IT & Security Factsheet

Peakboard — die wichtigsten Fakten für IT-, Sicherheits- und Infrastruktur-Teams

1. April 2026 (2026-04-01) · Version 1.0

1. Über Peakboard

Peakboard ist eine Low-Code-Plattform zum Erfassen, Verarbeiten und Visualisieren von Daten aus Produktions- und Logistikumgebungen in Echtzeit. Anwendungen werden einmalig erstellt und laufen dann autonom auf Edge-Geräten direkt im Shopfloor – nah an den Maschinen, Anlagen und Menschen, die sie nutzen. Da die Daten lokal auf dem Gerät verarbeitet werden, funktioniert Peakboard ohne Cloud-Abhängigkeit und fügt sich in restriktive, segmentierte Industrienetzwerke ein.

Dieses Factsheet fasst die wichtigsten Fakten zur Peakboard-Architektur und ihrem Sicherheitsmodell zusammen.

2. Die Peakboard-Plattform: Komponenten und Zusammenspiel

Das Peakboard-Ökosystem besteht aus drei Bausteinen: einer Entwicklungsumgebung (Peakboard Designer), einer Runtime (Peakboard Box oder Peakboard BYOD) und einer zentralen Verwaltungsplattform (Peakboard Hub, verfügbar als Online- oder On-Premises-Edition).

Peakboard Designer ist die kostenlose, Windows-basierte Low-Code-Entwicklungsumgebung. Mit ihr werden Anwendungen erstellt: Datenquellen verbinden, die Anwendung per Drag & Drop gestalten und Logik mit Building Blocks oder Lua-Scripting hinzufügen. Die fertige Anwendung (eine einzelne .pbmx-Datei) wird über das Netzwerk auf ein oder mehrere Runtime-Geräte übertragen.

Peakboard Box ist die dedizierte Industrie-Hardware, auf der Anwendungen im Produktivbetrieb laufen. Die Box führt die Anwendung autonom aus, verbindet sich direkt mit den Datenquellen und rendert das Dashboard auf jedem angeschlossenen Bildschirm oder Touch-Display. **Peakboard BYOD** ("Bring Your Own Device") stellt exakt dieselbe Runtime als Software für eigene Windows-Hardware bereit – Industrie-PCs, Panel-PCs, Laptops oder Tablets. Box und BYOD sind funktional gleichwertig; sie unterscheiden sich nur darin, wer die Hardware stellt.

Peakboard Hub ist die optionale Schaltzentrale für größere Installationen. Er verwaltet alle verbundenen Boxen und BYOD-Geräte zentral, verteilt Anwendungen standortübergreifend, speichert gemeinsame Daten in Hub-Listen und -Variablen, verwaltet Zugangsdaten und bietet rollenbasierte Benutzer- und Gruppenverwaltung. Erhältlich als **Peakboard Hub Online** (SaaS, von Peakboard betrieben) und **Peakboard Hub On-Premises** (auf eigenem Windows-Server, Kommunikation bleibt im internen Netz).

Im typischen Rollout wird eine Anwendung im Designer erstellt, auf eine Box oder BYOD-Runtime übertragen und läuft anschließend selbstständig: Die Runtime bezieht Daten direkt aus den Quellsystemen, hält sie im Arbeitsspeicher und rendert das Dashboard lokal. Der Hub ergänzt das Fleet-Management – Anwendungen veröffentlichen, Geräte überwachen, Daten zwischen Anwendungen teilen.

