VSaaS by Bosch

en Service description

Table of contents

1 Main functions

Video-Surveillance-as-a-Service (VSaaS) by Bosch is a portfolio of functions that builds upon the main components Remote Portal and Cloud VMS. Bosch delivers Cloud VMS – a comprehensive remote video management and monitoring platform - as Software-as-a-Service (SaaS) to security operators of corporate control rooms, security staff in general, security operations centers or monitoring centers. Bosch delivers Remote Portal – a portal for management of devices and licenses to technical teams, installers, and integrators.
Both components and/or their VSaaS-related functions are summarized as "VSaaS by Bosch".
Cloud VMS hereby provides the core processes required for video monitoring, in particular commissioning and controlling video cameras, transmitting images and video clips, and recording and further processing of video alarms. A web interface provides the functions for commissioning, managing, and monitoring cameras at different end customer sites, and enables security or business-related functions. Smartphone users can use a portfolio of apps to access live video, local recordings and data or receive notifications on their devices.
These functions and processes support remote video surveillance for multi-site customers for Bosch and 3rd party cameras without requiring expensive on-site hardware or maintenance. Building on video analytics on the edge and in the cloud, the overall solution provides everything needed to react, investigate, and intervene quickly and effectively to security scenarios.
For a description of functions summarized in this portfolio, refer to the following datasheets or application notes:

- Main applications:
  - Datasheet Cloud VMS
  - Datasheet Remote Portal
  - Application note Alarm Verification
- Client applications:
  - Datasheet Project Assistant (MFT-PA)
  - Datasheet Configuration Manager (MFT-CM)
  - Datasheet Video Security Client (MFT-VSC)

Notice!
You can find the datasheets and application notes in the respective product catalog for your region or country.

2 System requirements

Software requirements

The Operator and Configuration interface of Cloud VMS and the Remote Portal web interface can be used with modern web browsers that support HTML5. For the best experience, Bosch recommends the use of Google Chrome.

In special use-cases of Cloud VMS it might be required to use the latest version of Internet Explorer with active VideoSDK from Bosch.

The mobile apps Site Monitor and Video Security require iOS for iPhone/iPad of version 11 or later, for Android OS version 8.0 or later. Refer to the respective app store for the latest compatibility information.

To receive push notifications in the Site Monitor app, specific settings may be required on the mobile device to allow these notifications. The mobile device needs to be registered with the push notification service in Cloud VMS.

The native application Video Security Client for Windows requires Windows 10 OS (64-bit).

Device requirements

To use Cloud VMS, any Bosch IP camera with firmware version 6.40 and later must be connected to Remote Portal first.

It is required that the camera is either equipped with a local SD card or a managed recording target (iSCSI NAS, Video Recording Manager, DIVAR IP).

3rd party cameras are currently connected directly to Cloud VMS first. A list of compatible cameras is publicly available and continuously updated. For more information, refer to the document *Cloud VMS Compatibility list*.

On Remote Portal, individual functional components of Cloud VMS can then be activated per camera. Additional hardware such as a cloud gateway is not required to connect a camera to Remote Portal.

The required bandwidth on site depends on the camera type, camera settings, stream settings, alarm scenarios and site structure (for example number of cameras on site). Bosch recommends a minimum of 512 kbit/s per Bosch IP camera. This bandwidth requirement can vary and the user should verify that the available bandwidth fulfills the requirement of the application. Bosch provides several tools for the calculation of the required bandwidth but takes no responsibility for actual bandwidth availability and proper configuration.

3 Web applications

The provided web applications consist of Cloud VMS and Remote Portal. The Cloud VMS web application provides functions to achieve the following:

AI Alarm Verification

Camera-generated events are sent to a centralized cloud service for post-processing using deep neural networks. Only events verified by this service are then shown to the operator. For more information, refer to the document *Application note Alarm Verification*.

Video Verification

Video verification of intrusion events, for example from Bosch B-Series and G-Series panels with live and recorded video from associated camera.

24/7 Live Intervention

Camera-generated events (detected motion, IVA, virtual and digital inputs and outputs) are preprocessed by the cloud application according to set filtering rules and optionally forwarded to remote monitoring centers/control monitoring stations for certified verification and intervention. Will store a 10-second alarm clip for quick investigation, review and export.

Virtual Guard Tour

Prompts the operator to perform visual checks of selected cameras at scheduled intervals.

Virtual Assistant

Remotely prompts the operator for assistance by means of push-button or other devices connected to a camera.

