Key Insight Brief

Tres estrategias para que mejores la seguridad de los accesos remotos en tu entorno industrial

wallix

El soporte remoto está cambiando por completo la forma en que gestionamos la eficiencia en los entornos industriales, y eso tiene un impacto directo en este mundo cada vez más digital y rápido en el que vivimos.

Piensa en todo lo que implica: desde la diagnosis y la monitorización hasta la transferencia de datos y la resolución de problemas, hoy en día las empresas industriales como la tuya necesitan soluciones de acceso remoto más robustas que nunca.

Pero, seamos sinceros, asegurar ese acceso no es una tarea sencilla; es un rompecabezas que requiere la adopción de un enfoque realmente estratégico.

Ponte a la cabeza en la gestión del acceso remoto

Hoy en día, el soporte remoto es más importante que nunca.

Sin embargo, **la implementación rápida y a menudo desorganizada de puertas de enlace VPN por parte de fabricantes y contratistas externos** ha aumentado de manera alarmante la superficie de ataque de las redes industriales.

Esto obliga a las organizaciones a encontrar el equilibrio entre **mantener la eficiencia operativa y garantizar una ciberseguridad sólida.**

Sé que proteger el acceso remoto no es precisamente un paseo. Es un proceso largo y complicado, y es fácil sentirse abrumado sin saber por dónde empezar. Lo que realmente puede marcar la diferencia es tener un **plan de acción bien estructurado.**

Y para que no te compliques, hemos simplificado todo en tres estrategias clave, fáciles de seguir.

Tres estrategias para asegurar el acceso remoto en tu entorno industrial

01 Implementa marcos de seguridad de Confianza Cero o Zero Trust

Seguro que has oído hablar de los marcos de seguridad Zero Trust. El concepto te suena, pero quizá aún no lo has puesto en marcha en tu organización.

Hoy en día, Zero Trust es una necesidad. Te resumo el por qué: a diferencia de los modelos de seguridad tradicionales, que confían automáticamente en lo que está dentro del perímetro de la red, la arquitectura Zero Trust exige una **verificación constante de todos los usuarios y dispositivos**, sin importar desde dónde se conecten o cómo accedan a la red.

Este enfoque garantiza que solo aquellos que estén autenticados y autorizados puedan acceder a los recursos específicos de la red.

¿Y por dónde puedes empezar? **Primero, evalúa y mapea** todos los activos y recursos de tu red. Una vez que tengas esa visión clara, **establece controles de acceso** detallados y utiliza tecnologías de verificación continua junto con la autenticación multifactor (MFA).

Eso sí, no te olvides de **monitorizar y auditar** constantemente el acceso y la actividad en la red. ¿Por qué vale la pena todo este esfuerzo?

> **Reduce** significativamente **el acceso no autorizado.**

> **Mejora la visibilidad y el control** sobre lo que ocurre en la red.

> **Evita el movimiento lateral** de hackers dentro de la red.

02 Centraliza y unifica para simplificar la tarea

Después de segmentar tu red, un paso fundamental para proteger tus entornos OT es establecer un único punto de acceso a tus sistemas OT.

Este método **facilita las conexiones remotas a través de una herramienta centralizada**, eliminando la necesidad de gestionar varios puntos de acceso VPN desorganizados.

Es importante que esto se haga con soluciones sencillas de usar y que se integren bien en los procesos OT, de manera que la seguridad no interfiera con la producción. ¿Qué debes tener en cuenta?

> **Garantiza que solo quienes tengan la contraseña correcta** puedan conectarse a tu red OT.

> **Verifica que la contraseña no haya sido robada**, mediante una autenticación robusta como MFA y una buena gestión de contraseñas.

> **Supervisa** qué hace la persona autenticada en los objetivos.

> **Limita el acceso a áreas o equipos específicos** para evitar acciones no autorizadas.

03 Monitorea de forma continua y detecta anomalías

En el tercer y último paso, te sugiero **implementar herramientas avanzadas y centralizadas que puedan detectar actividades sospechosas** o brechas en tiempo real.

Esto te permitirá reaccionar de manera rápida, evitando que los problemas lleguen a causar daños importantes.

Para desplegar un sistema de monitorización continua en entornos industriales, es fundamental instalar sensores y herramientas de seguimiento a lo largo de toda tu infraestructura.

También es necesario integrar soluciones que analicen comportamientos, detecten anomalías y configuren alertas en tiempo real para identificar cualquier actividad inusual o no autorizada.

La monitorización continua ofrece varias ventajas:

> **Detecta y mitiga amenazas** de forma temprana antes de que causen daños.

> **Registra y analiza eventos** para mejorar la postura de seguridad.

> **Unifica** la política de ciberseguridad.

Caso de éxito

Descubre cómo un líder en ropa de trabajo transformó su seguridad y optimizó su infraestructura crítica. Este fabricante mejoró la protección de sus servidores, garantizando un rendimiento estable y eficiente.

¿Te interesa saber cómo lo consiguieron?

Sigue leyendo.

Cómo el fabricante líder de ropa de trabajo protegió sus servidores e infraestructuras críticas

Hablemos de Engelbert Strauss, un conocido fabricante de ropa de trabajo de alta calidad. Con una infraestructura que incluye 80 servidores, 1.200 empleados y 10 oficinas, se enfrentaron a varios retos clave:

> **Mantener una infraestructura IT segura y estable:** Asegurar que su red siga siendo fiable y protegida.

