Información general sobre tecnología y seguridad:
Servicios de gestión remota de CARESTREAM Smart Link

Carestream Health adoptó una tecnología innovadora para brindar el servicio remoto más efectivo de la industria. Este documento está dirigido a los clientes de Carestream, en especial a los gerentes y administradores de TI. Describe la configuración, la seguridad y la tecnología de los servicios de gestión remota de Smart Link (Smart Link RMS).

Con Smart Link RMS, Carestream puede implementar servicios remotos de modo seguro a través de Internet para los equipos instalados detrás de los servidores de seguridad de los clientes. La solución está diseñada para brindar un alto rendimiento y seguridad en todos los niveles de su diseño.

Mediante el uso de servicios web para establecer una comunicación saliente segura por Internet, Smart Link RMS vincula los equipos de Carestream con los servidores corporativos de CARESTREAM Smart Link. Su equipo puede proporcionar datos de rendimiento, alertas y alarmas a nuestro equipo de soporte, lo que genera un servicio proactivo y rápido, junto con un soporte de funcionalidades avanzadas y remotas para la solución de problemas. Smart Link RMS no recopila información de los pacientes ni de los usuarios.

Función	Beneficio
Monitoreo de dispositivos	Notificaciones de alertas automáticas para el equipo de servicio. No es necesaria ninguna acción por parte del cliente.
Historial de datos consolidados del dispositivo para cada dispositivo	Solución de problemas avanzada a través de un historial integral del rendimiento del dispositivo.
Gestión y control remotos del escritorio	Facilidad de capacitación. Solución de problemas y correcciones rápidas.
Diagnóstico remoto	Solución de problemas y correcciones rápidas.
Gestión de software	Actualizaciones de software convenientes, oportunas y seguras.
Servicio y soporte remotos y centralizados	Respuestas rápidas y capacidades de soporte fuera de horario.

*Tabla 1: Funciones y beneficios***Componentes de la solución**

Los dos componentes técnicos más importantes de Smart Link RMS son el agente y el servidor.

Agente	Servidor
Está instalado en el sitio del cliente; el software incorporado está instalado directamente en el dispositivo médico.	Reside dentro de los centros de datos remotos autorizados de Carestream.
Maneja las funciones de Smart Link RMS en el sitio del cliente.	Se comunica con el agente a través de servicios web seguros.
• Establece comunicaciones seguras con el servidor a través de Internet. • Envía datos de la máquina y archivos de registro al servidor. • Monitorea el rendimiento del dispositivo y envía alarmas al servidor. • Brinda soporte a la descarga y la implementación de actualizaciones de software remotas desde el servidor corporativo de Smart Link.	• Procesa los archivos de datos y las alarmas desde el agente. • Es la consola de gestión para los servicios remotos de Smart Link.

Tabla 2: Componentes técnicos

Gracias al servidor, el equipo de soporte de Carestream puede realizar lo siguiente:

- consolidar y analizar datos
- ejecutar un diagnóstico remoto
- establecer reglas automatizadas para tomar medidas cuando ocurren eventos específicos

- determinar la seguridad y acceder a los dispositivos del cliente
- configurar actualizaciones de software para la distribución