Live View

Select from your list of sites any location and cameras from the map for permanent video live monitoring as either low-bandwidth or high-priority streaming with full control (PTZ, Audio, Intercom, etc.). Activate a secondary or multiple views for video display and trigger Intervention actions (open doors, switch light, e-mail notification of site owners etc.). Access cloud recordings if activated and select using an adaptable timeline with option to export. The operator can manually adjust for streaming technology, image quality or frame rate. Integrated 3rd party systems may offer this site access under a static reusable URL.

Smart Notification/Alarm Notification

Configuration of a Push Notification Service in combination with the Bosch Site Monitor app notifying customers or security guards about relevant events from their sites. These events could be the same events received by the central station but could also be events where no professional intervention is required but the user wants to be informed about, for example warehouse access during business hours. The user can access the related event clips. This function is also available as a stand-alone function when the license Alarm Notification is activated on Remote Portal.

Cloud Storage

On top of alarm handling, Cloud VMS offers cloud storage functionality for continuous or event-based recording of Bosch cameras and 3rd party cameras. Cloud storage is offered in different packages of retention and quality settings. Cloud storage is also available as a stand-alone functionality and needs to be ordered and activated separately from other functions.

Alarm Transmission

Forwards alarms to 3rd party alarm automation platforms. For a list of compatible platforms, refer to the Cloud VMS datasheet.

The web application of Cloud VMS is divided in three distinct interfaces: Configuration Interface, Event Monitor Interface and Diagnosis Module.

Remote Portal is distinct from Cloud VMS and provided as a web application under the URL https://remote.boschsecurity.com where it provides the following general functions:

Device management with a dashboard view

Devices can be grouped in hierarchical order to match customer or installation location, limit access for a set of devices or aggregate status of multiple devices. Status aggregations provide a dashboard view of device health, connectivity, service status and firmware level. Devices can be updated individually or in batches by starting the automated update process after switching to the list view in the dashboard.

Service overview

Services can be activated either on the device or by visiting Remote Portal after the initial commissioning of the device to Remote Portal.

User Management

Remote Portal allows fine-grained control of access to devices and services. Through role management administrators, technicians and end users can be individually associated with systems, groups and services.

Service License Management

Some services require licenses for activation. Licenses are managed and activated in Remote Portal. VSaaS by Bosch services are activated here.

Camera Counter Reports

Camera Counter Reports retrieve and store the values of camera VCA counters at regular intervals. Remote Portal stores values for visualization or exports to CSV files for further processing. Access to a REST API providing these counters is available upon request. This function requires a separate license.

Further VSaaS specific functions

Specifically for VSaaS by Bosch and connected Bosch IP cameras, Remote Portal provides the following functions:

- Initial point of commissioning devices to the cloud.
- Initial one-click camera configuration using VSaaS parameters.
- Access to camera pages for ad-hoc configuration.
- Remote Connect: Enables plug-and-play connection to devices with other applications or mobile apps for remote commissioning and configuration (for example Project Assistant and Configuration Manager).
- Video View: Enables plug-and-play connection to devices with other applications or mobile apps for on-demand viewing (for example Video Security App).
- Remote Alert: Remote Portal monitors devices with Remote Connect services for connectivity or health status changes. Remote Alert sends notifications to selected users based on configurable triggers.
- Camera Viewer: Camera Viewers are a lightweight viewing tool that gives end-customers browser-based access to live images and video streams of cameras. Up to four cameras can be displayed with live streaming or JPEG polling in the browser.
- More information on the detailed functionality of the web application of Cloud VMS and Remote Portal are described in the individual datasheets.

4 Mobile/desktop applications

Next to the web applications, the user can benefit from video surveillance functions in VSaaS by Bosch by using the following native applications, which can be used as a mobile and as a desktop version:

Site Monitor App

The Site Monitor app focuses on site managers and security guards that are on-site and need to react to alarm events. The app comes as part of Cloud VMS and provides the following functions:

- Site list map view
- Thumbnail view of cameras per site
- Live video stream
- Selected device alarms received by push notification, directly connect to device
- Access to event clips through event list
- Remotely arm/disarm site
- Password-protected, SSL/TLS encrypted connection
- iOS and Android smart phone and tablet platforms supported

Video Security

The Video Security app and client focuses on on-demand live streaming and access to the cameras for staff that is not on-site. The app provides:

- List of groups of cameras created in Remote Portal
- Live video stream
- Flexible cameo and grid view
- Access to the local recordings of the individual cameras
- Use of camera functions (PTZ, Relay, Audio)
- Interactive timeline for local recordings
- Base forensic search
- Export of video clips
- iOS, Android (for Video Security app) and Windows compatible (for Video Security Client)

5 Documentation

The user documentation and datasheets for all individual components contained in the VSaaS by Bosch portfolio can be found and accessed here:

Technical trainings:	https://academy.boschsecurity.com/
How-to's/Configuration notes:	https://community.boschsecurity.com/
Datasheets/Application notes:	https://www.boschsecurity.com/xc/en/product-catalog/
Camera compatibility sheet:	https://www.boschsecurity.com/xc/en/product-catalog/

6 Open Source Software components

The Open Source Software components included in the components can be found here:

- Remote Portal: https://remote.boschsecurity.com/open_source/open_source_licenses.txt
- Cloud VMS: https://<cloud application URL>/static/open_source_licenses.txt

Example: https://demo.cbs.boschsecurity.com/static/open_source_licenses.txt

Each client application provides the Open Source Software component information within the application.

