Mehr Sicherheit mit BenQ

Display-Lösungen mit Fokus auf Sicherheit

Mehr Sicherheit mit BenQ

BenQ weiß, dass die Einführung neuer Geräte in Ihrem Unternehmen immer gewisse Risiken mit sich bringt. Ohne ausreichende Sicherheitsmaßnahmen können diese Produkte Ihre Netzwerke angreifbar machen – mit möglichen Folgen wie Datenlecks, Verletzungen der Privatsphäre oder betrieblichen Ausfällen.

Vertrauen Sie auf BenQ, wenn es darum geht, Lösungen zu liefern, die perfekt zu Ihrer bestehenden Sicherheitsstrategie passen. Ob interaktive Displays, Smart Signage oder smarte Projektoren – wir bieten nicht nur herausragende Bildschärfe, Farbgenauigkeit, Klangqualität und Interaktivität, sondern auch erstklassige Sicherheitsfunktionen, die Ihr Unternehmen schützen.

Unsere End-to-End-Lösungen – von einzelnen Geräten bis hin zur Cloud-Infrastruktur – bieten mehrere Sicherheitsebenen, mit denen Sie jeden Punkt Ihrer unternehmensweiten Sicherheitsanforderungen erfüllen.

Gerätesicherheit

Netzwerksicherheit

Cloud-Sicherheit

01 Wir halten uns an internationale Standards und wahren Ihr Recht auf Datenschutz.

02 Wir schützen Ihre Organisation vor Sicherheitsbedrohungen

03 Wir bieten sicheren Zugriff auf Ihre BenQ Smart Displays, Benutzerkonten und Dateien.

01

Wir halten uns an internationale Standards und wahren Ihr Recht auf Datenschutz

Die BenQ Smart Displays und die zugehörigen Cloud-Dienste haben strenge Prüfungen durchlaufen und die hohen Datenschutzanforderungen folgender Vorschriften erfolgreich erfüllt: die Datenschutz-Grundverordnung der Europäischen Union (DSGVO und DSGVO-K), der California Consumer Privacy Act (CCPA), das britische Regime für Produktsicherheit und Telekommunikationsinfrastruktur (PSTI), die Cloud Application Security Assessment (CASA) der App Defense Alliance (ADA), das Children’s Online Privacy Protection Act (COPPA) sowie die Sicherheitsstandards ISO/IEC 27001.

Wir halten uns an internationale Standards und wahren Ihr Recht auf Datenschutz.

Ethische Datenerhebung und -nutzung

BenQ hält sich an internationale Datenschutzvorschriften wie die DSGVO und den CCPA und garantiert, dass wir keine personenbezogenen Daten (PII) sammeln oder speichern, es sei denn, dies ist von unseren Kunden ausdrücklich erlaubt.

BenQ stellt zudem sicher, dass Kundendaten, wie beispielsweise Benutzerverzeichnisse der Organisation, ausschließlich für die ausdrücklich vereinbarten Zwecke verwendet werden. Dazu kann etwa die Aktivierung und Verbesserung bestimmter Cloud-Dienste und Gerätefunktionen gehören.

BenQ verkauft oder gibt die Daten unserer Kunden nicht unrechtmäßig weiter.

Geprüfte Cloud-Dienste und Infrastruktur

Das BenQ Account Management System (AMS) hat die Anforderungen der CASA Tier-2-Bewertung der App Defense Alliance (ADA) erfolgreich bestanden. Alle Aspekte von AMS – einschließlich Cloud-Architektur, API und End-to-End-Prozesse wie Zugriffskontrolle, Verschlüsselung und weitere Sicherheitsfunktionen – wurden gründlich geprüft, getestet und als sicher gegenüber Datenbedrohungen validiert.

Darüber hinaus betreiben wir das BenQ Service-Portal und unsere Datenbanken auf Amazon-Webservern (Standort: Frankfurt, Deutschland), die nach den höchsten Standards für Datensicherheit, Datenschutz und Zuverlässigkeit aufgebaut sind. Die BenQ Cloud-Dienste werden regelmäßig von unabhängigen Prüfern im Rahmen der AWS-Compliance-Programme getestet.

