CLAROTY

CLAROTY SECURE REMOTE ACCESS (SRA)

Ficha técnica | Acceso remoto sencillo y muy seguro para entornos de TO

EL DESAFÍO DEL ACCESO REMOTO A LOS ENTORNOS DE TO

El acceso remoto a los entornos de tecnología operativa (TO) requiere un equilibrio entre las necesidades de seguridad de TI y de operaciones de las plantas. Desde el punto de vista de la seguridad de TI, causa preocupación el alto riesgo que implica el acceso remoto al entorno de TO, ya que el uso de cuentas con privilegios para acceder a activos fundamentales a distancia es un vector de ataque obviamente peligroso.

Por otra parte, en cuanto a las operaciones de las plantas, el problema es que el personal de TO tiene necesidades de acceso remoto especiales, en comparación con los requisitos empresariales típicos. Los equipos de TO deben mantener en funcionamiento la planta con seguridad y tomar la mayoría de las decisiones en cuanto a acceso remoto, incluso en situaciones de emergencia. Sin embargo, suelen carecer de experiencia en seguridad de TI y, por lo tanto, requieren una solución que sea fácil de utilizar y que esté adaptada a los flujos de trabajo de TO.

SECURE REMOTE ACCESS - CARACTERÍSTICAS PRINCIPALES

- Solución especialmente diseñada para el acceso administrativo remoto a entornos de TO.
- Arquitectura que admite el acceso de alta disponibilidad a instalaciones distribuidas en todo el mundo.
- Consola sencilla, centrada en entornos de TO para la gestión de acceso de administradores y personal de soporte externo.
- Admite todos los principales casos de acceso remoto a entornos de TO.
- Flujos de trabajo incorporados para aprobaciones de acceso y acceso de emergencia.
- Pista de auditoría local para la rápida solución de problemas.

Seguridad de TI

- Gestión de riesgos de TO
- Control del acceso con privilegios
- Detección de actividad anómala

Operaciones de las plantas

- Autorización local del acceso a terceros
- Facilidad de uso
- Flujos de trabajo de aprobación y emergencia

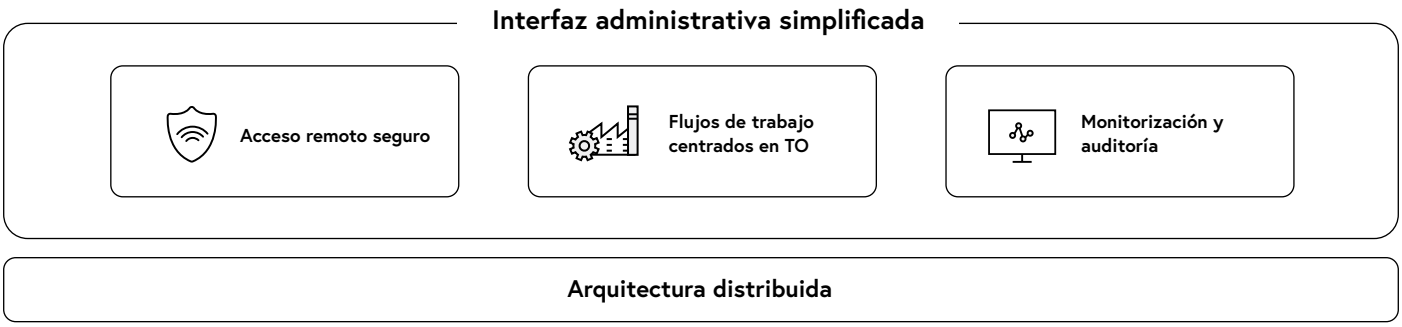
La seguridad de TI y las operaciones de plantas tienen necesidades de acceso remoto antagónicas

Las dificultades del acceso remoto para los entornos de TO se incrementan cuando las plantas están distribuidas y geográficamente aisladas, con un ancho de banda de red WAN limitado. Desafortunadamente, la mayoría de las soluciones de acceso remoto para empresas son demasiado complejas y centralizadas para admitir el acceso remoto a entornos de TO.

CLAROTY SRA – ACCESO REMOTO ESPECÍFICO PARA TO

La solución Claroty Secure Remote Access (SRA) está especialmente diseñada para el acceso remoto a entornos de TO. Disponible como dispositivos físicos o virtuales, SRA presenta las siguientes características principales:

- Simplicidad: a diferencia de las soluciones de acceso remoto empresariales, la solución SRA está diseñada para que el personal de planta pueda configurarla y utilizarla con total facilidad.
- Arquitectura distribuida: SRA admite plantas e instalaciones muy distribuidas, con administración tanto local como centralizada.
- Compatibilidad con entornos de TO: SRA es una solución especialmente diseñada para casos de uso y flujos de trabajo de tecnología operativa (TO).



