MAKE THE
WORLD SEE

Version 1.0: June 2020
Version 2.0: July 2023

White Paper (Version 2.0, July 2023)

XProtect® on AWS

Originally Written by:
Jan Lindeberg, Senior Product Manager, Milestone Systems
Revised and Updated by:
Bahman Kahinpour, Product Owner, Milestone Systems

milestone

Table of Content

Executive summary

Businesses worldwide put their efforts in building organizational readiness that will enable them to grow when conditions are right. When it comes to Video Management Software (VMS), deploying a large on-premise system usually calls for a lengthy procurement process, costly hardware, and recurring maintenance. XProtect on AWS removes this friction, enabling system integrators and end customers to deploy XProtect in minutes, scale fast with no hardware or location dependencies, and cut down on hardware and maintenance.

XProtect on AWS is a cloud deployment alternative to on-premises video surveillance systems. It utilizes resources and services in the AWS cloud such as compute, storage, and networking, to deliver an elastic solution that can be scaled on demand to fit the business need. Milestone Systems now offers XProtect Bring Your Own License (BYOL) CloudFormation product deployable directly from AWS Marketplace. It can be activated to run any XProtect product, and requires a paid license sold through Milestone's existing distribution channels.

Single- and multi-site organizations across all AWS regions deploying XProtect on AWS can enjoy a reliable solution with a user-experience identical to XProtect on-premise and full feature-compatibility. Such organizations can now scale easily to meet business demand and reduce risk of service disruptions to enjoy a continuous operation. Reduced initial investment in hardware and AWS predictable cost model further support businesses in optimizing costs and delivering better results.

This paper discusses how XProtect can be deployed on AWS, leveraging AWS global infrastructure and platform services, and the advantages of such a deployment. With the outset in the Virtual Private Cloud (VPC) design orchestrated by the XProtect (BYOL) CloudFormation template, the paper further elaborates on suitable architectures for specific customer deployments. As a part of this, the paper discusses possible designs and considerations for the deployment. With the understanding of the architecture and which AWS services that are applied, the paper is concluded with a discussion around performance and operational topics: This includes AWS service costs and opportunities for post deployment optimization.

Introduction

Purpose and target audience

The purpose of this white paper is to provide insight to the benefits of deploying Milestone XProtect video management software (VMS) on Amazon Web Service (AWS) cloud infrastructure, and discuss the over-all concepts applied in an AWS deployment of XProtect. The paper provides an overview of different deployment architectures and introduces relevant AWS services that are either a part of the Milestone XProtect VMS product on AWS Marketplace or can be applied to extend and customize the standard offering.

Furthermore, this white paper will give recommendations for service and infrastructure designs and dimensioning and provide references to more information on specific topics. This white paper should enable the reader to understand the overall Milestone XProtect AWS Marketplace offering and how it can be deployed and adapted to meet specific customer needs.

The primary audience for this white paper is system integrators and IT administrators with limited experience of using Milestone XProtect VMS products who are in the process of selecting, deploying, administrating, maintaining or expanding a VMS system. The reader is assumed to have a general understanding of Milestone XProtect VMS, AWS cloud services and infrastructure concepts and traditional on-premises IT and network installations. Specific knowledge about streamed media is recommended but not required.

The paper only discusses the XProtect BYOL product. Although the XProtect Essential+ is deployed with the same Milestone XProtect VMS software, the CloudFormation templates are different, resulting in a different deployment in the end customer's AWS account.

About XProtect VMS

Milestone XProtect is a global market leading Video Management Software (VMS) that brings the puzzle pieces of a video surveillance installation together in a solution that keeps people, premises, and property safe today and tomorrow. Built on an open platform architecture, you can customize your surveillance system and integrate other business applications into it for increased usability and performance. With over 25 years in the market, XProtect has proven to be the right answer for more than 500,000 installations worldwide, from flower shops to universities, stadiums, and cities. With the market's broadest device support, XProtect VMS is compatible with extensive number of devices.

Readers who are not familiar with Milestone XProtect can get an introduction to Milestone XProtect video management software and its principal system architecture in Appendix A – Milestone XProtect VMS on page 46.

About AWS

In 2006, Amazon Web Services (AWS) began offering IT infrastructure services to businesses in the form of web services, now commonly known as cloud computing. One of the key benefits of cloud computing is the opportunity to replace up-front capital infrastructure expenses with low variable costs that scale with your business. Using cloud infrastructure, businesses no longer need to plan for and procure servers and other IT infrastructure weeks or months in advance. Instead, they can instantly spin up hundreds or thousands of servers in minutes and deliver results faster.

Today, Amazon Web Services provides a highly reliable, scalable, low-cost infrastructure platform in the cloud that powers hundreds of thousands of businesses in many countries around the world. With data center located all across the world, customers across all industries are taking advantage of the following benefits:

- Low Cost

  AWS offers low, pay-as-you-go pricing with no up-front expenses or long-term commitments. AWS can build and manage a global infrastructure at scale and pass the cost saving benefits onto you in the form of lower prices. Visit the AWS Cloud Economics Center to learn more.

- Agility and Instant Elasticity

  AWS provides a massive global cloud infrastructure that allows you to quickly innovate, experiment and iterate. Instead of waiting weeks or months for hardware, you can instantly deploy new applications, instantly scale up as your workload grows, and instantly scale down based on demand.

  Whether you need one virtual server or thousands, whether you need them for a few hours or 24/7, you still only pay for what you use. Visit the AWS Architecture Center to learn more.

- Open and Flexible

  AWS is an agnostic platform. You choose the development platform or programming model that makes the most sense for your business. You can choose which services you use, one or several, and choose how you use them. This flexibility allows you to focus on innovation, not infrastructure. Download the AWS Overview Whitepaper.

- Secure

  AWS is a secure, durable technology platform with industry-recognized certifications and audits: PCI

DSS Level 1, ISO 27001, FISMA Moderate, FedRAMP, HIPAA, and SOC 1 (formerly referred to as SAS 70 and/or SSAE 16) and SOC 2 audit reports. AWS services and data centers have multiple layers of operational and physical security to ensure the integrity and safety of your data. Visit the AWS Cloud Security to learn more.

Reasons for considering cloud deployment of XProtect

There are many reasons why enterprises and organizations should consider deploying XProtect on AWS cloud infrastructure. These can be grouped in two principal categories: general cloud deployment advantages and advantages specifically related to XProtect.

While the general advantages of AWS cloud deployment (see section: About AWS above) are assumed to be known and appreciated, this section covers some of the derived and specific advantages with deploying XProtect on an AWS infrastructure and service platform.

Speed of Deployment

Video surveillance systems are complex IT systems that are both compute and storage intensive. Commissioning such a system requires careful solution design, selection of server and storage hardware, all the logistics with ordering, shipment, unpacking and installation of the hardware.

With a cloud deployment of XProtect, many of these activities can be vastly simplified if not eliminated. Overall, it allows organizations to deploy XProtect VMS faster and cheaper. Without much of the friction known from on-premises deployments, XProtect on AWS, can far easier support organizations that operate with seasonal, or temporary deployments.

The actual deployment of the XProtect BYOL product from AWS Marketplace into a specific customer's AWS account is orchestrated by a CloudFormation template. The CloudFormation template deploys the Windows operating system and the XProtect BYOL included in the AMI on the Elastic Compute Cloud (EC2) instance selected for the deployment. This gives an instant and predicable deployment where the CloudFormation template also defines a new dedicated VPC with subnets, Security Groups and Elastic Block Store (EBS) for VMS configuration data and short-term storage of video data.

Elastic Scalability

Needs and operational circumstances change. AWS cloud infrastructure allows customers to seamlessly grow their XProtect deployment with their needs. An XProtect VMS deployment can seamlessly up to hundreds and thousands of cameras on a single EC2 instance. Leveraging the ability to shift EC2 compute platform makes the scaling instant while maintaining an attractive balance between performance and cost.

In surveillance installations with higher needs, the deployment can be scaled out on additional EC2 instances to support thousands of cameras and IoT devices.

Post deployment optimization

With the many assumptions that need to be taken into consideration as a part of the complex dimensioning of a video surveillance installation, there is an evident risk for errors in the system design. Such errors can result in system suboptimal system performance. To make an on-premises installation robust against these kinds of miscalculations or errors in the design assumptions, end-customers and system integrators prefer to factor some degree of system overprovisioning as a good system design principle.

This, however, often results in over dimensioned systems with expensive underused hardware aging without providing full return on its investment. In a cloud deployment, excess system capacity can be eliminated as a part of a post deployment cost optimization, which results in reduced AWS cost.

The elastic scalability discussed in the earlier section also works the other way around. If you have allocated a too powerful EC2 instance for your deployment, you can change it to a smaller more price effective instance type within minutes.

