



# **cbb edge.SHIELDOR**

## **Solution Brief**



## Die Krux der optimalen IT-Sicherheit für Fertigungsanlagen

Maschinen und Anlagen in der produzierenden Industrie sind hochpreisige Investitionsgüter, die nur dann wirtschaftlich sind, wenn sie über eine lange Laufzeit betrieben werden. Daraus resultiert, dass die Techniken zur Steuerung und Vernetzung der Maschinen und Anlagen teilweise auf einem veralteten technologischen Stand basieren.

Diese langen Laufzeiten stehen im starken Kontrast zu den kurzen Entwicklungszyklen im Bereich der IT-Infrastruktur, der Betriebssysteme und der Anwendungssoftware. Der Grundsatz der IT-Sicherheit sagt, dass für einen optimalen Schutz von (IT-)Geräten regelmäßige und über die gesamte Laufzeit garantierte Sicherheitsupdates erforderlich sind. Folglich gilt dieses auch für Maschinen und Anlagen (OT-Netzwerkteilnehmer), sobald diese vernetzt werden. Mit steigender Laufzeit wird jedoch der Aufwand zur Bereitstellung dieser Updates von Software und später auch Hardware immer höher.

Ein mögliches Upgrade der Hardware, Betriebssysteme und Applikationen kommt in vielen Fällen einer Neuprogrammierung gleich und ist oft nicht wirtschaftlich. Zusätzlich dazu sind die Maschinen und Anlagen oft komplexe Systeme mit hohen Abhängigkeiten, sodass ein Austausch mit zusätzlichem Aufwand verbunden ist.

**Drei von vier Unternehmen pro Jahr sind Opfer von Cyberangriffen wie Datendiebstahl, Industrie-Spionage oder -Sabotage.**

**Allein in Deutschland entsteht ein Schaden von 100 Mrd. Euro jährlich durch Ersatzmaßnahmen, Rechtsstreitigkeiten, Patentverletzungen und Produktionsausfällen.**

Quelle: Bitkom, Studiebericht 2020, Spionage, Sabotage und Datendiebstahl  
– Wirtschaftsschutz in der vernetzten Welt

## Funktionen des cbb edge.SHIELDOR

- ✓ Unterstützt eine Vielzahl von Protokollen und Diensten (Industrieprotokolle, Dateiaustausch, Remote-Desktop, Backup)
- ✓ Analysiert und kontextualisiert alle Datenströme
- ✓ Performanter, gut gesicherter Zugriff; Verifikation von Diensten
- ✓ Entscheidungen basierend auf Machine-Learning
- ✓ Benutzerfreundliche Bedien- und Konfigurationsoberflächen
- ✓ Langfristiger Support

## Vorteile des cbb edge.SHIELDOR

Der cbb edge.SHIELDOR garantiert neben der uneingeschränkten Verwendung aller Maschinen und Anlagen langfristige Kompatibilität und Sicherheit der gesamten Fertigungsanlagen. Alle Funktionsweisen des cbb edge.SHIELDOR werden unter ständiger Weiterentwicklung mehrfach unabhängig getestet. Neben höchster Sicherheit und Zuverlässigkeit bietet der cbb edge.SHIELDOR einen möglichst vollständigen, performanten und gut gesicherten Zugriff auf die ihm anvertrauten Maschinen und Anlagen.

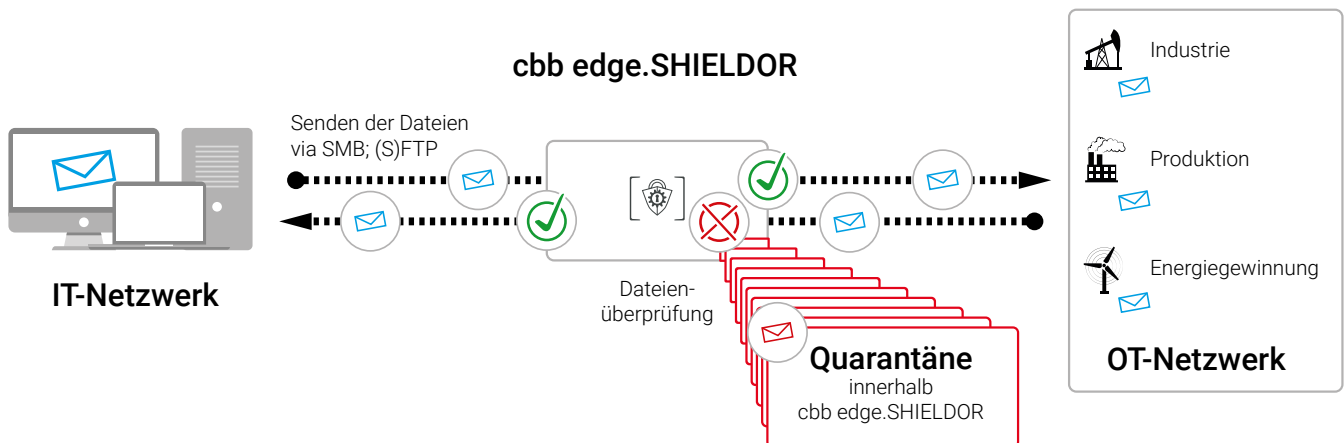
Definierte Dienste des cbb edge.SHIELDOR sollten nicht nur für Netzwerkteilnehmer, sondern auch für Netzexterne zur Verfügung gestellt werden. So kann ein künftiges Update einer Maschine oder Anlage über ein zeitlich limitierten, überwachten Fernzugriff mit vollständiger Rückverfolgbarkeit erfolgen. Über eine Benutzeroberfläche können spezifische Dienste freigeschaltet werden.

