Cynap Security White Paper

v6.5.1, 2.2.2024

WolfVision GmbH

Table of Contents

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, a wireless presentation system 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 Security White Paper is to ensure that people and enterprises responsible for procurement, installation, maintenance, and operation of Cynap solutions (Cynap Pro, Cynap Core Pro, Cynap Pure, Cynap Pure Pro, Cynap Pure Mini, Cynap Pure Receiver), 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 White Paper is intended to provide relevant information that may be required during the procurement and selection process for Cynap solutions, therefore enabling fully informed purchasing decisions to be made.

This Security White Paper describes the main technical aspects of Cynap Pro, Cynap Core Pro, and Cynap Pure 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. Note: References to Cynap Pure also apply to the Cynap Pure SDM currently supplied by Panasonic.

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 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 product family 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 devices.

2.3 Secure configuration

Secure configuration of Cynap 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 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 systems, like all wireless presentation and collaboration 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 Pro, Cynap Core Pro, and Cynap Pure Pro 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 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

3. What is a Cynap system?

3.1 Cynap Pro

vSolution Cynap Pro is an all-in-one AV/IT appliance, designed to be the centrepiece of a modern classroom, meeting room, courthouse or other workspace. It is a wireless presentation and collaboration system, featuring a media player, multi-platform web conferencing, recording and streaming capability, 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.

For larger active learning classrooms, training rooms, and collaboration spaces where multiple workstations are required, a Cynap Pro can be installed as the main unit in a room, and then linked together with multiple smaller Cynap Core Pro systems, using existing network infrastructure. This provides a scalable, AV over IP collaborative working and learning environment, where on-screen content materials are shared between the multiple display screens in the room.

The 'top-of-the-line' model in the Cynap product range, this device is equipped with a wide range of configurable security features and functionality, designed to keep systems free from vulnerabilities.

Cynap uses 4 different networking interfaces on which 3 are configurable and the 4th is being used for Miracast only.

	ETH1	ETH2	WLAN 1 (AP Mode)	WLAN 1 (Infra Mode)	WLAN 2 (MIRACAST)
IPv4	DHCP or manual	DHCP or manual	Manual (set starting address)	DHCP or manual	preset
Security	▪ PEAP-MSCHAP V2 ▪ TTLS-PAP	▪ PEAP-MSCHAP V2 ▪ TTLS-PAP	▪ None ▪ WPA2	▪ None, ▪ WEP, ▪ WPA2, ▪ WPA2 Enterprise	WPS (PIN)
Features	Option to set IF as default gateway	Option to set IF as default gateway	Option to set IF as default gateway	802.11 ac/a/b/g/n	WPS client or master
	vSolution Matrix	Optional DHCP	Customizable transmit power	BSSID lock	P2P or MS-MICE

No routing among networking interfaces

3.2 Cynap Core Pro

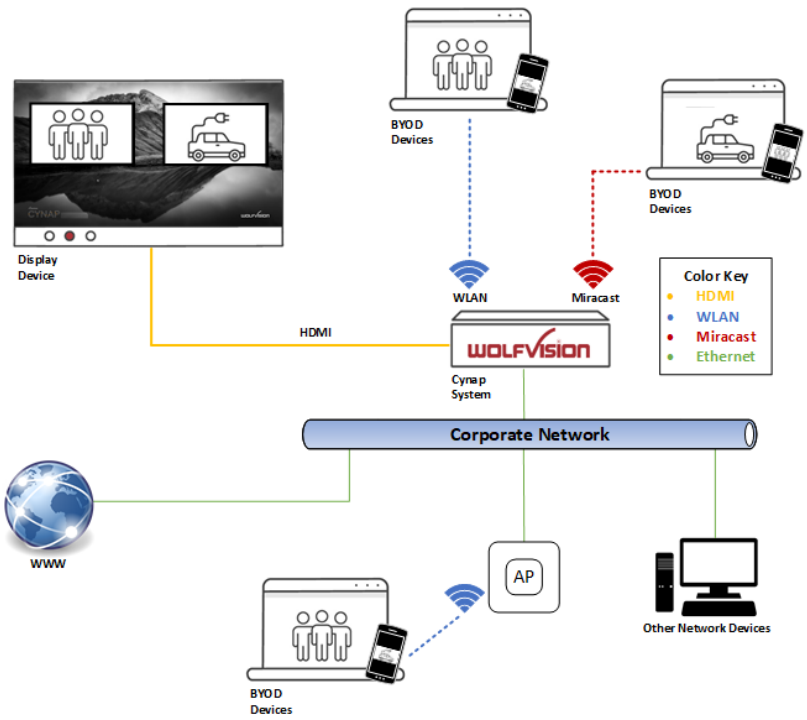
	ETH1	ETH2	WLAN 1 (AP Mode)	WLAN 1 (Infra Mode)	WLAN 2 (MIRACAST)
IPv4	DHCP or manual	DHCP or manual	Manual (set starting address)	DHCP or manual	preset
Security	▪ PEAP-MSCHAP V2 ▪ TTLS-PAP	▪ PEAP-MSCHAP V2 ▪ TTLS-PAP	▪ None ▪ WPA2	▪ None, ▪ WEP, ▪ WPA2, ▪ WPA2 Enterprise	WPS (PIN)
Features	Option to set IF as default gateway	Option to set IF as default gateway	Option to set IF as default gateway	802.11 ac/a/b/g/n	WPS client or master
		Optional DHCP	Customizable transmit power	BSSID lock	P2P or MS-MICE
			Limit number of user client sessions		

