

Visão geral da tecnologia e da segurança: Serviços de gerenciamento remoto do CARESTREAM Smart Link

A Carestream Health adotou uma tecnologia inovadora para fornecer a oferta de serviço remoto mais eficaz do setor. Este documento é destinado a clientes da Carestream, especificamente gerentes e administradores de TI, e descreve a configuração, segurança e tecnologia dos Serviços de gerenciamento remoto [Remote Management Services (RMS)] do Smart Link.

Os RMS do Smart Link permitem que a Carestream implante serviços remotos com segurança por meio da internet em equipamentos instalados e protegidos por firewalls dos clientes. A solução foi projetada para apresentar alto desempenho e segurança em todos os níveis de sua arquitetura.

Ao utilizar serviços via Web para estabelecer comunicação de saída segura por meio da internet, os RMS do Smart Link conectam os equipamentos da Carestream aos Servidores Empresariais do CARESTREAM Smart Link. Seus equipamentos podem fornecer dados de desempenho, alertas e alarmes à sua equipe

de suporte, resultando em serviços e suporte proativos e rápidos com recursos remotos de diagnóstico de falhas. Nenhuma informação dos pacientes ou usuários é coletada pelos RMS do Smart Link.

Componentes da solução

Os dois principais componentes técnicos dos RMS do Smart Link são o Agente e o Servidor.

O Servidor permite que a equipe de suporte da Carestream:

- Consolide e analise dados.
- Execute diagnósticos remotamente.
- Configure regras automatizadas para desempenhar ações quando eventos específicos ocorrem.
- Defina especificações de segurança e acesso para os dispositivos do cliente.
- Configure atualizações de software para distribuição.

Recurso	Benefício
Monitoramento de dispositivos	Notificações automáticas de alerta para a equipe de suporte. Não se exige nenhuma ação do cliente.
Histórico consolidado de dados armazenado sobre cada dispositivo	Diagnóstico avançado de falhas por meio de um histórico abrangente sobre o desempenho do dispositivo.
Gerenciamento e controle de desktop remotos	Facilidade de treinamento. Diagnóstico de falhas e correções rápidas.
Diagnóstico remoto	Diagnóstico de falhas e correções rápidas.
Gerenciamento de software	Atualizações de software convenientes, oportunas e seguras.
Serviço e suporte remotos centralizados	Respostas rápidas e recursos de suporte após o expediente.

Tabela 1: Recursos e benefícios

Agente	Servidor
É instalado na instituição do cliente; o software integrado é instalado diretamente no dispositivo médico.	Permanece nos data centers remotos autorizados da Carestream.
Gerencia funções dos RMS do Smart Link na instituição do cliente.	Comunica-se com o Agente utilizando serviços seguros via Web.
- Estabelece comunicações seguras com o Servidor por meio da internet. - Envia dados de máquina e arquivos de registro para o Servidor. - Monitora o desempenho do dispositivo e envia alertas ao Servidor. - Oferece suporte a download remoto e à implementação de atualizações de software a partir do Servidor Empresarial do Smart Link.	- Processa os arquivos de dados e alarmes do Agente. - É o painel de gerenciamento dos Serviços Remotos do Smart Link.

Tabela 2: Componentes técnicos

Configuração da solução

O Agente se conecta ao Servidor Empresarial do Smart Link a partir dos parâmetros de segurança de seu firewall corporativo, em cumprimento às suas políticas de segurança. Não há necessidade de nenhuma alteração para um servidor proxy.

Em sua rede, o Agente funciona como se fosse outro computador pessoal na LAN. A configuração do Agente em sua instituição

exige:

- Uma conexão física ou sem fio a uma LAN existente (TCP/IP)
- Acesso de saída à internet para o dispositivo (ou por meio de um proxy)

Um engenheiro de campo (Field Engineer, FE) da Carestream configurará o Agente no(s) dispositivo(s), bem como as conexões de rede, de acordo com seus requisitos de TI.