Unlimited Video Storage with Disaster Redundancy Option

In the same way as the compute capacity being scaled elastically, additional video storage can be added, when needed. Utilizing the multi-Availability Zone configuration, video data is replicated across muiltiple and separately operated data-centers providing disaster-proof storage of video data.

Various storage options are available on AWS. FSx storage is an option which can be used without any third-party plugins. Also, S3 storage is available and supported through a 3rd party Surveillance Bridge software. Creation of S3 storage and installation of Surveillance Bridge software is supported by XProtect BYOL CloudFormation template. It should be noted that usage of Surveillance Bridge software requires a purchase of the mentioned software through Tiger Surveillance company and mentioned software is supported by Tiger Surveillance company.

Ideal for geographically dispersed operations

Implementing geographically distributed video surveillance solutions often imply a mix of VPN networks and distributed hardware, that need to be kept operational and secure at all times. Cloud deployment is in these situations a perfect alternative where the different sites and premises are rolled into the customer's virtual cloud environment in which XProtect is staged.

Here tangible savings can be made both in the deployment phase, but even more so in the operations phase, where costly on-premises service and support visits can be reduced to a minimum.

Flexible User Access

Cloud deployment unlocks the full potential of the XProtect client suite, where remote users can access the video management system through secure connections using the XProtect Mobile application or the XProtect Web client.

As an alternative to on-premises deployment of the XProtect Smart Client, AWS offers the possibility to run client applications as hosted user sessions in the AWS cloud using the Amazon AppStream 2.0 service.

This makes it possible to use the Smart Client on virtually any device, including browsers, computers, and tablets. AppStream 2.0 is also a good and secure way of providing Smart Client access for remote users, and law enforcement bodies, without the need to install any XProtect software.

Target customers and deployment scenarios

The ability to run XProtect on AWS cloud infrastructure is an opportunity for a wide set of enterprises and organizations of any size and active in different vertical segments and industries and with different IT maturity levels. This includes private businesses and enterprises, educational institutions, as well as public and governmental bodies.

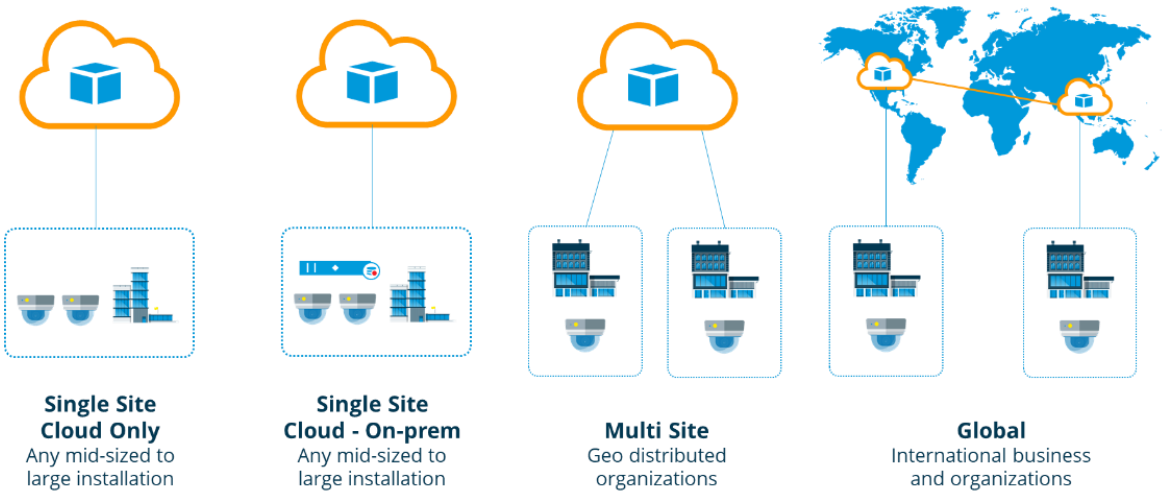


Figure 1. Typical deployment scenarios for XProtect VMS on AWS

Single site – cloud only deployment

The simplest deployment scenario is customers with only one location, where the XProtect video surveillance system is to cover cameras and other IoT devices commissioned in one specific location. In this scenario all XProtect VMS server functions are deployed on the end-customer's service infrastructure in AWS. Using the various XProtect clients, users can access the XProtect VMS application from both on-premises users and remote users using the web or mobile clients.

The cloud only deployment is the default deployment scenario when deploying XProtect from AWS Marketplace, and it is suitable in regions with reliable high-speed internet connectivity. A customer with single site deployment would normally deploy XProtect in the AWS Region with closest proximity to the customer's physical location. However, network connectivity and data privacy matters may influence the selection of deployment regions.

Single site – cloud and on-premises deployment

Like the previous scenario, this scenario covers one location only, but instead of deploying all XProtect server functions on AWS, this scenario will be a hybrid deployment. This means that some XProtect VMS

service functions are in the cloud and some physically in the customer's premises. In some deployments, it makes sense to outplace one or more XProtect recording servers on-premises. This would be the case when the size of the XProtect system measured in number of connected cameras and IoT deices is very large, or when it is difficult to obtain sufficient and reliable network connectivity to the AWS datacenter.

This deployment architecture is recommended in regions with lower penetration and availability of reliable high-speed internet connectivity. This architecture is also a natural steppingstone for migrating existing on-premises XProtect installations to AWS cloud infrastructure.

Multi-site deployment

Many companies and organizations operate across two or more geographically dispersed sites where the video surveillance system needs to seamlessly span across multiple sites. The advantages of cloud deployment video management solutions become evident for such types of customer deployments, as a cloud hosted VMS application not only provides a centrally managed video surveillance platform covering all sites uniformly, but the cloud architecture also allows the on-premises deployment to be simplified and lean. This not only optimizes the initial deployment time and cost, but it also significantly reduces the maintenance costs as less on-premises hardware immediately translates into less maintenance and less on-site visits.

Customers with multi-site deployment would normally deploy XProtect in an AWS Region located centrally to the customer's geographically dispersed sites. If some sites are larger than others, it can be an advantage to deploy XProtect in the AWS Region in the closest proximity to the largest site. However, network connectivity and data privacy matters may influence the selection of deployment region.

Additionally, multi-site deployments can be realized with hybrid deployment on one or more sites, where XProtect recording servers are outplaced on the individual locations to provide local compute and storage capabilities or to mitigate capacity and reliability issues in the internet connectivity. Hybrid deployments are also a natural step on a cloud migration path, where some sites can continue to use existing hardware in good condition, while other sites can be served by a cloud only.

Global deployment

Some enterprises and organizations have a need to coordinate and align video security operation on a global level, spanning sites in multiple countries and across different continents. In these cases, AWS is the ideal cloud provider with true global presence and their global network infrastructure, where every data center, availability zone (AZ), and AWS Region is interconnected via a purpose-built, highly available, and low-latency private global network infrastructure.

This means that customers can utilize AWS globally, fully redundant, parallel 100 GbE fiber network to interlink different sites of operation. For more information about AWS global network infrastructure, please refer to: https://aws.amazon.com/about-aws/global-infrastructure/global_network/.

When designing a truly global XProtect deployment, there are several relevant principal design options:

- Single XProtect VMS system with regionally deployed XProtect recording servers

  In this design, the main parts of the XProtect VMS system would be deployed in one primary AWS Region, while offices in remote countries and continents would be served by XProtect recording servers deployed in an AWS Region nearby the customer's remote location. The remote XProtect recording servers would then be connected to the XProtect VMS system in the primary AWS Region using AWS global network infrastructure.

- Federated XProtect VMS regional systems

  Individual complete XProtect VMS systems[1] deployed in different AWS Regions can be federated across AWS global backbone to form a centrally managed video surveillance system with virtually no limits to how many cameras and other IoT devices that are connected to it. A federated system hierarchy can naturally be hybrid, where on-premises deployed XProtect systems can be federated into a cloud base XProtect Corporate deployment. For further details about Milestone Federated Architecture, please refer to Milestone Federated Architecture White Paper.

- Interconnected XProtect VMS regional systems

  Milestone Interconnect™ is a unique concept that allows all of Milestone's video management software (VMS) products to be interconnected with a XProtect Corporate headend system. This allows for design of a large-scale and geographically dispersed video surveillance installations where each independent surveillance site can be designed with the required functionality and be deployed as traditional on-premises systems or cloud deployed, or any combination of the two, while still offering the benefits of a centralized surveillance installation.

  Milestone Interconnect is in some respects similar to Milestone Federated Architecture. There is however difference in the intra-system communication and how much video information that is exchanged between the systems. Milestone Interconnect also supports a wider selection of Milestone's VMS products versions that Milestone Federated Architecture. An elaborated description of these capabilities can be found in the Milestone Interconnect White Paper.