Configuración de la solución

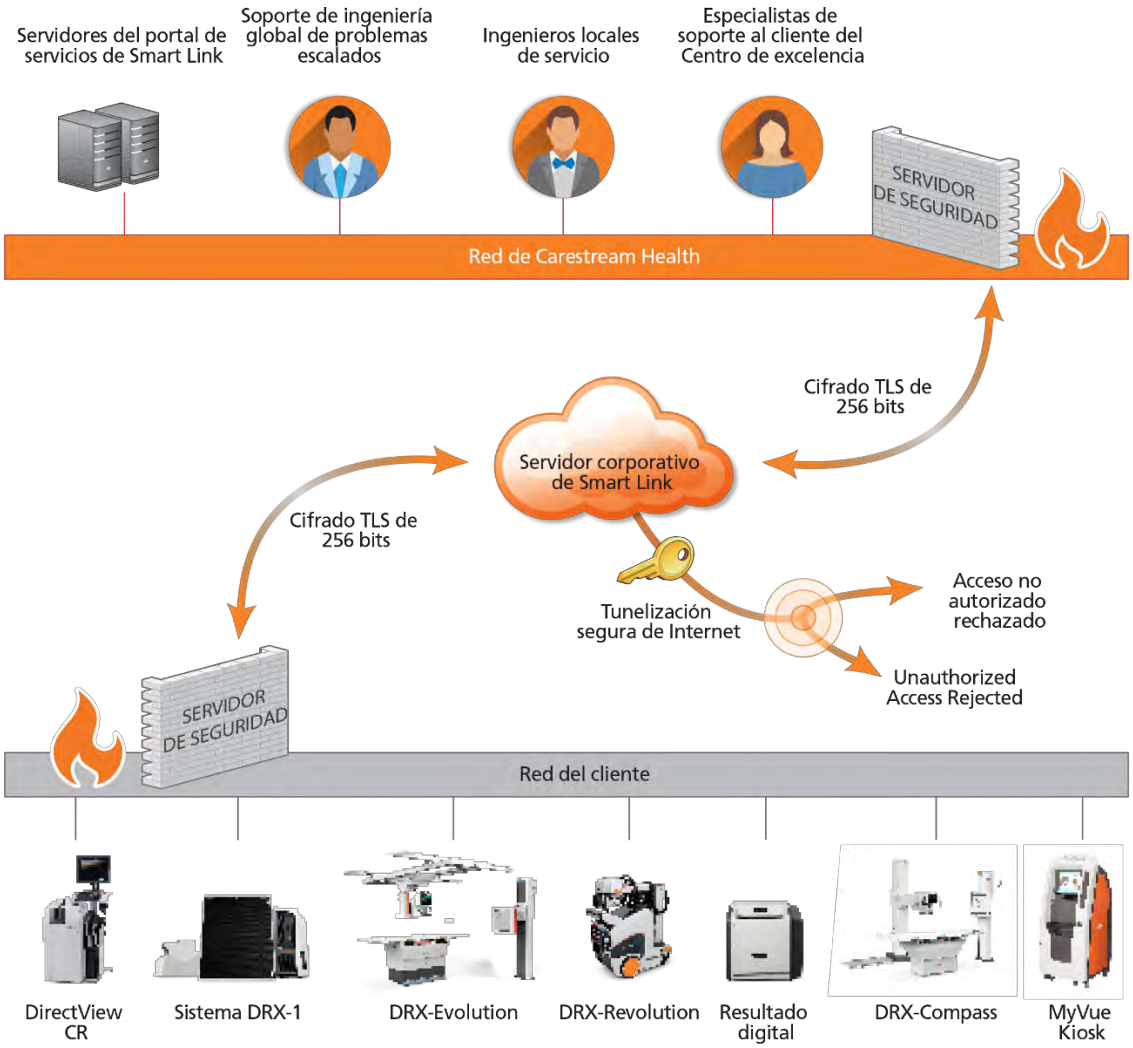
El agente realiza una conexión con el servidor corporativo de Smart Link desde la seguridad de su servidor de seguridad corporativo, adhiriendo a sus políticas de seguridad. No es necesario ningún cambio especial a un servidor proxy.

Dentro de su red, el agente es como otra computadora personal de la LAN. La configuración del agente en su sitio requiere lo siguiente:

- una conexión física o inalámbrica a una LAN (TCP/IP) existente
- acceso a Internet de salida para el dispositivo (o a través de un proxy)

Un ingeniero de servicio (Field Service Engineer, FE) de Carestream configurará el agente en los dispositivos y configurará conexiones de red de acuerdo con sus requerimientos de TI.

Figura 1: Los dispositivos con el agente Smart Link RMS están configurados del mismo modo que cualquier otro dispositivo de computación habilitado por red en su LAN.


Servidores del portal de servicios de Smart Link
Soporte de ingeniería global de problemas escalados
Ingenieros locales de servicio
Especialistas de soporte al cliente del Centro de excelencia
SERVIDOR DE SEGURIDAD
Red de Carestream Health
Cifrado TLS de 256 bits
Servidor corporativo de Smart Link
Cifrado TLS de 256 bits
Tunelización segura de Internet
Acceso no autorizado rechazado
Unauthorized Access Rejected
SERVIDOR DE SEGURIDAD
Red del cliente
DirectView CR
Sistema DRX-1
DRX-Evolution
DRX-Revolution
Resultado digital
DRX-Compass
MyVue Kiosk

Carestream

Tecnología y seguridad

El agente es eficiente y no afectará el rendimiento óptimo de su equipo debido a tres funciones de diseño principales:

- El agente sondea el dispositivo en intervalos de gestión de 60 segundos.
- El agente puede transmitir datos al servidor en horarios programados o cuando un código de error indica que se necesita una notificación inmediata.
- El protocolo de mensajes proporciona mensajes breves y eficientes (0,5 a 3 KB); las comunicaciones Smart Link RMS no afectarán el ancho de banda de la red.