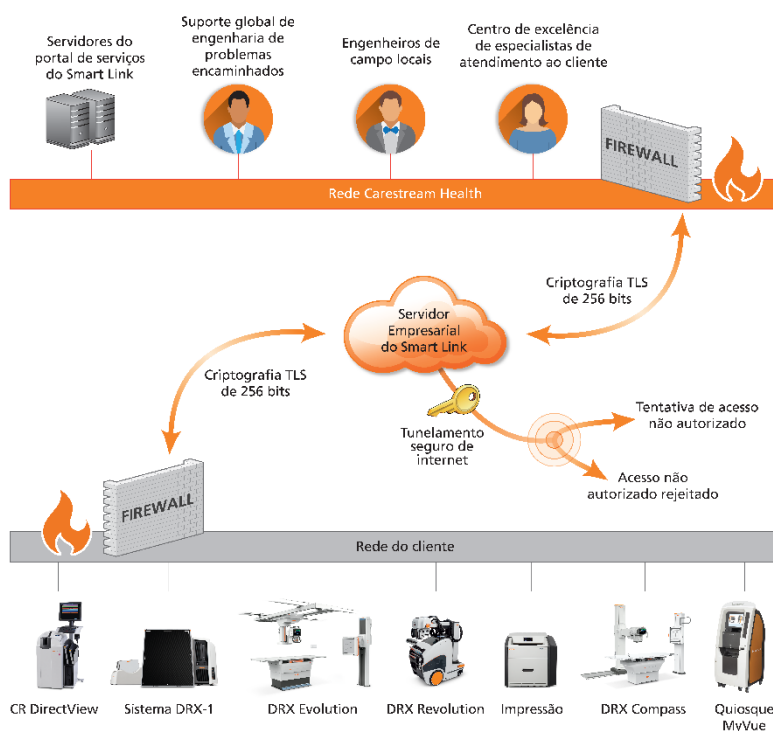


Figura 1: Dispositivos com o Agente dos RMS do Smart Link são configurados da mesma forma que qualquer outro dispositivo computacional habilitado para rede em sua LAN.

Tecnologia e segurança

O Agente é eficiente e não afetará o desempenho ideal de seus equipamentos, uma vez que conta com três recursos principais de projeto:

- O Agente sonda o dispositivo em intervalos gerenciáveis de 60 segundos.
- O Agente pode transmitir dados ao Servidor em horários agendados ou quando um código de erro indica a necessidade de notificação imediata.
- O protocolo de mensagens entrega notificações pequenas e eficientes (de 0,5 a 3 KB); as comunicações dos RMS do Smart Link não afetarão a largura de banda da rede.

Segurança da rede

O objetivo dos RMS do Smart Link é fornecer suporte aos padrões e às práticas de

segurança existentes de sua rede, enquanto mantém um alto nível de comunicações seguras e confidencialidade de dados. Os RMS do Smart Link exigem apenas uma conexão de saída por meio da porta 443 (https). A Carestream não exige que seu departamento de TI estabeleça exceções às suas políticas de TI, o que comprometeria seu firewall. Os RMS do Smart Link aplicam a segurança em três camadas: de dispositivo, de rede e empresarial. As camadas são elaboradas utilizando tecnologia projetada para comunicações seguras e eficientes do Smart Link.

A tecnologia inclui:

- Um projeto de software reforçado para segurança dos aplicativos e dados
- Suporte para padrões do setor, como TCP/IP, HTTPS, SOAP e XML

Camada de dispositivo	Camada de rede	Camada empresarial
• É reforçada para operações em ambientes de produção 24 horas por dia, sete dias por semana; reinicia automaticamente em caso de falha do sistema ou do software • É executada como um serviço do sistema, em vez de um aplicativo • Compatível com criptografia TLS de 256 bits • Compatível com certificados digitais para autenticação de terminal • Compatível com auditoria local de eventos do sistema de dispositivos médicos, assim como no Servidor Empresarial do Smart Link, possibilitando acesso local a registros e arquivos de auditoria	• Compatível com criptografia TLS de 256 bits • Utiliza comunicações de sondagem baseadas no Servidor para operar em firewalls corporativos • Compatível com balanceamento de carga de tráfego de rede	• Oferece criptografia TLS como padrão para todas as comunicações • Exige autenticação com nome de usuário e senha • Compatível com certificados digitais para aumentar a segurança • Compatível com autorização de nível de usuário para acesso às funcionalidades dos aplicativos, o que limita o acesso a dispositivos, visualização de dados e interações • Compatível com auditoria robusta de acesso a dispositivos, interações de usuários e eventos do sistema

Tabela 3: Especificações técnicas de segurança em cada camada

Não são necessárias portas especiais

As soluções de acesso remoto de outros fabricantes poderão exigir a utilização de um número de porta específico. Dessa forma, o administrador de rede deve configurar o firewall para que as conexões com uma porta TCP específica no lado público do firewall, como a 5631, sejam mapeadas até a porta 5631 no dispositivo, exigindo a atribuição de um endereço IP estático ao dispositivo. Se houver vários dispositivos na LAN empresarial, os dispositivos adicionais deverão receber a atribuição de portas diferentes, estáticas e atípicas no firewall.

Nesse caso, o firewall deve ser configurado para que somente dispositivos autorizados estabeleçam conexões nessas portas específicas, sobrecarregando o administrador da rede. Usuários não autorizados também poderiam explorar a porta específica e utilizar protocolos para descobrir o conteúdo dessa conexão. **O Agente dos RMS do Smart Link não exige uma porta específica.**

Não é exigido nenhum endereço IP fixo para comunicação

A capacidade do Agente de se comunicar com o Servidor Empresarial não depende do endereço IP do dispositivo compatível. Configurações típicas de firewall permitem que as conexões de saída sejam iniciadas com segurança atrás do firewall por meio da porta 443 (https). O Agente se comunica por meio do firewall utilizando a porta 443 e inicia a comunicação de saída com o Servidor Empresarial dos RMS do Smart Link. Como todas as comunicações são de saída, sua rede corporativa não precisa aceitar conexões externas ou abrir portas adicionais. Os equipamentos habilitados para os RMS do Smart Link não aceitarão conexões de nenhum sistema externo ao firewall corporativo do cliente.

