White Paper

InTouch^{SM} Remote-Services

IT-Sicherheit

IT-Sicherheit ist für METTLER TOLEDO und seine Kunden, die Remote-Services nutzen, von grösster Wichtigkeit. METTLER TOLEDO bietet eine bewährte Remote-Servicelösung an, die vor Hackern schützt, die intelligenten Produkte von METTLER TOLEDO unterstützt und innerhalb der Standard-Netzwerksicherheitsmodelle agiert, sodass keine Änderungen an den IT- oder Sicherheitsinfrastrukturen unserer Kunden nötig sind.

Da Produkte von METTLER TOLEDO in den Kundennetzwerken verbunden sind, müssen Kunden auch die Gewissheit haben, dass die Remote-Servicelösung das Sicherheitsmodell des Kunden unterstützt, eine detaillierte Kontrolle der Benutzerrechte bietet und für Audit- sowie Nachverfolgungszwecke einsatzbereit ist.

Unsere Verpflichtung:

- Die Integrität des Systems beibehalten und schützen
- Daten von unberechtigten Personen schützen
- Sicherstellen, dass Systembenutzer authentifiziert werden
- Jeden Benutzer auf spezifische Daten, Ansichten und Aktionen begrenzen
- Flexibilität und Kontrolle bieten, um die Unternehmenspolitik durchzusetzen
- Die Prozesse und Technologielösung regelmässig von einem Drittanbieter auditieren und zertifizieren

Inhaltsverzeichnis

METTLER TOLEDO

1 IT-Sicherheit – Remote-Services

InTouch-Remote-Services bieten eine nahtlose Verbindung zwischen den Kundendiensttechnikern von METTLER TOLEDO und den intelligenten Produkten von METTLER TOLEDO innerhalb einer Kundenumgebung. Da diese Produkte häufig sensible Kundendaten sowie andere private und geschützte Informationen enthalten, zählen Sicherheits- und Compliance-Funktionen zu den wichtigsten Anforderungen einer Remote-Servicelösung. In diesem White Paper werden die Sicherheitsanforderungen von METTLER TOLEDO und seinen Kunden beschrieben. Darüber hinaus wird erklärt, wie InTouch-Remote-Services in Ihrer Umgebung funktionieren und wie sie Ihren technischen Sicherheitsanforderungen gerecht werden. Zudem werden in diesem Paper die wichtigsten Fragen beantwortet, wie etwa zur Kommunikation durch Firewalls und zur Netzwerksicherheit.

Unsere Verpflichtung
Datenschutz und Sicherheit sind für unsere Kunden von grösster Wichtigkeit. Aus diesem Grund verpflichtet sich METTLER TOLEDO zu folgenden Sicherheitsgrundsätzen:

- Die Integrität des Systems aufrechterhalten und schützen – Netzwerk, Ausrüstung und Daten
- Daten von unberechtigten Personen schützen
- Sicherstellen, dass Systembenutzer authentifiziert werden
- Jeden Benutzer auf spezifische Daten, Ansichten und Aktionen begrenzen
- Flexibilität und Kontrolle bieten, um die Unternehmenspolitik durchzusetzen
- Die Prozesse und Technologielösung regelmässig von einem Drittanbieter auditieren und zertifizieren

2 METTLER TOLEDOs Anforderungen an die Sicherheit von Remote-Services

Die Lösung von METTLER TOLEDO muss die strengsten Sicherheitsanforderungen erfüllen, damit Remote-Services effektiv und routinemässig genutzt werden können. Damit erhalten Kunden die Gewissheit, dass ihre Verbindungen geschützt und vertraulich sind.

Zu den Anforderungen von METTLER TOLEDO zählen:

Bewährtes Design
Wenn ein Computer an das Internet angeschlossen wird, treten immer Sicherheitsbedenken auf. Dies ist beim Anschluss intelligenter Produkte nicht anders. Ein Remote-Support- und Überwachungssystem muss vor allen IT-Sicherheitsbedrohungen schützen.

Support für mehrere Geräte
METTLER TOLEDO muss sicheren Support für eine grosse Bandbreite und Anzahl verschiedener Produkttypen und komplexer Kundenkonfigurationen bieten, ohne dass bei den Kunden wesentliche Änderungen notwendig sind.

Schnelle Bereitstellung
Damit Kunden Remote-Servicesysteme einführen können, müssen die Sicherheitsfunktionen bereits im aktuellen Netzwerksicherheitsmodell des Kunden bestehen.