Seguridad de la red

El objetivo de Smart Link RMS es brindar soporte a sus estándares de red y prácticas de seguridad existentes, a la vez que se mantiene un alto nivel de comunicaciones seguras y confidencialidad de datos. Smart Link RMS solo requiere una conexión de salida sobre el puerto 443 (https). Carestream no requiere que su departamento de TI haga excepciones a las políticas de TI establecidas que comprometerían su servidor de seguridad. Smart Link RMS aplica seguridad a las tres capas: dispositivo, red y empresa. Las capas se implementan con tecnología diseñada para comunicaciones Smart Link seguras y eficientes.

La tecnología incluye lo siguiente:

- un diseño de software reforzado para la aplicación y la seguridad de los datos
- soporte para estándares de la industria como TCP/IP, HTTPS, SOAP y XML

Capa del dispositivo	Capa de la red	Capa de la empresa
• Está reforzada para operaciones las 24 horas del día, los 7 días de la semana, en entornos de producción; se reinicia automáticamente en caso de falla en el sistema o en el software. • Se ejecuta como un servicio para el sistema más que como una aplicación. • Admite el cifrado TLS de 256 bits. • Admite certificados digitales para la autenticación de terminales. • Admite la auditoría local de los eventos del sistema del dispositivo médico y también del servidor corporativo de Smart Link, lo que permite el acceso local a registros y archivos de auditoría.	• Admite el cifrado TLS de 256 bits. • Utiliza el sondeo de las comunicaciones basadas en el servidor para que funcionen dentro de los servidores de seguridad corporativos. • Brinda soporte al balanceo de cargas del tráfico de red.	• Brinda cifrado TLS de forma predeterminada a todas las comunicaciones. • Requiere autenticación con nombre de usuario y contraseña. • Admite certificados digitales para una mayor seguridad. • Admite la autorización a nivel del usuario para la funcionabilidad de la aplicación, lo que limita el acceso a los dispositivos, las vistas de los datos y las interacciones. • Admite una auditoría robusta del acceso al dispositivo, las interacciones del usuario y los eventos del sistema.

Tabla 3: Especificaciones técnicas para la seguridad en cada capa

Sin puertos especiales

Es posible que las soluciones de acceso remoto de otros fabricantes exijan el uso de un número de puerto específico. El administrador de red debe configurar el servidor de seguridad para que esas conexiones a un puerto TCP específico, como el 5631, del lado público del servidor de seguridad estén mapeadas al puerto 5631 en el dispositivo. Esto requiere un dirección IP estática asignada al dispositivo. Si hay múltiples dispositivos en la LAN corporativa, se les debe asignar puertos diferentes, estáticos y atípicos en el servidor de seguridad a los servicios adicionales.

En esa situación, el servidor de seguridad se debe configurar de modo tal que solo los dispositivos autorizados establezcan conexiones en esos puertos específicos, colocando más carga en el administrador de red. Los usuarios no autorizados también podrían revisar el puerto específico y usar protocolos para descubrir qué hay en esa conexión. **El agente de Smart Link RMS no requiere un puerto especial.**

No se requiere dirección IP fija para la comunicación

La capacidad del agente de comunicarse con el servidor corporativo es independiente de la dirección IP admitida por el dispositivo. Las configuraciones típicas del servidor de seguridad permiten que las conexiones de salida se inicien de forma segura desde detrás del servidor de seguridad, sobre el puerto 443 (https). El agente se comunica a través del servidor de seguridad a través del puerto 443 e inicia la comunicación de salida con el servidor corporativo Smart Link RMS. Como toda la comunicación es de salida, su red corporativa no necesita aceptar conexiones desde afuera ni abrir puertos adicionales. El equipo habilitado para Smart Link RMS no aceptará conexiones desde ningún sistema por fuera del servidor de seguridad corporativo del cliente.