Conexão apenas com o Servidor Empresarial do Smart Link

Uma questão importante para gerentes de TI é saber se uma conexão é estabelecida com o Servidor Empresarial do Smart Link ou com uma entidade desconhecida. Se o Agente identifica uma porta TCP durante a espera pela conexão, o dispositivo pode se tornar alvo em potencial de acesso não autorizado. Com os RMS do Smart Link, a Carestream pode confirmar a identidade do Servidor Empresarial do Smart Link em relação ao Agente do Smart Link utilizando certificados digitais. Dessa forma, a identidade nunca é um problema. O Agente envia uma solicitação criptografada de novas instruções ao Servidor Empresarial confiável do Smart Link e só age mediante a obtenção de respostas do respectivo servidor.

Flexibilidade

O Agente de Serviço não depende de um endereço IP estático ou de sub-redes e é compatível com infraestruturas de rede corporativa que exigem servidores proxy de internet (proxy de configuração automática, proxy HTTP). A flexibilidade e compatibilidade do Agente permitem a adequação a mudanças nas infraestruturas de rede.

Túnel seguro exclusivo para usuários dos Serviços Remotos do Smart Link

Depois que o Agente define um túnel ponto a ponto seguro com o Servidor Empresarial do Smart Link, a conexão se torna visível apenas aos clientes e serviços dos RMS do Smart Link (usuários e aplicativos). Clientes e serviços não autorizados que tentarem ocupar uma porta e um protocolo TCP livres não conseguirão utilizar a conexão ou estabelecer uma nova conexão. Portanto, entidades não autorizadas não conseguirão utilizar a conexão, mesmo que ela esteja visível.

Segurança sem VPN

O Agente inicia um túnel de comunicação bidirecional em conformidade com o ambiente de computação seguro na instalação do cliente, eliminando a necessidade de uma rede virtual privada (virtual private network, VPN) apoiada por hardware. O Agente exige somente uma conexão com a internet. Este método é mais simples e mais econômico do que fornecer, configurar e manter um hardware de VPN.

A equipe de serviço e os equipamentos da Carestream permanecem alocados em uma rede diferente, enquanto a equipe de VPN se localiza na mesma rede.

Além disso, a equipe de serviço da Carestream só pode acessar os equipamentos da Carestream por meio dos servidores dos RMS do Smart Link. NENHUM outro equipamento na mesma rede se torna visível para a Carestream. No entanto, por meio da VPN, toda a rede e todos os recursos permanecem abertos aos usuários.

Transmissão de dados segura

Todas as transmissões de dados são criptografadas por meio do protocolo TLS de 256 bits, a mesma tecnologia que os bancos utilizam para a realização de transações financeiras on-line seguras. Os agentes de dispositivos dos RMS do Smart Link validam os certificados digitais com o Servidor Empresarial do Smart Link antes de aceitar solicitações ou enviar dados.

Coleta de dados segura

O Agente coleta apenas dados do dispositivo relevantes para o desempenho e a utilização de seu equipamento. A Carestream não coleta nem armazena suas informações confidenciais ou informações protegidas por direitos de propriedade. A Carestream monitora dados, como códigos de erro, arquivos de registro e outras propriedades do dispositivo que auxiliam a diagnosticar falhas nos equipamentos, detectar tendências de desempenho e solucionar problemas. O acesso ao equipamento a partir de uma área de trabalho remota utilizando os RMS do Smart Link exige cumprimento rigoroso da política da Carestream (conforme descrito no treinamento de serviço), que está em conformidade com a LGPD, uma vez que NÃO coleta, transmite ou armazena nenhuma informação pessoal.

Acesso seguro ao Servidor

No nível corporativo, o Servidor Empresarial do Smart Link só permite que usuários autorizados pela Carestream efetuem login com autenticação de nome de usuário e senha. Os perfis de login de

usuário controlam quais clientes, equipamentos e arquivos o usuário pode acessar, assim como o nível de acesso permitido. Todas as sessões de acesso remoto são registradas para fins de auditoria. Os clientes também podem habilitar a notificação de área de trabalho remota. Depois de habilitada, os clientes são notificados quando uma solicitação de área de trabalho remota é iniciada. Se o cliente não responde, a solicitação de área de trabalho remota é rejeitada automaticamente.

Conclusão

A Carestream está comprometida com a melhoria contínua de sua experiência de serviço ao investir em novos métodos de suporte e implementá-los. Os RMS do Smart Link utilizam tecnologias atuais para oferecer um conceito de serviço otimizado e simplificado ao seu produto Carestream, enquanto cumpre regulamentações críticas relacionadas à segurança e privacidade. Para obter mais informações, entre em contato com seu representante local da Carestream ou acesse www.carestream.com/smart-link-services.