Validierung durch unabhängige Sicherheitsfirma
Die offizielle Zertifizierung in Form einer Sicherheitsprüfung eines akkreditierten Drittanbieters gibt METTLER TOLEDO das Vertrauen in die Fähigkeiten seiner Geschäftspartner, die Technologie und deren Prozesse und Verfahren.

3 Kundenanforderungen an die Sicherheit von Remote-Services

Intelligente Produkte werden an die Netzwerke der Kunden angeschlossen. Jeder Kunde verfügt über seine eigenen Sicherheitsrichtlinien und Netzwerkschutzmechanismen in Form von Firewalls, Proxy-Servern und Adressierungsschemata. Ein Produkt, das an das Kundennetzwerk angeschlossen ist, muss durch diese Sicherheitsebenen geschützt werden. Wenn ein Remote-Service-Angebot Änderungen am Netzwerkschutz des Kunden erforderlich macht, wird es höchstwahrscheinlich abgelehnt werden. Daher ist es wichtig, die Anforderungen des Kunden zu beachten, einschliesslich:

Beibehaltung des aktuellen Sicherheitsmodells
Die intelligenten Produkte von METTLER TOLEDO unterstützen die Art, wie die IT-Organisation des Kunden Sicherheitsmassnahmen, Richtlinien und Abläufe verwaltet und die anerkannten Branchenstandards einhalten soll.

Kontrolle des Benutzerzugangs
In Übereinstimmung mit dem Sicherheitsmodell des Kunden müssen InTouch-Remote-Services dem Kunden eine detaillierte Kontrolle bieten und Aktionen festlegen, die am Gerät ausgeführt werden können, wie etwa Datensammlung sowie Software-Updates, und festlegen, wann diese durchgeführt werden können. Diese Richtlinien können zentral für alle angeschlossenen Geräte am Standort des Kunden festgelegt werden.

Aktivitäten prüfen und nachverfolgen
Richtlinien und gesetzliche Auflagen schreiben häufig vor, dass ein Remote-Servicesystem die Prüfung und Nachverfolgung aller Benutzer- und Administratoraktivitäten vereinfachen muss.

Datenintegrität und Sicherheit
Daten, die vom angeschlossenen Gerät von METTLER TOLEDO an den Unternehmensserver gesendet werden, sind durch Datenverschlüsselung und SSL/TLS-Zertifikatvalidierung geschützt. Es werden nur die Daten gesammelt, die zur Überwachung, Diagnose und Fehlerbehebung des METTLER TOLEDO-Geräts notwendig sind. Der Datensatz, der dem Unternehmen übergeben wird, enthält keine sensiblen Kundendaten.

InTouch-Remote-Services liefern die erforderliche Leistung, Flexibilität und Skalierbarkeit, um die Anforderungen der diversen Kunden von METTLER TOLEDO zu erfüllen, denn sie bieten die grösste Auswahl an Datenschutzgarantien und Sicherheitsfunktionen.

4 Wie funktionieren InTouch-Remote-Services?

InTouch-Remote-Services überwachen den Status, die Betriebsparameter und die Konfiguration der Ausrüstung von METTLER TOLEDO an Ihrem Standort. Dies erfolgt über einen softwarebasierten Monitoring Agent, der sicher mit dem gehosteten Cloud-Enterprise-Server kommuniziert.

Die InTouch-Remote-Service-Anwendung, die in der Cloud läuft, wertet die Leistung Ihres Geräts aus, wenn Daten und Alarme empfangen werden, und speichert die Daten zur Trendanalyse. Wenn ein Problem erkannt wird, benachrichtigt der gehostete Cloud-Enterprise-Server das entsprechende Service-Personal. Der Remote-Support-Techniker diagnostiziert anschliessend das Problem durch Analyse der Daten am gehosteten Cloud-Enterprise-Server – aus der Ferne und ohne Unterbrechung Ihres Betriebs.

Wenn eine weitere Diagnose erforderlich ist, kann der Remote-Support-Techniker mit Ihrer Erlaubnis aus der Ferne auf das Gerät zugreifen und direkt am System arbeiten.

Wenn die Diagnose bestätigt ist, kann das Problem dann sofort korrigiert werden, so wie bei einem erforderlichen Software-Update oder einer anderen Konfigurationsanpassung. Mit Ihrer Genehmigung kann der Remote-Servicetechniker zahlreiche Probleme für Sie aus der Ferne beheben.

