

Die Digitalplattform hiXserver für intelligente
Gebäudesicherheit und -steuerung

Sicherheit 4.0 für Ihr Unternehmen



hiXserver



Digitalplattform hiXserver:

Enorme Vorteile – höchste Sicherheit für jede Gebäudeart



Vorteil 1 ✓

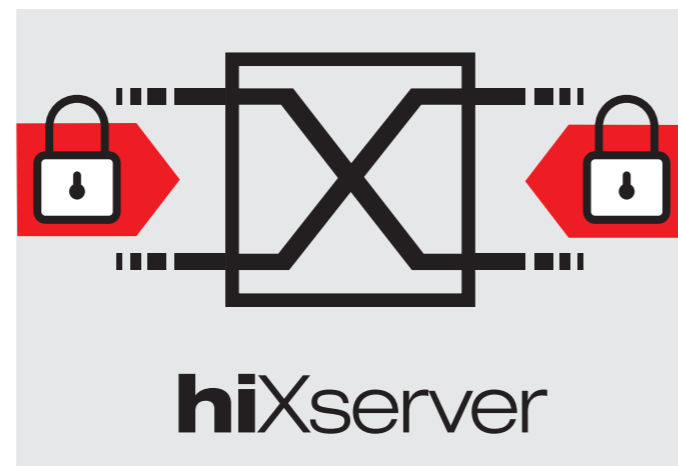
Daten liegen nicht in der Cloud



Als erste Digitalplattform ermöglicht hiXserver die vollumfängliche und komfortable Fernservice-Verbindung und Verwaltung zu einer Einbruch- und Gefahrenmeldeanlage von TELENOT, unabhängig von der Netz-Infrastruktur, in welcher diese betrieben wird. hiXserver ermöglicht von jedem Ort der Welt die gesicherte, komplette Datenverwaltung und Regelung sämtlicher Zugriffsrechte auf das jeweilige Objekt.

- **Transponder einlernen**
- **Personen- und Transponderverwaltung**
- **Anzeige des Ereignisspeichers**
- **Statusabfrage**

Ebenso ermöglicht die neue Digitalplattform hiXserver die sichere, intelligente Steuerung und Bedienung der Einbruch- und Gefahrenmeldeanlagen und smarter Zusatzfunktionen über die App BuildSec 4.0 (vgl. S. 6/7).



Bei üblichen IoT- (Internet of Things) oder Cloudlösungen werden die Systemzustände auf Servern abgelegt, dort über mobile Endgeräte gesteuert und mit der Anlage synchronisiert. Damit wird neben den unvermeidbaren Kommunikationswegen ein weiteres Angriffsziel geboten – der Cloud-Server.

Durch Manipulation der dort abgelegten Daten kann die Anlage vor Ort direkt beeinflusst werden – im schlimmsten Fall lässt sich eine Einbruch- und Gefahrenmeldeanlage unscharf schalten. Selbst, wenn es nur möglich ist, die in der Cloud abgelegten Anlagendaten zu lesen, gibt dies direkte Einblicke in das Nutzerprofil, was wiederum zu Sicherheitsrisiken führt.

Nicht so bei der Digitalplattform hiXserver. Aus Sicherheitsgründen besitzt sie zu keiner Zeit sensible Informationen über

den Zustand der Einbruch- und Gefahrenmeldeanlage, wie z.B. den Schärfezustand. Sämtliche Anlagen- und Objektinformationen werden vollständig anonym zwischen den Endgeräten ausgetauscht. Anfällige Cloudlösungen werden so vermieden.

Firmennetzwerk bleibt geschützt

Da die Kommunikation ausschließlich und direkt zwischen PC/Mobilgerät und Einbruch- und Gefahrenmeldeanlage erfolgt, ist die Freigabe Ihres Firmennetzwerks nicht notwendig. Ihre Unternehmensdaten bleiben vor dem Zugriff durch Dritte geschützt. Damit beschreitet die neue Digitalplattform hiXserver von Telenot ein neues, deutlich sichereres und zuverlässigeres Digitalzeitalter des externen Zugriffs auf Sicherheitstechnik.

✓ **Unabhängigkeit von Netzwerkstruktur**

✓ **Firmennetzwerk bleibt geschützt**

✓ **Daten liegen nicht in der Cloud**

Vorteil 2 ✓

TLS und AES für eine sichere Ende-zu-Ende-Verschlüsselung

Die Digitalplattform hiXserver nutzt für die Kommunikation die hochsicheren Verschlüsselungen TLS (Transport Layer Security) mit beidseitig zertifikatsbasierter Authentifizierung der Kommunikationspartner und AES (Advanced Encryption Standard) auf zwei voneinander getrennten Kanälen.