No routing among networking interfaces

3.3 Network setups

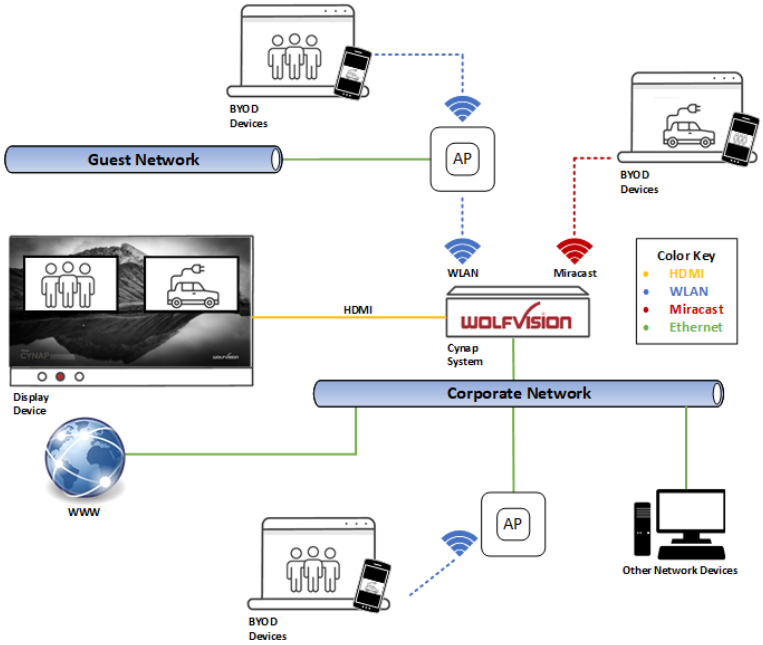
Cynap Pro and Cynap Core Pro Wi-Fi in Access Point mode

- Cynap Pro LAN ports connected to existing network
- Wi-Fi NIC provides a non-bridged guest network (WLAN configuration mode: Access point),
- Miracast NIC provides Miracast Wireless Display services (not bridged as well).



Cynap Pro and Cynap Core Pro Wi-Fi in SSID client mode

- Cynap Pro LAN ports connected to existing network
- Wi-Fi is connected to existing Wi-Fi SSID (separated NIC – not bridged)
- Miracast NIC provides Miracast Wireless Display services (not bridged as well).



3.4 Cynap Pure

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

	ETH1	WLAN1 (AP Mode)	WLAN1 (Infra Mode)	WLAN1 (Bridged)
IP	DHCP or manual	Manual (set starting address)	DHCP or manual	Manual
Security	▪ PEAP-MSCHAP V2 ▪ TTLS-PAP	▪ WPA2	▪ None, ▪ WEP, ▪ WPA2, ▪ WPA2 Enterprise	▪ WPA2
Features	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		