Wenn ein Servicetechniker zur Behebung des Problems zu Ihrer Anlage geschickt werden muss, stellen die durch InTouch gesammelten Informationen sicher, dass er mit den erforderlichen Teilen und dem nötigen Wissen am Standort ankommt.

5 Technologieübersicht

Das InTouch-Remote-Servicesystem besteht aus zwei Hauptkomponenten: der Remote-Service-Agent-Software, die auf dem Gerät von METTLER TOLEDO am Standort des Kunden läuft, und dem gehosteten Cloud-Enterprise-Server mit den Anwendungen, die Zugang zu den Geräteinformationen bieten.

Die Remote-Service-Agent-Software am Standort des Kunden überwacht regelmässig das Gerät von METTLER TOLEDO. Dabei wird der Status der wichtigsten Datenelemente überprüft, um ein Bild über den Zustand und die Konfiguration des Systems zu vermitteln. Zudem kommuniziert der Remote-Service-Agent regelmässig mit der Umgebung des Cloud-Enterprise-Servers, um über die Daten und den Status des Geräts zu informieren.

InTouch-Remote-Services nutzen Ihre bestehende Netzwerk- und Sicherheitsinfrastruktur in vollem Umfang. Solange der Agent eine ausgehende Verbindung zum Cloud-Enterprise-Server mithilfe von Port 443 öffnen kann, sind keine Änderungen zur Erstellung einer Remote-Verbindung erforderlich.

Bei der sicheren Kommunikationsmethode Firewall-Friendly™ ist es nicht nötig, dass der Agentcomputer über eine feste oder öffentlich sichtbare TCP/IP-Adresse verfügt. Dies liegt daran, dass METTLER TOLEDO niemals eine eingehende Verbindung zum Agent an Ihrem Standort initiiert. Der Agent initiiert alle Kommunikationen mit den gehosteten Cloud-Enterprise-Servern und nachdem die Verbindung initiiert und authentifiziert wurde, besteht eine bidirektionale Kommunikation.

Der Agent überwacht einen spezifischen Parametersatz und sendet nur Datenänderungen an die Cloud-Enterprise-Server. Dadurch wird der Datenverkehr an METTLER TOLEDO in Ihrem Netzwerk minimiert. Zudem sendet der Agent regelmässig eine kurze Mitteilung in Form eines „Herzschlags" an die Cloud-Enterprise-Server, um zu bestätigen, dass der Agent aktiv ist. Diese Mitteilungen ermöglichen es den Support-Mitarbeitern von METTLER TOLEDO, eine Handlungsanforderung zu senden. Zum Beispiel können die Support-Mitarbeiter ein Fehlerprotokoll anfordern oder eine Remotesitzung initiieren. Das nächste Mal, wenn der Agent sich anmeldet, wird die Anfrage übermittelt.

6 Aufrechterhaltung der Integrität der Netzwerksicherheit

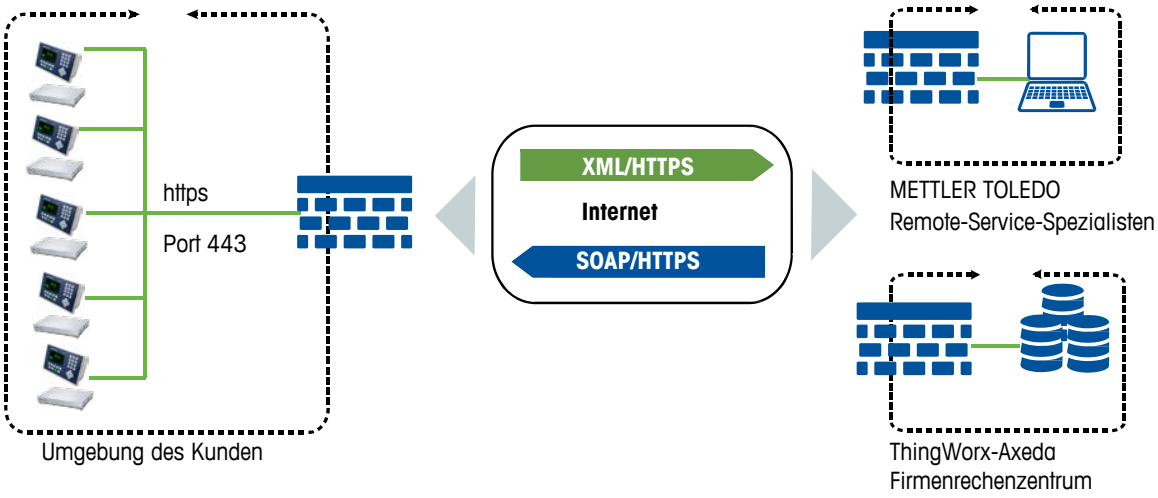
Das Unternehmen ThingWorx-ThingWorx-Axeda setzt bewährte Branchenverfahren zur Verschlüsselung seines Netzwerkverkehrs ein. Transport Layer Security (TLS) stellt Support für SSL-Zertifikate von global anerkannten Zertifizierungsstellen bereit und bietet ausserdem Sicherheit auf der Kommunikationsebene. Der Inhalt der Mitteilungen wird dann weiter mit dem Advanced Encryption Standard (AES) 256 Algorithmus gesichert. Der Algorithmus RSA 2048 wird für Schlüsselaustausche verwendet.