[1] Please note that it is only XProtect Corporate that can be the head end system in a federated hierarchy, while the federated (child) systems can be XProtect Corporate or XProtect Expert.

Cloud readiness

Milestone XProtect VMS is a compute and data intensive workload, which due to its real-time processing needs to be designed and deployed with professional considerations. Deployment of XProtect on an AWS is therefore particularly relevant for enterprises and organizations with a cloud first strategy, or a clear migration path to cloud. Organizations with high cloud readiness and established AWS IT competences are best destined to fully explore the synergies between Milestone's open and scalable VMS solution and the elastic scaling, reliable operation offered by AWS infrastructure and platform services.

XProtect on AWS

A cloud deployment of Milestone XProtect VMS on AWS takes full advantage of the XProtect software architecture, enabling a flexible and diverse usage of XProtect across various functions in the customer's organization. This allows enterprises and organizations with operations distributed across multiple sites to centralize and manage their video surveillance installation as one system.

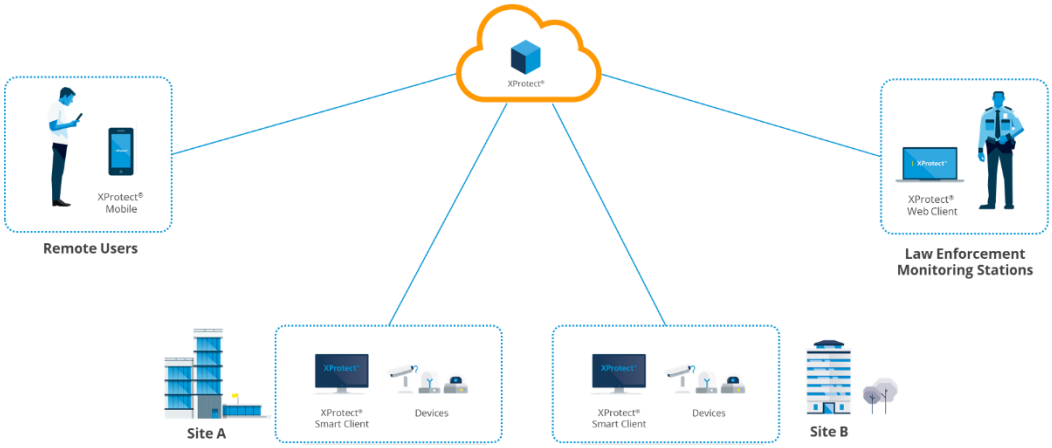


Figure 2. AWS cloud infrastructure unlocks the full potential of XProtect VMS in distributed deployment and usage

Cloud deployment further unlocks the full potential of the XProtect client suite, where remote users can access the video management system through secure connections using the XProtect Mobile application or the XProtect Web client. This means that roaming users and connections to law enforcement and monitoring stations can be facilitated without opening firewalls in the different sites.

This section elaborates on the system and service architecture when utilizing AWS global cloud infrastructure as platform for the XProtect video management system.

Principal Architecture

A deployment of Milestone XProtect video management software on AWS cloud infrastructure implies that all XProtect server components are deployed on a managed compute and storage infrastructure in a Virtual Private Cloud (VPC). Cameras, sensors and other IoT devices making up the surveillance solution on the customer's on-premise are connected to the cloud environment via secure connections carried over VPN connections or dedicated direct connections into the AWS cloud. The on-premises security devices transmit video, audio, metadata, and other streams to the cloud deployed XProtect VMS without the need for any additional on-premises hardware or gateway equipment for aggregation or buffering.

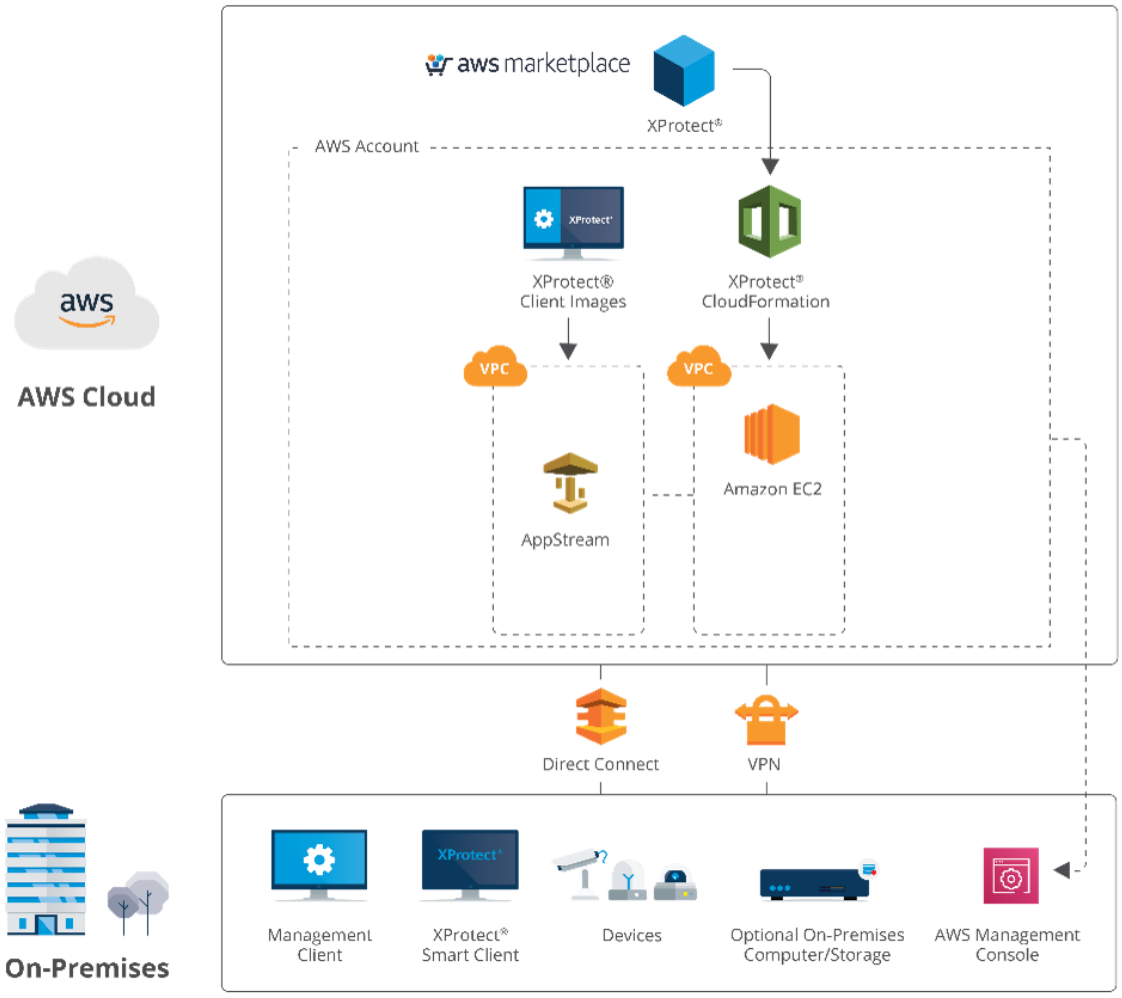


Figure 3. Principal system architecture of an AWS cloud deployment of XProtect VMS, with the option for steamed client access via Amazon AppStream 2.0

Users access the XProtect VMS system through the normal suite of XProtect client applications. As a design option, it is possible to run XProtect Smart Client and the Management Client applications as hosted applications using the Amazon AppStream 2.0 service. AppStream 2.0 not only makes it possible to use the full Smart Client on virtually any device, including Chromebooks, Macs, and PCs, thin clients and tablets, it is an easy and secure way of providing remote users with the full Smart Client experience. To read more about AppStream 2.0, please see section: Amazon AppStream 2.0 on page 38.

As shown in the figure above, it is also possible to run Smart Client on-premises and access the recording servers running on EC2 instances remotely. CloudFormation Template will not instantiate AppStream, instead the users can install and utilize AppStream feature if they choose to do so.

XProtect BYOL CloudFormation Product

Milestone distributes its XProtect VMS software as CloudFormation stack delivery in AWS Marketplace. The product is made up by the following four main components:

- XProtect VMS software
- Windows Server Operating System
- CloudFormation Template
- Optional 3rd party Plugins and Addons (For instance, Surveillance Bridge from Tiger Surveillance)

The CloudFormation template deploys the XProtect VMS software in a new Virtual Private Cloud (VPC) with subnet and security group topology within the AWS service infrastructure on the customer's account, in the selected AWS Region and Availability Zone. The template also configures an Elastic Compute Cloud (EC2) instance based on the customer's selection, on which all XProtect VMS server components are installed on, including the management server, recording server, event server, mobile server. Also, CloudFormation template provides an option to install plugin for S3-enablement. Please refer to Appendix B – XProtect BYOL CloudFormation Template on page 49 for complete overview of the CloudFormation template.

