LIMITACIONES DE SO

No todos los sistemas operativos pueden permitir que las soluciones de Acceso Remoto tengan todas las capacidades, como control remoto, transferencia de archivos, grabación de sesiones y más. No se trata necesariamente de un problema

con la solución del Acceso Remoto, sino de una limitación del sistema operativo SO.

CONSOLIDAR LAS SOLUCIONES DE ACCESO REMOTO

Los informáticos siempre encontrarán la manera de trabajar con varias soluciones... si es necesario. Pero la realidad es que - en un mundo perfecto - todos los profesionales de TI utilizarían una única consola con visibilidad completa de todos los dispositivos a los que pueden acceder de forma remota. Esto elimina cualquier necesidad de aprender "otra" solución, preocuparse por el acceso adecuado para garantizar una sesión de soporte productiva, y poner un conjunto coherente de herramientas (salvo las limitadas por el anfitrión SO) en manos de TI.





INTEGRANDO LA GESTIÓN DE DISPOSITIVOS TO & IOT

"Si las TI se salieran con la suya, la gestión de los sistemas de TI y TO seguiría prácticamente los mismos pasos utilizando las mismas herramientas. Puede que sea necesario separar los dos entornos en redes lógicamente diferentes por motivos de seguridad o rendimiento. Aun así, al profesional de TI responsable de ayudar con un problema de TO le encantaría simplemente gestionarlo de la misma manera que lo hace con un sistema de TI.

Pero hoy en día, según los datos de la encuesta, no es el caso.

La segunda necesidad más crítica en 2024 para las soluciones de Acceso Remoto dentro de la Manufactura es dar soporte a un número nuevo/aumentado de equipos y dispositivos de fabricación. Y es razonable incluir los retos de Acceso Remoto de la encuesta, como la gestión de operaciones de Manufactura remotas y la integración de tecnologías emergentes, en este reto de integración, que es aún más importante abordar.

"Los dispositivos TO y IoT seguirán construyéndose (en un futuro previsible) en el vacío (es decir, sin tener en cuenta cómo se supone que debe gestionarlos la organización de Manufactura... y todos los demás dispositivos construidos con la misma falta de consideración). La buena noticia es que los sistemas operativos como Windows y Linux se utilizan ampliamente en la Manufactura, por lo que el Acceso Remoto robusto es un hecho. A pesar de que muchos proveedores compiten por el dominio del SO/plataforma en el mundo de la IoT, los ordenadores de placa única como Raspberry Pi se utilizan para una amplia gama de sensores y gestión.

Mientras los proveedores que apoyan las necesidades de la Manufactura sigan por este camino, el mundo de la Manufactura estará cada vez más cerca de un entorno en el que la gestión de estos dispositivos sea casi homogénea. "



MEJORAR LA GESTIÓN DE DISPOSITIVOS TO & IOT CON ACCESO REMOTO

Aunque este último reto va a ser el más difícil de mejorar a través del Acceso Remoto, todavía hay algunas recomendaciones:

1. Incluir la capacidad de gestión del Acceso

Remoto al considerar los dispositivos – Esto no se resuelve mediante una solución o función específica de Acceso Remoto. En su lugar, se trata de poner el Acceso Remoto al mismo nivel de importancia que la funcionalidad del dispositivo TO o IoT. Cuando se trata de encontrar un dispositivo IoT que controle la presión en un sistema hidráulico, las consideraciones deben ir más allá de "¿Puede controlar el sistema que tenemos?" e incluir preguntas como "¿Podemos acceder a él y gestionarlo fácilmente?". Claro, es fácil decirlo ya que TI no siempre forma parte de la conversación, pero elevar la discusión a su CISO o CTO para, a su vez, llevar el tema a la junta puede ser todo lo que se necesita para asegurarse de que TI está incluido en el proceso

de selección para asegurarse de que el dispositivo puede ser soportado.

2. Garantizar que el Acceso Remoto vea la TO/IoT como si fuera infraestructura

- Una cosa es ver, por ejemplo, todos los escritorios Windows de la organización desde una solución de Acceso Remoto, pero es igualmente esencial poder tener visibilidad de todos los dispositivos gestionados de forma organizada. Con la posibilidad de que haya miles de sensores, se espera que el departamento de TI sea capaz de dar soporte a un dispositivo en poco tiempo - lo que significa que la solución de Acceso Remoto no sólo proporciona la capacidad de conectarse al dispositivo de forma remota, sino que lo encuentra rápidamente, determina su estado actual y puede enviarle comandos, todo ello sin necesidad de establecer una sesión remota.