ThingWorx-ThingWorx-Axedas patentierte Firewall-Friendly™ Technology bietet eine bidirektionale Kommunikation auf Basis von Webservicestandards, einschliesslich Hypertext Transfer Protocol (HTTPS), Simple Object Access Protocol (SOAP) und Extensible Markup Language (XML). Es sind keine Änderungen an der IT-Sicherheitsinfrastruktur des Kunden erforderlich, um Support für sein angeschlossenes Gerät zu bieten.

Der Remote-Service-Agent an den Geräten von METTLER TOLEDO initiiert die gesamte Kommunikation mit dem gehosteten Cloud-Enterprise-Server. Diese intelligente Agent-Software ermöglicht es dem Gerät, als Web-Client zu agieren, und leitet Mitteilungen an den Enterprise-Server weiter, die als HTTPS POST-Befehle verschickt werden. Jede Mitteilung enthält im XML-Format verschlüsselte Daten, die mithilfe von SSL-Verschlüsselung über Port 443 verschickt werden. Der Software-Agent kann nur auf die spezifischen Server zugreifen, die für InTouch-Remote-Services identifiziert werden.

Da das Gerät die gesamte Kommunikation initiiert, ist es nicht notwendig, VPNs einzurichten oder zu warten, um InTouch-Remote-Services einzusetzen oder die Sicherheit durch Verwendung von Dial-up-Kommunikation zu gefährden.
Das Gerät hat keine öffentliche IP-Adresse. Alle Geräte bleiben sicher hinter den IT-Sicherheitsinfrastrukturen des Kunden verborgen, die aus Firewalls, Routern und Proxy-Servern bestehen.

Im Grunde genommen verhält es sich wie folgt: Wenn ein Webbrowser mithilfe der aktuellen Netzwerkinfrastruktur des Kunden auf das Internet zugreifen kann, kann das mit InTouch-Remote-Services ausgerüstete Gerät über dieselbe Netzwerkverbindung mit dem Unternehmensserver kommunizieren. Aus diesem Grund sind keine Änderungen an der IT-Sicherheitsinfrastruktur erforderlich.



7 Benutzerauthentifizierung, Zugangskontrolle und Audit-Protokollierung

Benutzer-Authentifikation

Der Zugriff auf die Anwendungen von InTouch-Remote-Services ist auf die hochqualifizierten Service- und Support-Mitarbeiter von METTLER TOLEDO beschränkt, sodass sie ihre Arbeit effizient erledigen können und gleichzeitig der Zugriff auf sensible Informationen gesichert ist.

Der gehostete Cloud-Enterprise-Server macht es erforderlich, dass jeder Benutzer über eine eigene Benutzernamen-ID und ein Passwort verfügt, um auf das System zuzugreifen. Die Passwörter müssen sicher sein und jeder Benutzer muss sein Passwort alle 90 Tage ändern.

Daten sind jedes Mal gefährdet, wenn eine Anwendung geöffnet ist und der Computer angelassen wird und unbeaufsichtigt bleibt. Um eine nicht autorisierte Nutzung zu verhindern, werden inaktive Benutzer automatisch nach 20 Minuten abgemeldet.

Benutzerzugangskontrolle

Die Benutzerzugangskontrolle erfolgt durch die aktivitäts- und Device-basierte Zugangskontrolle.
Diese Methoden werden in vielfältiger Weise miteinander kombiniert, damit Benutzer ihre Arbeit effektiv erledigen können, während gleichzeitig der Zugriff auf sensible Informationen geschützt ist.