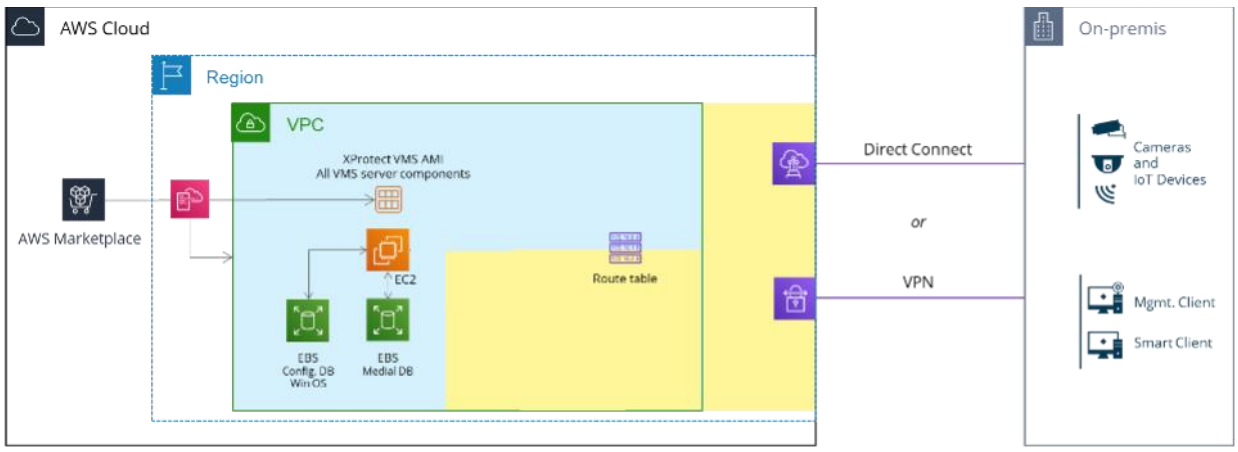


Figure 4. Default deployment of the XProtect CloudFormation product (blue area) and recommended customer extensions (yellow area)

Two Elastic Block Store (EBS) general purpose SSD volumes linked to the EC2 instance are orchestrated by the template, for:

- XProtect VMS configuration data and Windows operating system
- XProtect VMS media database

As illustrated in
Figure 4, the CloudFormation template orchestrates the topology depicted with blue color. In addition to this automated orchestration, customer specific extensions need to be made covering VMS video archive storage and establishment of connectivity to the customer's on-premises site(s). Please refer to relevant sections under Deployment Considerations, for further information on these architectural aspects.

The installed XProtect VMS software can be used to run any XProtect product variant, by applying an applicable XProtect Software License Code (refer to section: XProtect VMS Licensing, below).

System scaling

As mentioned in the section above, the default deployment of the XProtect BYOL CloudFormation orchestrates a single server installation of the XProtect VMS software on the EC2 instance selected for a deployment. This means that all XProtect VMS server components are installed on the selected EC2 instance, including the Management Server, Recording Server, Event Server, and Mobile Server.

Hence, the deployment can be scaled easily to be cost efficient across a wide range of solutions from small deployments with 10-20 cameras with the smallest EC2 instances, to 400-500 cameras solutions with the largest EC2 instance type. Please refer to Appendix C – EC2 performance, for detailed performance measurements of different EC2 instance types.

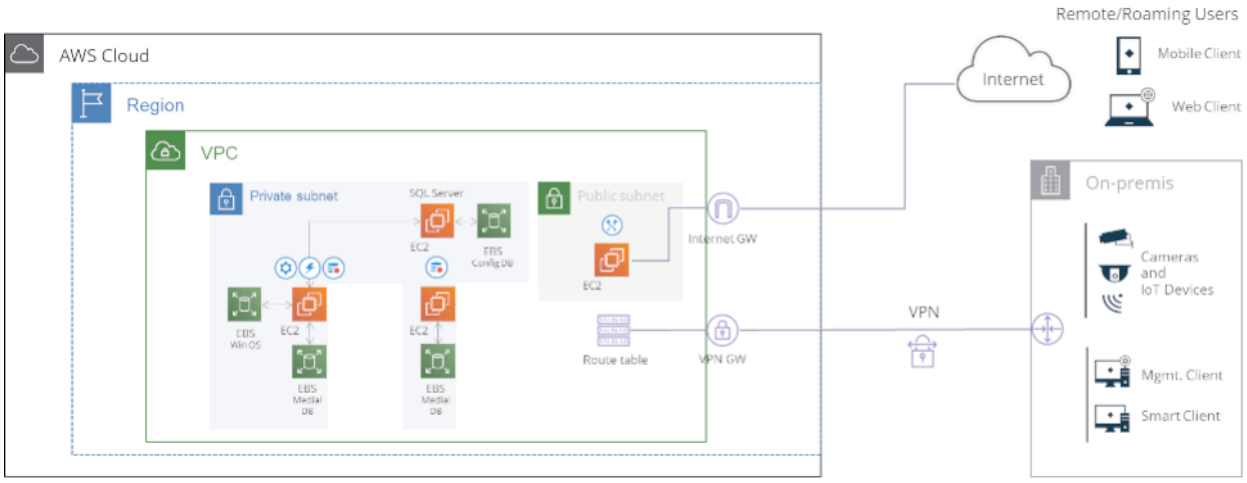


Figure 5. Scaled out XProtect VMS deployment in a single VPC deployment

A second level scaling is made possible by distributing the XProtect VMS server components on different EC2 instances. By installing the Recording Server service on additional EC2 instances, the XProtect deployment can grow to serveral ten thousand cameras, or more. In deployments with significant use of

XProtect Mobile and XProtect Web Client, the overall system performance can be optimized by running the mobile server on one or more dedicated EC2 instances, as illustrated in
Figure 5. The scaling out can be made in the same VPC as the original deployment or deployed in a different Availability Zone (AZ), or a different Region altogether. It is of course also possible to scale-out by deploying physical servers on-premises hosting the XProtect Recording Server service.

Additional instances can also be initiated through CloudFormation template or manually in the AWS management console.

XProtect VMS Licensing

The XProtect BYOL CloudFormation product is licensed under the same license terms with the same Software License Code (SLC) as used for traditional on-premises deployments. The XProtect BYOL product is offered on AWS Marketplace under Bring-Your-Own-License (BYOL) terms. This does not imply that Milestone XProtect licenses are sold in AWS Marketplace, but rather obtained through Milestone's existing channel network of distributors and system integrators. The deployed XProtect VMS software can be used to run any XProtect product variant (see list of products in section: Appendix A) by applying a valid SLC for the desired XProtect product variant.

The BYOL concept offers full license portability between on-premises and cloud deployments. Meaning that customers with existing XProtect on-premises installations can reuse their existing licenses when moving to a complete or partial AWS cloud deployment. In the same way, customers will be able to redeploy their XProtect license if they for one reason or another want to move off the cloud. Hence, any existing XProtect license can be used to activate XProtect on AWS.

Please note that the license may need to be upgraded to match the XProtect release versions available on AWS Marketplace.

Geographical availability

The Milestone XProtect BYOL CloudFormation product is available for deployment almost all AWS regions. This makes the offering globally applicable, and enables truly distributed and international organizations and companies to deploy a centrally managed and fully integrated video surveillance solution utilizing AWS backbone network (see section: Global on page 14).

As AWS is expending their cloud data center infrastructure continuously, please refer to AWS (https://aws.amazon.com/about-aws/global-infrastructure/regional-product-services/) for the latest information about active regions and the offered services in the specific Regions. Please note that AWS managed application streaming service, AppStream 2.0, is only available in a subset of AWS global regions.

Deployment Considerations

Selecting EC2 instance type

One of the greatest advantages of deploying XProtect on an elastically scalable cloud infrastructure is the possibility to freely select the configuration of the compute infrastructure at the system design point, and the ability to dynamically resize that platform as needs and operational conditions change. AWS offers a wide set of EC2 instance types that makes it possible to continuously optimize the compute infrastructure, to obtain the best possible performance and cost ratio.

Prior to the publication of the XProtect on AWS Marketplace, Milestone has conducted extensive system performance tests to short list a set of EC2 instances recommended for XProtect VMS deployments. This has resulted in seven EC2 instances offering the most advantageous cost per connected camera across the range of 10 to 500 cameras per XProtect recording server.