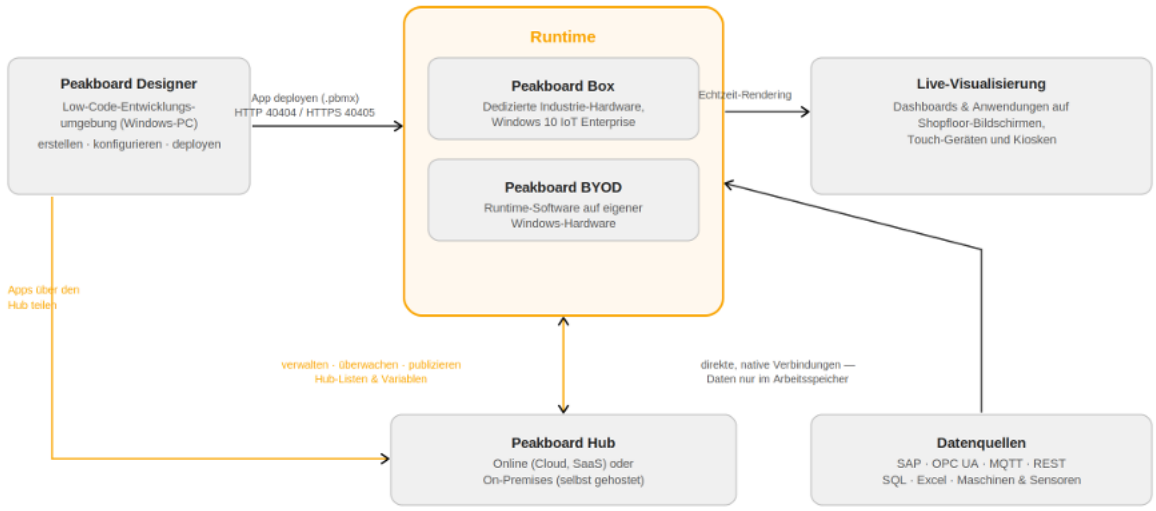

Abbildung 1: Das Peakboard-Ökosystem — Designer, Runtime (Box/BYOD), Hub und Datenquellen

3. Peakboard Box: Hardware- und Betriebssystemsicherheit

3.1 Betriebssystem

Die Peakboard Box läuft unter **Windows 10 IoT Enterprise LTSC** (Long-Term Servicing Channel), Microsofts Langzeit-Wartungsedition für Spezialgeräte. Diese Edition ist **von Microsoft bis Januar 2032 unterstützt**. **Windows Updates sind standardmäßig deaktiviert**, damit das Gerät deterministisch arbeitet und nie durch ungeplante Update-Neustarts unterbrochen wird. Administratoren können Updates bei Bedarf selbst einpflegen.

3.2 Keine Internet-Abhängigkeit

Die Peakboard-Umgebung (Box, Designer und Hub On-Premises) **benötigt keinen Internet-Zugang**. Die gesamte für den Betrieb notwendige Kommunikation findet im lokalen Netzwerk statt. Internet-Konnektivität wird nur relevant, wenn gezielt Cloud-Funktionen wie Peakboard Hub Online oder Online-Datenquellen genutzt werden.

3.3 Schutz vor unberechtigtem Zugriff

Im Normalbetrieb läuft die Box unter einem **eingeschränkten Windows-Benutzer** ohne Installations- oder Desktop-Rechte (Kiosk-Prinzip). Für Hintergrundsystemaufgaben existiert ein separates Windows-Administratorkonto (pbadmin); dessen Passwort wird getrennt mit dem Gerät geliefert.

Wichtig: Ändern Sie das Administrator-Passwort unmittelbar nach Erhalt der Box und bewahren Sie es im Passwort-Safe auf – es kann bei Verlust nicht zurückgesetzt werden.

3.4 Domain-Integration und Virenscanner

Die Peakboard Box kann, muss aber nicht in eine Windows-Domäne integriert werden – sie funktioniert innerhalb und außerhalb von Active-Directory-Umgebungen. Mit Administrator-Zugang ist die Installation eines Virenscanners möglich; aufgrund des gesperrten Kiosk-Setups und der geschlossenen Firewall ist dies möglich, aber nicht zwingend erforderlich.

