Better Security with BenQ

Display solutions designed with security in mind

Better Security with BenQ

BenQ knows that bringing in new devices to your organization always comes with a few risks. Without sufficient security, these products may leave your networks exposed, increasing chances of data leaks, privacy violations, and operational setbacks.

Trust BenQ to deliver solutions that perfectly fit your current security strategy. When it comes to interactive displays, smart signage, and smart projectors, we not only offer the best in terms of image clarity, color accuracy, sound quality, and interactivity, we also provide top-end security to safeguard your organization.

Our end-to-end solutions—from individual devices to cloud infrastructure—offer multiple levels of security that help you tick every item on your corporate security checklist.

Device Security

Network Security

Cloud Security

01 We adhere to international standards and uphold your right to data privacy

02 We help you protect your organization against security threats

03 We offer secure access to your BenQ smart displays, user accounts, and files

01

We adhere to international standards and uphold your right to data privacy

BenQ smart displays and their related cloud services have gone through rigorous screening and have passed the strict data privacy criteria imposed by the European Union's General Data Protection Regulation (GDPR and GDPR-K), the California Consumer Privacy Act (CCPA), the UK's Product Security and Telecommunications Infrastructure (PSTI) regime, the App Defense Alliance's (ADA) Cloud Application Security Assessment (CASA), the Children's Online Privacy Protection Act (COPPA), and ISO/IEC 27001 security standards.

We adhere to international standards and uphold your right to data privacy

Ethical data collection and usage

Compliant with international data regulations such as GDPR and CCPA, BenQ guarantees that we do not collect or store personal identifiable information (PII) unless permitted by our customers.

BenQ also ensures that any customer data, such as their organization's user directories, will only be used for the purposes explicitly agreed upon by both parties; these may include enabling and improving specific cloud services and device functionalities.

BenQ will not sell or unlawfully share our customers' data.

Vetted cloud services and infrastructure

The BenQ Account Management System (AMS) has passed the CASA Tier 2 assessment requirements set by the ADA. Each aspect of AMS such as its cloud architecture, API, and its end-to-end processes including access control, cryptography, and others have undergone thorough scanning and lab testing, and are validated secure against data security threats.

We also host the BenQ service portal and our databases on Amazon web servers (located in Frankfurt, Germany), which are built to meet the highest standards for data security, privacy, and reliability. BenQ cloud services are regularly tested by third-party auditors in line with AWS Compliance programs.

We adhere to international standards and uphold your right to data privacy

Secure communications

BenQ websites use internet security protocols such as SSL and HTTPS to secure your connection, encrypt any transmitted data, and prevent attackers from intercepting data sent between BenQ online portals and your devices.

Convenient authorization

BenQ web services make use of OAuth 2.0 and JSON web tokens, industry standards that are utilized for efficient authorization across multiple devices without requiring our users to share their private credentials with BenQ.

Multi-factor authentication

BenQ gives IT admins the power to enforce two-factor authentication that requires users to input a security code sent to their mobile device when logging in.

We adhere to international standards and uphold your right to data privacy

Passwords stay private

BenQ smart displays provide login methods that help prevent users from entering their credentials on screen and ensure that their passwords are not publicly exposed. Additionally, BenQ offers a seamless solution that allows teachers to access both their display and their cloud drives with their school credentials. This reduces the hassle of remembering multiple passwords and ensures that all accounts comply with your organization's password policies.

QR code login

Users can scan a QR code on a BenQ Board, digital signage, or smart projector with their mobile device to securely log in.

NFC login

Some BenQ Board models come with built-in NFC sensors. System administrators can issue NFC cards to each user for controlled access and easy login.

SSO

BenQ smart displays support secure single sign-on (SSO) services from Microsoft Entra ID, Google Workspace, Clever, ClassLink, LDAP servers, and other SAML-based identity providers that use encrypted tokens to protect user credentials.