7 Service hosting

The services listed here are hosted on AWS infrastructure-as-a-service.

The application Remote Portal is a global multi-tenant platform. This platform, its database, backend and frontend is hosted in the AWS region Frankfurt, Germany. Remote Portal provides three global endpoints for device connectivity and streaming of video data. These endpoints are called “Video Relay”. These video relays are hosted regionally in the AWS regions USA-EAST (USA), ASIA-PACIFIC (Singapore) and EUROPE (Germany). The user can select during the device commissioning process of a device to Remote Portal which of these video relays is to be used for device connectivity.

The application Cloud VMS is either hosted as a regional multi-tenant service or a dedicated single-tenant service. This depends on the required system set-up and order of the customer. For the dedicated single-tenant option, customers can choose the hosting location from the main AWS availability/infrastructure regions. The available regions are listed here: https://aws.amazon.com/de/about-aws/global-infrastructure/regions_az/

During the set-up of a dedicated instance of Cloud VMS the customer then needs to specify to which “video relay” this instance should connect (EUROPE, ASIA-PACIFIC, USA-EAST). The hosting specifications for a dedicated single-tenant instance are gathered in a structured onboarding process once legitimate business interest is established.

8 Maintenance and Service level

Bosch offers a dedicated Service Level Agreement (SLA) for signed resellers of VSaaS by Bosch. This SLA outlines the guaranteed availability, maintenance and support process in detail for VSaaS by Bosch and contains contact details for emergency hotlines, penalty clauses etc.

Contact your local sales representative for more information.

9 Customer and user obligations

For direct customers of Bosch acceptance of the Terms and Conditions for Software as a Service Resellers as well as of the respective Service Level Agreement (SLA) is required to be able to obtain VSaaS licenses or subscriptions. For the activation of service licenses or subscriptions users need to agree to the terms and conditions of Remote Portal. Users of the VSaaS by Bosch applications and clients need to agree to the respective Service Terms of Use. Further obligations include:

9.1. The Internet connection between customers, their monitoring center/control room, and the installation site of compatible devices (including video cameras, hereinafter referred to as "Devices") up to the data center's Internet interface used by Bosch, as well as the end customer relationship between customer and its contractual partners are the sole responsibility of customers.

9.2. Installing, operating, maintaining, and – where necessary – repairing devices are the sole responsibility of customers.

9.3. The application is not designed or warranted for use in high-risk applications requiring special fail-safe performance, such as in the operation of nuclear facilities, air traffic control, life support, or other applications, devices or systems in which the failure of a device or application could lead directly to death, personal injury, or severe physical or environmental damage (“high risk activities”). Notwithstanding any other provision customers shall not use or permit any third party to use the Application with any high-risk activity.

9.4. To obtain the necessary consent of the persons affected in accordance with data security and data protection regulations as personal data is collected, processed, or used in the course of said persons’ use of the application and no legislation permitting such collection, processing, or use without the need to obtain consent applies to the case in question.

9.5. Check data and information for viruses or other malware before sending the data and information to Bosch, and to ensure that antivirus programs meet the latest requirements.

9.6. Report defects in the contractual services to Bosch immediately after being made aware of the defect. If there is a delay in sending the notification or if notification is not provided despite customer being aware of the defect, a unilateral reduction in the fee or suspension by customer, as well as extraordinary termination, is excluded.

9.7. The following roles and tasks are the sole responsibility of customer:

9.7.1. Assigning roles and authorizations to the corresponding persons or units for the user roles available in the Application, and managing these roles and authorizations.

9.7.2. Allocating devices to contractual partners of customer and to the contractual partners' sites.

9.7.3. Activating contractual partners to use the Site Monitor App or Event Monitor.

9.7.4. Procuring, installing, and connecting suitable devices for operation in accordance with the system requirements. The Application supports the operation of devices by customer by means of the functions outlined.