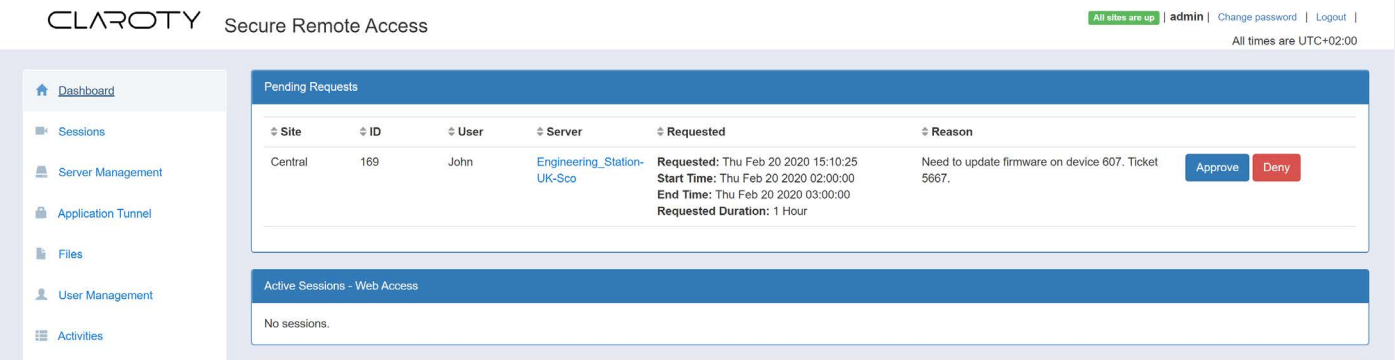
Claroty SRA admite los tres casos habituales en los que el personal remoto o externo necesita utilizar los sistemas de TO:

- Web: acceso a los sistemas de TO a través de un navegador web estándar.
- Aplicación de TO: acceso a los sistemas de TO mediante una aplicación propietaria en el dispositivo cliente remoto.
- Transferencia de archivos: los archivos de configuración o documentación confidenciales se transfieren a PLC u otros dispositivos de TO.

SRA aprovecha un único túnel cifrado de alta seguridad para la comunicación entre instalaciones. Esto simplifica enormemente la configuración del firewall de red y respeta las mejores prácticas de segmentación, como exige, por ejemplo, el modelo Purdue.

FLUJOS DE TRABAJO SENCILLOS Y ESPECÍFICOS PARA ENTORNOS DE TO

SRA está diseñada para ser utilizada localmente por el equipo de TO, que es el más indicado para autorizar el acceso remoto a sus instalaciones. La interfaz está adaptada para las necesidades de acceso remoto a entornos de TO, de manera que se reducen los requisitos de formación y la probabilidad de que se produzcan errores de configuración. Su sencilla interfaz de usuario admite la incorporación rápida de usuarios remotos (internos o externos) y de los sistemas de TO que necesitan.



La interfaz administrativa de SRA es fácil de utilizar y está disponible tanto localmente como para toda la empresa

Los claros flujos de trabajo admiten tanto aprobaciones secundarias como acceso prioritario en caso de emergencia extrema. Esto significa que el acceso con privilegios se concede siguiendo el criterio de las mejores prácticas de seguridad, pero también ofrece la posibilidad de responder inmediatamente en situaciones de crisis o emergencia, cuando no pueden producirse retrasos.

Monitorización y auditoría completas

El carácter confidencial que tiene el acceso remoto a los entornos de TO obliga a disponer de una pista de auditoría completa de toda la actividad. SRA proporciona una grabación completa de las acciones realizadas a través de una conexión de acceso remoto. A esa monitorización puede accederse directamente en tiempo real o bien a posteriori. La pista de auditoría se puede guardar localmente y esto es muy importante, ya que permite a las personas que la necesiten utilizarla sin demora in situ. De esta manera, se eliminan problemas relacionados con la exportación de la monitorización de la actividad de los empleados fuera de las fronteras nacionales.

Claroty Platform ofrece acceso total y seguridad completa para entornos de TO

Secure Remote Access complementa la oferta de Continuous Threat Detection (CTD) de Claroty para ofrecer una solución de seguridad de TO integral. La plataforma combinada proporciona el más amplio conjunto de controles de seguridad de TO de la industria, con descubrimiento y visibilidad de los activos, gestión de vulnerabilidades, detección de amenazas y política de segmentación. Con Claroty Platform, el personal de TO y de TI puede gestionar el riesgo en sus entornos de TO con un mínimo de formación y sin necesidad de interrumpir los flujos de trabajo de la infraestructura y la seguridad.

ACERCA DE CLAROTY

Claroty cierra la brecha de ciberseguridad industrial entre los entornos de tecnología de la información (TI) y de tecnología operativa (TO). Esto es particularmente importante para las organizaciones con fábricas y centros de producción muy automatizados, que se enfrentan a un importante riesgo financiero y de seguridad. Equipadas con las soluciones de TI/TO convergentes de Claroty, estas empresas y operadores de infraestructuras críticas pueden aprovechar sus procesos y tecnologías de seguridad de TI existentes para mejorar la disponibilidad, seguridad y fiabilidad de sus activos y redes de TO, sin necesidad de interrumpir la actividad ni disponer de equipos dedicados. El resultado es más tiempo de actividad y una mayor eficacia en las operaciones empresariales y de producción.

Gracias al respaldo y la confianza de los principales proveedores de automatización industrial, Claroty se despliega en los siete continentes a nivel mundial. La empresa tiene su sede central en Nueva York y desde que fue lanzada en 2015 por el reconocido grupo Team8 ha recibido 100 millones de dólares de financiación. Para obtener más información, visite www.claroty.com.