Jabra GN

WHITE PAPER

PANACAST SERIES

Protect personal privacy and sensitive data with the PanaCast Portfolio

The PanaCast series

Jabra's use of industry security standards brings IT security departments confidence in our products when using features like PeopleCount and Virtual Director. From adhering to security standard protocols to using third party security tests, the Jabra PanaCast portfolio puts security at the forefront.

The Jabra PanaCast series takes security into consideration from both a software and hardware level. Online privacy is also a priority, and Jabra respects privacy-related choices. Jabra supports the protection of consumer privacy on the Internet and the principles of disclosure and fair information practices. If you share personal information with Jabra, the information will be treated according to the Jabra privacy policy.

JABRA PANACAST SERIES

PanaCast 40 VBS and PanaCast 50 VBS

Get inclusive meetings at your fingertips, with our Android™-based all-in-one room systems.

PanaCast 50

Our original Bring-Your-Own-Device video bar offers plug-and-play access for more equal meeting experiences.

PanaCast 50 Room System

A complete solution with a Jabra PanaCast 50, ThinkSmart Core computing device, and ThinkSmart Controller that enables small and medium rooms to play host to more inclusive, more immersive virtual meetings.

PanaCast 20

Make picture-perfect presentations and nail those all-important pitches with our PanaCast 20 personal video camera.

Security by feature

Anonymous PeopleCount

Using Jabra Direct, it is possible to set a safety capacity limit for a meeting room. This data point is supported in Jabra PanaCast Camera, PanaCast 50, and PanaCast 50 VBS.

PeopleCount technology detects the heads and bodies of any brightly-lit visible people within 1-4 meters of the camera (3-12 feet). Head recognition on PanaCast 50, PanaCast 50 Room System, PanaCast 40 VBS and PanaCast 50 VBS works even when the face is covered or turned away from the camera.

The device automatically detects if the configured safety capacity limit is exceeded by using PeopleCount technology. It can then alert people in the meeting room in real time. This anonymous PeopleCount data can be tracked and managed using Jabra Xpress.

The PeopleCount feature does not look for or store personally identifiable information. The only information that leaves the PanaCast product is the people count, or in other words, the number of people detected in the room.

Intelligent Zoom

Intelligent Zoom automatically includes everyone in the field of view and zooms in on the participants to present the most optimized view with regards to screen real-estate. This feature is available on the Jabra PanaCast Camera, PanaCast 20, PanaCast 50, PanaCast 50 Room System, PanaCast 40 VBS and PanaCast 50 VBS. Intelligent Zoom only detects people that are covered in the 180-degree field of view. Intelligent Zoom does not capture or store personally identifiable information.

Virtual Director

Virtual Director, available on PanaCast 50, PanaCast 50 Room System, PanaCast 40 VBS and PanaCast 50 VBS, is an automatic zoom mode that features speaker tracking, focusing on the active speaker present in the field of view. Virtual Director uses a combination of person detection and audio direction of arrival to detect and zoom in on the active speaker. Virtual Director does not capture or store personally identifiable information. Users can access Virtual Director using the camera controller in Jabra Direct or Jabra Plus.

Edge AI Based Processing

Edge AI based processing is used in the entire PanaCast series. Because data is anonymized and processed before it ever leaves the device, video devices enabled by Edge AI minimize the number of transfer points, reducing the risk of data being exposed. This allows users to benefit from advanced video analytics functions without the fear of breach of data security.

PanaCast 40 VBS & PanaCast 50 VBS

SECURE SOFTWARE DEVELOPMENT PRINCIPLES

Jabra follows a secure software development life cycle for the PanaCast 40 VBS and PanaCast 50 VBS. Architecture reviews, code reviews, penetration and internal security testing are performed to verify the implementation.

Product creation and delivery lifecycle includes considerations for confidentiality, integrity (data and systems), and availability. These extend to all systems that Jabra uses, both on-premises and in the cloud.