Die aktivitätsbasierte Zugangskontrolle ermöglicht es dem Systemadministrator, Benutzer zu Anwendungen von InTouch-Remote-Services zuzuweisen, diese zu klassifizieren und die durchführbaren Aktivitäten festzulegen. Jede Benutzergruppe erhält kontrollierten Zugang zu den Anwendungen von InTouch-Remote-Services auf Grundlage ihrer beruflichen Aufgabe und ihrer Erfahrung mit Produkten von METTLER TOLEDO.

Mit der Device-basierten Zugangskontrolle können spezifische Geräte bestimmt werden, auf die jede Benutzergruppe zugreifen kann. Diese Kontrollmethode begrenzt die Einsicht von Geräteinformationen auf die Geräte, für die ein Benutzer verantwortlich ist.

Audit-Protokollierung
Darüber hinaus erstellt das Unternehmenssystem einen vollständigen Audit Trail, in dem alle Aktivitäten und Ereignisse sowohl der intelligenten Geräte als auch der Remote-Support-Benutzer dokumentiert werden. Das Auditprotokoll enthält Informationen über Benutzerinteraktionen innerhalb des Systems und mit Maschinen. Die Daten des Auditprotokolls werden auf dem gehosteten Cloud-Enterprise-Server gespeichert und können nicht aus dem System entfernt werden. Die Benutzer von InTouch-Remote-Services können nur das Auditprotokoll für die METTLER TOLEDO-Produkte einsehen, auf die sie zugreifen dürfen. Wenn ein Benutzer oder Produkt aus dem System entfernt wird, bleiben alle Daten über den Benutzer oder das Produkt weiterhin im Auditprotokoll gespeichert. Daher bewahrt das System Protokolle darüber auf, wer was wann und an welchen Geräten getan hat.

8 Sicherstellen der Vertraulichkeit von Daten

Die Technologie, die zur Bereitstellung von InTouch-Remote-Services verwendet wird, setzt Secure Sockets Layer/Transport Layer Security Protocol (SSL/TLS) zur sicheren Datenübertragung ein. SSL/TLS bietet ein Protokoll zur Übertragung privater Daten über das Internet. Neben der Verschlüsselung von Daten ermöglicht der SSL-Standard auch eine Authentifizierung, um sicherzustellen, dass sowohl der Sender als auch der Empfänger von Daten einander bekannt sind. SSL unterstützt eine Schlüssellänge von 2048 Bit sowie die gegenseitige Authentifizierung mithilfe von Zertifikaten. SSL ist derselbe Verschlüsselungsstandard, der von Banken für Online-Transaktionen verwendet wird.

Der InTouch-Remote-Service-Agent, der in die intelligenten Produkte von METTLER TOLEDO integriert ist, überwacht und analysiert nur spezifische Datenelemente, die für den Betrieb und die Leistung des Produkts relevant sind. Sensible Kundendaten sind nicht in dem Datensatz enthalten, der regelmässig die Produktleistung überwacht. Im Unternehmen werden nur die Daten gesammelt und analysiert, die benötigt werden, um das spezifische Produkt zu überwachen, zu diagnostizieren und Probleme zu beheben.

Datenschutz und Nutzungserklärung
Die Daten, die von METTER TOLEDO mithilfe der InTouch-Remote-Services gesammelt werden, werden streng kontrolliert und sind nur autorisierten Mitarbeitern zugänglich. Die Datenelemente, die durch die Verwendung von InTouch-Remote-Services gesammelt und vom Modelltyp festgelegt werden, enthalten nur Geräteparameter, die zur Diagnose und Behebung von Geräteproblemen erforderlich sind. METTLER-TOLEDO wird unter keinen Umständen Daten oder Informationen, die mithilfe von InTouch-Remote-Services gesammelt wurden, gegenüber Dritten offenlegen, überlassen, verkaufen.

9 Zusätzliche Sicherheitsmerkmale

ISO/IEC 27001:2013

ThingWorx-ThingWorx-Axeda umfasst eine ganzheitliche Sicherheitsstrategie, die alle Ebenen abdeckt, einschliesslich Netzwerk, Anwendung, Benutzer und Datensicherheit. ThingWorx-ThingWorx-Axeda verfügt über die ISO 27001:2013 Zertifizierung, die dem Unternehmen bei seinem Ziel hilft, das höchste Mass an Sicherheit, Leistung und Verfügbarkeit des ThingWorx-Axeda M2M Cloud Services bereitzustellen.