ACCESO REMOTO: UNA DE LAS CLAVES PARA MEJORAR LAS OPERACIONES DE MANUFACTURA

Es probable que los departamentos de TI de las empresas manufactureras se enfrenten a más retos que una empresa de tamaño equivalente de otro sector sin ningún tipo de TO. Por ello, los departamentos de TI -además de ocuparse de todo lo relacionado con TI, como cualquier otra organización- necesitan una ventaja para mejorar la seguridad de su organización, facilitar el soporte y la gestión de TI, y hacer que el soporte y la gestión de TO funcionen y se sientan muy parecidos a cuando se trabaja en TI.

Hay muy pocos tipos de soluciones que combinen TI y TO. El Acceso Remoto es una de ellas. Por lo tanto, tiene sentido que las organizaciones de Manufactura busquen formas de garantizar mejor la seguridad de las sesiones remotas. Todo esto, mientras encuentran formas de aprovechar las soluciones de Acceso Remoto que implementan para satisfacer las necesidades de ambos entornos de TI y TO.

Utilizando los datos que se encuentran en este documento técnico como contexto potencial para su organización y siguiendo las recomendaciones que se incluyen en él, se crea una oportunidad para hacer la vida de TI más accesible, las operaciones de la organización más productivas y la propia organización más segura.





INVIRTIENDO EN EL FUTURO

Esta encuesta demuestra que las manufactureras se enfrentan a importantes desafíos en 2024 y más allá. Los participantes en la encuesta informaron de que los principales retos que esperan este año incluyen la gestión de dispositivos TO e ICS, seguir apoyando la transformación digital y garantizar la seguridad de la red. Seleccionar un proveedor de Acceso Remoto que pueda hacer frente a estos retos será fundamental para su estrategia de TI.

RealVNC ha demostrado tener un historial soportando a las manufactureras con sus necesidades de TI, incluyendo:

- **Garantizando la privacidad y seguridad de los datos:** RealVNC puede ayudar a mejorar la seguridad con la única solución de Acceso Remoto con certificación de "auditoría de caja blanca". RealVNC es la solución más centrada en la seguridad, con cifrado AES y túnel SSH de eficacia probada.
- **Reducción de costes:** RealVNC es una de las soluciones de Acceso Remoto más rentables del mercado, con precios transparentes, sin cargos ocultos y un coste total de propiedad que es uno de los más bajos del sector. Con RealVNC, no hay restricciones durante la sesión. Puede conectarse tantas veces como desee durante todo el tiempo que quiera desde cualquier dispositivo.
- **Apoyo a la transformación digital:** Según los resultados de la encuesta, el apoyo a la transformación digital es uno de los principales retos para el personal de TI en la Manufactura. RealVNC puede ayudar a respaldar la transformación digital al apoyar al personal de TI que necesita conectarse con personal y dispositivos remotos de forma segura, rápida y eficiente en tiempo real.
- **Apoyo a la tecnología operativa (TO):** No es ningún secreto que la TO es una tendencia en la Manufactura. RealVNC puede ayudar al personal de TI y TO a acceder, gestionar y supervisar los dispositivos TO, ya sea un sensor en una máquina de envasado de consumo en una planta en Atlanta, Georgia, o un sensor remoto que mide la calidad del material farmacéutico desde una planta en Greenville, Carolina del Norte."



El software de Acceso Remoto y gestión de RealVNC® es utilizado por cientos de millones de personas en todo el mundo en todos los sectores de la industria, la administración pública y la educación. Nuestro software ayuda a las organizaciones a reducir costes y mejorar la calidad del soporte de ordenadores y aplicaciones remotas. RealVNC® es el desarrollador original de software de Acceso Remoto VNC y es compatible con una combinación inigualable de plataformas de escritorio y móviles. Mediante el uso de nuestro software SDKs, las empresas tecnológicas de terceros también integran la tecnología de Acceso Remoto directamente en sus productos a través de acuerdos OEM.

Copyright© RealVNC® Limited 2016. RealVNC® y VNC® son marcas comerciales de RealVNC® Limited y están protegidas por registros de marca y/o solicitudes de marca pendientes en la Unión Europea, Estados Unidos de América y otras jurisdicciones. Las demás marcas comerciales pertenecen a sus respectivos propietarios. Protegido por las patentes británicas 2481870, 2491657; las patentes estadounidenses 8760366, 9137657; la patente europea 2652951

