

# Cynap Videobar Security White Paper



# Table of Contents

- Table of Contents ..... 2
- 1. Introduction..... 3
- 2. WolfVision security programme overview ..... 3
  - 2.1 Security by design..... 3
  - 2.2 Security testing ..... 3
  - 2.3 Secure configuration ..... 4
  - 2.4 Contact in the event of a discovered vulnerability..... 4
- 3. What is a Cynap Videobar system? ..... 4
  - 3.1 Cynap Videobar ..... 4
  - 3.5 Network setups ..... 6
  - 3.6 Cynap Videobar use of Bluetooth..... 7
- 4. Technical description..... 8
  - 4.1 Custom Linux OS..... 8
  - 4.3 Cynap Videobar web user interface (built-in web server) ..... 8
  - 4.4 Administrator security..... 9
  - 4.5 Feature lock options ..... 9
  - 4.6 Usage and requirements of ports for specific functionality..... 10
  - 4.7 Wireless communication components..... 10
  - 4.8 BYOD Screen Sharing..... 10
    - 4.8.1 Notes on security for vSolution Cast users..... 11
  - 4.9 Protected and Open Mirroring Modes..... 11
  - 4.10 PIN ..... 11
  - 4.11 HTTP, HTTPS, WS, and WSS access by networking interface ..... 11
  - 4.13 TLS 1.2..... 11
- 5. vSolution App security considerations ..... 11
  - 5.1 General Data Protection Regulation..... 12
  - 5.2 Notes on security for vSolution App users when using Microsoft Teams / Zoom and additional WebRTC services on local laptop (BYOM) ..... 12
- 6. Network Security ..... 12
  - 6.1 Systems hardening ..... 12
- 7. Security best-practices ..... 13

# 1. Introduction

The subject of security is of paramount importance when considering the functionality of wireless presentation and collaboration systems. It is absolutely essential to take proper steps to ensure their secure operation in their intended environment.

To ensure security in operation, the Cynap Videobar has to be designed, implemented and properly tested - but it also needs to be installed, configured, maintained, and operated as intended by the manufacturer.

If any of these criteria are not observed, system security of the wireless presentation system could be compromised, with potentially serious consequences.

The intention of this Cynap Videobar Security White Paper is to ensure that people and enterprises responsible for procurement, installation, maintenance, and operation of Cynap Videobar solutions have relevant security-related information available to them in order to assist them with the secure installation and operation of their systems:

In addition, this Security Videobar White Paper is intended to provide relevant information that may be required during the procurement and selection process for Cynap Videobar solutions, therefore enabling fully informed purchasing decisions to be made.

This Security White Paper describes the main technical aspects of Cynap Videobar systems that are relevant for IT security. It is intended mainly for systems integrators, administrators and other personnel that are responsible for procurement, installation, configuration, and maintenance of these devices.

## 2. WolfVision security programme overview

WolfVision takes the subject of security for all its products extremely seriously, and it has developed sophisticated processes that are used throughout the design, testing, and manufacturing operations of the company, to ensure that appropriate levels of security are made available in its products that are supplied to customers.

### 2.1 Security by design

WolfVision utilises a ‘security by design’ approach to hardware and software development, and strives to keep systems as free from vulnerabilities, and impervious to attacks as possible. This is achieved through pro-active measures such as continuous testing, authentication safeguards, and adherence to best available programming practices.

WolfVision focuses on building security features into its products from the start, which counters the commonly seen tendency for security to sometimes be an afterthought in development. Addressing existing vulnerabilities and patching security holes as they are found can be a time-consuming, hit-and-miss process, and it can never be as effective as designing systems from the ground up, to be as secure as possible from the beginning.

### 2.2 Security testing

WolfVision’s testing department incorporates security testing into its daily activities. Processes are in place that are intended to reveal flaws in Cynap Videobar security mechanisms that are designed to protect data and maintain functionality as intended. Due to the limitations of security testing, passing

security testing cannot be an indication that no flaws exist, or that the system completely satisfies the desired security requirements.

