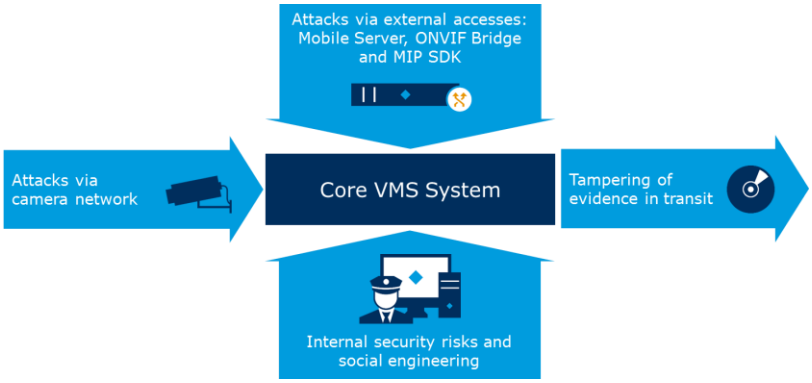
Milestone XProtect VMS - secure by design

- providing high protection resilience against cyber attacks

Milestone XProtect VMS products are designed to provide the highest security protection against external and internal security threats. Tiered administrator and user rights, enforced on the server side, combined with the use of standard IT security procedures, make XProtect VMS the perfect choice for organizations with focus on cybersecurity.

Video surveillance systems are one of several ways organizations safeguard assets and people. As with other protection systems, video surveillance systems can be exposed to attacks in conjunction with criminal activities. However, unlike the physical protection systems, the attacks on IT and video surveillance systems are more refined and subtler, and often difficult to detect as there often are no visible traces.

Video surveillance systems are, like any other IT infrastructure, exposed to both internal and external security threats. Potential threats include: distributed denial-of-service (DDoS) attacks, hacking, social engineering, port scanning and general software vulnerabilities, among others.



Principal risk exposures in a VMS system

The exposure to cyberattack depends on three primary parameters: the overall risk profile of the company or organization in question, the cybersecurity maturity level of the organization and the degree of attention on cybersecurity when designing and installing the system.

Key benefits

- Protects the system integrity from cybersecurity attacks
- Secure end-to-end handling of exported forensic material
- Secure access for web and mobile users
- Secure integration of third-party applications and systems

Key features

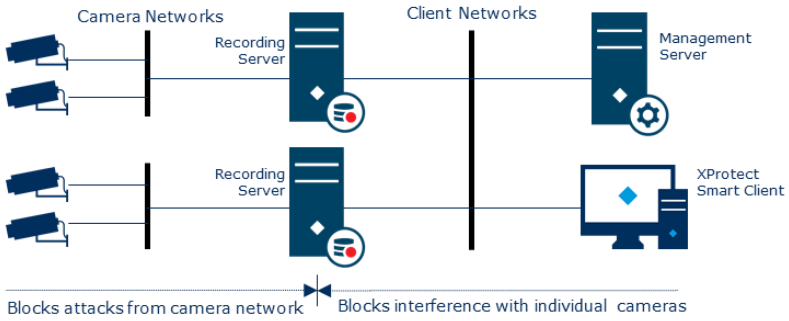
- Possibility for physical separation of camera networks and client network
- HTTPS – secure camera connectivity
- Encryption and password protection of video databases and exports
- Digital signing of video databases and exports
- Option for Windows AD user authentication via Microsoft NTLM or Kerberos authentication
- Strict and time-controlled user rights management, enforced server side
- Secure and encrypted (HTTPS) access for web and mobile client users
- Audit log provides full tractability of user actions
- Full authentication and authorization of third-party applications integrated via Milestone Integration Platform SDK (MIP SDK)

The solution dilemma

Designing a modern IP video surveillance solution is often a compromise between security on one hand, and flexibility and user friendliness, on the other. Milestone XProtect VMS software offers an array of security mechanisms described in this feature brief. Using these capabilities, it is possible to protect the system from both internal and external security threats, without compromising the system's flexibility or usability.

Security through network separation

Milestone's VMS architecture builds on a tiered system architecture, which makes it possible to separate the camera network and the core server/client network. With the recording server as a gateway between the camera and the system networks, there is no direct routing between the two network segments.



Network separation protects the system integrity

This means that a cyberattack potentially may reach the recording server on a particular network segment but will have difficulties penetrating beyond this point. Likewise, the recording server will prevent internal hacker attempts on the camera network.

HTTPS – secure camera connection

Milestone XProtect VMS products support HTTPS communication between the recording servers and the connected cameras and other security devices. HTTPS provides bidirectional encryption of communication and prevents eavesdropping and tampering with the contents of the communication.

Secure video storage

To protect recorded video, audio and metadata while stored in the recording servers and the associated storage, XProtect Corporate offers the ability to encrypt and password-protect the media data. This means that the recorded data is protected even if someone gains access to the database files

Cameras with support for HTTPS

Visit the Milestone website for information about which cameras support HTTPS:

Video encryption

The video database encryption is made in real-time as data is stored in the databases. The encryption is available in two levels:

- Light encryption
  Encrypts the data header information which prevents the media data from being decoded. The light encryption is recommended for minimizing the impact on CPU load

- Full encryption
  Encrypts all data and is stronger but slightly more CPU intensive

System hardening

Read more about how to protect surveillance installations based on Milestone XProtect VMS software against cybersecurity threats.