Solo se conecta al servidor corporativo de Smart Link

Un asunto importante para los administradores de TI es si la conexión se realiza con el servidor corporativo de Smart Link o con una entidad desconocida. Si el agente escucha un puerto TCP mientras espera una conexión, el dispositivo podría convertirse en un objetivo potencial para el acceso no autorizado. Con Smart Link RMS, Carestream puede garantizar la identidad del servidor corporativo de Smart Link para el agente de conexión de Smart Link mediante el uso de certificados digitales. Por lo tanto, la identidad nunca es un problema. El agente envía una solicitud cifrada al servidor corporativo Smart Link de confianza para obtener nuevas instrucciones y luego actúa sobre las respuestas que recibe de su parte.

Flexibilidad

El agente del servicio no depende de una dirección IP estática ni de subredes y admite infraestructuras de redes corporativas que requieren servidores proxy de Internet (proxy de configuración automática, proxy HTTP). La flexibilidad y compatibilidad del agente pueden alojar infraestructuras de red cambiantes.

Túnel seguro exclusivo para usuarios de los servicios remotos de Smart Link

Una vez que el agente establece un túnel seguro e integral con el servidor corporativo de Smart Link, la conexión es visible solo para clientes y servicios Smart Link RMS (usuarios y aplicaciones). Los clientes y servicios no autorizados que intentan ocupar un puerto y protocolo TCP libres no pueden usar la conexión ni establecer una nueva. Por lo tanto, las entidades no autorizadas no pueden usar la conexión, aunque puedan verla.

Seguridad libre de VPN

El agente inicia un túnel de comunicación bidireccional que cumple con el entorno de computación seguro en el sitio del cliente, lo que elimina la necesidad de una red privada virtual (virtual private network, VPN) admitida por hardware. El agente requiere solo una conexión a Internet. Esto es menos complicado y menos costoso que proporcionar, configurar y mantener el hardware de la VPN.

El personal de servicio de Carestream y el equipo de Carestream están en redes diferentes, mientras que el personal de VPN está en la misma red.

Además, el personal de servicio de Carestream solo puede acceder al equipo de Carestream a través de los servidores Smart Link RMS. Todos los demás equipos de la misma red NO son visibles para Carestream. Aunque sea a través de VPN, toda la red y todos los recursos están abiertos para los usuarios.

Transmisión segura de datos

Todas las transmisiones de datos están cifradas con un protocolo TLS de 256 bits, la misma tecnología que usan los bancos para transacciones financieras seguras y en línea. Los agentes del dispositivo Smart Link RMS validan los certificados digitales en el servidor corporativo de Smart Link antes de aceptar las solicitudes o de enviar datos.

Recopilación segura de datos

El agente solo recopila datos relevantes del dispositivo para el rendimiento y uso de su equipo. Carestream no recopila ni almacena su información confidencial o propietaria.

Carestream monitorea datos como códigos de error, archivos de registro y otras propiedades del dispositivo que colaboran con la solución de problemas del equipo, las tendencias del rendimiento y la resolución de problemas. El acceso remoto del escritorio al equipo mediante el uso de Smart Link RMS requiere una adhesión estricta a la política de Carestream (tal como se define en la capacitación del servicio), que cumpla con el Reglamento General de Protección de Datos (General Data Protection Regulation, GDPR) y NO recopila, transmite ni almacena información personal de ningún tipo.

Acceso seguro al servidor

En el nivel empresarial, el servidor corporativo Smart Link solo permite que se registren usuarios autorizados por Carestream con la autenticación de nombre de usuario y contraseña. Los perfiles de registro de usuario controlan a qué clientes, equipos y archivos puede acceder el usuario, así como el nivel de acceso permitido. Todas las sesiones de acceso remoto se registran con fines de auditoría. Los clientes también pueden habilitar la notificación de escritorio remoto. Una vez habilitados, se notificará a los clientes cuando se inicie una solicitud de escritorio remoto. Si el cliente no responde, se rechazará automáticamente la solicitud de escritorio remoto.

Conclusión

Carestream se compromete a mejorar de forma continua su experiencia con el servicio mediante la inversión e implementación de nuevos métodos de soporte. Smart Link RMS usa la tecnología actual para brindar un enfoque de servicio optimizado y simplificado para su producto Carestream, a la vez que cumple con todas las regulaciones importantes relacionadas con la seguridad y la privacidad. Para obtener más información, comuníquese con su representante local de Carestream o visite www.carestream.com/smart-link-services.