Additionally, WolfVision uses external companies to conduct in-depth penetration testing on its Cynap Videobar systems (further details available on request). The resulting feedback and advice received from this third-party testing is used by WolfVision's R&D department to continuously upgrade and improve the security performance of its Cynap Videobar devices.

### 2.3 Secure configuration

Secure configuration of Cynap Videobar systems means the security measures that are implemented when actually installing and setting up the devices in order to avoid unnecessary vulnerabilities. Misconfiguration of device security can present opportunities that criminal hackers often look to exploit.

For example, WolfVision strongly recommends that Cynap Videobar systems are not installed on publicly accessible networks, and that additional login protection should be added by changing the default password as part of the installation process.

Cynap Videobar systems come with a default configuration, and whilst it is often convenient to start using a new device with its default settings, WolfVision takes care to provide information about system security features, many of which are user-configurable in order to suit an individual organisation's security requirements. Information on available security measures is provided both as documentation, and also through personal consultation, helping to provide crucial knowledge and support for integrators and administrators on how to securely set up their systems. It is of importance also to note that vSolution Cynap Videobar systems may only be sold by resellers who have successfully completed a Cynap certification programme. Certification is strictly enforced, and refresher courses occur at regular planned intervals in order to keep product knowledge comprehensive, and up to date.

An advantage of Cynap Videobar systems is that many features and functions can be either enabled/disabled in the system settings. This allows an organisation to configure the device exactly, in order to provide only the services that are actually required in order to fulfil their intended function.

### 2.4 Contact in the event of a discovered vulnerability

In the event of a systems vulnerability being discovered, detailed information should be submitted immediately to:

WolfVision GmbH  
Oberes Ried 14  
Klaus 6833  
Austria  
Tel: +43 (0)5523 52250  
Website: [www.wolfvision.com](http://www.wolfvision.com)

## 3. What is a Cynap Videobar system?

### 3.1 Cynap Videobar

vSolution Cynap Videobar is an all-in-one AV/IT appliance, designed to be the centrepiece of a meeting room or other workspace. It is a wireless presentation and collaboration system, featuring a high end 4k intelligent camera system, audio components made by Fohn, whiteboard, BYOD wireless screen

sharing, plus annotation functionality. Its user interface is designed to be extremely easy to use, and it comes with a variety of available control options designed to suit a broad range of user environments.

The device is equipped with a wide range of configurable security features and functionality, designed to keep systems free from vulnerabilities.

Cynap Videobar uses 2 networking interfaces on which both are configurable.

	ETH1	WLAN1 (AP Mode)	WLAN1 (Infra Mode)	WLAN1 (Bridged)
<b>IP</b>	DHCP or manual	Manual (set starting address)	DHCP or manual	Manual
<b>Security</b>	<ul style="list-style-type: none"> <li>▪ PEAP-MSCHAP V2</li> <li>▪ TTLS-PAP</li> </ul>	<ul style="list-style-type: none"> <li>▪ WPA2</li> </ul>	<ul style="list-style-type: none"> <li>▪ None,</li> <li>▪ WEP,</li> <li>▪ WPA2,</li> <li>▪ WPA2 Enterprise</li> </ul>	<ul style="list-style-type: none"> <li>▪ WPA2</li> </ul>
<b>Features</b>	Option to set IF as default gateway	Option to set IF as default gateway	802.11 ac/a/b/g/n	DNS and web traffic routed from ETH1
		Customizable transmit power	BSSID lock	
		Limit number of user client sessions		