INSTANCE FAMILY	DESCRIPTION	INSTANCE TYPE
T3	Burstable general-purpose instance type	t3.large
C5	Optimized for compute-intensive workloads	c5.large c5.xlarge c5.2xlarge
G4	Optimized for graphics-intensive workloads Include NVIDIA T4 Tensor Core GPUs	g4dn.xlarge g4dn.2xlarge g4dn.4xlarge

Table 1. Recommended EC2 instance types for XProtect BYOL

Appendix C – EC2 performance presents the recommended EC2 instances and the performance metrics measured for these instance types.

On-premises – AWS cloud connectivity

The customer's on-premises environment(s) with camera assets and client applications need to be connected to the XProtect VPC using standard AWS networking services such as AWS Site-to-Site VPN and Direct Connect, or similar third-party networking technologies. This section discusses how AWS Site-to-Site VPN service can be applied to an XProtect deployment. For more advance methods using AWS Direct Connect, or AWS Transit Gateway, please refer to AWS documentation.

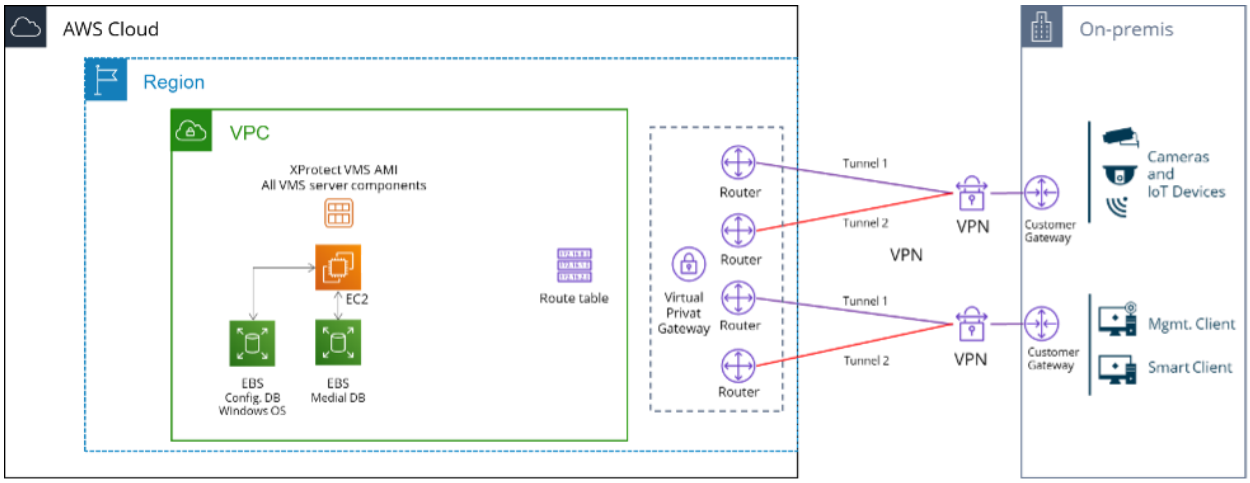


Figure 6. Principal design of a redundant Site-to-Site VPN topology for a single site deployment

Designing the network topology connecting the customer site(s), one should consider required bandwidth for video streams and client access, and factor in peak situations and the need for redundancy.
Figure 6 presents a principal redundant VPN design for a single site deployment. It should be noted that each VPN connection is made up by two separate IPsec tunnels, which represent the first level of redundancy in the event of a device failure within AWS. Second level redundancy is achieved by the two separate VPN connections, each handled by its dedicated customer gateway device. It is further recommended that these two VPN connections are routed via two different Internet Service Providers to ensure maximal redundancy. The VPN gateway that facilitates the Site-to-Site connectivity is attached to the XProtect VPC via the routing table.

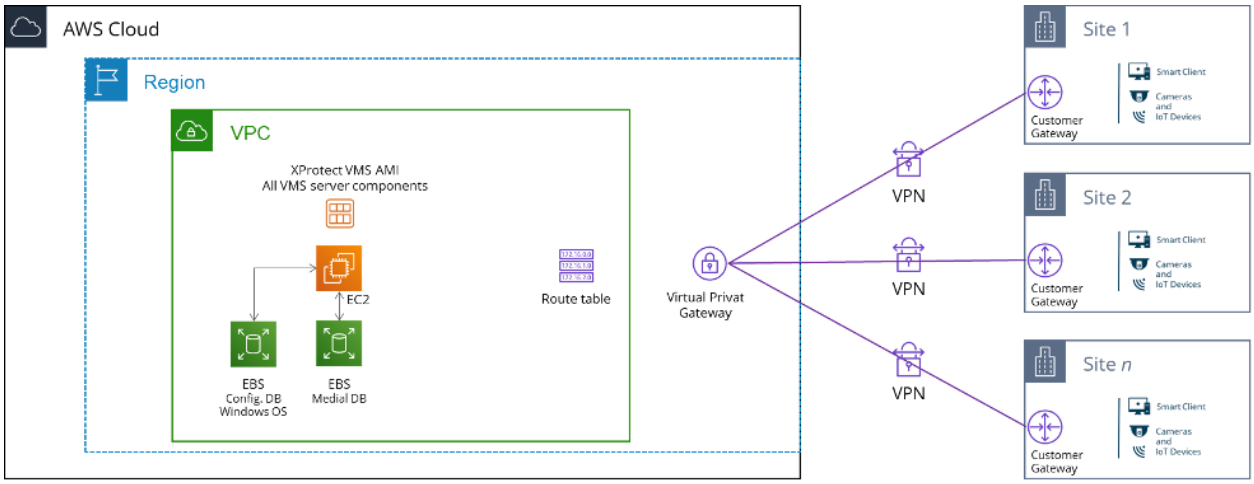


Figure 7. Example of a multi-site deployment using AWS Site-to-Site VPN

Enterprises and organizations often have geographically dispersed facilities and offices, where the security operation is to be coordinated in one centrally managed video management system. To support this, the individual sites can be connected to the XProtect VPC using the AWS Site-to-Site VPN service, as illustrated in
Figure 7. Please note that the figure does not consider redundancy in the VPN topology.

In larger deployments it is important to consider that the maximum throughput of an individual VPN tunnel is 1,25 Gbps, and that the Virtual Private Gateway are bound by an aggregate throughput limit from AWS to on-premises of up to 1,25 Gbps. For AWS Direct Connect connection on a Virtual Private Gateway, the throughput is bound by the Direct Connect physical port itself. To connect to multiple VPCs and achieve higher throughput limits, use AWS Transit Gateway.

The AWS Transit Gateway connects to the customer's on-premises environment using the same VPN mechanisms as the Virtual Private Gateway. This white paper will not cover designs including the Transit Gateway further. Instead system integrators and end customers are advised to study AWS documentation on the Transit Gateway (see: https://docs.aws.amazon.com/vpc/latest/tgw/what-is-transit-gateway.html). While designing the VPN infrastructure system, integrators should also consider AWS Site-to-Site VPN quotas, which can be increased upon request: https://docs.aws.amazon.com/vpn/latest/s2svpn/vpn-limits.html

Please note that customer gateway devices used with both the VPN Gateway and the Transit Gateway must support the Internet Key Exchange (IKE) protocol, which is used to exchange keys during the establishment of the IPsec security association. AWS also requires special configuration of the customer gateway devices. For more information and a list of tested customer gateway devices, please refer to AWS Site-to-Site VPN user guide (https://docs.aws.amazon.com/vpn/latest/s2svpn/VPC_VPN.html).

Media storage

The XProtect recording server operates with a tiered storage architecture made up by a media database and one, or more, levels of archives, which enables optimization of system performance and storage costs. Media archived to an archive storage remains on-line and is seamlessly accessible for navigation and playback by any client application. Please see the XProtect Storage Architecture and Recommendations white paper for complete information around media storage in XProtect.

There are two approaches possible for archiving:

(1) Using another archive storage: In deployments where video is to be retained for longer than just a few days and another file storage is preferred for archiving, Milestone recommends the use of a two-tiered storage with the short-term storage (media database) and long-term archive storage.

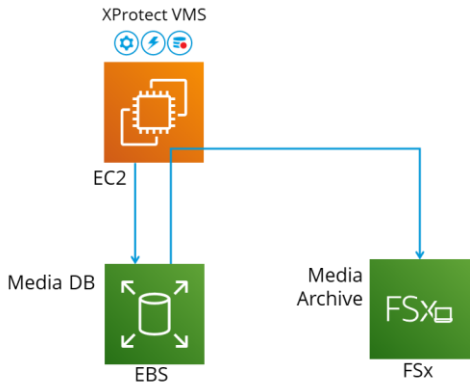


Figure 8. XProtect media storage utilizes a combination of EBS and FSx storage for optimal combination of storage performance and cost

Figure 8 above depicts the recommended storage infrastructure when running XProtect on AWS without any third party plugin or add-on that facilitates archiving, where the recording server's media database is hosted in an EBS general purpose SSD (gp2) storage volume and the media archives are stored in one of more Amazon FSx for Windows File Server storage volumes, dependent on the amount of video and other media data that is to be stored. In this setup the native XProtect video archiving function is used to move, and life cycle manage the video across the EBS and the FSx storage arrays.