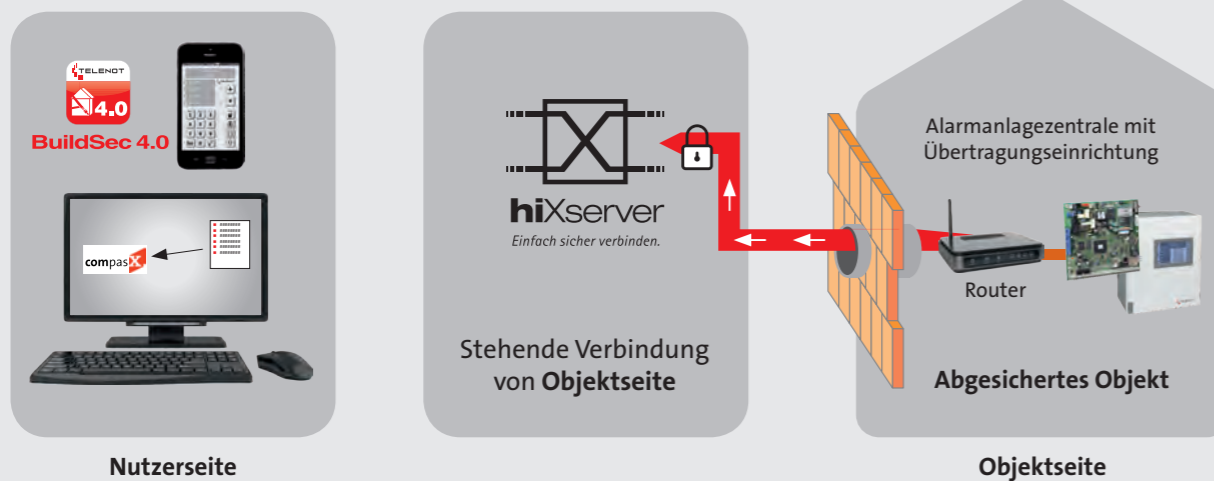
Aufbau und Funktionsweise der Fernservice-Verbindung zwischen Software und Gefahrenmeldeanlage über die Digitalplattform erfolgt wie nachfolgend beschrieben.

✓ **Kommunikation auf zwei getrennten Kanälen**

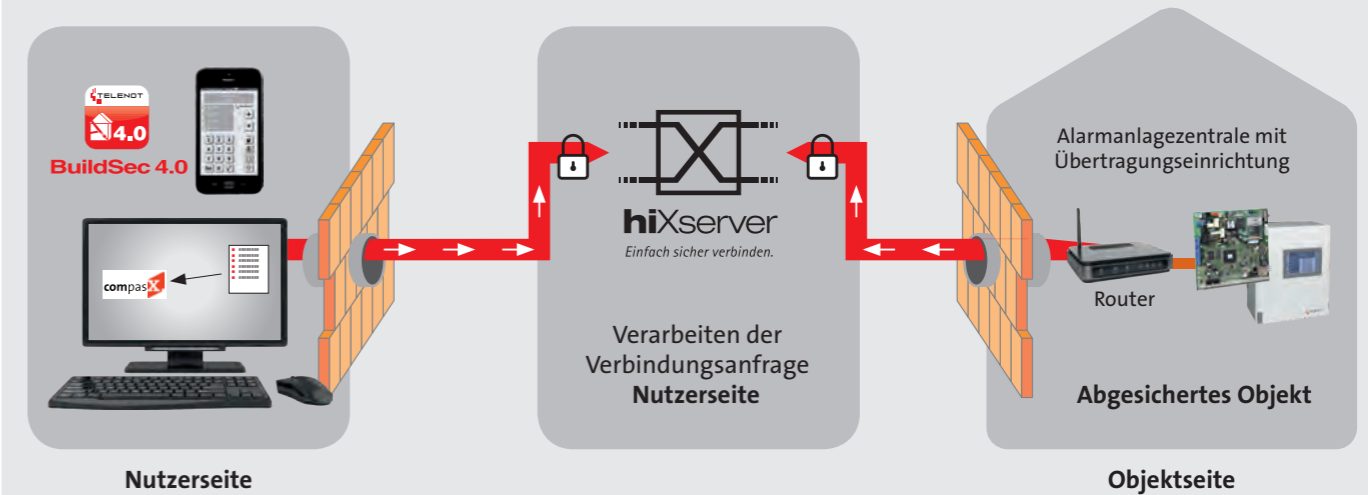
✓ **Zertifikatsbasierte Authentifizierung**