## Use Case 1: Definierte Sicherheit in den Teilnetzen - Dateiübertragungen

Eine Firewall kann nur Dateidienste wie SMB, FTP oder HTTP freigeben, hat aber keinen Einfluss auf Dateien, die übertragen werden. Durch eine Paketanalyse können zwar unverschlüsselte Dateien überprüft werden, allerdings ist das schon zu spät, da die Datei beim Scan bereits übertragen wurde und sich auf der Zielhardware befindet.

Daten unterschiedlicher Protokolle werden in dem cbb edge.SHIELDOR in einen gesicherten Bereich aufgenommen. Danach erfolgt die Überprüfung auf Viren und sonstigen Schadprogramme. Sollte die Prüfung erfolgreich durchgeführt worden sein, wird die Datei an die entsprechenden Kommunikationsteilnehmer weitergeleitet. Die Übertragung kann je nach Konfiguration für jede Richtung (vom bzw. zum Netzwerk) mit individuellen Einstellungen betrieben werden.

### cbb edge.SHIELDOR für Dateiübertragungen



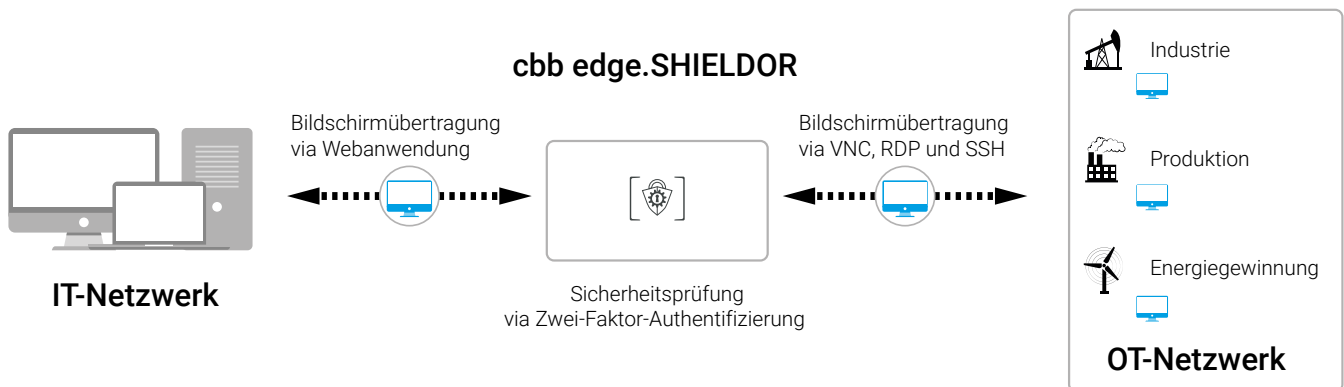
#### Ihr Vorteil

Alte Protokolle aus dem OT-Netzwerk werden in das IT-Netzwerk übersetzt (z.B. SMBv1 nach SMBv4); ausschließlich nicht schädliche, vollständige Dateien werden bereitgestellt.

## Use Case 2: Definierte Sicherheit in den Teilnetzen - Bildschirmübertragungen

Der cbb edge.SHIELDOR ermöglicht Ihnen die direkte Steuerung Ihrer Maschinen und Anlagen über die Bildschirmübertragung. Unterstützt werden die Protokolle RDP, VNC und SSH. Durch diesen Dienst entsteht keine Gefahr, dass Dateien unkontrolliert über Remotedesktopverbindung auf die Anlagen kopiert werden, wie es in einer normalen RDP Verbindung möglich wäre. Im cbb edge.SHIELDOR wird diese Funktion zwischen IT und OT Teilnehmern blockiert. Dateien können über die bereits genannte Dateiübertragung kontrolliert ausgetauscht werden. Diese Verbindung erfordert zusätzlich die Anmeldung am edge.SHIELDOR über eine Zwei-Faktor-Authentifizierung, sodass im Vergleich zum RDP ein höheres Sicherheitslevel garantiert werden kann. Alle Bildschirm-Aktivitäten werden zudem aufgezeichnet, damit explizite Tätigkeiten und Zugriffe an den Anlagen und Maschinen nachverfolgt werden können.

