XMS Security Whitepaper

DATE 22/05/2019
AUTHORS David Martens | Willem Van Iseghem

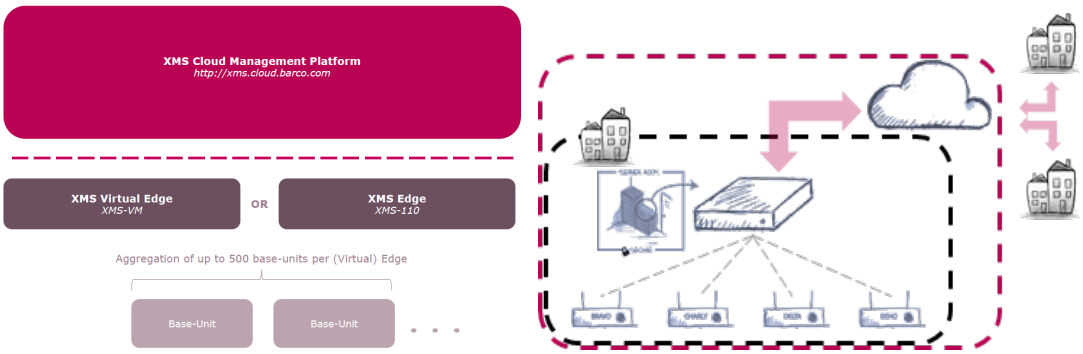
Table of content

Introduction

XMS Cloud Management Platform allows remote access and control from any location of your Barco managed ClickShare and wePresent devices, with the highest security possible. The Platform will provide a live cloud dashboard with status information and allow monitoring of all your connected devices, next to offering you additional features like maintenance, configuration and issue solving. System administrators, integrators and managed service providers (or anyone who was granted access) can enjoy unlimited flexibility and improved service capabilities.

As with the managed Barco solutions, security and privacy are key elements in the design and architectural decisions of the XMS Cloud Management Platform. Careful consideration and decisions have resulted in a secure, but still easy-to-use management system.

This technical whitepaper will go in depth on the possible threats for different components and features, and the measures that have been taken to mitigate these. The whitepaper applies to both on premise instances (XMS Edge) and the XMS Cloud Management Platform.



Following the privacy by design principle, the amount of personal data collected by XMS is kept to a bare minimum, and is not transferred outside the XMS solution.

Modelling the XMS threats

Since the launch of the ClickShare product line, many questions have been raised by customers about security, user scenarios, integration methods, etc. These questions have been taken into account when an extensive threat modelling exercise was held for the development of the XMS components. Threat modelling is one of the most powerful security engineering activities because it focuses on actual threats rather than just actual vulnerabilities. A threat is an external event that can damage or compromise an asset or objective, whereas a vulnerability is a weakness in a system that makes an exploit possible. Threats are of a long-term duration and can change over time, while vulnerabilities cease to exist once they are solved. Threat modelling facilitates a risk-based product development approach by uncovering external risks and encouraging the use of secure design and development practices. As such threat modelling does not only focus on software, but also hardware and third-party providers. This extensive exercise covers as such all the necessary topics to create a secure product in every aspect.

What does the system look like?

XMS consists out of an optional cloud component (XMS Cloud) and an on premise component (XMS Edge). ClickShare and wePresent devices can communicate via the XMS Edge instance which is an on premise gateway, which will be the unique link towards the XMS Cloud instances within the corporate network of the customer. If the customer does not want to have any outbound communication towards XMS Cloud, the local management interface of XMS Edge can be used for managing the ClickShare and wePresent install base. The choice between both deployment scenarios depends on the cloud adoption maturity of the customer. Barco cannot guarantee that the features offered by XMS Cloud will be on par with single deployment of XMS Edge. Depending on the architecture of the company network, multiple XMS Edges can be deployed when the install base is stretched across multiple geographically different physical sites with a limitation of 500 managed units per XMS Edge. The XMS Edge can be deployed in two different ways, either virtual or via a hardware appliance.

The table below lists the possible usage scenarios and which components are present in said scenario.

	Local deployment	Cloud deployment
Device(s) to manage	x	x
(Virtual) XMS Edge	x	x
XMS Cloud	N/A	x

Who is using and who is managing the system?

Both administrators and resellers will be able to manage the installed ClickShare and wePresent devices via XMS. Administrators can define different roles with specific access rights, e.g. local administrators per geographical site, to tailor management of the devices according to the company structure.

XMS Cloud provides the following features:

- Configuration management
- Software update management
- Analytics and diagnostics

These will enable administrators to manage the full install base from one single digital place, it will help to discover usage patterns of the deployed services and increase the ROI.

XMS Edge

What data needs to be protected?

All data transferred between devices to be managed and the management systems (e.g. XMS Cloud, XMS Edge) needs to be protected. Data on the management systems also needs to be protected against unauthorized access.

Which physical system interfaces and services can be detected?

This section will only focus on the physical XMS Edge. For the managed devices, please refer to the product information available on the Barco website.

	XMS Edge
	

Externally accessible	• Ethernet
	  • Web UI
	  • Communication with XMS Cloud
	  • Communication with managed device
	• USB
	• External serial port
	• Display

Internally accessible	• USB • SATA/M.2 • PCI-e

Where is the XMS Edge physically located?

The XMS Edge is primarily located in a data centre that is managed by the IT administration of a company. This usually implies that physical access to the device is restricted, nonetheless the physical interfaces described in the section above need to be protected in an appropriate way.

