La fornitura di supporto e servizio remoti per dispositivi intelligenti

Per Leica Microsystems e per gli utenti che impiegano i servizi remoti, la sicurezza rappresenta una fonte di preoccupazione primaria.Leica Microsystems richiede una soluzione sperimentata di servizi remoti che sia in grado di proteggere da virus e hacker e che supporti gli strumenti intelligenti senza la necessità di grandi modifiche presso l'utente finale, operando all'interno del nostro corrente modello di sicurezza di rete e ottenendo una certificazione ufficiale da parte di una società di sicurezza esterna. Poiché gli strumenti di Leica Microsystems sono collegati alla rete dei clienti, i clienti finali devono avere la sicurezza che le soluzioni di servizi remoti supportino anche il loro modello di sicurezza, che offrano un controllo dettagliato degli accessi degli utenti e funzioni di audit e tracking di facile uso.

Come molti altri produttori di equipaggiamenti, per il nuovo sistema di servizio remoto Leica RemoteCare Leica Microsystems fornisce servizi remoti business-critical usando il software Axeda® ServiceLink™ ed un'infrastruttura a server. Axeda ServiceLink allevia le preoccupazioni di sicurezza di Leica e dei suoi clienti riducendo attivamente al minimo i tempi di fermo, gestendo i rischi e garantendo che l'equipaggiamento sia sempre pronto a fornire i massimi risultati.

Usando l'Axeda ServiceLink, il RemoteCare Leica Microsystems collega senza soluzione di continuità Leica Microsystems e gli strumenti Leica Microsystems presso il cliente. Poiché spesso tali strumenti tracciano i dati dei pazienti ed altri tipi di informazioni private e protette, le capacità di offrire sicurezza e compatibilità sono tra i requisiti più importanti considerati in qualsiasi soluzione di servizio remoto. Questo documento esamina sia i requisiti di Leica Microsystems e dei suoi clienti, sia il modo in cui Axeda ServiceLink offre un supporto remoto sperimentato e sicuro per soddisfare tali requisiti.

I requisiti di Leica Microsystems per la sicurezza del servizio remoto
Per soddisfare i più rigidi requisiti di sicurezza propri e dei propri clienti relativamente all'uso efficace e di routine dei servizi remoti, Leica Microsystems ha scelto per il RemoteCare i prodotti Axeda. I clienti hanno in tal modo la sicurezza che le proprie connessioni rimangano sicure e private.
Alcuni dei nostri requisiti più comuni comprendono:

- Design a prova di impresa – la connessione di qualsiasi computer a Internet accresce i problemi di sicurezza e la cosa non cambia nel caso di una connessione a dispositivi intelligenti. Se gli hacker tentano di danneggiare un dispositivo con dati corrotti o virus, di rubare dati accedendo al percorso tra lo strumento e Leica Microsystem, o di ottenere un accesso non autorizzato a informazioni critiche, un sistema di monitoraggio remoto deve essere in grado proteggere da queste e altre minacce.

- Supporto per più dispositivi – Leica Microsystems necessita di un supporto sicuro per tipi di dispositivi diversi e per le diverse complesse configurazioni dei clienti senza che presso l'utente siano necessarie grandi modifiche.

- Impiego rapido – Per i clienti che impiegano i sistemi di servizio remoto, le caratteristiche di sicurezza devono esistere all'interno del loro modello di sicurezza di rete attuale.

- Convalida da parte di aziende di sicurezza esterne – Certificazione ufficiale da parte di un audit di sicurezza che offre al cliente la fiducia nelle caratteristiche della tecnologia e nel venditore.

Impegno:
Leica Microsystems è convinta che per i clienti privacy e sicurezza siano della massima importanza. RemoteCare rispetta i seguenti principi di sicurezza:
- Proteggere l'integrità del sistema: rete, equipaggiamento e dati
- Seguire l'accesso e le attività in conformità con le norme
- Offrire flessibilità e controllo per rafforzare le regole del business
- Svolgere a intervalli regolari audit e certificazioni esterni dei processi e delle soluzioni Leica Microsystems

Requisiti del cliente per la sicurezza del servizio remoto
Alla rete dei nostri clienti sono collegati strumenti intelligenti. Ogni cliente dispone di proprie regole di sicurezza e di una protezione della propria rete sotto forma di firewall, server proxy e schemi di indirizzamento. Un dispositivo collegato alla rete dei clienti verrà protetto dietro questi livelli di sicurezza. Se un servizio remoto offerto richiede modifiche al sistema di protezione della rete del nostro cliente, esso non sarà probabilmente accettato. Per questo motivo, è importante considerare le esigenze del cliente includendo:

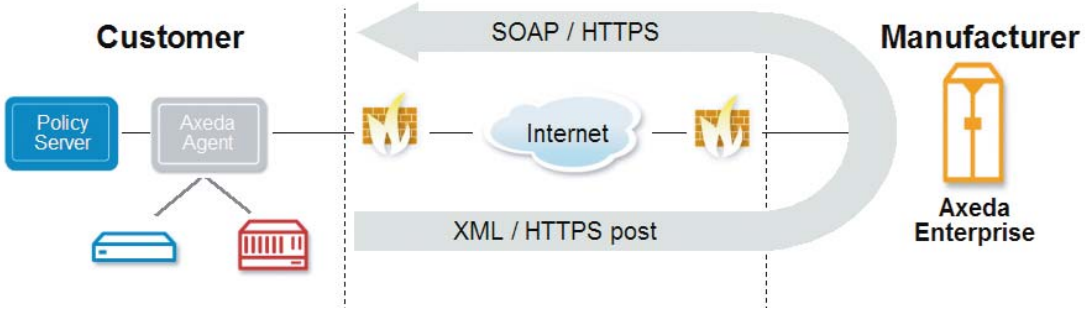
- Mantenimento del modello di sicurezza attuale – Il dispositivo Leica Microsystems deve supportare il modo in cui l'organizzazione gestisce le operazioni di sicurezza, le regole o le procedure e dovrebbe essere compatibile con gli standard industriali.

- Controllo dell'accesso degli utenti – Conformemente al modello di sicurezza dei clienti, il dispositivo di Leica Microsystems deve offrire al cliente (non a Leica Microsystems) un controllo dettagliato e deve stabilire delle regole relativamente a quali azioni possano essere eseguite sul dispositivo, come la raccolta di dati e l'aggiornamento del software e a quando ciò possa avvenire. Queste regole necessitano di una definizione centralizzata per tutti gli strumenti nella sede del cliente.

- Attività di audit e tracking – Le regole e la conformità alle norme comportano che il sistema dell'impresa debba facilitare audit e tracking di tutte le attività degli utenti e dell'amministrazione.

Axeda ServiceLink offre le prestazioni, la flessibilità e la scalabilità necessarie a soddisfare le esigenze della più vasta gamma dei clienti del RemoteCare Leica Microsystems offrendo il più largo range di protezione dei dati e di funzioni di sicurezza.

Figura 1: Comunicazioni Axeda Firewall-Friendly™



Nessun cambiamento necessario nelle infrastrutture IT o di sicurezza
Con l'uso della tecnologia Firewall-Friendly™ Axeda, RemoteCare è in grado di offrire una comunicazione bidirezionale basata su servizi Web standard inclusi l'Hypertext Transfer Protocol (HTTP), il Simple Object Access Protocol (SOAP) e l'eXtensible Markup Language (XML). Per il supporto del monitoraggio e della diagnostica remoti non sono necessarie modifiche all'infrastruttura della sicurezza IT del cliente finale. Inoltre, tutta la comunicazione tra il centro dati Leica o il service provider e il lato del cliente viene crittografata usando il Secure Sockets Layer (SSL) con un massimo di 168 bit.

Nessun VPN o modem necessario
L'agente RemoteCare inizia tutte le comunicazioni in conformità con l'ambiente di calcolo sicuro dal lato del dispositivo. Per implementare il RemoteCare non è neanche necessario impostare costosi VPN o compromettere la sicurezza usando comunicazioni di accesso remoto. Il solo requisito è una connessione a Internet.

I punti salienti della sicurezza di RemoteCare:
- Comunicazione Firewall-Friendly™
- Nessun cambiamento necessario nelle infra-strutture IT o di sicurezza
- Nessun VPN o modem necessario
- Il completo controllo del cliente finale per rafforzare le regole del business
- Sicurezza di utenti, applicazioni e dispositivi facile da impiegare e gestire
- HTTPS, PKI, e crittografia dati SSL a 128 bit

Autenticazione degli utenti e controllo dell'accesso di facile gestione
Per l'autenticazione degli utenti, il sistema RemoteCare usa lo standard Lightweight Directory Access Protocol (LDAP).

Il controllo dell'accesso degli utenti viene realizzato attraverso un controllo basato sull'attività e su uno basato sui dispositivi. Questi metodi vengono combinati in molti modi diversi per permettere agli utenti di eseguire il loro lavoro in modo efficace proteggendo l'accesso a informazioni sensibili.

