IT & Security Factsheet

Peakboard — key facts for IT, security and infrastructure teams

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

1. About Peakboard

Peakboard is a low-code platform for collecting, processing and visualizing data from production and logistics environments in real time. Applications are created once and then run autonomously on edge devices directly on the shop floor — close to the machines, systems and people that use them. Because the data is processed locally on the device, Peakboard works without any cloud dependency and fits into restrictive, segmented industrial networks.

This factsheet summarizes the most important facts about the Peakboard architecture and its security model.

2. The Peakboard platform: components and how they work together

The Peakboard ecosystem consists of three building blocks that complement each other: a development environment (Peakboard Designer), a runtime (Peakboard Box or Peakboard BYOD) and a central management platform (Peakboard Hub, available as an online or on-premises edition).

Peakboard Designer is the free, Windows-based low-code development environment. It is used to create applications: connecting data sources, designing the application via drag & drop, and adding logic with Building Blocks or Lua scripting. From the Designer, the finished application (a single .pbmx file) is deployed over the network to one or more runtime devices.

Peakboard Box is the dedicated industrial hardware on which applications run in production. The Box executes the application autonomously, connects directly to the data sources, and renders the application on any connected screen or touch display. **Peakboard BYOD** (“bring your own device”) provides exactly the same runtime as software for your own Windows hardware — industrial PCs, panel PCs, laptops or tablets. Box and BYOD are functionally equivalent runtimes; they differ only in who provides the hardware.

Peakboard Hub is the optional control center for larger installations. It manages all connected Boxes and BYOD devices centrally, distributes and updates applications across locations, stores shared data in Hub lists and variables, manages credentials, and provides role-based user and group management. The Hub is available in two editions with identical core functionality: **Peakboard Hub Online**, a cloud service operated by Peakboard (SaaS), and **Peakboard Hub On-Premises**, which is installed on your own Windows Server and keeps all communication inside your network.

In a typical rollout, an application is built in the Designer, deployed to a Peakboard Box or BYOD runtime, and from then on runs independently: the runtime pulls its data directly from the connected source systems, holds it in memory, and renders the dashboard locally. The Hub adds fleet management on top — publishing apps, monitoring devices, and sharing data between applications.

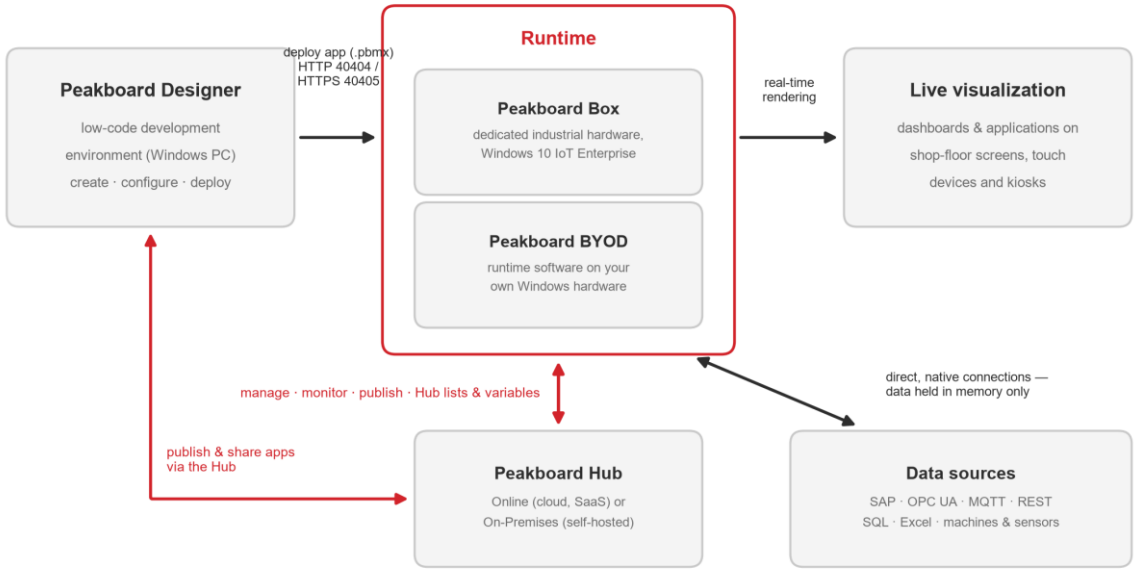

Figure 1: The Peakboard ecosystem — Designer, runtime (Box/BYOD), Hub and data sources

3. Peakboard Box: hardware and operating system security

3.1 Operating system

The Peakboard Box currently runs **Windows 10 IoT Enterprise LTSC** (Long-Term Servicing Channel), Microsoft's long-term-servicing edition for dedicated devices. This edition is **supported by Microsoft until January 2032**, which gives the platform a long, stable security-update lifecycle without feature-update churn. **Windows Updates are disabled by default** so that the device behaves deterministically and is never interrupted by unplanned update reboots during operation. Administrators with the corresponding access can manage updates themselves if their security policy requires it.

