BenQ

Better Security with BenQ
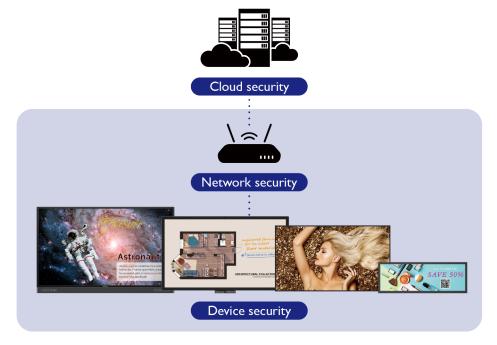## Display solutions designed with security in mind

Bringing in new devices to your organization always comes with risks. Without sufficient security, these products leave your networks exposed, increasing chances of data leaks, privacy violations, and business compromise.

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

BenQ's 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.

Security checklist

- ✓ Data protection
- ✓ Data privacy
- ✓ Regulatory compliance
- ✓ Business resilience

Cloud security

Network security

Device security

Compliance

Technical support

Android EOL support

Device security

McAfee™ Mobile Security is available to install from BenQ Suggests. It not only protects your displays from malware, but also includes web reputation technology that effectively blocks access to malicious websites and domains. Its data privacy features also ensure that both user and device data are not exposed, collected, or used without your explicit consent.

Security

- Provides real-time protection against malware and rogue apps
- Blocks malicious websites
- Scans and removes malicious apps
- Checks for unsecure Wi-Fi connections

Privacy

- Limit user access to apps using PINs
- Monitor the data apps can access and remove suspicious ones using one-tap uninstall
- Set special privilege settings for guests and kids

Productivity

- Automatically closes unused background apps to boost device speed and decrease power consumption
- Frees up internal storage space by removing unnecessary files and apps
- Allows you to set data caps for each app

Network security

Our display solutions offer the flexibility IT administrators need to configure device settings according to their organization's in-place security measures. It allows them to use certificates, apply stricter proxy and WPA2 settings, and implement the use of secure network communication protocols such as HTTPS, SSL, and TLS. All these strategies can be used to secure your network.

Enterprise-grade authentication

Our displays allow you to set up WPA2-Enterprise, ensuring data security on your Wi-Fi network. This protocol not only encrypts communication over a network, it also allows you to authenticate users either through a local user list or through a Remote Authentication Dial-In User Service (RADIUS) server.

Encrypted data transmission

BenQ displays support the use of Certificate Authority (CA) certificates required by trusted cryptographic protocols such as SSL and TLS. Certificates can be used to validate the identity of other devices, secure connections between your display and other servers, ensure data integrity, and encrypt data to prevent snooping.

Proxy-level protection

By configuring the proxy settings of your BenQ displays, you can effectively regulate your network bandwidth use, restrict access to malicious and unproductive sites, and better protect user privacy.

Cloud security

BenQ uses a resilient hybrid of reliable public cloud (such as AWS and Amazon S3) and private cloud solutions configured to host our user portals and securely store device and user data. Our online device and account management systems (DMS and AMS) use a mix of JSON web tokens and OAuth 2.0 for secure and convenient authorization.

Vetted cloud infrastructure

We host the BenQ service portal and our databases on Amazon cloud servers (Locates 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 as part of the AWS Compliance Programs.

Convenient authorization

Our web services make use of OAuth 2.0 and JSON web tokens, industry standards that are utilized for easy authorization across multiple devices without ever requiring you to share your private credentials with BenQ.

Secure communications

BenQ websites use tried and tested internet security protocols such as SSL and HTTPS to secure your connection and encrypt any transmitted data. These measures prevent cybercriminals from freely intercepting sensitive data sent between BenQ online portals and your devices.

Interactive Displays	Device Security	Network Security	Cloud Security
DuoBoard • CP01K series	✓	✓	✓
RP series • RP03 models • RP02 models • RP01K models	✓	✓	✓
RM series • RM03 models • RM02K models • RM02S models • RM01K models	✓	✓	✓
RE series • RE03 models • RE01 models	✓	✓	✓
IL series • IL0 models • IL01 models	✓	✓	✓

Non-touch Displays	Device Security	Network Security	Cloud Security
CS series • CS01 models	✓	✓	✓
SL series • SL02K models • SL01 models	✓	✓	✓
ST series • ST02S models • ST02 models • ST01K models	✓	✓	✓
BH series • BH01 models		✓	✓

Cover all the bases

Secure your assets

Your data is important. Whether your displays and data reside on a local environment or are remotely managed via our cloud service portals, BenQ guarantees both device and data protection. We have fixed security measures at the endpoint, gateway, and cloud levels that prevent attackers from stealing your data or hacking your devices.

Be compliant

Organizations looking to keep their businesses compliant with global industry standards can rest assured that BenQ and our display solutions have gone through rigorous screening and have all passed the strict data privacy criteria imposed by the European Union's General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and ISO/IEC 27001 information security standard.

Protect your privacy

Your personal, private information stays private with BenQ. Whenever you use any of our products or portals, we ensure that your data never gets exposed. We not only block threats that may compromise your privacy, we also let you easily configure settings to limit data access. Our cloud service providers also adhere to the highest standards for data privacy.

Ensure continuity

Vulnerable devices stall operations, either when they malfunction because of malware or when remote attackers find ways to target crucial processes in your organization's network. Our built-in security solutions and over-the-air updates help keep your BenQ displays operational, preventing attacks while boosting your device efficiency with the latest features.

Stay secure

If your display's Android OS has reached its end-of-life date, BenQ is still able to ensure your device's security and functionality through regular firmware updates that include new BenQ display features, bug fixes, and security and privacy patches. Your device will continue operating smoothly and securely.