The PanaCast 40 VBS and PanaCast 50 VBS are submitted to an in-depth threat assessment and risk analysis, to identify critical assets, map business use cases, and avoid all potential attack vectors of the device. Based on this analysis, security testing and validation allow Jabra to manage, monitor, and maintain product security.

As of Value Pack 3 for PanaCast 50 VBS and the launch of PanaCast 40 VBS, Jabra has partnered with Microsoft to implement Microsoft Device Ecosystem Platform (MDEP). MDEP enhances the standard Android platform by adding a robust security layer and seamless integration with relevant Microsoft services. Learn more about MDEP here: aka.ms/mdep.

WEB CONSOLE

The video bar and touch controller can be managed, upgraded, and configured remotely using the Web Console. Security is integral to the design of the Web Console, and includes the following security considerations:

- Based on HTTPS
- Access is restricted by account credentials that can be customized by the customer
- Data is kept secure both at rest and in transit
- Internal Storage is encrypted
- The private encryption key is stored in hardware-protected storage where no one has direct acccess
- The key is generated on the device

LOCAL ADMINISTRATION

The video bar can also be directly managed and configured locally, using a touch display (or a keyboard and mouse) that is directly connected, via USB, to the device. Additionally, both PanaCast 40 VBS and PanaCast 50 VBS can be managed by the pre-installed Video Provider's Cloud Management agents (Microsoft Teams admin center and Zoom Device Management). Refer to the third-party security and audit section for further details.

FIRMWARE

Each new firmware release is submitted to a formal Quality Assurance process and run through a thorough set of tests for both functionality and security to ensure that the required levels of security and privacy are always satisfied. The firmware version is released to end customers only after the final approval from Jabra Product Quality Management and partner UC providers.

NETWORK

PanaCast 40 VBS upon launch and PanaCast 50 VBS as of Value Pack 3 Service Release 1 have enabled support for IPv6 and 802.1X. See support documents **VBS 802.1X Whitepaper** and **VBS Network Protocols** on **jabra.com/support** for more detailed information.

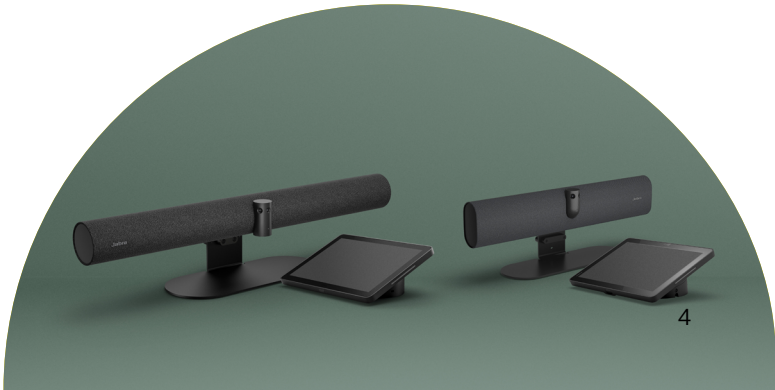
FIREWALL

Both devices can use the Online Certificate Status Protocol (OCSP) to check the revocation status of digital certificates (SSL/TLS certificates) through HTTP/S proxies. All OCSP requests and responses will pass through the web proxy server. There is no need to open specific ports on the firewall or open any extra port for OCSP.

Protocol		Info
Transport Protocol	UDP	Destination port is UDP 123
HTTPS Transport Protocol	TCP/TLS	Destination port is TCP 443
Default Network Time Protocol	ntp.jabra.com	Mapped to pool.ntp.org

Firewall configuration guidelines must be implemented to support Microsoft Teams Rooms and Zoom Rooms.

Prepare your organization's network for **Microsoft Teams**: https://learn.microsoft.com/en-us/microsoftteams/prepare-network



PanaCast 40 VBS & PanaCast 50 VBS

THIRD PARTY SECURITY CERTIFICATIONS

Both the Touch Controller and Video Bar components of the PanaCast 40 VBS and PanaCast 50 VBS are certified for Microsoft Teams Rooms and Zoom Rooms. Therefore, they are submitted to a comprehensive security certification from Microsoft and Zoom. Requirements of both Video-as-a-Service (VaaS) providers include security audit from a third-party audit company.