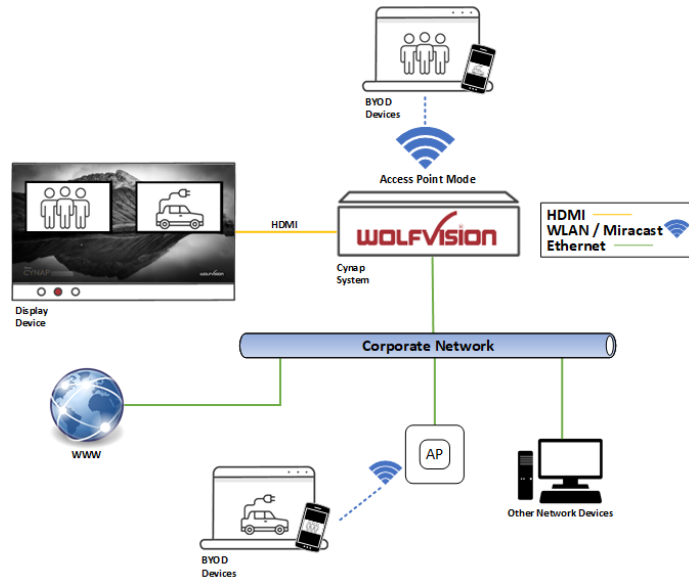
*Optional routing among networking interfaces for DHCP, DNS and HTTP/S*

### 3.5 Network setups

Cynap Videobar lacks the additional Miracast Wireless Display Adapter NIC. P2P Miracast when Wi-Fi adapter is tied to existing SSID is not available (use Miracast MS-MICE mode).

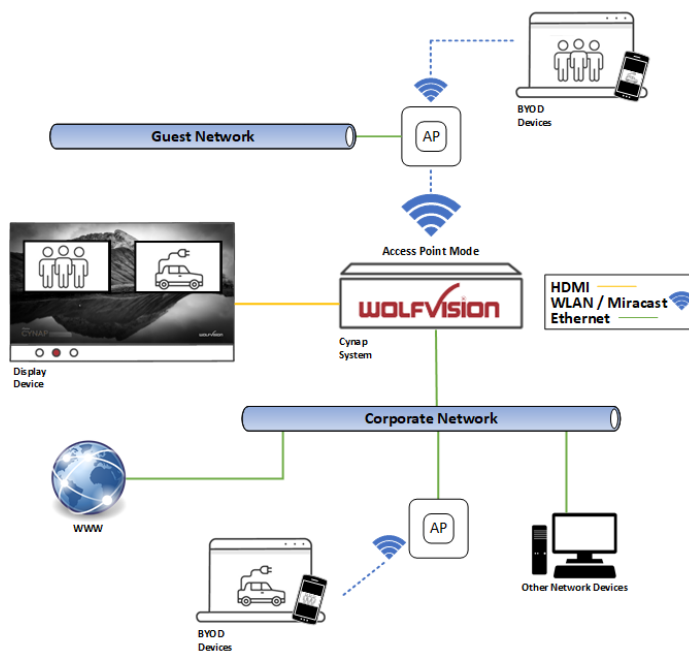
#### Cynap Videobar Wi-Fi in Access Point mode

- Cynap Videobar LAN port connected to existing network
- Wi-Fi NIC provides an optional available bridged guest network (WLAN configuration mode: Access point)



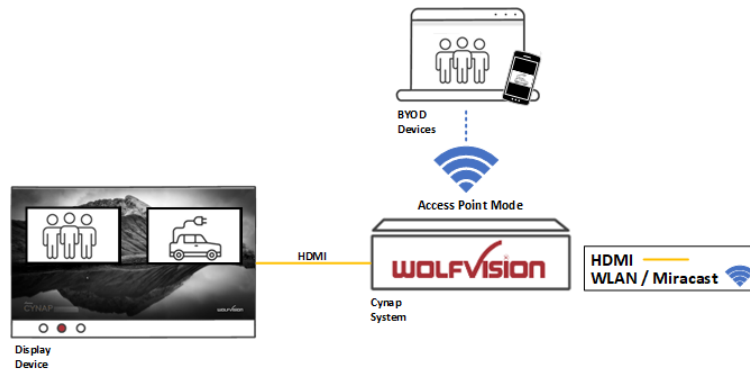
#### Cynap Videobar Wi-Fi in SSID client mode (infrastructure mode)

- Cynap Videobar LAN port connected to existing network
- Wi-Fi is connected to existing Wi-Fi SSID (separated NIC – not bridged)



## Cynap Videobar Wi-Fi in Stand-alone mode

- Cynap Videobar LAN port not in use
- Wi-Fi NIC provides a non-bridged guest network (WLAN configuration mode: Access point),



### 3.6 Cynap Videobar use of Bluetooth

Cynap Videobar systems support device discovery over Bluetooth 4.2 in (native for iOS/macOS and in combination with the vSolution App for all other operating systems).