The default deployment of XProtect BYOL CloudFormation configures the Elastic Block Store (EBS) for the media database only. This means that the FSx storage shall be added to the installation when and as needed. The FSx storage is available in single-AZ and multi-AZ deployment options, which offers an additional level of redundancy for end-customers with high demands on data resilience. Also, another option for storage is S3 as now the option is provided in the CloudFormation Template.

It is possible to use S3 with provided plugin. In that case, using Archiving is not needed, instead that task can be handled through Surveillance Bridge plugin. It is possible to configure movement of data into various storage options. In case user does not want to use S3 or use the plugin, to obtain maximum system performance while keeping the AWS service costs to a minimum, Milestone recommends keeping minimum amount of video (normally around 24 hours of recordings) in the EBS based media database, with frequent archiving to the long-term FSx HDD based storage. The overall performance of the combined EBS and FSx storage infrastructure is constrained by baseline bandwidth and IOPS allocations for not only the EBS and FSx storages, but also the specific EC2 instance used. It is therefore important to consider the combined performance of all these three elements, when dimensioning the storage infrastructure. Appendix D – Media storage dimensioning, details the specific dimensioning considerations.

Please note that FSx requires an active directory (AD) to be defined. The XProtect VPC should therefore be connected to an AD before the FSx storage is defined.

(2) Milestone XProtect on AWS CloudFormation template also supports third-party plugin or add-on Surveillance Bridge from Tiger Surveillance. Using that plugin enables archiving to be handled by the mentioned plugin. Refer to Appendix for more information.

Alternative storage options

AWS offers a wide range of storage services, where Milestone recommends S3 in case user wishes to use third party plugins or FSx for long term media storage in case no third party plugin is to be used. So viable options are: AWS S3 or AWS FSx or AWS EBS.

An additional option to the EBS storage that the CloudFormation template defines for the media database is to define a second EBS storage for archiving. The block storage should be throughput optimized HDD (st1) volumes and could be particularly relevant for deployments with shorter retention times (less than 1 week), cf. Appendix D – Media storage dimensioning, page 53.

The AWS Simple Storage Service (S3) can be used as an alternative or complement to the FSx based archive storage. The S3 storage can be particularly relevant when on-premises recording servers are configured to archive to an AWS cloud storage. The XProtect recording server does not integrate natively with the S3 object storage through its storage APIs. Therefore, a separate AWS Storage Gateway service needs to represent the object storage bucket as an addressable network drive for the VMS software. Furthermore, Surveillance Bridge can be utilized as well for using S3 for archiving (or as main Media Database). Dependent on the retention time and access patterns to recorded video data, customers can optimize their storage costs by selecting the most optimal S3 storage class.

Use of camera-based edge storage

It is sometimes difficult to obtain a satisfactory level of reliability and redundancy in the interconnecting VPN topology between the AWS cloud and the customers various sites. There are many reasons for this, including general regional scarcity of high-speed internet connectivity, high connectivity costs or technical limitations. In these cases, Milestone recommends the use of camera-based edge storage.

The use of camera-based storage is an ideal solution as it ensures that video and other data is continuously recorded even in the event of shorter interruptions in the connectivity between the customer's on-premises environment and AWS cloud environment. Once the connection is restored, recordings will be automatically transferred to the XProtect recording server in the AWS cloud, thus ensuring continuous recording of video despite possible intermissions in the connectivity.

For details about the use of edge storage, please refer to the Edge Storage with flexible retrieval white paper.

Data Protection

Video surveillance data is sensitive data that need to be protected from unauthorized access and use. Unlike a Software as a Service (SaaS) offering, in which the customer has no or little control over where the applications run and data is stored, XProtect on AWS puts the customer in full control of where the video data is stored and how it is protected. That means, no video data leaves the specific AWS data center (Availability Zone) in which the XProtect VMS is deployed at, unless otherwise is configured specifically in the actual customer architecture.

SQL Database

The XProtect VMS system stores and maintains all its configurations, event data and logs in Microsoft SQL databases. As a part of the deployment of the XProtect BYOL CloudFormation, a local Microsoft SQL Express database is installed in the EC2 instance. This database is configured as the default SQL database for the vital XProtect VMS system data. This database shall be backed up and managed manually. In larger installation, where a dedicated SQL server may exist, the XProtect system can be configured to use a separate EC2 instance to host a dedicated SQL server, as illustrated in
Figure 5 on page 20.

Another option is using Amazon RDS for SQL Database. This is supported by XProtect as well. Milestone is planning to provide option for using Amazon RDS for SQL Database through CloudFormation template in future.

Deployment instructions

System integrators and end-customers considering a deployment of XProtect on AWS are advised to study eLearning courses and deployment guides provided by Milestone. The material is published on the Milestone website, and available as a part of the XProtect BYOL listing in AWS Marketplace.

e-Learning courses:

- Milestone Cloud Fundamentals
- Communicating the value of XProtect on AWS
- Designing XProtect on AWS solutions
- Deploying XProtect on AWS

User Access

The deployment of XProtect on AWS cloud infrastructure opens for a wide set of ways to provide flexible access to the XProtect VMS system for both on-premises users, remote users and roaming users (cf. Figure 2 on page 17). This section discusses these access options and suitable architectures for the user access provisioning. No single client access architecture is the right solution, as the choice is highly dependent on the individual user's access and usage patterns.

On-premises deployed XProtect clients

The most straightforward way of facilitating user access to the cloud deployed XProtect VMS system is to install the Windows-based XProtect Smart Client application for security operators, and the Windows based XProtect management client for system administrators. Both these clients are available from a download service that is installed together with the XProtect VMS software in the XProtect VPC.

As illustrated in
Figure 4 (page 19), the XProtect clients are using the network topology connecting the customer's on-premises environment(s) to the AWS cloud to access the VMS system in the XProtect VPC. This setup is to a large degree similar to a traditional on-premises deployment, with the difference that the XProtect VMS servers resides in the AWS cloud, rather than as physical servers on-premises. However, as there is an AWS service charge for transmitting data out of a VPC, the consumption of data egress should be carefully considered in this setup.

Adaptive Streaming

To optimize the Smart Client performance and reduce the AWS data egress costs, Milestone recommends the use of the Adaptive Streaming feature, available in XProtect Corporate and XProtect Expert. Adaptive Streaming enables the Smart Client to automatically select the media video stream with the most appropriate resolution[2] for a given camera view. By selecting the stream that is most optimal, the amount of data to be transferred to and handled by the Smart Client is reduced, thus increasing the performance of the Smart Client.

[2] Most appropriate resolution means the stream with the lowest resolution, which is greater than the size of the Smart Client view item in which the stream is to be shown.

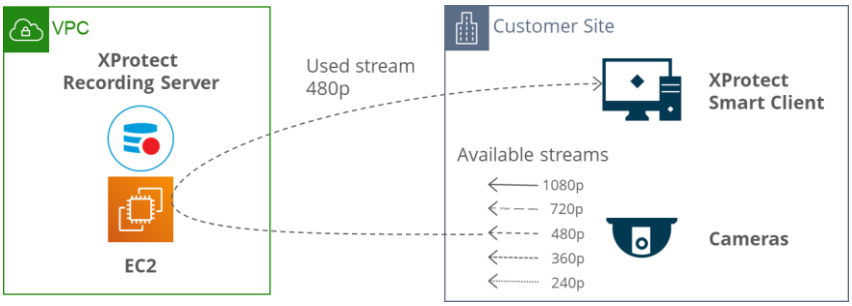


Figure 9. Adaptive streaming is used to start the camera stream that is most suitable for the displayed view

The graph below illustrates the reduction in data egress from the XProtect VPC, when using adaptive streaming to select the most suitable stream for the Smart Client, rather than transmitting the full 1080p stream. The graph depicts the reduction in data throughput of adapted streams compared with the throughput when transmitting a full 1080p stream for different number of video streams displayed on a Smart Client workstation with a HD 1080p monitor and an UHD 2160p monitor, respectively. The graph assumes that the default camera resolution for all cameras in the XProtect VMS system is 1080p, while each camera has a set of additional lower resolution streams (720p, 480p, 360p and 240p) defined too, that can be used when the camera is included in a camera view containing several other cameras.