Wir halten uns an internationale Standards und wahren Ihr Recht auf Datenschutz

Sichere Kommunikation

BenQ-Websites nutzen Internet-Sicherheitsprotokolle wie SSL und HTTPS, um Ihre Verbindung zu schützen, übertragene Daten zu verschlüsseln und zu verhindern, dass Angreifer Daten abfangen, die zwischen den BenQ-Online-Portalen und Ihren Geräten gesendet werden.

Bequeme Autorisierung

BenQ-Webdienste nutzen OAuth 2.0 und JSON Web Tokens, Industriestandards, die eine effiziente Autorisierung über mehrere Geräte ermöglichen, ohne dass unsere Nutzer ihre privaten Zugangsdaten mit BenQ teilen müssen.

Mehrstufige Authentifizierung

BenQ gibt IT-Administratoren die Möglichkeit, eine Zwei-Faktor-Authentifizierung durchzusetzen, bei der Benutzer beim Anmelden einen Sicherheitscode eingeben müssen, der an ihr Mobilgerät gesendet wird.

Wir halten uns an internationale Standards und wahren Ihr Recht auf Datenschutz

Passwörter bleiben privat

BenQ Smart Displays bieten Anmeldemethoden, die verhindern, dass Benutzer ihre Zugangsdaten auf dem Bildschirm eingeben, und gewährleisten, dass Passwörter nicht öffentlich einsehbar sind. Darüber hinaus bietet BenQ eine komfortable Lösung, mit der Lehrkräfte sowohl auf ihr Display als auch auf ihre Cloud-Laufwerke mit ihren Schulzugangsdaten zugreifen können. Dies reduziert die Notwendigkeit, sich mehrere Passwörter zu merken, und stellt sicher, dass alle Konten den Passwort-Richtlinien Ihrer Organisation entsprechen.

QR-Code-Anmeldung

Benutzer können einen QR-Code auf einem BenQ Board, einer Digital Signage-Anzeige oder einem Smart-Projektor mit ihrem Mobilgerät scannen, um sich sicher anzumelden.

NFC-Anmeldung

Einige BenQ Board-Modelle sind mit integrierten NFC-Sensoren ausgestattet. Systemadministratoren können jedem Benutzer NFC-Karten ausstellen, um den Zugriff zu kontrollieren und die Anmeldung zu vereinfachen.

SSO

BenQ Smart Displays unterstützen sichere Single-Sign-On-Dienste (SSO) von Microsoft Entra ID, Google Workspace, Clever, ClassLink, LDAP-Servern und anderen SAML-basierten Identitätsanbietern, die verschlüsselte Token zum Schutz der Benutzeranmeldedaten verwenden.