✓ **Verbindungsaufbau erst, wenn Authentizität, Vertraulichkeit und Integrität sichergestellt sind**

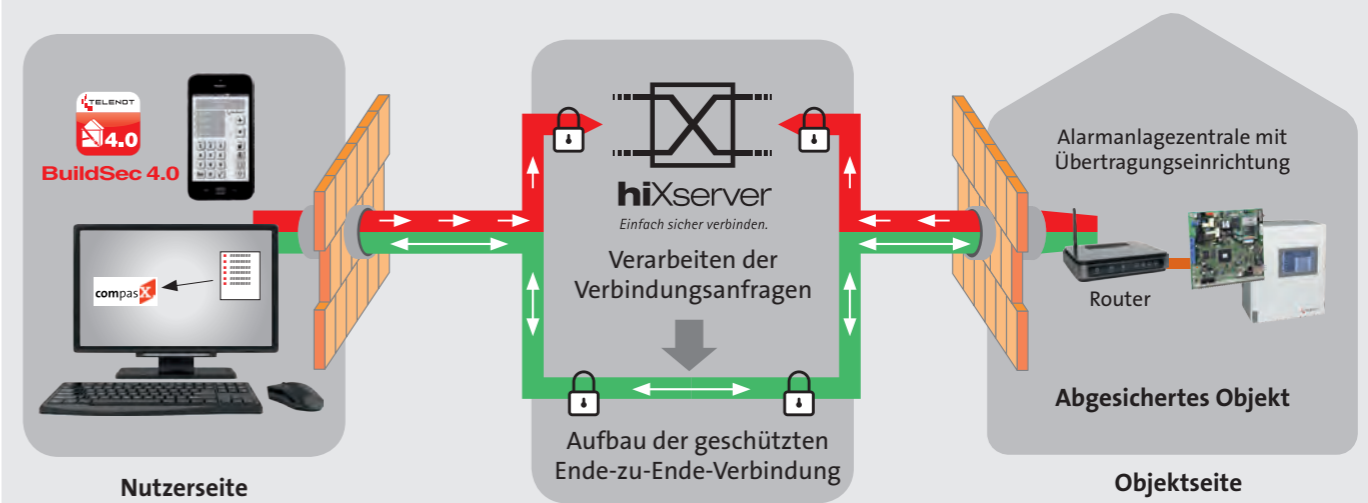
1 Der Steuerkanal der Gefahrenmeldeanlage ist permanent mit dem hiXserver verbunden.



2 Bei Bedarf verbindet sich die Nutzerseite über den Steuerkanal mit dem hiXserver. Dies wird mittels des Verschlüsselungsprotokolls TLS realisiert, das die Aspekte „Vertraulichkeit“, „Authentizität“ und „Integrität“ sicherstellt. Die Überprüfung beider Seiten findet über die beidseitige zertifikatsbasierte Authentifizierung statt unter dem Motto „Wir kennen uns.“



3 Ist diese Überprüfung positiv, erfolgt die Kommunikation separat über einen zweiten AES-verschlüsselten Kanal. Für die sichere, geschützte Ende-zu-Ende-Verbindung wird jedes Mal ein neuer einmaliger AES-Schlüssel erzeugt unter dem Motto „Wir kennen uns und kommunizieren sicher (verschlüsselt)“.



→→→ TELENOT-Management-Protokoll (TLS-Verschlüsselung)

↔↔↔ Verschlüsselte Ende-zu-Ende-Kommunikation im VdS-Protokoll (AES-Verschlüsselung)

TLS und AES über zwei getrennte Kanäle.

Kanal 1: TLS stellt Vertraulichkeit, Authentizität und Integrität sicher → „Wir kennen uns!“
Kanal 2: AES stellt verschlüsselte Kommunikation her → „Wir kommunizieren sicher!“