Cynap Videobar is using its Bluetooth signal for AirPlay device discovery over Bluetooth. If mDNS/Bonjour is not available or used, it provides an alternative for multicast device discovery.

Cynap Videobar offers Bluetooth audio pairing and receiver connection.

# 4. Technical description

This document addresses security aspects for Cynap Videobar solutions.

There are many installation and configuration options possible for each device, and this flexibility in configuration enables a customised installation to be carried out, not only providing a wireless presentation and collaboration system that is best suited to each individual environment, but also allowing a custom level of security measures to be implemented according to the individual needs of a specific organisation.

## 4.1 Custom Linux OS

Cynap Videobar uses a closed custom-built Linux operating system. This distribution is a WolfVision specific variant, which in addition to the Linux kernel, contains only the individual libraries and packages necessary for the functionality of Cynap Videobar. This type of operating system is efficient, secure and lean. The operating system, including the periodic firmware updates are installed as a read-only partition that cannot be modified after the installation process. This fact, plus the strict separation of system and user data (images, videos, etc.) helps to ensure a very high level of system security. In short:

- Modifications on operating systems are prevented
- No installation of software (no malware or virus)
- No recognition for unsupported file types whatsoever
- No sessions are saved, and all files are purged at the end of each session.
- The built-in SSD can be encrypted, and the loading of unsigned firmware files is blocked by default.

The above points deliver an advantage when compared for example to a system running on Windows, which requires frequent security updates, and periodic urgent security patches. It is also positive to note that with no possibility to install additional third-party software, or modify existing software, that there is no possibility of infection from viruses or malware. It is important to note that after the end of each Cynap Videobar session, no recorded files, other files, passwords, etc. are allowed to remain on the system.

Cynap Videobar Webserver uses a self-signed certificate (SHA-256 with RSA Encryption) which is recreated on every Cynap Videobar firmware update.

## 4.3 Cynap Videobar web user interface (built-in web server)

The Cynap user interface is built as a web service and can be operated by a large number of devices:

- Mouse and keyboard
- Remote control
- Touch screen
- 3<sup>rd</sup> party control system using the Cynap APIs
- Web browser

Access to Cynap’s web app interface can be restricted with a password.

User Level	Description	Functions	Examples
Moderator “user level”	The common user level which allows to operate all Cynap functions.	Cynap Videobar operations	<ul style="list-style-type: none"><li>• Open whiteboard</li><li>• Start recording</li><li>• Allow Miracast</li></ul>



RMA (room management system) "user level"	Common user level access for 3 <sup>rd</sup> party control systems	Cynap Videobar operations	<ul style="list-style-type: none"> <li>• Open whiteboard</li> <li>• Start recording</li> <li>• Allow Miracast</li> </ul>
Collaborator	A minimum user level which allows invited users to draw on the online collaboration function using their browser	Cynap Videobar online annotation	Participate in group annotations
Administrator "admin level"	The admin user level allowing to change Cynap settings on the WebUI	Cynap Videobar setup and settings	<ul style="list-style-type: none"> <li>• Change multicast group address</li> <li>• Disable recording function</li> <li>• Change HDMI resolution</li> </ul>

Cynap Videobar uses a self-signed certificate for secure HTTP which is recreated whenever Cynap firmware is being updated.

#### 4.4 Administrator security

All administrative settings are contained in the Cynap Videobar 'Settings' area. This area is password protected, and therefore can only be accessed by authorised personnel.

If the Administrator password has been lost, then WolfVision needs to be contacted with the following details provided:

- Support PIN
- Serial Number

WolfVision will check if the serial number matches the client, will inform the relevant partner before an end user is able to restore the administrator password.

The password reset process requires local access to a Cynap Videobar system.