02

Wir schützen Ihre Organisation vor Sicherheitsbedrohungen

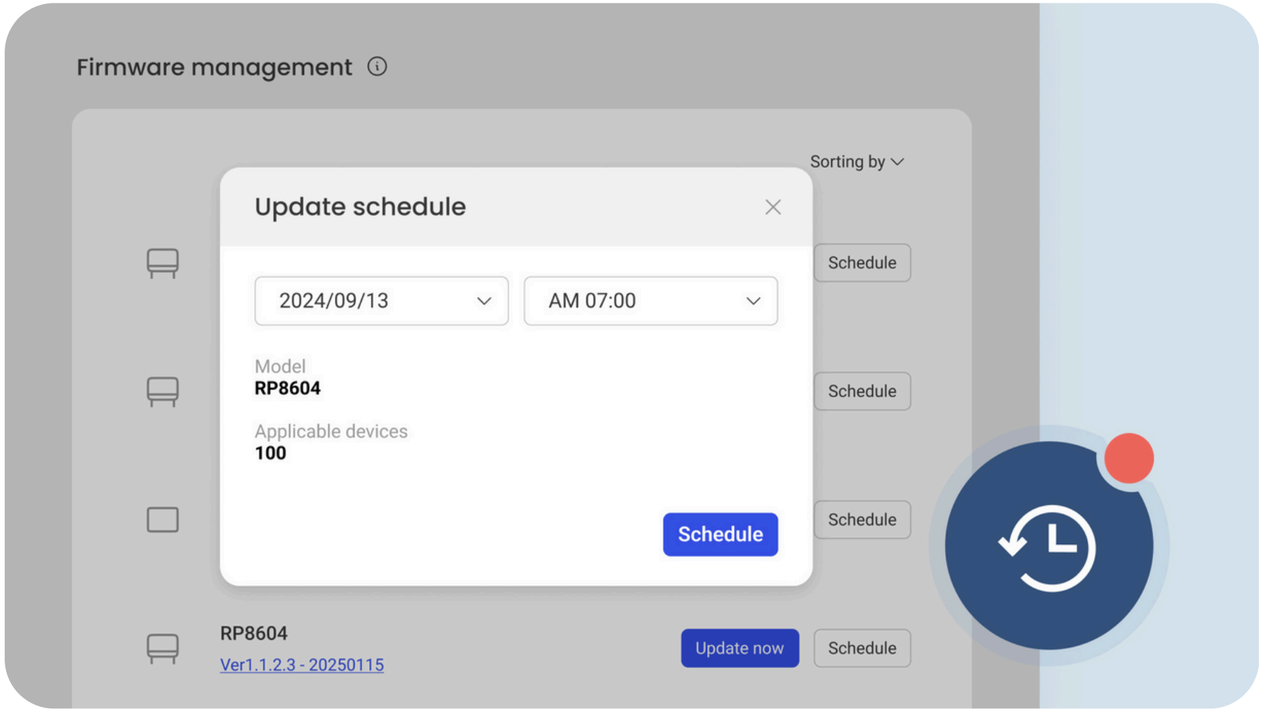
BenQ unterstützt Schulen und Unternehmen dabei, ihre Systeme und Daten vor Bedrohungen wie Malware und Hackerangriffen zu schützen, indem wir umfassende Sicherheitslösungen anbieten, die alle Ebenen der Dateninfrastruktur abdecken.

Wir schützen Ihre Organisation vor Sicherheitsbedrohungen

Schutz vor Sicherheitslücken

BenQ stellt regelmäßig die neuesten Sicherheitspatches und Firmware-Updates für unsere BenQ Boards, Digital Signage-Lösungen und Smart-Projektoren bereit. Administratoren können die Over-the-Air-(OTA)-Updatefunktion ihrer BenQ Smart Displays vollständig nutzen und diese Patches remote auf alle ihre Smart Displays übertragen.

Damit wird nicht nur sichergestellt, dass die Displays rechtzeitig vor Exploits und ähnlichen Angriffen auf das Netzwerk geschützt sind, sondern auch, dass das Betriebssystem der Boards und die BenQ-Software stets mit optimaler Leistung funktionieren.



Wir schützen Ihre Organisation vor Sicherheitsbedrohungen

Flexible Netzwerksicherheit

BenQ Smart Displays verfügen über flexible Netzwerkeinstellungen, mit denen IT-Administratoren ihre Displays so konfigurieren können, dass sie optimal zu ihrer bestehenden Sicherheitsstrategie passen.

Authentifizierung auf Unternehmensniveau

WPA2-Enterprise für sichere Benutzeranmeldung und Kommunikation

Verschlüsselte Datenübertragung

Zertifikate verwenden, um andere Geräte zu validieren und Daten zu verschlüsseln.

Proxy-Schutz

Proxy-Einstellungen konfigurieren, um den Zugriff auf schädliche Websites zu verhindern.

Antimalware- und Anti-Phishing-Maßnahmen

Nutzer der Google-zertifizierten 04-Serie von BenQ Boards und Smart Signage profitieren von Google Play Protect und Safe Browsing.