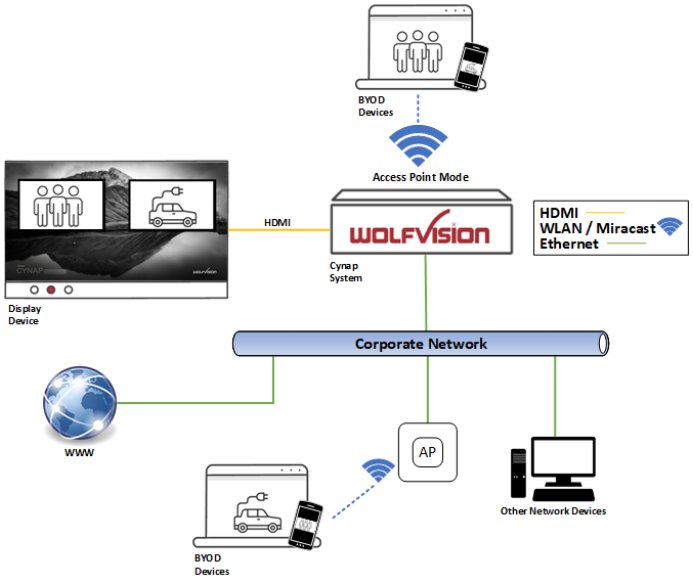
Optional routing among networking interfaces for DHCP, DNS and HTTP/S

3.5 Network setups

Cynap Pure 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).

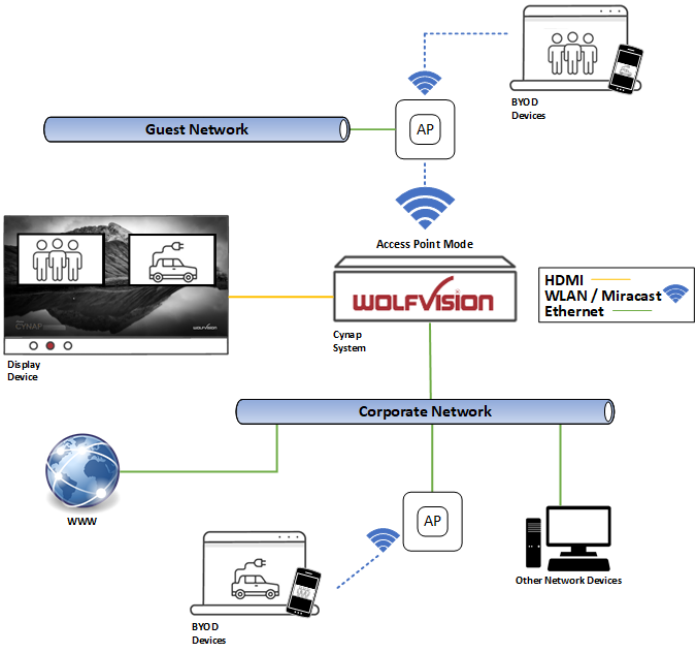
Cynap Pure Wi-Fi in Access Point mode

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



Cynap Pure Wi-Fi in SSID client mode (infrastructure mode)

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



3.6 Cynap use of Bluetooth

All Cynap systems support device discovery over Bluetooth 4.0 in (native for iOS/macOS and in combination with the vSolution App for all other operating systems).

Cynap 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.

4. Technical description

This document addresses security aspects for all Cynap solutions, and whilst each of them shares many of the same features and core functionality, this document will highlight instances where certain information is applicable only to a specific Cynap model.

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 Pro, Cynap Core Pro, Cynap Pure, Cynap Pure Pro, and Cynap Pure Mini use 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. 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 or browser extensions (no malware or virus)
- Disabled pop-ups
- No recognition for unsupported file types whatsoever
- No cookies are stored when using the built-in web browser (Cynap Pro, Cynap Core Pro, Cynap Pure Pro)
- 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 session, no recorded files, other files, passwords, cookies, history files etc. are allowed to remain on the system.

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

4.2 Built-in web browser

Cynap Pro, Cynap Core Pro, and Cynap Pure Pro have a built-in web browser feature which makes it very convenient to display web-based content on-screen side-by-side with other presentation materials. For security reasons downloading of files is blocked.

No history files are saved on completion of a session and no cookies are stored on Cynap.