Il controllo dell'accesso basato sulle attività permette all'amministratore del sistema RemoteCare di assegnare e classificare gli utenti usando l'Axeda ServiceLink e di definire le attività che possono essere eseguite. Ogni gruppo di utenti dispone di un accesso controllato all'applicazione Axeda, alla pagina e ai livelli funzionali.

Il controllo dell'accesso basato sui dispositivi offre un metodo per definire gli specifici dispositivi accessibili ad ogni gruppo di utenti. Questo metodo di controllo permette la visione delle informazioni solo sui dispositivi di cui un utente è responsabile.

Comunicazioni sicure e privacy dei dati
Molte delle informazioni che attraversano la rete Internet pubblica, lo fanno sotto forma di testo normale incapsulato all'interno dei messaggi standard HTTP. Gli hacker possono accedere alla rete nel punto vicino alla fonte o alla destinazione del messaggio e catturare e spiare il testo all'interno di tali messaggi HTTP tramite degli strumenti comunemente disponibili.

RemoteCare, attraverso il software Axeda e l'infrastruttura a server, supporta lo stesso standard di crittografia SSL usato dalle banche per le transazioni online. SSL supporta una lunghezza massima delle chiavi di 168 bit ed un'autenticazione mutuale usando dei certificati. RemoteCare può anche attivare una crittografia del messaggio con una chiave AES a 256 bit che può essere usata con SSL per crittografare i dati dietro la zona demilitarizzata (DMZ).

Impiego sperimentato
RemoteCare è impiegato in tutto il mondo dai produttori di campi di industrie come quelle relative alla sicurezza nazionale, alle scienze mediche, alle scienze della vita, alla tecnologia di informazione, alle telecomunicazioni, alla stampa e alla visualizzazione, ai chioschi, ai semiconduttori, alle produzioni industriali e all'automazione degli edifici.

Caratteristiche della sicurezza e vantaggi

La tecnologia Axeda dota RemoteCare delle seguenti caratteristiche di sicurezza e dei seguenti vantaggi

Sicurezza della rete

Caratteristiche:
- La tecnologia Firewall-Friendly™ è basata su servizi standard Web inclusi HTTP, SOAP, e XML.
- L'agente Axeda inizia tutte le comunicazioni, per cui i dispositivi non hanno bisogno di indirizzi IP pubblici e non sono visibili al di fuori del firewall.

Vantaggi:
- Gli utenti non devono effettuare alcuna modifica alle proprie impostazione di firewall e di server proxy, facilitando l'impiego e raggiungendo gli obiettivi di conformità
- Nessuna necessità di connessioni VPN o via modem.

Sicurezza del sistema e dei dati

Caratteristiche:
- La crittografia SSL supporta una lunghezza massima delle chiavi di 168 bit ed un'autenticazione mutuale usando certificati digitali bidirezionali.
- Crittografia del messaggio con una chiave AES a 256 bit che può essere usata con SSL per crittografare i dati dietro la DMZ.

Vantaggi:
- Hanno accesso ai dati e ai dispositivi previsti solo le parti autorizzate. I clienti finali possono limitare l'accesso, la visione e perfino le operazioni sulla base del ruolo dell'utente avendo quindi il controllo su utenti e operazioni.
- La sperimentata comunicazione basata su standard assicura la conformità con i requisiti delle norme.

Sicurezza degli utenti e delle applicazioni

Caratteristiche:
- L'accesso al sistema è controllato in modo centralizzato ed è autenticato tramite un sistema LDAP per imprese.
- Obbligo d'uso di password sicure – un minimo di sei caratteri con una combinazione di lettere, numeri, e simboli.
- Tutte le attività di accesso remoto vengono seguite e registrate.

Vantaggi:
- Gli utenti possono sfruttare gli account utente LDAP esistenti potendo così iniziare facilmente.
- Gli utenti finali hanno un dettagliato audit trail nell'analisi dell'attività del venditore per le esigenze di conformità.

Sommario
Leica Microsystems sceglie Axeda ServiceLink per il RemoteCare per offrire il massimo livello di sicurezza. Le aziende in tutto il mondo forniscono i servizi remoti ai propri clienti usando Axeda ServiceLink. Ciò avviene poiché Axeda implementa con attenzione i principi e gli standard di sicurezza nel design e nell'uso dell'infrastruttura e dei processi Axeda. Come per Leica Microsystems, per Axeda la massima priorità è un'elevata sicurezza che permetta ai clienti di raggiungere i propri obiettivi di servizio remoto in modo efficiente e sicuro.