Google Play Protect stellt sicher, dass Apps sorgfältig geprüft werden, bevor Benutzer sie auf dem Display herunterladen und installieren können. Darüber hinaus werden installierte Apps auf verdächtige Aktivitäten gescannt und bei Bedarf entfernt.

Google Safe Browsing schützt die Nutzer beim Surfen im Internet, indem es Warnungen anzeigt, wenn sie potenziell schädliche Websites besuchen, die Phishing oder andere webbasierte Bedrohungen enthalten.

Google Play Protect

Google Safe Browsing

03

Wir bieten sicheren Zugriff auf Ihre BenQ Smart Displays, Benutzerkonten und Dateien.

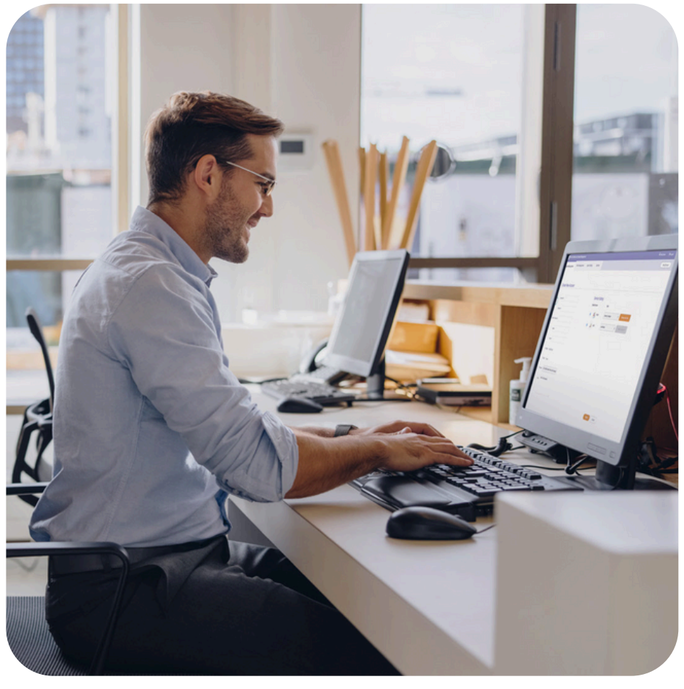
Das BenQ Account Management System (AMS), die BenQ Device Management Solution (DMS) und das BenQ Identity and Access Management (IAM) bieten IT-Administratoren Werkzeuge zur Erstellung und Verwaltung von Benutzerkonten. So können sie unbefugten Zugriff verhindern und Manipulationen an den Einstellungen der BenQ Smart Displays sowie an Benutzerdateien und -ordnern vermeiden.

Wir bieten sicheren Zugriff auf Ihre BenQ Smart Displays, Benutzerkonten und Dateien.

	Gastbenutzer	Eingeschränkte Benutzer	Authentifizierte Benutzer
Anmelden	Nicht erforderlich	Erforderlich	Erforderlich
Änderung der Einstellungen	Nicht erlaubt	Nur Grundeinstellungen	Einstellungen für reguläre Benutzer
Angeschlossene Geräte (über HDMI oder USB-C)	✓	✓	✓
Öffentlicher Ordner	×	✓	✓
Persönliche Ordner	×	✓	✓
Cloud-Speicher	×	✓	✓
EZWrite-Whiteboard (BenQ Boards)	✓	✓	✓
InstaShare Wireless Bildschirmfreigabe	✓	✓	✓
Webbrowser	×	✓	✓

Erhalten Sie detaillierte Informationen zu den sicheren Zugriffskontrollen für das BenQ Board.
https://www.benq.com/de-de/education/edtech-blog/access-authority-security-user-roles-settings-benq-board.html

Wir bieten sicheren Zugriff auf Ihre BenQ Smart Displays, Benutzerkonten und Dateien.



Sicherer Benutzerzugang

BenQ bietet zwei Möglichkeiten, mit denen IT-Administratoren strengere Zugriffskontrollen für ihre BenQ Smart Displays durchsetzen können.