4. Netzwerksicherheit: Ports und verschlüsselte Kommunikation

4.1 Offene Ports

Die Windows-Firewall der Peakboard Box blockiert standardmäßig alle eingehenden Ports. Nur die folgenden Ausnahmen sind geöffnet:

Port / Protokoll	Dienst	Zweck
ICMP v4/v6	Ping	Netzwerkdiagnose
6	Broadcast (optional)	Geräteerkennung
7	Echo/Ping	Netzwerkdiagnose
5985 / 5986	WinRM (HTTP/HTTPS)	Remote-Wartung via PowerShell
40404	Peakboard (HTTP)	Unverschlüsselte Kommunikation mit Designer/Hub
40405	Peakboard (HTTPS)	Verschlüsselte Kommunikation mit Designer/Hub (empfohlen)
40407	Peakboard	Peakboard-Kommunikation

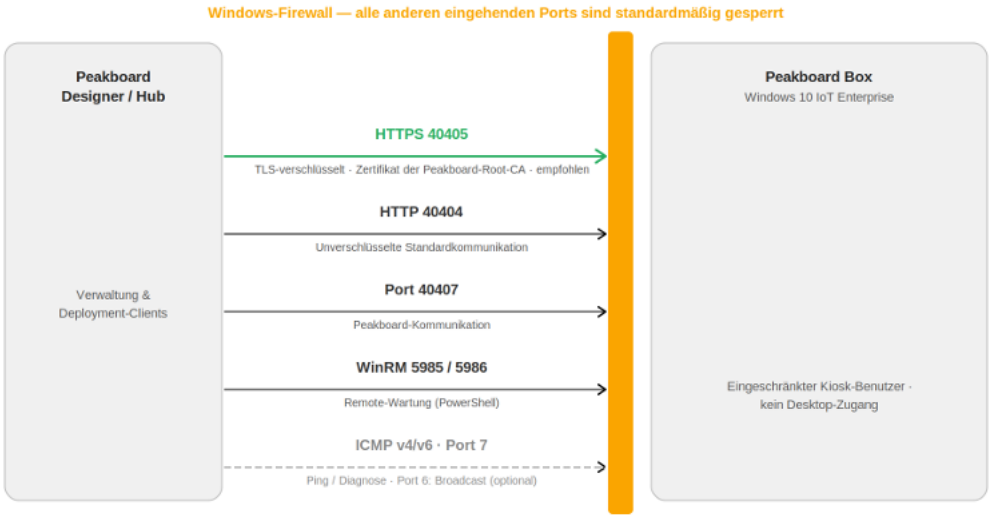

Abbildung 2: Standard-Firewall-Konfiguration der Peakboard Box — alles andere ist gesperrt

4.2 Verschlüsselte Kommunikation mit der Peakboard Box

Die Kommunikation zwischen Peakboard Designer (oder Hub) und einer Peakboard Box kann über zwei Kanäle laufen: Über **Port 40404 (HTTP)** ist die gesamte Kommunikation – Statusabfragen, Anwendungsübertragungen, Zugangsdaten und Token – unverschlüsselt; über **Port 40405 (HTTPS)** ist sie vollständig TLS-verschlüsselt.

Bei Nutzung der verschlüsselten Verbindung präsentiert die Peakboard Box ein Zertifikat der Peakboard-Root-CA. Der Designer validiert es gegen die Root-CA im Windows-Zertifikatsspeicher und schützt die Verbindung so vor Abhören und Manipulation.

Empfehlung: Aktivieren Sie die verschlüsselte Verbindung, damit Zugangsdaten, Zugriffstoken und Anwendungen ausschließlich über Port 40405 übertragen werden.

5. Anwendungs- und Datensicherheit

5.1 Verschlüsselte Anwendungsdateien (.pbmx)

Eine Peakboard-Anwendung wird als einzelne .pbmx-Datei gespeichert. Diese Datei kann im Peakboard Designer mit einem Passwort geschützt werden (Projekteinstellungen → Projektinfo → Dateischutz). Der Schutz verschlüsselt den gesamten Dateiinhalt – einschließlich aller Zugangsdaten, Skripte, Variablen und Ressourcen –, sodass die Datei ohne das Passwort weder geöffnet noch analysiert werden kann.

Wichtig: Bewahren Sie das Passwort sicher auf. Ohne es kann eine verschlüsselte Peakboard-Datei weder geöffnet noch wiederhergestellt werden.

