



## Sicherheit für BeckmanConnect Remote Support

BeckmanConnect Remote Support ist vom Kunden auf jedem Beckman Coulter vernetzten Instrumentensteuerungs-PC installierbar, der Zugang zu erlaubten Netzwerkendpunkten hat und auf dem der Kunde Administratorzugriff hat.

Zu den Funktionen von BeckmanConnect Remote Support gehören:

- Benachrichtigungen über Probleme mit der Systemkonfiguration oder über Leistung/Ausfälle des Geräts
- Kundeninitiiertes Fernsupport über eine richtlinien- und zugriffsbeschränkte angepasste TeamViewer-Version
- Suche nach neuen verfügbaren Upgrades für BeckmanConnect, um neue Funktionen zu installieren

Dieses Dokument enthält Informationen zu den Sicherheitsfunktionen von BeckmanConnect Remote Support.

### Komponenten

#### TeamViewer Client



Eine angepasste, zugriffsbeschränkte und richtliniengesicherte TeamViewer-Installation, die den Fernsupport für ein System **nur** örtlichen Beckman Coulter-Supportmitarbeitern ermöglicht, nachdem die Verbindung vom Labortechniker initiiert und genehmigt wurde. TeamViewer wird als Service ausgeführt und verfügt über eine Verknüpfung innerhalb der Betriebssysteme. Der Client ist so konfiguriert, dass er immer ausgeführt wird und mit den TeamViewer-Servern kommuniziert.

#### Benachrichtigungsclient



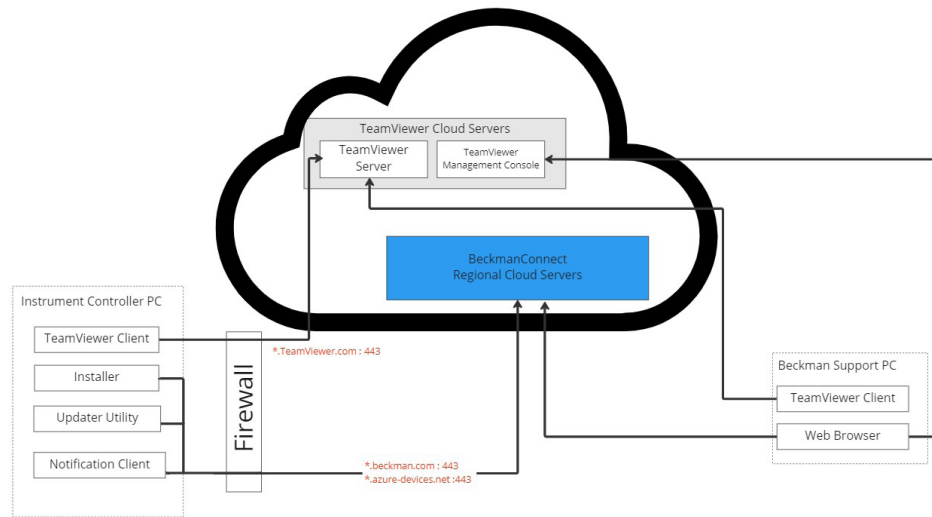
Ein Softwaredienst, der Echtzeit-Benachrichtigungen über den Software- und Gerätestatus an den Gerätesteuerungs-PC sendet und aktive Systembenachrichtigungen protokolliert.

#### BeckmanConnect-Upgrade-Dienstprogramm



Ein Softwaredienst, der die Komponenten von BeckmanConnect Diagnostic Support auf Software-Updates überwacht und Benutzer benachrichtigt, wenn ein Upgrade zur Installation verfügbar ist.