Der ThingWorx-Axeda M2M Cloud Service ist darauf ausgelegt, die wichtigsten Probleme zur Informationssicherheit zu lösen, und zwar mit Funktionen, die:

- **Die Netzwerksicherheit an den Kundenstandorten aufrechterhalten** – Mithilfe von ThingWorx-Axedas patentierter Firewall-Friendly-Kommunikation nutzt ThingWorx-Axedas Lösung die bestehende Sicherheitsinfrastruktur Ihrer Kunden.
- **Daten vor unberechtigten Personen verbergen** – Die gesamte Kommunikation zwischen Ihnen und Ihrem Kunden wird mithilfe der SSL-Verschlüsselung gesichert, dieselbe Methode, die Banken für sichere Online-Transaktionen nutzen.
- **Eine sichere und skalierbare On-Demand-Infrastruktur bieten** – ThingWorx-Axedas ISO 27001:2013-zertifizierte Rechenzentren werden einer jährlichen SAS 70-Prüfung unterzogen und profitieren von modernster Ausrüstung, Technologieinvestitionen und Fachkenntnissen. Die Datenzentren beinhalten redundante Untersysteme, Energieversorgung, Klimaanlage und Netzwerkverkabelung. Dadurch wird eine Verfügbarkeit von mehr als 99,95 % bereitgestellt.
- **Sicherstellen, dass Systembenutzer authentifiziert werden** – Alle Zugriffe auf das System werden zentral kontrolliert, sodass eine Authentifizierung mit Passwort erforderlich ist. Alle Benutzeraktionen werden umfassend auf Rückführbarkeit geprüft.
- **Jeden Benutzer auf spezifische Daten, Ansichten und Aktionen begrenzen** – Nach der Authentifizierung sind Aktionen der Benutzer auf die Produkte beschränkt, für die sie verantwortlich sind, sowie gemäss der Zugriffsebene ihres Aufgabenbereichs.

Bewährte Bereitstellung

InTouch-Remote-Services verwenden dieselbe Technologie, die aktuell auf der ganzen Welt von Herstellern aus verschiedensten Branchen eingesetzt wird. Dazu zählen auch Anwendungen in den Bereichen Heimatschutz, Medizin, Biowissenschaften, Informationstechnologie, Telekommunikation, Druck und Bildverarbeitung, Kiosksysteme, Halbleiter, industrielle Automatisierung und Gebäudeautomation. ThingWorx-Axeda bietet diesen Herstellern und ihren Kunden das gleiche hohe Mass an Sicherheit und Datenschutz, das unsere Kunden erwarten.

Zudem ist ThingWorx-Axeda ein führender Anbieter von Remote-Service-Lösungen für zahlreiche wichtige Lieferanten von Netzwerkspeicherungs- und IT-Infrastrukturhardware. Daher verwendet Ihre IT-Abteilung Lösungen für diese Unternehmen. Sie sind also vielleicht bereits vertraut mit der Technologie von ThingWorx-Axeda, da diese Unternehmen dieselbe Technologie von ThingWorx-Axeda einsetzen, die METTLER TOLEDO verwendet.

10 Zusammenfassung

METTLER TOLEDO hat ThingWorx-ThingWorx-Axeda als seinen Anbieter von Remote-Service-Infrastruktur ausgewählt, um InTouch-Remote-Services optimal nutzen zu können. Damit kann METTLER TOLEDO seinen Kunden das höchste Mass an Sicherheit bieten, ohne ihre aktuelle IT-Sicherheitsinfrastruktur zu ändern. Unternehmen auf der ganzen Welt nutzen ThingWorx-ThingWorx-Axeda, um ihren Kunden Remote-Services zu liefern. Dies ist das Ergebnis einer sorgfältigen Umsetzung von Sicherheitsgrundsätzen und -standards im Design und Betrieb der Infrastruktur und Services, die ThingWorx-ThingWorx-Axeda bereitstellt.

Eine hohe IT-Sicherheit ist für METTLER TOLEDO von grösster Wichtigkeit. Daher möchten wir unseren Kunden die Gewissheit geben, dass wir InTouch-Remote-Services sicher und effizient bereitstellen. So erhalten Kunden letztendlich eine höhere Produktverfügbarkeit sowie eine bessere Produktleistung und es ermöglicht ihnen, das Beste aus ihren METTLER TOLEDO Produkten herauszuholen.

www.mt.com/service

Mehr Informationen

Mettler-Toledo GmbH
Industrial
CH 8606 Greifensee
Schweiz
Tel.: +41-44-944 22 11
Fax: +41-44-944 30 60

MTSI 30259895