Vorteil 3 ✓

BuildSec 4.0:
Zuverlässig und sicher –
jederzeit und überall

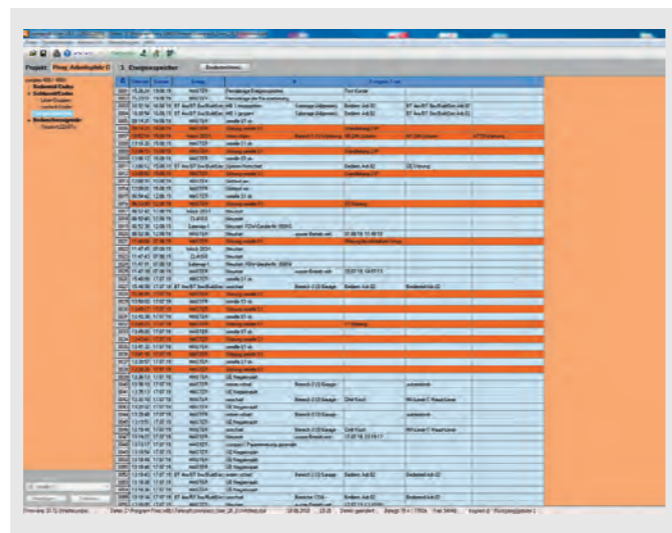
Vorteil 4 ✓

hiXuser –
Einfachste Verwaltung
durch Betreiber und
Wachdienste

Vorteil 5 ✓

hiXremote –
sicherer und
effizienter Fernservice

Die App BuildSec 4.0 ist eine Anwendersoftware für Smartphones und Tablets zur Bedienung und zur Darstellung von Betriebszuständen Ihrer mehrfach ausgezeichneten TELENOT-Einbruch- und Gefahrenmeldeanlage. Welches Objekt auch immer gegen unbefugten Zutritt, Wasserschäden, Brandgefahr, Einbruch, technische Störungen oder den Zutritt unberechtigter Personen geschützt werden soll, mit der App BuildSec 4.0 wissen Sie immer, ob wirklich alles in Ordnung ist. Sie können alle wichtigen Statusinformationen auf Ihrem Smartphone oder Tablet abrufen. Sie sehen, ob und an welcher Stelle ein Einbruch- oder Brandalarm ausgelöst ist oder ein Wasserschaden auftritt. Mit diesen Informationen sind Sie in der Lage, umgehend weitere Maßnahmen in die Wege zu leiten.



Die App BuildSec 4.0 ist über die Digitalplattform hiXserver der TELENOT Smart Services GmbH mit der Einbruch- und Gefahrenmeldeanlage über eine sichere Ende-zu-Ende Verschlüsselung verbunden. Diese Kommunikation erfolgt auf zwei voneinander getrennten Kanälen mittels TLS- und AES-Verschlüsselung. Sie erhalten auch in der Ferne alle wichtigen Statusinformationen auf Ihr Smartphone.

Neben der komfortablen und sicheren Fernbedienung über die App BuildSec 4.0 ermöglicht Ihnen das Tool hiXuser als Betreiber oder den von Ihnen beauftragten Wachdiensten

- **Personen- und Transponderverwaltung,**
- **Anzeige des Ereignisspeichers oder**
- **Fernbedienung**

der Einbruch- und Gefahrenmeldeanlage Ihres Unternehmens.

Bei der Kommunikation werden dabei – wie beschrieben – die höchst-sicheren TLS- und AES-Verschlüsselungen genutzt.

BuildSec 4.0 lässt sich für alle mobilen Endgeräte für Android oder iOS in den entsprechenden App-Stores herunterladen. Die App-Funktionalität und damit ihre Nutzung muss freigeschaltet werden. Die Einrichtung erfolgt zusammen mit Ihrer Alarmanlage durch Ihren Fachbetrieb in Ihrer Nähe.