5.2 Datenpersistenz: Daten verbleiben im Arbeitsspeicher

Die Peakboard-Runtime hält Daten aus Ihren Datenquellen **ausschließlich im Arbeitsspeicher**, solange die Anwendung läuft. Beim Stoppen oder Neustart werden sie verworfen. Es wird nichts auf den Datenträger geschrieben, sofern eine Anwendung dies nicht explizit tut (z. B. über Building Blocks). Eine stillgelegte oder gestohlene Box enthält daher keine historische Kopie Ihrer Produktionsdaten.

5.3 Zertifikatsverwaltung

Zertifikate für Datenquellen (z. B. OPC UA oder MQTT) werden zentral im Peakboard Hub oder in der Anwendung über den Designer verwaltet (Projekteinstellungen → Zertifikate). Zertifikate werden in gängigen Formaten importiert (.cer, .crt, .der, .pfx, .p12, …) und einem von zwei Speichern zugewiesen: *TrustedPeople* für vertrauenswürdige und *Disallowed* für abzulehnende Zertifikate.

Standard-Anwendungszertifikate werden nur während der Laufzeit in den Windows-Zertifikatsspeicher der Box geladen und beim Stoppen wieder entladen. MQTT- und OPC-UA-Zertifikate werden mit der Anwendungsdatei ausgeliefert und direkt von der jeweiligen Datenquelle verwendet.

6. Authentifizierung und Zugriffskontrolle

6.1 Authentifizierung gegenüber Datenquellen

Peakboard führt kein eigenes Anmeldeschema für externe Systeme ein – es nutzt die nativen Authentifizierungsmechanismen des jeweiligen Quellsystems:

- **SAP:** Anmeldung über die RFC-Schnittstelle mit einem dedizierten SAP-Benutzer; Zugriff kann in SAP selbst eingegrenzt und auditiert werden.
- **OPC UA und MQTT:** Zertifikatsbasierte Authentifizierung; Zertifikate werden im Designer gespeichert und gemeinsam mit der Anwendung auf die Box übertragen.
- **REST-basierte Quellen (XML, JSON, CSV, Web-APIs):** Standard-HTTPS mit Server-Zertifikaten; Client-Zertifikate können ergänzend genutzt werden, wenn die API mutual TLS erfordert.

Für Datenquellen eingegebene Zugangsdaten werden Teil der Anwendungsdatei und sind durch die in Abschnitt 5.1 beschriebene .pbmx-Verschlüsselung geschützt.

6.2 Benutzerverwaltung auf der Runtime

Der Zugriff auf jede Peakboard Box (und BYOD-Runtime) wird über eine eigene Benutzerverwaltung gesteuert. Jedes Gerät wird mit einem Standard-Administrator (PeakboardAdmin) und zwei vordefinierten Rollen ausgeliefert: *Administrator* (nicht löschbar oder änderbar) und *User* (beschränkt auf Anwendungsverwaltung und Screenshots). Benutzerdefinierte Rollen können mit granularen Berechtigungen definiert werden:

- Benutzer verwalten und Protokolle verwalten

- Anwendungen verwalten (hochladen, ändern, löschen)
- Daten lesen/schreiben (Variablen, Listen, Funktionen)
- Eigenschaften festlegen, einschließlich Lizenzverwaltung
- Ressourcen definieren und Screenshots erstellen
- Systemeinstellungen und Cloud-Kommunikation

Passwörter für Runtime-Benutzer werden automatisch als sichere Passwörter generiert. Bei größeren Geräteflotten kann die Konfiguration auf gruppierte Boxen repliziert werden. Das Windows-Betriebssystem hält unabhängig davon ein eigenes Administratorkonto (siehe 3.3).

6.3 Zentrale Benutzerverwaltung über den Peakboard Hub

Anstatt Benutzer auf jedem Gerät separat zu pflegen, kann die Verwaltung im Peakboard Hub zentralisiert werden. Dazu wird eine Box mit einem Hub verbunden; anschließend werden Benutzer und Rollen für alle verbundenen Boxen zentral im Hub verwaltet.