## Systemarchitektur



## Sicherheitsübersicht

### Sicherheit von Softwarekomponenten

	Benachrichtigungsclient-Updater Installationsprogramm	TeamViewer Client-Installationsprogramm
Verschlüsselung während der Übertragung	SSL/TLS 1.2	AES-256-Bit-Sitzungsverschlüsselung
Authentifizierung	Eindeutige Schlüssel mit AES-256-Bit-Verschlüsselung für jedes Gerät	RSA 4096-Bit-Schlüssel für Sitzungen
Firewall-Regeln am Ziel	Beckman Cloud-Server  Ausgehend: *.beckman.com:443 (außerhalb Chinas) *.azure-devices.net:443 (außerhalb Chinas) *.mybeckman.cn:443 (China) *.azure-devices.cn:443 (China)	TeamViewer Cloud-Server  Ausgehend *.teamviewer.com:443
Codesignatur		Digicert

### Serversicherheit

	Beckman-Server	TeamViewer-Server
Übertragene und gespeicherte Daten	Registrierung: E-Mail-Adresse und Name, Gerät, Geräte-ID und Seriennummer des Teilnehmers  Laufend: Online-Status  Alle Daten werden serverseitig von einer aktuellen Malware-Schutzsoftware gescannt.	Geräte-ID, Seriennummer, Online-Status/-Verlauf, Sitzungs- und Sitzungsereignisprotokoll
Verschlüsselung ruhender Daten	256-Bit-AES	Vertrauliche Daten: AES/RSA 2048 Bit verschlüsselt
Zugriffsbeschränkungen	Datenzugriff ist auf Beckman Support-Mitarbeiter beschränkt, die über Beckman SSO in lokalen Datenschutzbestimmungen (z. B. DSGVO, HIPAA) geschult sind.	Datenzugriff ist auf Beckman Support-Mitarbeiter beschränkt, die in lokalen Datenschutzbestimmungen (z. B. DSGVO, HIPAA) geschult sind.
Bandbreite Anforderungen	6 Mbit oder mehr empfohlen	
Rechenzentren	ISO/IEC 27001-zertifiziert DSGVO-konform	
Eindringenschutz	Eindringenschutz-Software vorhanden	Für die Authentifizierung vom neuen Standort aus ist eine E-Mail-Verifizierung erforderlich

## Sicherheit für die Remotedesktop-Freigabe

Vor der Aktivierung der Fernsupport-Funktionen sind das gründliche Durchlesen unserer IT-Anforderungen sowie die Zustimmung zu den Dienstleistungsbedingungen erforderlich.

BeckmanConnect Remote Support umfasst die folgenden Sicherheitsmerkmale:

- Der Zugriff ist auf authentifizierte Mitarbeiter von Beckman Coulter beschränkt, die eine Schulung zu den für die Region des Kunden geltenden Daten- und Datenschutzrichtlinien absolviert haben.
- Die Zulassungsliste für TeamViewer-Verbindungen wird bereitgestellt, um den Zugriff auf Geräte aus Quellen außerhalb des Wartungs- und Support-Netzwerks von Beckman Coulter zu verhindern.
- Anfragen nach einer ausgehenden TeamViewer-Verbindung sowie die Meeting-Funktion innerhalb des Client sind deaktiviert.
- TeamViewer stellt für jede Verbindung ein einzigartig generiertes Passwort mit 8+ Zeichen zur Verfügung. Dieses Passwort ändert sich mit jeder neuen Sitzung und bietet Schutz vor Brute-Force-Angriffen durch eine exponentielle Passwortsperrung, die unautorisierte Verbindungen verhindert.
- Nach der erfolgreichen Authentifizierung einer sicheren TeamViewer-Sitzung müssen Benutzer jede Bildschirmansichts-, Fernsteuerungs- oder Dateiübertragungsanforderung manuell über den TeamViewer-Client genehmigen. Verbindungsanfragen und Dateiübertragungen werden zu Auditzwecken auf sicheren TeamViewer-Servern protokolliert.
- Hinweis: Die Dateiübertragung während Remote-Sitzungen ist derzeit nicht für Gerätesteuerungs-PCs aktiviert, die persönliche Gesundheitsinformationen enthalten (Navios EX, DxFLEX, Data Innovations Instrument Manager, AQUIOS CL, CellMek SPS, Navios). Wenn diese Funktion in einer zukünftigen Version aktiviert wird, müssen Benutzer ein Update herunterladen und die neue Funktion während der Installation autorisieren, bevor sie aktiviert wird.