JABRA PANACAST TOUCH CONTROLLER

Jabra PanaCast Control is a touch screen controller that can be used to control your video bar. Within the local network, the video bar can be managed using a paired touch controller. The communication from PanaCast Control to PanaCast 40 VBS or PanaCast 50 VBS is a proprietary development based on gRPC protocol (Google Remote Procedure Call). Security is based on TLS 1.3 over the entire underlying protocol.

DATA COLLECTION

The PanaCast 40 VBS and PanaCast 50 VBS collect personal information only for specific needs. For example, to save a Jabra serial number to pair with a selected companion device owned by a specific person later, or to discover the IP address/serial number of available Jabra devices on the same subnet to propose a device pairing.

Data Collection Type	Categories	Business Purpose
Persistent Device Information	• Device ID • Mac address • Serial number	Customer support Detecting incidents Debugging
Configurable Information	• Device name • IP address • Time zone & language • Admin name and password (hashed) • Log files • Contact email address	Customer support Detecting incidents Debugging

	FEATURES	SECURITY BENEFITS
Software	AndroidOS	Locked down to prevent side-loading of applications
	Applications	Pre-installed apps comply with Google Privacy & Security Guidelines
	Anti-Rollback	Prevents reinstallation of potential security risks or outdated features
	Passwords	All passwords are hashes and encrypted using AES-256
	OTA Updates	Restricted to Jabra signed update packages
	Secure Boot	Protects from unathorized software during boot up
	Kiosk Mode	Only pre-selected and pre-installed apps can run
	PHA Classification	All pre-installed apps must be classified as safe
Hardware	Kensington Security Slot	Secures the device to the room
	Privacy Cover	Provides an additional layer of camera security
	Cable compartment cover	Restricts physical access to ports and hardens down cables

PanaCast 50 & PanaCast 50 Room System

PROXY SUPPORT

Proxies provide a gateway between users and the internet, helping to prevent cyber attackers from entering a private network. The PanaCast 50 and PanaCast 50 Room System supports the following proxy types: HTTP, SOCKS4, SOCKS4A, SOCKS5, and SOCKS5H.

AUTOMATIC FIRMWARE UPDATES

Automatic firmware updates are a Jabra Direct feature that enables connected Jabra devices to be automatically updated to a later firmware version. This ensures that any potential security patches in an update are installed quickly without manual intervention needed.

INTELLIGENT MEETING SPACE

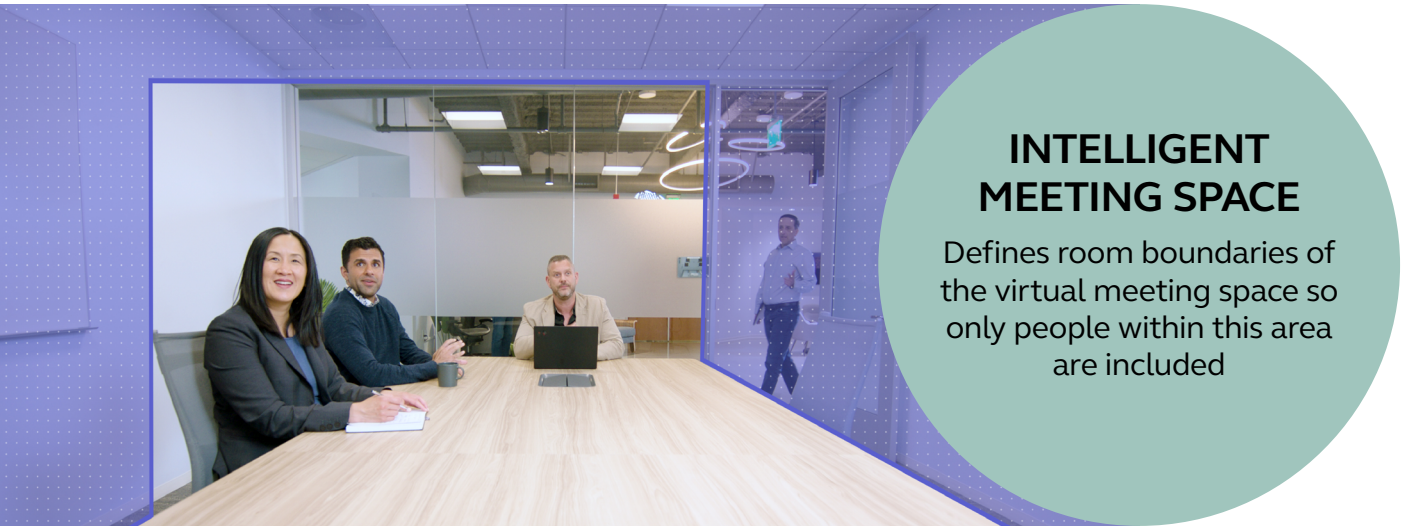
Define room borders on both PanaCast 50 and PanaCast 50 Room System to prevent those not in the conference room from being framed in the video. This feature is especially useful for conference rooms with glass walls or open space meeting areas.