#### 4.5 Feature lock options

Administrators can use the feature lock option to enable or disable a wide range of functionality if required, to suit an organisation's individual security policy. This allows for configuration of Cynap Videobar devices that provide exactly the services that are actually required in order to fulfil their intended function. For example, the following features can be disabled (check individual model specifications because not all models offer all features):

- Support for USB drives
- Snapshots
- Usage of Apps
- Web browser interface (Browser interface can also be restricted to only HTTPS)
- Mirroring protocol support for AirPlay, Chromecast or Miracast, can be individually activated/deactivated for each of the two available network interfaces.

#### 4.6 Usage and requirements of ports for specific functionality

Please read the Cynap Videobar Network Integration Guide to learn more about secure network integration and required open ports for all Cynap Videobar services to work.

#### 4.7 Wireless communication components

A key functionality of Cynap Videobar devices is their ability to enable wireless on-screen presentation of content from a variety of devices (smartphones, laptops, tablets). Cynap Videobars support AirPlay, Chromecast and Miracast mirroring protocols, enabling swift wireless mirroring of materials using the technology already built into individual mobile devices. Similarly, support for these protocols enables the same levels of security that are available when these devices are in general usage. Support for WEP, WPA2, and WPA2 Enterprise protocols provides encryption of all wireless data traffic.

Security settings for mirroring can be customised on Cynap Videobars, either to permit or deny connection requests. Each mirroring protocol can be enabled/disabled separately for each configured network.

#### 4.8 BYOD Screen Sharing

Please refer to manufacturers on further protocol information about their screen sharing protocol encryption.

##### Miracast

Protocol	Type of encryption	Key	PIN
Wi-Fi Direct	Transport encryption	WPA2 – Windows client dependent	No PIN required
MS-MICE	Transport encryption	Based on network configuration (and mandatory WPA2 encryption)	Key or certificate required
MS-MICE	Video encryption	DTLS (ECDHE-RSA-AES256-SHA384)	PIN pairing required

##### AirPlay

Encryption	Key
Copyright DRM	Apple FairPlay
Transport	Based on network configuration
Media content	DTLS (ECDHE-RSA-AES256-SHA384)

Please note: AirPlay uses SSL and a multitude of ciphers throughout a connection life cycle such as Curve25519-Donna, ED25519, ChaChaPoly1305, AES, SHA-512 / SHA-256

##### Chromecast

TLS encryption

#### 4.8.1 Notes on security for vSolution Cast users

The vSolution Cast application is a standalone desktop application for Windows. vSolution Cast mirrors either the screen or a specific application window to a Cynap Videobar system. If multiple screens are detected, the user can select which one is required to be mirrored.

- The screen mirroring protocol is based on custom WolfVision mirroring traffic, combined with Cynap Videobar control commands (e.g.: a mirrored vSolution Cast source can be made fullscreen on a Cynap).
- vSolution Cast connects to a single selected Cynap Videobar only, and needs to stop mirroring before a different Cynap Videobar can be selected for mirroring.
- A PIN requirement function can be activated on a Cynap Videobar to prevent unauthorised screen sharing.
- For networking requirements please refer to the Cynap Videobar Networking Guide
- For further information on the vSolution Cast application, please check the vSolution Cast Help in the application itself.

#### 4.9 Protected and Open Mirroring Modes

In Open Mode, all users can share their mobile device screens on a Cynap Videobar system (if PIN pairing has been successfully completed).

In Protected Mode, each individual mirroring connection has to be manually enabled by a moderator.

#### 4.10 PIN

AirPlay PIN protection is also available for enhanced security, enabling a moderator to control who is able to display content on-screen. For increased security, AirPlay notifications can be set to display the PIN as a pop-up message. Settings can also be configured to display the Mirroring PIN on a second HDMI display (e.g. a moderator screen).