Authentifizierungsmodus

Dieser Modus bietet ein höheres Maß an Zugriffskontrolle, da er Gäste vollständig daran hindert, das Smart Display zu nutzen oder dessen Einstellungen zu verändern. Die Aktivierung dieses Modus in DMS stellt sicher, dass nur authentifizierte Benutzer das Display und seine Funktionen verwenden können.

Eingeschränkte Benutzerrolle

Die Zuweisung dieser Rolle gewährleistet das höchste Maß an Zugriffskontrolle, da selbst autorisierte Benutzer und Gruppen daran gehindert werden, Änderungen an kritischen Smart-Display-Einstellungen vorzunehmen, während sie weiterhin Zugang zu allen wesentlichen Funktionen und Features des Displays haben.

Automatische Abmeldung bei Inaktivität

Geräte, die unverschlossen und unbeaufsichtigt bleiben, sind eine der häufigsten Ursachen für Datenlecks. Administratoren können dies auf dem BenQ Smart Display verhindern, indem sie in AMS eine automatische Abmeldezeit für inaktive Sitzungen festlegen. Wenn ein Benutzer einmal vergisst, sich vom Display abzumelden, meldet AMS das Konto automatisch ab.

Wir bieten sicheren Zugriff auf Ihre BenQ Smart Displays, Benutzerkonten und Dateien.

App-Nutzung mit BenQ DMS verwalten

IT- und Schuladministratoren haben verschiedene Möglichkeiten, die Nutzung von Apps auf BenQ Smart Displays aus der Ferne zu steuern.

Apps zulassen

Allowlisting ist der strengste Ansatz und stellt sicher, dass nur zuvor genehmigte Apps auf dem Display genutzt werden können. Diese Methode eignet sich besonders für Organisationen, die eine sichere Umgebung aufrechterhalten möchten, indem Ablenkungen minimiert und die Installation unautorisierter Apps verhindert wird.

Apps blocken

Blocklisting ermöglicht es, bestimmte Apps zu sperren, während der allgemeine Zugriff auf den Google Play Store weiterhin möglich bleibt. Dies ist nützlich, um Apps zu verhindern, die Ablenkungen verursachen oder ein Sicherheitsrisiko darstellen könnten, ohne den Zugriff auf alle Apps vollständig einzuschränken.

Apps verbergen

Wenn Benutzer eine App auf einem BenQ Smart Display installiert haben und Sie möchten, dass sie diese nicht mehr nutzen, können Sie die App in DMS einfach ausblenden. Dies eignet sich besonders für Organisationen mit wenigen Geräten, die den Nutzern in der Regel uneingeschränkten Zugriff auf den Play Store erlauben.

Blockieren Sie den Play Store

Wenn Sie strikte Kontrolle über alle Apps benötigen, können Sie den Zugriff auf den Play Store vollständig deaktivieren. Dadurch werden unautorisierte App-Installationen verhindert und es wird sichergestellt, dass auf dem Smart Display nur von der IT genehmigte Apps verfügbar sind.

Wie können Organisationen ihre Smart Devices sicherer machen?

Nachfolgend finden Sie eine Checkliste, die Ihnen als Leitfaden dient, um sicherzustellen, dass Ihre Smart Displays sicher genutzt werden können.

- [ ] Verfügt Ihre Organisation über Richtlinien für die Nutzung von Smart Displays?
- [ ] Können Sie Benutzerrechte für Ihre Smart Displays zuweisen und ändern?
- [ ] Erhalten Sie Firmware-Updates und Sicherheitspatches für Ihre Smart Displays?
- [ ] Können Sie Sicherheitssoftware installieren?
- [ ] Können Sie die Netzwerkeinstellungen Ihres Smart Displays konfigurieren, um es sicherer zu machen?
- [ ] Verwendet Ihr Smart Display sichere Cloud-Systeme?
- [ ] Entsprechen Ihr Smart Display und dessen Cloud-Dienste den Datenschutzbestimmungen?