> **Gestionar contraseñas e identidades**: Implementar un sistema eficiente para gestionar contraseñas e identidades.

> **Mejorar la experiencia del usuario:** Simplificar los procedimientos para garantizar una experiencia fluida.

> **Tener un equilibrio entre seguridad y usabilidad**: Alcanzar altos niveles de seguridad sin sacrificar la facilidad de uso para su equipo.

Soluciones al rescate

Implementamos una solución que **centralizó el control y la monitorización del acceso privilegiado a los activos críticos** de Engelbert Strauss, lo que permitió un control detallado sobre quién accedía a cada recurso.

Además, integramos el sistema de Gestión de Acceso Privilegiado (PAM) con el Sistema de Gestión de Seguridad y Eventos (SIEM) que ya utilizaban.

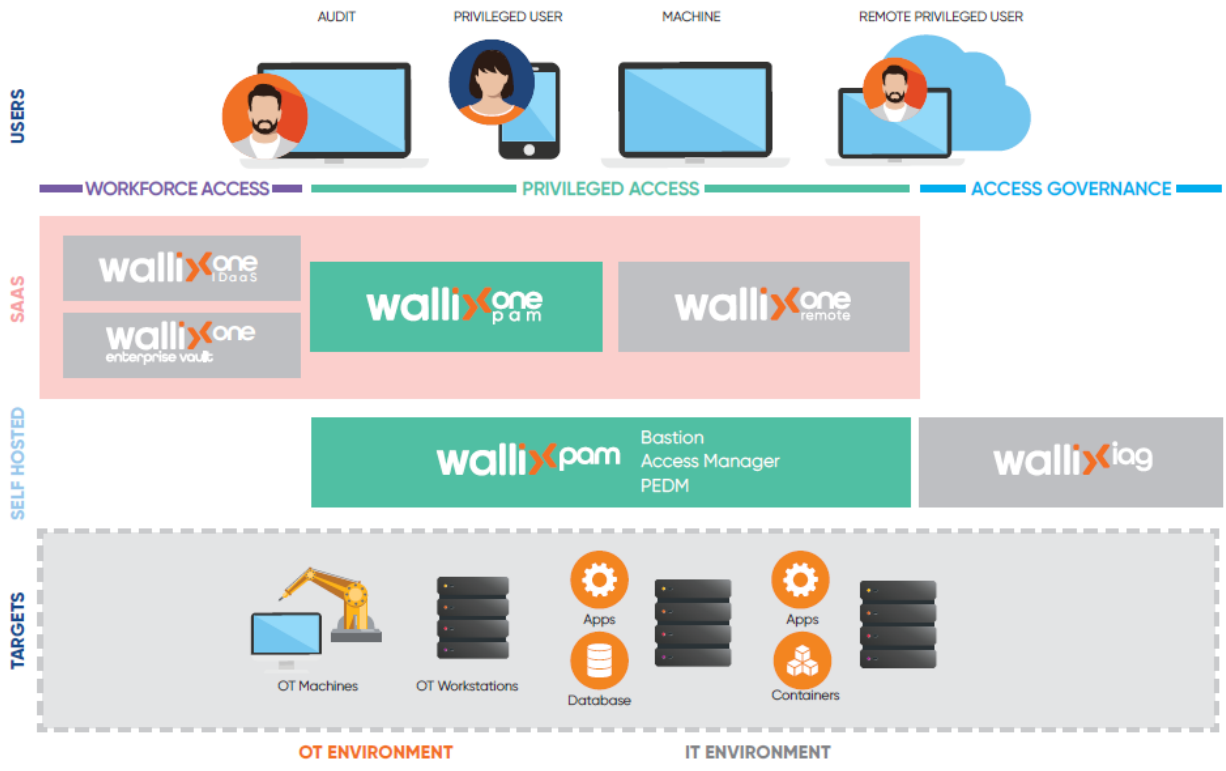
Esta integración facilitó el control del acceso autorizado a los sistemas y aseguró un aislamiento estricto entre las conexiones de sesión primaria y secundaria.

Los principales beneficios fueron:

> Mayor eficiencia en el uso de los recursos del departamento de IT.

> Mejor control y monitorización del acceso a los servidores.

> Reducción de las solicitudes de soporte.



Resumen

GWENDAL AZOUS

› Especialista en OT y grandes cuentas

Espero que este documento te haya aclarado algunas dudas. Cuando comencé a trabajar en él, mi intención era enfocarme en las ventajas de la digitalización en la fabricación. Sin embargo, mientras avanzaba, me di cuenta de que también era importante mostrar todo lo que implica este proceso, incluidos sus retos y dificultades. La transformación digital es un camino emocionante, pero debe hacerse de manera adecuada: garantizando que el acceso remoto sea seguro y cumpla con todas las normativas.

Si te surgen más preguntas, no dudes en contactar conmigo o mis compañeros por aquí.

wallix

WALLIX es un desarrollador de software de ciberseguridad que opera a nivel mundial. Fundada en 2003, WALLIX es hoy en día un líder mundial en seguridad de identidades y accesos, reconocido por las firmas de analistas más prestigiosas. Su misión es ofrecer un servicio de acceso identificado sencillo y seguro, para que nuestros clientes puedan operar con seguridad en cualquier lugar, tanto en entornos digitales como industriales.

- Calle Copenhague, 12, Las Rozas de Madrid , 28232 Madrid, España
- +34 910 53 40 37
- contact@wallix.com