3.2 No internet dependency

The Peakboard environment (Peakboard Box, Peakboard Designer and Peakboard Hub On-Premises) **does not require internet access**. All communication that is needed for operation takes place inside the local network between the Designer, the Box and the connected data sources. Internet connectivity only becomes relevant if you deliberately use cloud features such as Peakboard Hub Online or online data sources.

3.3 Protection against unauthorized access

In normal operation the Box runs under a **restricted Windows user** that has no rights beyond those necessary for displaying the application: software cannot be installed and the Windows desktop cannot be accessed (kiosk principle). For background system tasks, a separate Windows administrator account (pbadmin) exists; its password is delivered separately with the device.

Important: change the administrator password immediately upon receipt of the Box and keep a record of it in your password vault — it cannot be reset if lost.

3.4 Domain integration and antivirus

The Peakboard Box can, but does not have to, be integrated into a Windows domain — it works both inside and outside Active Directory environments. With administrator access it is also possible to install a virus scanner on the Box; because of the locked-down kiosk setup and the closed firewall this is possible, but not necessary.

4. Network security: ports and encrypted communication

4.1 Open ports

The Windows firewall on the Peakboard Box blocks all inbound ports by default. Only the following exceptions are open:

Port / protocol	Service	Purpose
ICMP v4/v6	Ping	Network diagnostics
6	Broadcast (optional)	Device discovery
7	Echo/Ping	Network diagnostics
5985 / 5986	WinRM (HTTP/HTTPS)	Remote maintenance via PowerShell
40404	Peakboard (HTTP)	Unencrypted communication with Designer/Hub
40405	Peakboard (HTTPS)	Encrypted communication with Designer/Hub (recommended)
40407	Peakboard	Peakboard communication

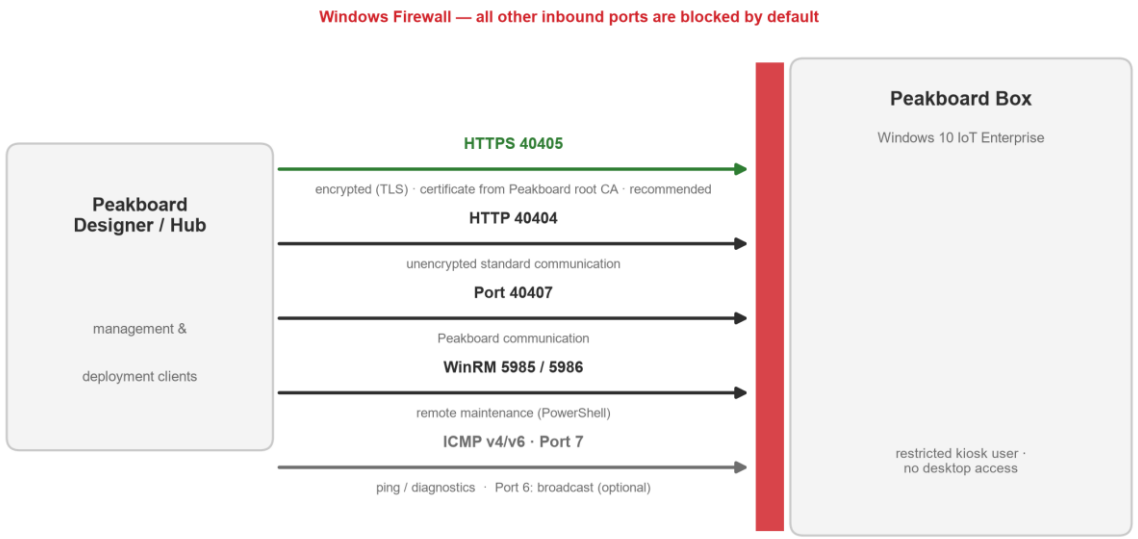

Figure 2: Default firewall configuration of the Peakboard Box — everything else is blocked

4.2 Encrypted communication with the Peakboard Box

Communication between the Peakboard Designer (or Hub) and a Peakboard Box can run over two channels, configured per Box in the Box settings: over **port 40404 (HTTP)**, all communication — status queries, application transfers, credentials and tokens — is unencrypted; over **port 40405 (HTTPS)**, the entire communication is TLS-encrypted.

When the encrypted connection is used, the Peakboard Box presents a certificate issued by the Peakboard root certification authority. The Designer validates this certificate against the root CA in the Windows certificate store, which guarantees the authenticity of the Box and protects the connection against eavesdropping and tampering.