The guide outlines best practices for system design, operating system configuration, servers, workstations and the Milestone XProtect VMS software. It also contains input on cybersecurity policies, risk evaluation and mitigation.

on the storage system, a network share or in conjunction with an actual system hacker attack.

In addition to media data encryption, XProtect Corporate supports a digital signature on the recorded media data in the system. The signature can be used to prove that the video has not been altered or manipulated while stored in the system.

Strict server-side authentication and authorization

Milestone XProtect VMS products use consistent user authentication and authorization across all clients and integration interfaces that are enforced on the server side. This authentication and authorization process applies to both human users, and system services accessing the VMS system via the Milestone Integration Platform (MIP) SDK or Milestone Open Network Bridge.

Building on user role definitions, it is possible to apply strict and granular user rights to specific roles (individual or groups of users) in terms of:

- Client interfaces the user may use
- Cameras and other security devices and device functions the user can access
- System functions the user has the right to use
- System configuration data the user can see/edit

The user rights can be defined to be both static and time conditioned. This, for example, makes it possible to block a user from accessing the system outside normal working hours, or limiting access rights to cameras and functions during certain time periods. The time-conditioned user rights also make it possible to block access to recordings older than a given time.

Certificate-based encryption

To secure the communication of data (video, audio, metadata) originated in the Recording Server and retrieved by connected components such as the Management, Mobile and Event servers as well as the Management, Mobile and Smart clients, XProtect uses SSL/TLS certificate-based encryption forced on both ends.

Builds on Windows security infrastructure

Milestone XProtect VMS products support Windows Active Directory (AD) based authentication, where both native Microsoft NTLM and Kerberos authentication may be used.

Audit logging

Milestone XProtect VMS products maintain an audit log, which makes it possible to perform detailed user activity monitoring. The audit log tracks all user accesses and activities, including changes to the system configuration. This enables system administrators to detect and investigate potential attempts to intercept the system.

Kerberos

Kerberos (RFC 3244) is a security authentication protocol that offers a more secure way to authenticate users than NTLM. Kerberos builds on symmetric key cryptography and requires a trusted third party. Milestone supports Kerberos authentication as a complement to Microsoft NTLM authentication.

Dual authentication

Dual authentication offers an additional level of system security for customers operating high-security installations. The dual authentication only grants a user access to the system when a second user (for example a supervisor) has confirmed the login with a successful authorization by the second user.

The dual authentication may optionally be applied to users accessing the VMS system via the XProtect Smart Client or the Management Client.

Secure remote user access

To facilitate remote system access via the XProtect Web Client and the Milestone Mobile application, the XProtect VMS products use a dedicated mobile server as a gateway to the system. Apart from being responsible for the connection management for web and mobile users, the mobile server plays an important role in protecting the integrity when used by remote users.
The communication between the mobile server and the two clients support HTTPS, which provides secure authentication and bidirectional encryption of all information exchanged, including user credentials, configuration and media data. This prevents eavesdropping and tampering of the communication. To protect the VMS system from attacks via the Internet, Milestone recommends placing the mobile server in a demilitarized zone with two separate network connections.

Secure systems integration via MIP SDK

To address potential security threats imposed by third-party applications integrated via the MIP SDK, the XProtect VMS applies the same strict authentication, authorization and certification policies on integrated applications as on the client interfaces.

External video access using Milestone Open Network Bridge

External systems and applications can access live and recorded video in Milestone XProtect VMS systems via an ONVIF-based RTSP interface using the Milestone Open Network Bridge. As with internal VMS users, external systems using the Milestone Open Network Bridge must run under a registered account. This makes it possible to apply the same strict authentication and authorization policies on integrated applications and users. Similar to the mobile server (see above), Milestone recommends placing the Milestone Open Network Bridge in a DMZ with two separate network connections.

Protection of evidence material

The ultimate output of any video surveillance installation is the evidence material it can provide. When exporting forensic material using the XProtect Smart Client, the video material can be password protected, encrypted and digitally signed. These security measures can be applied in addition to signing recorded data in the recording server.

Encryption and password protection ensure that the forensic material can be viewed by the authorized receiver only, while

Two-step verification

To protect the VMS system from attacks via the remote web and mobile interfaces, it is possible to apply a two-step verification process for users accessing the VMS system via the XProtect Web Client or the Milestone Mobile application. In addition to the normal username and password-based verification, with two-step verification the VMS system sends a random one-time code to the user via email or SMS. The user is only permitted access to the system if the correct one-time access code is provided.

Want to know more

Read more about the benefits of advanced management rights and the use of inherited device permissions in the Advanced Security Management white paper:

Feature availability

The security capabilities described in this brief are fully available in XProtect Corporate, and partially available in rest of the VMS products. For details please refer to the specification sheets of the individual products.

the digital signature proves that the video has not been altered or manipulated while in transit.