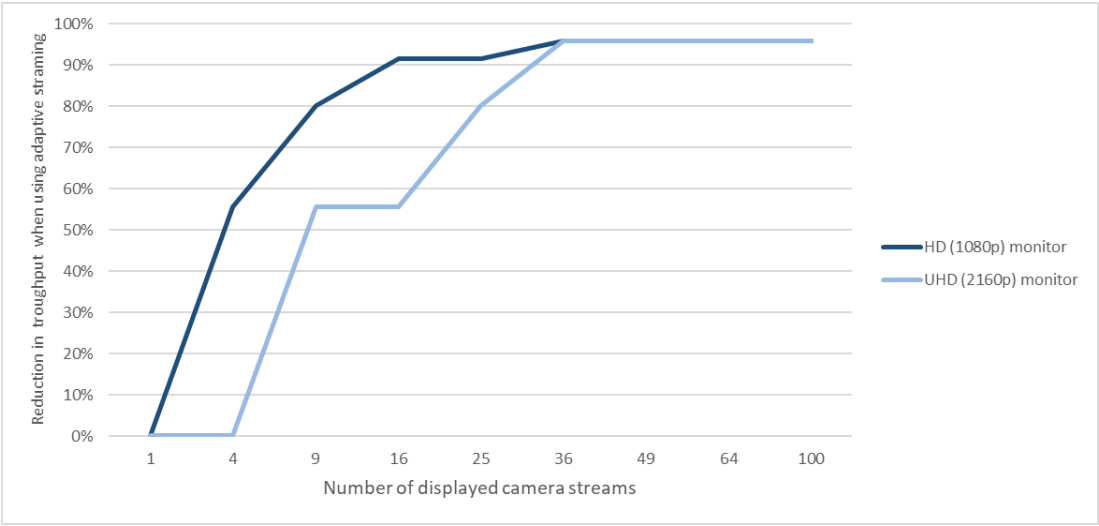


Figure 10. Reduction in transferred data when using adaptive streaming

An example of the potential savings that can be achieved with the Adaptive Streaming capability is when a Smart Client user is viewing 16 cameras (in a four by four view) on a display with HD (1080p) resolution. Without Adaptive Streaming, 16 1080p streams would need to be transmitted. However, as a four by four camera split on a HD monitor with 1080 x 1920 pixels would only leave each camera tile with less than 270 x 480 pixels, the Adaptive Streaming function can select the 360 x 480 video streams from the cameras. This corresponds to a 92% reduction in data egress from the AWS Cloud, which translates to an equally large saving in data egress costs.

In addition to providing substantial savings on data egress costs, Adaptive Streaming reduces the video processing load on the workstation used to host the Smart Client, which opens for additional savings on hardware as powerful workstations are needed.

Please note that Adaptive Streaming requires definition of multiple stream resolutions for each camera device that dynamically can be selected by the Smart Client. For playback of recorded video, it is only possible to view the video in the resolution it was recorded in.

Amazon AppStream 2.0

As an alternative to running the XProtect clients on workstations on-premises, AWS offers the possibility to run client applications as hosted user sessions in the AWS cloud using the Amazon AppStream 2.0 service. This makes it possible to use the full Smart Client virtually on any device, including Chromebooks, Macs, and PCs, thin clients, and tablets.

Users can access AppStream 2.0 hosted applications either view a browser, or an AppStream 2.0 client application. AppStream 2.0 is compatible with all major browsers and is hence an ideal solution for remote access by both the end-customers own personnel and trusted third parties such as monitoring stations and law enforcement. The AppStream 2.0 client exposes workstation peripherals as USB connected joysticks and input keyboards to the Smart Client application hosted in the cloud.

One of the primary reasons for AppStream 2.0 being an interesting architecture for user access is that the AppStream 2.0 service pricing includes the AWS cloud egress costs. As discussed in the earlier section (Adaptive Streaming), transferring multiple raw high resolution video streams from the cloud to on-premises can be relatively costly, and a cost that can be eliminated with AppStream 2.0.

In addition to the savings on data out transfer, AppStream 2.0 offers several additional advantages for efficient and secure user access to the XProtect VMS system, including:

- Reduced workstation HW costs

  As video decoding and rendering is made in the AppStream 2.0 service, significant savings can be made on the workstation infrastructure. Less powerful workstation or even, thin client PCs can be used reducing the initial capital expenditure.

- Centrally managed applications

  Eliminating the need for local installation of the XProtect clients, and related plugins and third-party applications, the application layer can be managed and updated centrally.

- Optimized workstation fleet management

  Manage workstation deployment and operating system updates from a single point.

- Secure applications and data

  XProtect clients or data are not stored on users' devices. The client experience is streamed as encrypted pixels and access to data is secured within the customer's network. AppStream 2.0 runs on AWS, and leverages the data center and network architecture infrastructure built for the most security-sensitive organizations.

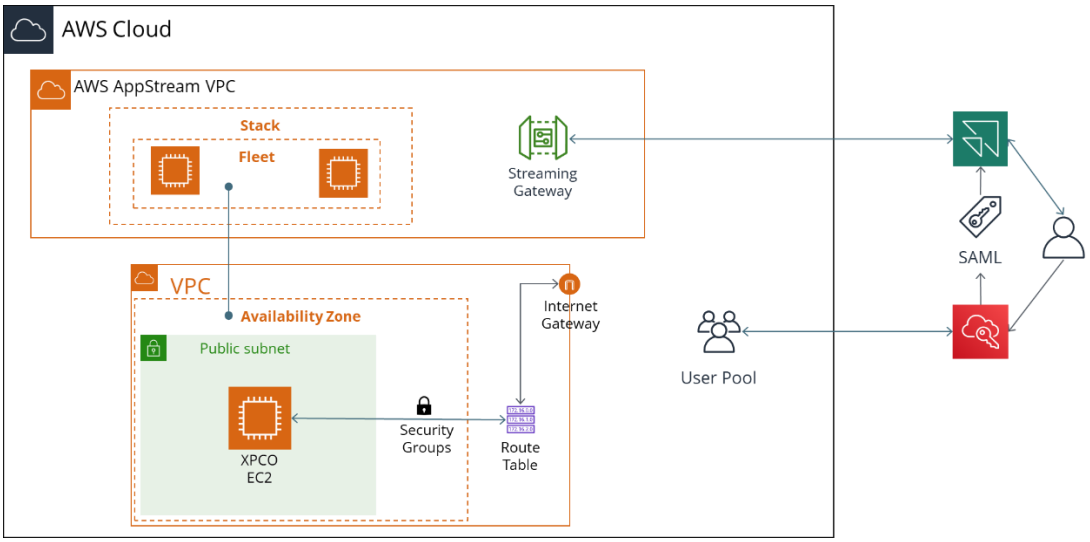


Figure 11. Principle architecture for Amazon AppStream 2.0 deployment

As illustrated in the figure above, AppStream 2.0 is deployed in a separate VPC outside the customer's AWS account offered as an AWS managed service connected to the XProtect VPC. User instances of the XProtect Smart Client and management client applications run on a so-called Fleet of AppStream 2.0 EC2 instances, where streamed client experiences are provided through a Streaming Gateway to the user. The use of AppStream 2.0 is governed by a Stack definition, which includes available AppStream 2.0 images, user access policies, storage configurations and an associated AppStream 2.0 Fleet.

Appendix E – AppStream 2.0 includes performance test results for Smart Client execution on AppStream 2.0, as well as recommendations for suitable EC2 AppStream 2.0 Fleet instance types.

Milestone does not provide client images for AppStream 2.0. Instead system integrators and end-customers are advised to use the AppStream 2.0 image builder, which is a tool used for creating AppStream 2.0 images, and available as part of the AppStream 2.0 console. Please refer to AWS service information for more details about AppStream 2.0: https://aws.amazon.com/appstream2/

Web and Mobile access

The XProtect VMS software includes native support for remote users accessing the system via web browsers (XProtect Web Client) and roaming users using tablets or smartphones (XProtect Mobile). While XProtect Web Client is an ideal system access for occasional users, and IT environments with zero install footprint policies, XProtect Mobile is an optimized application for a wide set of roaming users, including guards and first responders.

The XProtect mobile server facilitates secure and encrypted HTTPS communication with the web and mobile clients. Dependent on the specific customer use case and IT policies, the mobile server can be co-hosted in the XProtect VMS on AWS or placed on the customer's premise. A cloud deployed mobile server would provide the greatest flexibility and scalability in most customer deployments.

As illustrated in
Figure 5 on page 20, Milestone recommends deploying the XProtect mobile server component on one, or more, dedicated EC2 instances. It is also recommended to configure the EC2 instance(s) for the mobile server in a separate public subnet attached to an internet gateway. The mobile server subnet shall be secured with proper Security Group settings on both the incoming side and on the attachment towards the subnet used for the core XProtect VMS services.