10 GDPR-related information

Purpose of the data processing

Bosch processes personal data only to the extent, and in such a manner, as is necessary:

1. in order to meet Bosch's obligations under the agreement/terms of use and applications of VSaaS functions; and

2. to comply with customers instructions from time to time (which may be specific instructions or instructions of a general nature as set out in this agreement or as otherwise notified by customer to Bosch),

and shall not process the personal data for any other purpose.

Data categories

- User configuration data: data entered by Data Controller while using the solution such as user access information including first name, last name and e-mail address necessary to provide user application access.
- User action logs: documentation of users' system use including performed actions and associated timestamps. Used to help resolve maintenance cases and to improve user experience. In action logs, user names are encoded with a key and cannot directly be read from action logs.
- Non personal data such as site, customer account and service configuration data incl. types and flows.
- In case of complying to customers' instructions to Bosch as laid out in 10.1: video data such as livestream and recordings: used for remote setup, configuration, optimization specifically for camera intelligent video analytics.

Data subjects

- Employees of customer
- End-users or contractual partners of customer ("customer-of-customer")

Subcontractors

All subcontractors are listed in Table 1.

	Name and address of subcontractor and name of data privacy officer / contact person for privacy related questions	Scope of service (scope of the order placed by the contractor)	Place of data processing	Transfer/access to personal data of the client (type of data and group of data subjects)
1	Amazon Web Services (AWS)	Infrastructure/Hosting Provider (as outlined in security concept)	AWS Infrastructure Regions (see section 7)	
2	Robert Bosch India Data Protection Officer Bosch India (RBEI/DSO) DPO.India@in.bosch.com	Restricted group of Technical Operations Support	No.123, Industrial Layout, Hosur Road, Koramangala Bengaluru-560095 Karnataka, India	All categories and data subjects listed in data 10.2 OPs-team has only OS level access to application and storage, not account or site-level

Table 1

Technical and organizational measures

The following TOMS are agreed between the Data Controller and the Data Processor and specified in the present individual case, see specimen list.

I. Measures to ensure confidentiality (Art. 32 para. 1 lit. b of the GDPR)

I. Physical access control: No unauthorized access to data processing systems, e.g.: magnetic or smart cards, keys, electric door openers, plant protection or security guard, alarm systems, video systems.

II. Logical access control: No unauthorized system use, e.g.: (secure) passwords, automatic locking mechanisms, two-factor authentication, data encryption.

III. Data access control: No unauthorized reading, copying, changing or removing within the system, e.g.: authorization concepts and user-specific access rights, logging of access.

IV. Separation control: Separate processing of data collected for various purposes, e.g. multi-client capability, sandboxing.

II. Measures to ensure integrity (Art. 32 para. 1 lit. b of the GDPR)

I. Transfer control: No unauthorized reading, copying, changing or removing during electronic transmission or transport, e.g.: encryption, Virtual Private Networks (VPN), electronic signature.

II. Input control: Determination of whether and by whom personal data was entered, changed or removed in data processing systems, e.g.: logging, document management.

III. Measures to ensure availability and resilience (Art. 32 para. 1 lit. b of the GDPR), e.g.

I. Availability control: Protection against accidental damage or destruction or loss, e.g.: backup strategy (online/offline; on-site/off-site), uninterrupted power supply (UPS), virus protection, firewall, escalation ways and emergency plans.

II. Order control: No data processing under commission according to Art. 28 of the GDPR without corresponding instructions from the Data controller, e.g.: explicit contract design, formalized or-der management, stringent selection of the service provider, obligation to convince in advance, follow-up inspections.

III. Resilience: Systems and services (e.g. storage, access, line capacities, etc.) are designed in a way that even intermittent high stresses or high constant loads of processings can be ensured.

IV. Measures for the pseudonymisation of personal data, e.g.

I. Separation of customer data controller master data and customer data

II. Use of personnel, customer, and supplier ID instead of names

V. Measures for the encryption of personal data, e.g.

I. Symmetrical encryption

II. Asymmetrical encryption

III. Hashing

VI. Measures to quickly restore the availability of personal data to them after a physical or technical incident, e.g.

I. Back-up concept

II. Redundant data storage

III. Double IT infrastructure

IV. Backup datacentre

VII. Procedures for periodical review, assessment and evaluation (Art. 32 para. 1 lit. d of the GDPR; Art. 25 para. 1 of the GDPR), e.g.

I. Privacy management

II. Incident response management

III. Data protection by default (Art. 25 para. 2 of the GDPR)

IV. Assessment by DSO, IT audits

V. External assessment, audits, certifications

Bosch Security Systems B.V.
Torenallee 49
5617 BA Eindhoven
Netherlands
www.boschsecurity.com

Building solutions for a better life.

202211241953