Die Authentifizierung erfolgt entlang einer Vertrauenskette: Der Designer authentifiziert sich gegenüber der Box; die Box überprüft Benutzername und Passwort beim Hub. Nur wenn der Hub die Zugangsdaten bestätigt, wird Zugriff gewährt. Zentrale Änderungen – Benutzer hinzufügen, Rolle ändern, Zugang entziehen – wirken sofort auf alle betroffenen Boxen.

7. Peakboard Hub: Deployment-Optionen und Sicherheit

Beide Hub-Editionen bieten dieselben Kernfunktionen – Geräteverwaltung, Anwendungsverteilung, Hub-Listen und -Variablen, verschlüsselte Zugangsdatenverwaltung und rollenbasierte Zugriffskontrolle. Sie unterscheiden sich darin, wo sie laufen und welche Netzwerkpfade sie nutzen.

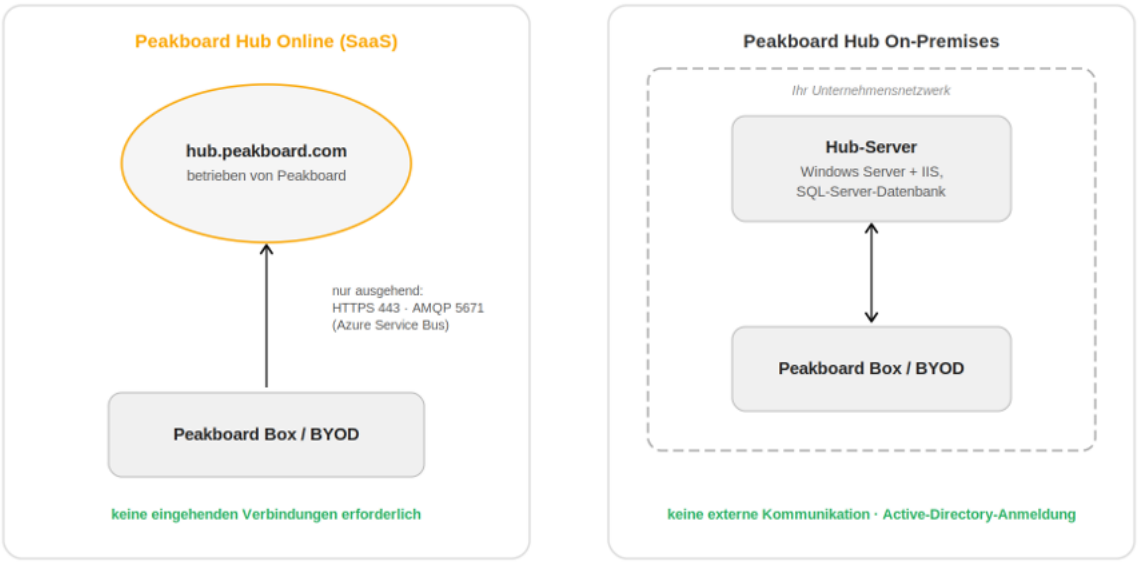

Abbildung 3: Peakboard Hub Online (nur ausgehende Cloud-Verbindung) vs. Hub On-Premises (keine externe Kommunikation)

7.1 Peakboard Hub Online (SaaS)

Peakboard Hub Online wird von Peakboard als Cloud-Dienst betrieben. Geräte registrieren sich mit ihrer Cloud-ID und bauen ausschließlich ausgehende Verbindungen auf – in der Firewall muss kein eingehender Port geöffnet werden. Eine Box darf nur dann mit der Cloud verbunden werden, wenn die Berechtigung "Cloud-Kommunikation erlauben" erteilt wurde. Benutzer melden sich mit passwortgeschützten Konten an; Designer authentifizieren sich mit Gruppenschlüsseln.