### cbb edge.SHIELDOR für Bildschirmübertragungen



#### Ihr Vorteil

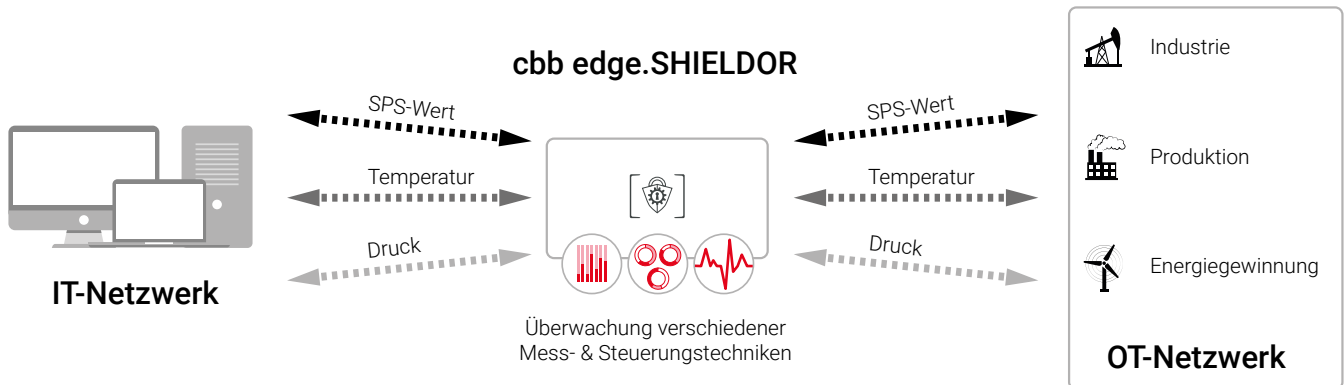
Erhöhung der Zugriffskontrolle auf OT-Systeme durch zusätzliche Zwei-Faktor-Authentifizierung aller Anwender sowie Protokollierung der durchgeführten Arbeitsschritte.

## Use Case 3: Erfassen von Prozessdaten – Bidirektionaler Datenaustausch

Als eine seiner Hauptfunktionen ermöglicht der cbb edge.SHIELDOR Daten einer Vielzahl von Feldkomponenten direkt auszulesen. Ob Sensorik oder Aktorik in Form von SPSs, Ventilen oder ähnlichen Komponenten, die im Prozessnetzwerk verbaut sind - der cbb edge.SHIELDOR ist in der Lage diese Daten auszulesen, zu überwachen und zu konfigurieren.

Somit wird eine Übertragung von Prozess-, Mess- und Steuerungsdaten zwischen zwei separaten Netzwerken ermöglicht. Durch eine aktive Überwachung der Endgeräte und Visualisierung der Daten, zum Beispiel auf einem Dashboard kann zugleich der Anwender informiert werden, sollte ein Gerät ausfallen oder sich außergewöhnlich verhalten.

## cbb edge.SHIELDOR für den bidirektionalen Datenaustausch



### Ihr Vorteil

Anbindung unterschiedlichster Sensorik und Aktorik über diverse Protokolle; veraltete Protokolle werden vereinheitlicht.

## Zusammenfassung

Der cbb edge.SHIELDOR dient als Schutz für Industrieanlagen und -maschinen vor Angriffen sowohl von innen als auch von außen. Durch den Einsatz von ausschließlich benötigten Diensten und der Segmentierung sowie Überwachung dieser Dienste kann eine Abgrenzung zwischen dem Netzwerk der Maschinen und Anlagen und dem übergeordneten IT-Netzwerk erfolgen und verhindert somit den unkontrollierten Informationsaustausch.

Dabei besteht die Möglichkeit Protokolle umzuwandeln. Beispielsweise können veraltete unsichere Protokolle dadurch gesichert werden, indem sie in nach heutigem Kenntnisstand sichere Protokolle gewandelt werden. So können komplexe und veraltete Anlagen updatefrei genutzt werden. Unterstützt werden dabei nicht nur gängige Industrieprotokolle, sondern auch administrative Dienste und Protokolle.

Möglichen Angreifern wird das gesamte OT-Netzwerk verschleiert, sodass diese keinerlei Möglichkeiten bei einer Kompromittierung eines Teilnetzwerkes haben, auf weitere Teilnehmer hinter dem edge.SHIELDOR zuzugreifen.



Sie möchten mehr über unseren cbb edge.SHIELDOR erfahren?  
Schreiben Sie uns direkt an:

cbb software GmbH E: [sales@cbb.de](mailto:sales@cbb.de)



cbb edge.SHIELDOR Technisches Datenblatt zum Download:

[https://cbb.de/wp-content/uploads/2021/10/2110\\_cbb-edge-shieldor-technisches-datenblatt.pdf](https://cbb.de/wp-content/uploads/2021/10/2110_cbb-edge-shieldor-technisches-datenblatt.pdf)



**cbb software GmbH**

Isaac-Newton-Straße 8, 23562 Lübeck

T: +49 (0)451 39 77 1 - 10

E: [sales@cbb.de](mailto:sales@cbb.de)

[www.cbb.de](http://www.cbb.de)