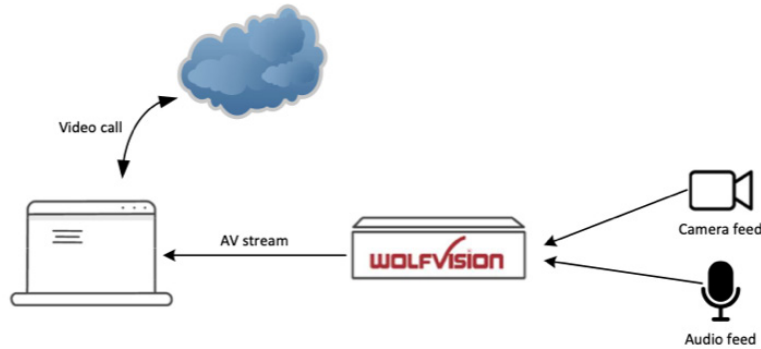
#### 4.11 HTTP, HTTPS, WS, and WSS access by networking interface

Traffic to Cynap Videobar's web server can be prevented by switching off all or selected networking interfaces.

#### 4.13 TLS 1.2

Cynap uses TLS 1.2 for its encryption (recommended). TLS 1.0/1.1 can still be activated in Cynap Videobar security settings if it is being operated in such an environment.

## 5. vSolution App security considerations



Laptop/PC (only) uses OS installed MS Teams and Zoom app and uses Cynap attached AV resources via vSolution App.

## 5.1 General Data Protection Regulation

The vSolution App does not transfer any personal data to WolfVision GmbH.

By default, the vSolution App checks the WolfVision homepage for updates when the application is started.

## 5.2 Notes on security for vSolution App users when using Microsoft Teams / Zoom and additional WebRTC services on local laptop (BYOM)

- Available on Microsoft Windows and macOS.
- Windows / macOS device will receive and share video and audio stream from vSolution App (prior mandatory driver installation)
- Windows / macOS will use local installed video conferencing software
- Windows / macOS user will authenticate in vSolution App

## 6. Network Security

Please read the Cynap Videobar Network Integration Guide to learn more about secure network integration and required open ports for all Cynap Videobar services to work.

### 6.1 Systems hardening

Systems hardening refers to security measures and best practices that are designed to reduce security risks. By reducing potential areas for attack, WolfVision systems offer potential attackers fewer opportunities for access. Some security measures are inherent in Cynap Videobar designs, and others are customisable by administrators, allowing them to select their chosen level of protection:

- WolfVision custom Linux distribution operating system – non-modifiable, impervious to viruses, malware etc.
- Unneeded applications can be disabled by administrators
- Unneeded services and wireless mirroring protocols can be disabled by administrators
- Restriction of external USB devices is possible
- Unneeded ports are disabled
- Passwords and other credentials are not stored in plain text files. No user credentials such as cloud service passwords are stored on Cynap Videobar systems
- The default administrator password must be changed when first commencing operation of the system.
- All wireless data is encrypted
- When using a wired network, IEEE 802.1x authentication can be utilised to identify and authorise devices seeking to connect to a LAN or WLAN
- Use TLS 1.2 and try to update networking components to support TLS 1.2 too

## 7. Security best-practices

The subject of security is of paramount importance, and WolfVision has developed sophisticated processes throughout the design, testing, and manufacturing phases of production, to ensure that appropriate levels of security are made available to the customer. This document describes a range of measures that can be used to increase system security. Each individual organisation will decide the level of security it requires when using Cynap Videobar systems.

In terms of WolfVision best practice WolfVision recommends that the following points should be taken into consideration:

- Ensure that the administrator password is changed immediately when installing a Cynap Videobar system and use a password that is strong enough that it shall not easily be compromised.
- Encryption is important in keeping the two-way signals between devices and access points secure. It's crucial to use the best encryption available.
- Take advantage of Cynap Videobar support for multiple networks, and set up a guest network if you want to allow visitors to your organisation to use the system. This enables you to restrict access to your corporate network.
- Decide carefully how you will manage and maintain your Cynap Videobar systems. Use the vSolution Link Pro remote management software to assist with organising centralised management.
- Update Cynap Videobar firmware when updates are made available.
- Decide how the system will be used and configure it accordingly. Disable any features that you do not wish to use.
- Report any strange behaviour of the system to WolfVision

All security features are documented in the Cynap Videobar help, available on every Cynap Videobar and on the WolfVision website.