02

We help you protect your organization against security threats

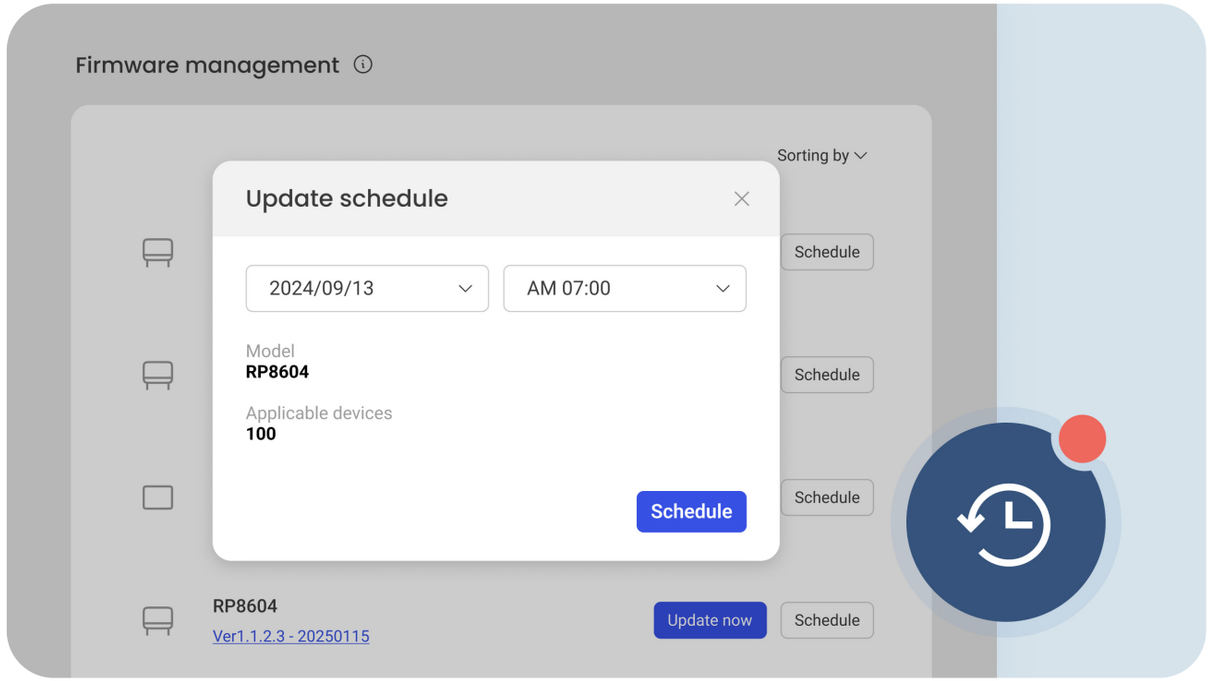
BenQ helps schools and companies safeguard their systems and data against threats such as malware and hacking by providing holistic security options that cover different levels of their data infrastructure.

We help you protect your organization against security threats

Protection against exploits

BenQ regularly provides the latest security patches and firmware updates for our BenQ Boards, digital signage, and smart projectors. Administrators can take full advantage of their BenQ smart display's over-the-air (OTA) update feature and remotely push these patches to all of their smart displays.

This not only ensures that their displays will have the necessary and timely protections against exploits and related attacks on their network, it also helps keep their board's operating system and BenQ software functioning at optimal performance.



We help you protect your organization against security threats

Flexible network security options

BenQ smart displays come with flexible network settings that allow IT administrators to configure their displays to better complement their existing security strategy.

Enterprise-grade authentication

Set up WPA2-Enterprise for user authentication and more secure communication.

Encrypted data transmission

Apply certificates to validate other devices and encrypt data.

Proxy-level protection

Configure proxy settings to restrict access to harmful sites.

Antimalware and anti-phishing measures

Users of the Google-certified 04 Series of BenQ Boards and smart signage can take advantage of Google Play Protect and Safe Browsing.

Google Play Protect ensures that apps are carefully vetted before users can download and install them on the display. It also scans and removes any installed app exhibiting suspicious activity.

Meanwhile, **Google Safe Browsing** safeguards users while they are browsing online as it warns them if they visit potentially harmful sites that involve phishing and other web-based threats.

Google Play Protect

Google Safe Browsing

03

We offer secure access to your BenQ smart displays, user accounts, and files

BenQ Account Management System (AMS), BenQ Device Management Solution (DMS), and BenQ Identity and Access Management (IAM), offer IT admins tools to create and manage user accounts, allowing them to prevent unauthorized access and possible tampering of BenQ smart display settings, user files, and folders.