PRIVACY COVER

The PanaCast 50 and PanaCast 50 Room System privacy covers provide a peace of mind that no video stream can be seen when the camera is in use. The PanaCast 50 has an easy-to-install privacy cover that sits into place.

KENSINGTON SECURITY SLOT

The Kensington security slot on the back of the PanaCast 50 allows for it to be secured to the room using a standard Kensington lock, making it harder to physically remove the device from the room.



PanaCast 20

ON-DEVICE BACKGROUND EFFECTS

With a powerful Edge AI chipset built in, PanaCast 20 is an intelligent personal video camera that performs all of the processing for the user's video image directly. This intelligence extends far beyond just processing video – it also drives the enhanced features by continuously scanning and analyzing the user's video image, and then optimizing according to the applied experience(s), which now includes on-device background effects.

On-device Background Effects, an intelligent feature that allows the user to optionally apply a real-time blur effect or replace their video background directly on PanaCast 20 provides for added privacy and security in the office, on location, or at home.

Traditionally, utilizing such effects during video calls would involve the user applying a virtual background within their preferred video client to obscure their environment from meeting participants on the far end. However, while this allows the user to feel a sense of security in front of their peers, the reality is that the entirety of the video image is still visible to the user's computer, their video client, and the cloud. It remains fully exposed as it passes through every secured and unsecured network along the way.

With PanaCast 20, the pixels that comprise a user's background are protected by having the background effects applied on the camera itself.

What cyber attackers see when attempting to access your video image

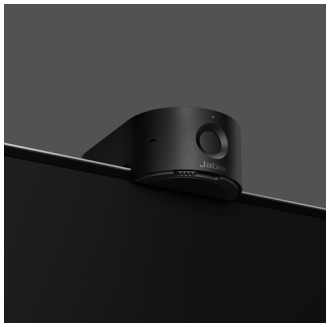
JABRA PANACAST 20 On-device Background Effects

Client-based blur effect/ virtual background

PRIVACY COVER

For calls when users aren't feeling camera-ready, PanaCast 20 provides instant protection with its integrated privacy cover. With the flick of a finger, it slides across the lens to effectively hide whatever they prefer to keep hidden.

Privacy cover – open



Privacy cover – closed

MIC OFF BY DEFAULT

The microphone on the PanaCast 20 is off by default. The microphone can be enabled through the Jabra Direct App that can be downloaded on the user's computer. Having the microphone off by default ensures that users remain in control over which device is accessing audio.

Incident Response

At Jabra, we understand that information security is your top priority. To help us identify potential areas for improvement in data protection and security, we welcome all feedback from our community regarding possible vulnerabilities in our products.

To contact the Jabra Product Security Office, or to report a potential product security issue, please email security-center@jabra.com. When you report a potential security issue to us, we'll work together with you to ensure that, if a fix is required, it's made available for all of our users as quickly as possible.