Recommendation: enable the encrypted connection so that credentials, access tokens and applications are transferred exclusively over the encrypted port 40405.

5. Application and data security

5.1 Encrypted application files (.pbmx)

A Peakboard application is stored as a single .pbmx file. This file can be protected with a password in the Peakboard Designer (Project Settings → Project Info → File Protection). The protection encrypts the entire file content — including all credentials for data sources, scripts, variables and resources — so that an application file cannot be opened or analyzed without the password. Encryption takes effect the next time the file is saved.

Important: keep the password in a safe place. Without it, an encrypted Peakboard file can neither be opened nor recovered.

5.2 Data persistence: data stays in memory

The Peakboard runtime keeps the data from your data sources **in memory only** while the application is running. As soon as the application is stopped or the device is restarted, this data is discarded. Nothing is written to disk unless an application explicitly stores data itself (for example through Building Blocks in scripts). A decommissioned or stolen Box therefore does not contain a historical copy of your production data.

5.3 Certificate management

Certificates that an application needs — for example for OPC UA or MQTT data sources — are managed centrally in the Peakboard Hub or in the application via the Peakboard Designer (Project Settings → Certificates). Certificates are imported in common formats (.cer, .crt, .der, .pfx, .p12, …) and assigned to one of two stores: TrustedPeople for certificates that should be trusted, and Disallowed for certificates that must be rejected.

Standard application certificates are loaded into the Windows certificate store of the Peakboard Box only while the application is running and are unloaded again when it stops. MQTT and OPC UA certificates are shipped with the application file and used directly by the respective data source.

6. Authentication and access control

6.1 Authentication against data sources

Peakboard does not introduce its own credential scheme for external systems — it uses the native authentication mechanisms of each source system:

- **SAP:** sign-in via the RFC interface with a dedicated SAP user, so access can be scoped and audited in SAP itself.
- **OPC UA and MQTT:** certificate-based authentication; the certificates are stored in the Designer and deployed to the Box together with the application.

- **REST-based sources (XML, JSON, CSV, web APIs):** standard HTTPS with server certificates; client certificates can be used in addition where the API requires mutual TLS.

Credentials entered for data sources become part of the application file and are covered by the .pbmx file encryption described in section 5.1.

6.2 User administration on the runtime

Access to each Peakboard Box (and BYOD runtime) is controlled through its own user administration, managed from the Designer. Every device ships with a default administrator (PeakboardAdmin) and two predefined roles: Administrator, which cannot be deleted or modified, and User, which is limited to managing applications and taking screenshots. Custom roles can be defined with granular permissions:

- Manage users and manage logs
- Manage applications (upload, change, delete)
- Read/write data (variables, lists, functions)
- Set properties, including license management
- Define resources and take screenshots
- System settings and cloud communication

Passwords for runtime users are auto-generated as secure passwords. For larger fleets, the user and role configuration can be replicated across grouped Peakboard Boxes to keep all devices consistent. Independently of this application-level user administration, the Windows operating system keeps its own separate administrator account (see section 3.3).

6.3 Central user management through the Peakboard Hub

Instead of maintaining users separately on every device, the user administration can be centralized in the Peakboard Hub. To enable this, a Peakboard Box is connected to a Hub. Once connected, users and their roles are managed centrally in the Hub for each connected Box, using the same role and permission model described above. This removes the need to configure accounts on each individual device and keeps user management consistent across the entire fleet.

Authentication is handled along a chain of trust: when a user signs in from the Designer, the Designer authenticates against the Peakboard Box, and the Box in turn verifies the supplied user name and password against the Hub. Only if the Hub confirms the credentials is access granted. This way, central changes — such as adding a user, changing a role, or revoking access — take effect immediately for all affected Boxes, without having to touch each device individually.

7. Peakboard Hub: deployment options and security

Both Hub editions provide the same core functions — device management, application distribution, Hub lists and variables for shared data, encrypted credential management and role-based access control. They differ in where they run and which network paths they use.