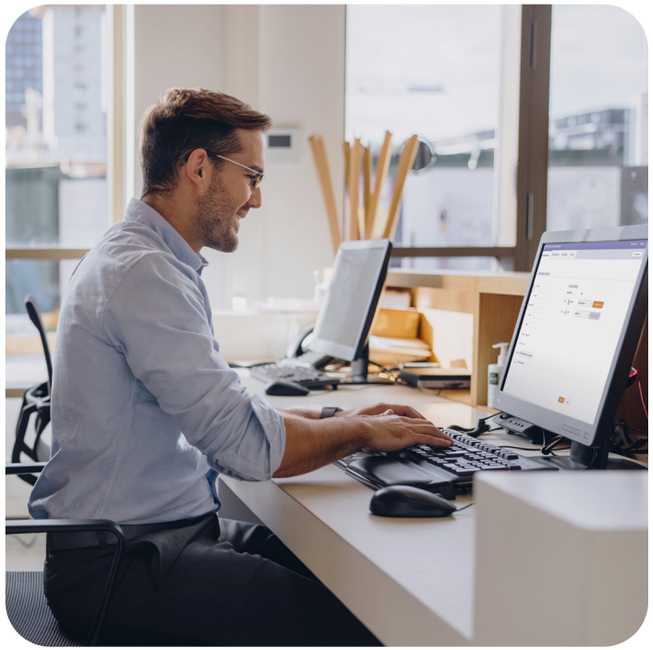
We offer secure access to your BenQ smart displays, user accounts, and files

	Guest users	Restricted users	Authenticated users
Login	Not required	Required	Required
Modification of settings	Not allowed	Only basic settings	Regular user settings
Connected devices (via HDMI or USB-C)	✓	✓	✓
Public folder	×	✓	✓
Personal folders	×	✓	✓
Cloud storage	×	✓	✓
EZWrite whiteboard (BenQ Boards)	✓	✓	✓
InstaShare wireless screen sharing	✓	✓	✓
Web browser	×	✓	✓

Get more in-depth information on secure access controls for the BenQ Board.

https://www.benq.com/en-us/education/edtech-blog/access-authority-security-user-roles-settings-benq-board.html

We offer secure access to your BenQ smart displays, user accounts, and files



Secure user access

BenQ offers two ways that IT administrators can enforce stricter access controls for their BenQ smart displays.

Authentication mode

This mode offers a higher level of access control as it completely prevents guests from using the smart display and tampering with its settings. Enabling this mode on DMS ensures that only authenticated users will be able to use the display and its features.

Restricted user role

Assigning this role ensures the highest level of access control as it restricts even authorized users and groups from making changes to any critical smart display settings while still giving them access to all its essential features and functionalities.

Idle session logout

Devices that are left unlocked and unattended are one of the most common causes of data leaks. Administrators can prevent this from happening on the BenQ smart display by setting an idle session logout time on AMS. If ever a user forgets to log out of their display, AMS automatically logs out of the account.

We offer secure access to your BenQ smart displays, user accounts, and files

Manage app usage with BenQ DMS

IT and school admins have multiple options for remotely managing app usage on BenQ smart displays.

Allow apps

Allowlisting is the most controlled approach, ensuring that only apps that you pre-approve can be used on the display. This method is ideal for organizations that want to maintain a secure environment by limiting distractions and preventing unauthorized apps from being installed.

Block apps

Blocklisting allows you to specify which apps are not permitted while still allowing general access to the Google Play Store. This is useful for preventing apps that might cause distractions or security risks without entirely restricting access to all apps.

Hide apps

If users have installed an app on a BenQ smart display and you no longer want them to use it you can choose to simply hide the app in DMS. This is best for organizations that have fewer devices to manage and generally allow users unrestricted access to the Play Store.

Block the Play Store

If you need strict control over all apps, you can completely disable Play Store access. This prevents any unauthorized app installations and ensures that only IT-approved apps are available on the smart display.

How can organizations make their smart devices more secure?

Below is a checklist you can use as a guide to help ensure that your smart displays are safe to use.

- [ ] Does your organization have smart display usage guidelines?
- [ ] Are you able to assign and modify user privileges for your smart displays?
- [ ] Do you receive firmware updates and security patches for your smart displays?
- [ ] Can you install security software?
- [ ] Does your smart display allow you to configure its network settings to make it more secure?
- [ ] Does your smart display use secure cloud systems?
- [ ] Is your smart display and its cloud services compliant with data protection regulations?