Die folgenden ausgehenden Endpunkte werden verwendet:

Endpunkt	Port	Zweck
hub.peakboard.com (HTTPS)	443	Hub-Registrierung und Web-Zugang
peakboardhubonline.servicebus.windows.net (AMQP, Azure Service Bus)	5671	Laufende Kommunikation zwischen Gerät und Hub
downloads.peakboard.com (HTTPS)	443	Software-Updates

Die Remote-Verwaltung über Hub Online umfasst: Deployen, Stoppen und Entfernen von Anwendungen; Ausrollen von Runtime-Updates; Anzeigen von Live-Screenshots und Gerätestatus; Neustarten von Geräten; Zugriff auf und Export von Protokolldateien.

7.2 Peakboard Hub On-Premises

Peakboard Hub On-Premises wird auf der eigenen Infrastruktur installiert: ein Windows Server (2016 oder neuer) mit IIS und ASP.NET Core Runtime, plus eine SQL-Server-Datenbank (SQL Server Express ist enthalten; ein vorhandener SQL Server ab Version 2017 kann genutzt werden). Bei dieser Edition findet zu keinem Zeitpunkt externe Kommunikation statt – der Datenverkehr fließt ausschließlich innerhalb Ihres Netzwerks. Die Authentifizierung erfolgt über den Windows-Domänencontroller (Active Directory); alle Daten verbleiben unter Ihrer vollen Hoheit.

8. Sicherheitsfakten auf einen Blick

Thema	Fakt
Betriebssystem	Windows 10 IoT Enterprise LTSC auf der Peakboard Box; von Microsoft bis Januar 2032 unterstützt
Windows Updates	Standardmäßig deaktiviert; durch Administratoren verwaltbar
Internet-Zugang	Standardmäßig nicht erforderlich; Cloud-Funktionen sind opt-in
Lokaler Zugriff	Eingeschränkter Kiosk-Benutzer; keine Software-Installation, kein Desktop-Zugang
Admin-Konto	Separates Windows-Administratorkonto; Passwort bei Erhalt ändern – kann nicht zurückgesetzt werden
Domäne	Domain-Beitritt unterstützt, aber nicht erforderlich
Virenscanner	Kann mit Administrator-Zugang installiert werden; nicht notwendig
Firewall	Alle eingehenden Ports gesperrt außer ICMP, 6/7, 5985/5986, 40404, 40405, 40407
Transport-verschlüsselung	TLS über Port 40405 mit Peakboard-Root-CA-Zertifikat (empfohlen)
Anwendungsdateien	Optionale Passwortverschlüsselung der .pbmx-Datei inkl. Zugangsdaten, Skripte, Variablen, Ressourcen
Datenpersistenz	Quelldaten werden nur im Arbeitsspeicher gehalten und bei Stopp/Neustart verworfen
Datenquellen-Auth.	Native Mechanismen: SAP-RFC-Benutzer, OPC-UA/MQTT-Zertifikate, HTTPS für REST
Benutzerverwaltung	Pro Gerät oder zentral über Peakboard Hub; Rollen und granulare Berechtigungen; Replikation über Gerätegruppen
Hub Online	Ausschließlich ausgehende Verbindungen (443, AMQP 5671); Cloud-Berechtigung pro Gerät erforderlich
Hub On-Premises	Keine externe Kommunikation; Active-Directory-Anmeldung; Daten verbleiben im eigenen Netzwerk

9. Weitere Informationen

Die Fakten in diesem Dokument stammen aus der offiziellen Peakboard-Dokumentation. Die folgenden Ressourcen bieten weiterführende Informationen:

- FAQ – IT & Security — die Sicherheits-FAQ, auf der dieses Factsheet basiert
- Benutzerverwaltung — Rollen, Berechtigungen und Replikation im Detail
- Zertifikatsverwaltung — Zertifikate hinzufügen und deployen
- Peakboard Hub-Dokumentation — Leitfäden für Hub Online und Hub On-Premises
- www.peakboard.com — Produktübersicht, Datenschutzrichtlinie und Kontakt

Fragen? Das Peakboard-Support-Team (support@peakboard.com) beantwortet gerne weitere IT- und Sicherheitsfragen, z. B. für Lieferantenbewertungen oder Sicherheitsfragebögen.