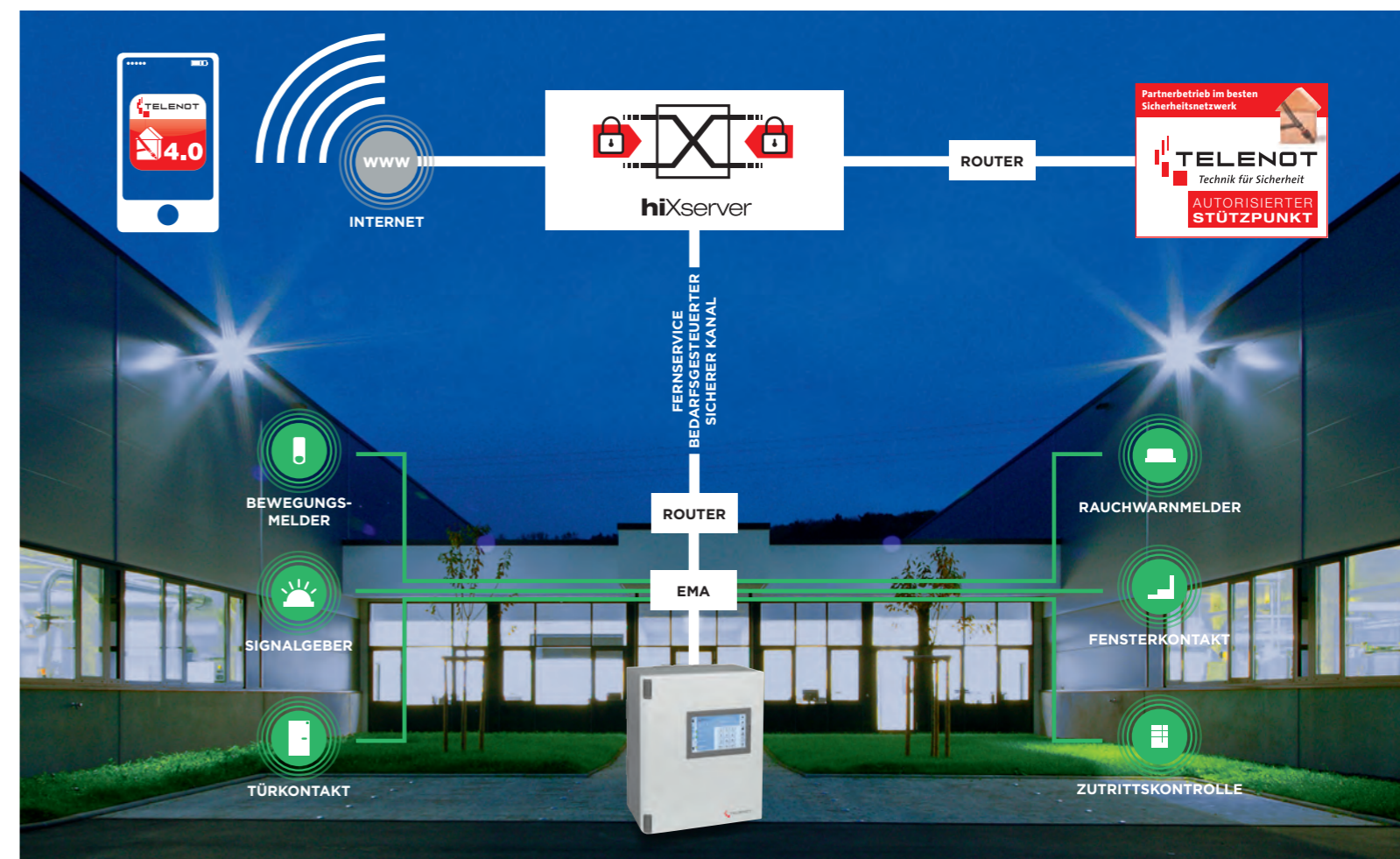
Die App BuildSec 4.0 ermöglicht einen komfortablen und zuverlässigen Zugriff auf Ihre Einbruch- und Gefahrenmeldeanlage. TLS- und AES-Verschlüsselungen verhindern, dass unberechtigte Personen die Kommunikation mitlesen können.

hiXremote ist das Werkzeug, das dem von Ihnen mit Wartung und Service beauftragtem Fachbetrieb eine sichere Fernservice-Verbindung für die Fernparametrierung inkl. Firmware-Updates für Ihr gesamtes Einbruch- und Gefahrenmeldesystem von TELENOT über die Digitalplattform hiXserver ermöglicht.

So kann Ihr Fachbetrieb schnell und flexibel

- **Störungen finden und beseitigen,**
- **das System Ihren Anforderungen entsprechend neu anpassen oder**
- **neue Transponder einlernen**

Ein über zwei getrennte Wege verschlüsselter Verbindungsaufbau garantiert jederzeit die Einhaltung höchster Sicherheitsstandards.





Sicherheitstechnik von TELENOT.
Schützt. Schön. Smart.

**Sie haben Fragen oder wünschen weitere Informationen?
Kontaktieren Sie uns.**

Kontakt Deutschland:

TELENOT ELECTRONIC GMBH

Wiesentalstraße 60
73434 Aalen
GERMANY

Telefon +49 7361 946-401
Telefax +49 7361 946-440

customer.care@telenot.de
www.telenot.de

Kontakt Österreich:

**TELENOT ELECTRONIC
Vertriebs-Ges.m.b.H.**

Josef-Haas-Straße 3
4655 Vorchdorf
AUSTRIA

Telefon +43 7614 8258-0
Telefax +43 7614 8258-11

info@telenot.at
www.telenot.at

Kontakt Schweiz:

TELENOT ELECTRONIC AG

Neumühlestrasse 42
8406 Winterthur
SWITZERLAND

Telefon +41 52 544 17 22
Telefax +41 52 544 17 25

info@telenot.ch
www.telenot.ch

Kontakt Luxemburg:

**marco zenner s.à r.l.
Offizieller Distributor TELENOT**

2b, Zone Industrielle Zare Est
4385 Ehlerange
LUXEMBOURG

Telefon +352 44 15 44-1

telenot@zenner.lu
www.zenner.lu