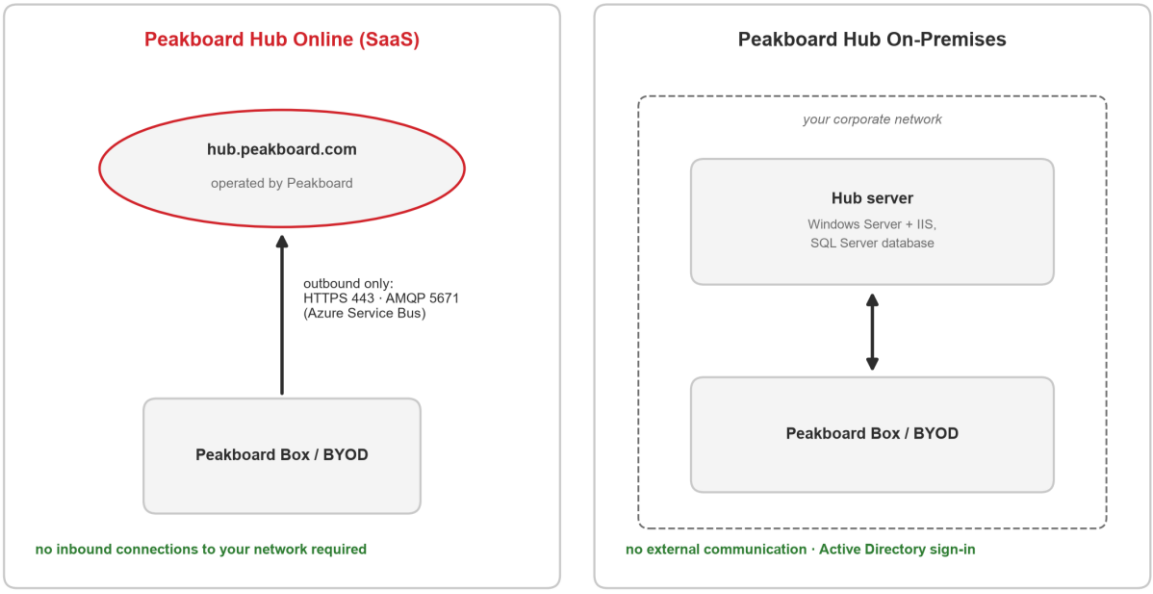

Figure 3: Peakboard Hub Online (outbound-only cloud connection) vs. Hub On-Premises (no external communication)

7.1 Peakboard Hub Online (SaaS)

Peakboard Hub Online is operated by Peakboard as a cloud service. Devices register with their cloud ID and then establish outbound connections only — no inbound port has to be opened in your firewall. A Box may only be connected to the cloud if the “Allow cloud communication” permission has been granted in its user administration. Users sign in to the Hub with password-protected accounts; Designers authenticate against the Hub with group keys, and user groups determine which resources each user can access.

The following outbound endpoints are used:

Endpoint	Port	Purpose
hub.peakboard.com (HTTPS)	443	Hub registration and web access
peakboardhubonline.servicebus.windows.net (AMQP, Azure Service Bus)	5671	Ongoing messaging between device and Hub
downloads.peakboard.com (HTTPS)	443	Software updates

Remote management through Hub Online includes deploying, stopping and removing applications, pushing runtime updates, viewing live screenshots and device status, restarting devices, and accessing and exporting log files.

7.2 Peakboard Hub On-Premises

Peakboard Hub On-Premises is installed on your own infrastructure: a Windows Server (2016 or later) with IIS and the ASP.NET Core runtime, plus a SQL Server database (SQL Server Express is included; an existing SQL Server from version 2017 can be used instead). With this edition there is no external communication at any time — traffic flows only between users, the Peakboard devices and the Hub server inside your network. Authentication is handled by your Windows domain controller (Active Directory), so users sign in with their existing Windows credentials, and all data remains under your full sovereignty.

8. Security facts at a glance

Topic	Fact
Operating system	Windows 10 IoT Enterprise LTSC on the Peakboard Box; supported by Microsoft until January 2032
Windows Updates	Disabled by default; manageable by administrators
Internet access	Not required by default; cloud features are opt-in
Local access	Restricted kiosk user; no software installation, no desktop access
Admin account	Separate Windows admin account; change the password on receipt — it cannot be reset
Domain	Domain join supported but not required
Antivirus	Can be installed with admin access; not necessary
Firewall	All inbound ports blocked except ICMP, 6/7, 5985/5986, 40404, 40405, 40407
Transport encryption	TLS via port 40405 with Peakboard root CA certificate (recommended)
Application files	Optional password encryption of the entire .pbmx file, including credentials, scripts, variables and resources
Data persistence	Source data is held in memory only and discarded on stop/restart
Data source auth	Native mechanisms: SAP RFC user, OPC UA/MQTT certificates, HTTPS for REST
User management	Per-device or centrally via the Peakboard Hub; roles and granular permissions; replication across device groups
Hub Online	Outbound-only connections (443, AMQP 5671); cloud permission required per device
Hub On-Premises	No external communication; Active Directory sign-in; data stays in your network

9. Further information

The facts in this document are taken from the official Peakboard documentation. The following resources provide more depth:

- FAQ – IT & Security — the security FAQ this factsheet is based on
- User administration — roles, permissions and replication in detail
- Certificate management — adding and deploying certificates
- Peakboard Hub documentation — Hub Online and Hub On-Premises guides
- www.peakboard.com — product overview, privacy policy and contact

Questions? The Peakboard support team (support@peakboard.com) is happy to answer further IT and security questions, e.g. for vendor assessments or security questionnaires.