XMS Cloud

What data needs to be protected?

All data transferred between devices to be managed and the management layer (e.g. XMS Cloud, XMS Edge) needs to be protected. Data on the management layer also needs to be protected against unauthorized access.

Where is the XMS Cloud physically located?

The XMS Cloud services are running on machines which are physically located in Europe.

Technical implementation

Layered approach

The cornerstone principle of information security is the CIA triad: Confidentiality, Integrity and Availability. All parts of a product or system must honour this concept throughout the system's life cycle to guarantee a secure environment.

A network connected system consists of a set of different layers: physical, network, host and the application layer. Mapping these layers onto the CIA triad shows what kinds of security measures are required for the system to be deemed secure. This layered approach with multiple safeguards in place ensures that a system can remain uncompromised if one safeguard should fail. The safeguards must correspond to the threats identified during the threat modelling exercise.

XMS Edge

In this section the different layers for the XMS (Virtual) Edge will be discussed one by one. Note that not all layers apply to the XMS Virtual Edge.

Physical layer

The XMS Edge is based on a regular PC motherboard, and as such it contains various interfaces that are also present on a regular PC. These interfaces are not used but could be abused by actors with malicious intents.

Therefore it is highly recommended to:

- Install the XMS Edge in a secure, restricted access area
- Disable boot from USB
- Protect the BIOS with a password

Please refer to the User Manual of the XMS Edge for steps on how to perform these hardening actions.

Access to the Ethernet interface of the XMS Edge allows to connect to the network stack and its services, requiring additional controls at the application layer. They are discussed in the next section.

OS layer

The XMS (Virtual) Edge runs microservices in containers that are launched by a minimal Linux OS. Updates to the system are provided as a signed and encrypted package.

Signing and encryption provide integrity and confidentiality of the software running on the XMS Edge. To ensure the confidentiality of the data, the hard disk of the XMS Edge is encrypted using a device unique encryption key. These two measures guarantee that the firmware has not been tampered with and originates from Barco.

All containers that run vital services are being monitored and restarted when a crash or hang of that service is detected.

The Linux OS of the XMS Edge contains multiple open-source software packages. The list of these packages is available in the End User License Agreement. Barco closely monitors for new vulnerabilities detected in the used open-source packages. If a vulnerability is detected or reported, it will be analysed and depending on the criticality and impact, planned in for a future release.

Application layer

The Web UI of the XMS Edge offers the possibility to manage the system in a secure way. It is only served over HTTPS to assure an authenticated and encrypted connection with the device. TLS cipher-suites and version are configured to resist the latest known attacks. Access to the administrative section is protected by password credentials. These credentials are hashed using a secure, modern algorithm that can resist to brute-forcing and rainbow table attacks. The administrative sessions are bound to a cookie that stays valid until logout or expiration. Furthermore all inputs are sanitized and/or validated to prevent injection vulnerabilities.

By default the XMS Edge will use a self-signed certificate for setting up the TLS connection. If desired it is possible to replace this with a self-chosen certificate and private key.

XMS Cloud

The traditional approaches to security in an enterprise environment have always been based on control of devices, infrastructure or information, and of processes inside the enterprise firewalled perimeter. In a borderless enterprise environment, information resides in the Cloud and is accessed from many devices outside the perimeter of the traditional enterprise.

XMS Cloud is a portal which allows administrators to manage and configure their ClickShare and wePresent install base. Optionally the portal will present usage statistics and diagnostics which will give insights on how the install base is used in the company and where it could be improved

or extended.

Network layer

The XMS Cloud Platform is partly hosted on Amazon Web Services and partly on Microsoft Azure.

The link between the XMS Edge and the XMS Cloud is based on Azure IoT Hub technology to securely connect, monitor and manage the ClickShare and wePresent install base.

Application layer

Access to the XMS frontend application happens over a secure HTTPS connection. All HTTPS traffic is load balanced to distribute traffic to several application servers and to improve performance, scalability and reliability of the application.

The complete application is behind authenticated access via myBarco ADFS. All ClickShare information which is presented in the frontend application is gathered via the Azure IoT Hub technology. The IoT Hub device identity permissions and access control features are used to finetune authentication and authorisation of data submitted to the Cloud by the managed ClickShare and wePresent devices.

Interoperability with first generation ClickShare products?

The first generation ClickShare products (CSM, CSC) are also fully supported in XMS Cloud via the XMS Edge.

WePresent devices will only upload data and statistics to the XMS Cloud via the XMS Edge, configuration (write access) of wePresent devices from XMS Cloud is not available for the moment.

Privacy by design

The amount of personal data which is collected is limited to the absolute minimum. At registration time only name, email address and company name will have to be provided. The system administrator can add users to the XMS Cloud Management Platform via specifying their email address.

The data of the managed devices (ClickShare and wePresent) which is uploaded to XMS Cloud does not contain any personal data.

Closing

The XMS Cloud Management Platform and XMS Edge were designed with security in mind during all stages of the Software Development Lifecycle. Barco also guarantees that no backdoors or hidden transfers have been implemented into the XMS solution.

If any questions might have been left unanswered, please let us know via clickshare@barco.com.

In case you discover a security vulnerability in XMS (Virtual) Edge or XMS Cloud Platform, please reach out to Barco via a responsible disclosure procedure complying with the following guidelines: https://www.barco.com/responsible-disclosure.