4.3 Cynap 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
- 3rd 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 operations	• Open whiteboard • Start recording • Allow Miracast
RMA (room management system) "user level"	Common user level access for 3rd party control systems	Cynap operations	• Open whiteboard • Start recording • Allow Miracast
Collaborator	A minimum user level which allows invited users to draw on the online collaboration function using their browser or Matrix client station	Cynap online annotation	Participate in group annotations
Administrator "admin level"	The admin user level allowing to change Cynap settings on the WebUI	Cynap setup and settings	• Change multicast group address • Disable recoding function • Change HDMI resolution

Cynap 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 '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 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 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
- Front panel login
- Snapshots and HD Recording
- Usage of Apps
- Streaming
- 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 three available network interfaces.

4.6 Usage and requirements of ports for specific functionality

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

4.7 Wireless communication components

A key functionality of all models in the Cynap range is their ability to enable wireless on-screen presentation of content from a variety of devices (smartphones, laptops, tablets). All Cynap models 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 all Cynap models, 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 encryption4.8.1 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 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 control commands (e.g.: a mirrored vSolution Cast source can be made fullscreen on a Cynap).
- vSolution Cast connects to a single selected Cynap only, and needs to stop mirroring before a different Cynap can be selected for mirroring.
- A PIN requirement function can be activated on a Cynap to prevent unauthorised screen sharing.
- For networking requirements please refer to the Cynap 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 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's web server can be prevented by switching off all or selected networking interfaces.

4.12 RTSP access by networking interface

RTSP audio/video streaming 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 security settings if it is being operated in such an environment.

5. vSolution App security considerations

Notes on security for vSolution App users when using Cynap and Microsoft Teams

- Username and encrypted password are only stored on the iOS / Android / Windows device after 'save' is pressed in the app
- For authentication, a WebView is opened in the app and username and password are automatically entered
- Following successful authentication, a token is stored in the app
- Password is stored in the App because periodically the token becomes invalid and re-authentication is made using the stored password.
- Authentication with username and password always done on the App
- When a Teams meeting is transmitted to a Cynap, the token is encrypted (via secure socket connection) and passed on to the Cynap
- Cynap then opens a Teams window and uses the token to authenticate itself automatically
- Note: The original authentication data (username & password) are not stored in this token meaning that the Cynap system does not store any usernames or passwords
- The Teams window is only controllable locally on the Cynap or via the iOS/Android device that started the Teams session.

Notes on security (authentication process) for vSolution App users when using Cynap and Zoom on a Cynap

vSolution App itself does not do any authentication with Zoom. Data is saved in the App and these are transferred to a Cynap system when a meeting starts. Examining the three modes:

My Meeting Room & Join Meeting Room

- For App My meeting Room & Join meeting room the Meeting ID and password are only saved on the iOS / Android device after 'save' is pressed in the app. The password is stored in encrypted form.

Local Meeting Room

- When starting a Cynap Local meeting room, no data is saved on the app

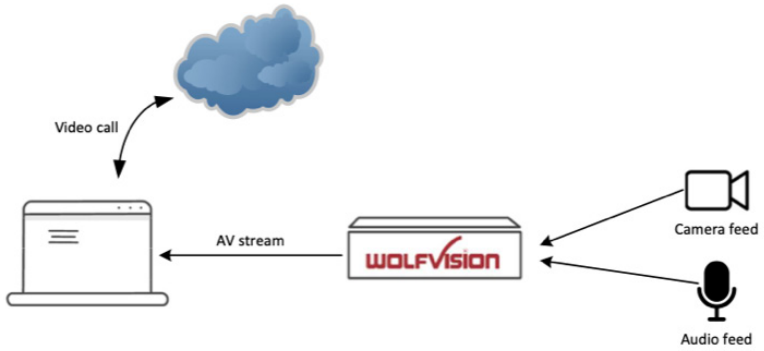
Authentication process

- All Zoom authentication takes place on the Cynap. Data is received via a secure socket connection, and a connection to the respective meeting room is established using the Zoom SDK.

- For Zoom to function, an API key and secret is stored on the Cynap and, if necessary, a personal meeting ID with name and password (these settings are stored in a settings file, which in turn is encrypted).

5.1 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



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

5.2 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.

6. Network Security

Please read the Cynap Network Integration Guide to learn more about secure network integration and required open ports for all Cynap 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 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 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 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 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 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 systems. Use the vSolution Link Pro remote management software to assist with organising centralised management.
- Update Cynap 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 help, available on every Cynap and on the WolfVision website.