In situations where the users of the Mobile and Web Clients primarily reside within the customers on-premises LAN environment, the mobile server used to facilitate the user remote access can be deployed on the customer's premise.

The mobile server offers two principal methods to optimize the communication and the data throughput for the web and mobile clients:

- Adaptive transcoding

  The mobile server transcodes video streams to a lower bandwidth intense format that adapts to the pace the clients can consume the video. This gives a robust communications and fluent rendering when used across low bandwidth connections. In this mode, it is possible to define thresholds for maximum framerate and throughput, which provides excellent means of controlling VPS data egress costs.

- Adaptive streaming

  In adaptive streaming mode, the mobile server applies the same stream handling methodology as the Smart Client (discussed in section: Adaptive Streaming, page 28), when sending streams to the XProtect Web Client.

Both these methods provide excellent opportunities for optimizing the data throughput used by remote users, and hence are a good way for cost control of data egress costs.

When utilizing adaptive transcoding Milestone recommends using EC2 GPU enabled instances, where the g4dn family is a good option.

Operations Cost

Cloud deployment of Windows applications, like XProtect VMS, is different from on-premises deployment especially concerning how the IT operation is orchestrated and structured. Cloud not only enables significant opportunities for outsourcing and optimization of the IT operations, but it changes the way that compute and storage infrastructure is acquired; from upfront purchase of static hardware, to a flexible pay-per-use purchase of hardware as a service.

As the list of parameters that impacts the operational cost is long, and it varies from enterprise to enterprise depending on nature of business, industry, and geographical location, it is difficult make an exact calculation of the operational costs. This section will therefore only discuss the direct operational costs associated with a deployment of XProtect on AWS.

The following subsections discuss the cost of AWS services when used with XProtect VMS.

Price calculator

To simplify the price calculation of running XProtect on AWS, Milestone provides a price calculator. The XProtect on AWS calculator is available on Milestone Documentation portal. Please note that this calculator is intended to provide an indicative price only. As it is based on a set of service execution assumptions, the final cost can only be determined by the final deployment and the contractual agreements with AWS.

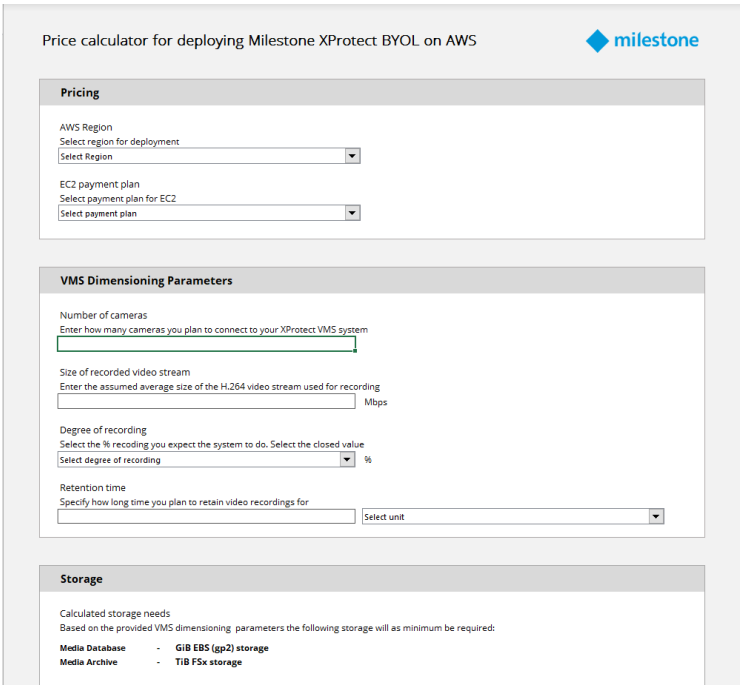


Figure 12. The XProtect BYOL price calculator makes it easy to calculate the AWS service costs for running XProtect on AWS

AWS EC2 instances

The instance type required for a specific XProtect VMS deployment will depend on a wide range of parameters, including number of cameras in the system, stream properties such as resolution and framerate and the use of server-side motion detection. Please note the significant savings that can be obtained by using RI saving plans (see: General AWS pricing logic on page 39).

Appendix C – EC2 performance discusses the details around the selection of the EC2 instance.

AWS EBS storage

XProtect defines two EBS general purpose SSD (gp2) storage for:

- Windows OS system and XProtect VMS configuration data
- VMS media database repository

The EBS storage used for the Windows OS and the XProtect VMS configuration data is defined as 100 GB as default.

The EBS volume defined for the media database shall, as discussed in Appendix D – Media storage dimensioning (page 53), be defined to accommodate roughly 24 hours of recordings, where the actual size will depend on degree of recording and video stream properties such as resolution, framerate and image complexity. One should aim to optimize the allocation of the EBS storage, as it is relatively costly compared to the far more cost efficient FSx storage used for archiving databases. Another more cost efficient scenario is also available using S3 storage, but that requires Surveillance Bridge software from Tiger Surveillance. See appendix.

AWS FSx storage

The Amazon FSx for Windows File Server is used for long-term video storage, where the primary cost drivers are dependent on how much data is to be retained and for how long, as discussed in Appendix D – Media storage dimensioning (page 53). The Amazon FSx for Windows File Server is a flexibly priced storage service, where customers only pay for the resources they use. Whereas the native FSx service have several pricing parameters, only a reduced set are relevant when used together with XProtect:

- Storage capacity

  The average amount of storage provisioned in the file systems per month, measured in gigabyte-months "GB-Months".

- Throughput capacity

  The price of throughput capacity depends on the deployment type (single-AZ or multi-AZ) that is selected. The charge covers the average throughput capacity provisioned for the file systems per month, measured in "MBps-months". For multi-AZ file systems, the cost to transfer data between Availability Zones for replication of data is included in the throughput capacity price.

AWS offers two different storage types: SSD or HDD. With reference to Appendix D – Media storage dimensioning, Milestone recommends HDD.

FSx is available in two different deployment modes:

- Single-AZ

  Redundancy on disk level

- Multi-AZ

  Redundancy on data center (AZ) level, where media archives are replicated across two different data centers.

AWS FSx further operates with a data backup offering and a Data Deduplication capability, which reduces costs associated with redundant data by storing duplicated portions of your files only once. Due to the nature of video data, neither of these two services are relevant for XProtect video archives.

AWS S3 storage

Another storage type offered by AWS is S3. S3 is an object storage while XProtect stores the videos in a file system structure. Therefore a software is needed in order to enable using S3 for video storage. Milestone provides the option to install Surveillance Bridge of Tiger Surveillance in the CloudFormation template.

The CloudFormation template installs the Surveillance Bridge pluginfrom Tiger Surveillance automatically along the other XProtect components during the initialization process. See Appendix.

S3 storage pricing has now been changing recently with a decreasing trend and is yet another viable option for video storage.

AWS Site-to-Site VPN

The requirements on cloud connectivity varies significantly from organization to organization, and AWS offers several different networking services to meet these diverse needs. This white paper only discusses the basic AWS Site-to-Site VPN service. The Site-to-Site VPN service has a simple pricing logic of cost per VPN connection hour. The only data throughput charges that applies to Site-to-Site VPN service are the general VPC data egress charges accounted for in next section.

VPC data egress

Although AWS provides VPC without cost, there is a cost associated with data transfer out from the VPC, often referred to as data egress. XProtect VMS generates data egress when users access the XProtect system through the different XProtect clients (as discussed in section: User Access, page 28).

The amount of data egress is highly dependent on user behavior patterns, where the following aspects are the primary parameters in estimating the amount of egress data:

- Number of users
- Which XProtect clients is used
- Frequency and duration of use
- Amount of video streams viewed
- Use of XProtect network bandwidth optimization features

Figure 13 illustrates the complexity in estimating the data egress costs, and the importance of optimizing these costs. The graph presents the yearly cost for one user accessing the XProtect VMS system through different methods at different usage patterns both in terms of average usage time per day (the x-axis) and how many camera streams that are viewed (4 and 36 cameras respectively). The three user access methods illustrated in the graph are:

- XProtect Smart Client with Full HD (H.264 at 1080p) streams at 30 frames per second, corresponding to 4 Mbit/s per viewed stream.

- XProtect Smart Client with adaptive Streaming, where alternative streams with lower resolution have been selected. When viewing 4 streams, 720p streams have been selected, and when viewing 36 cameras, 240p streams have been selected.

- AppStream 2.0 with XProtect Smart Client hosted on a g4dn.xlarge EC2 instance type.

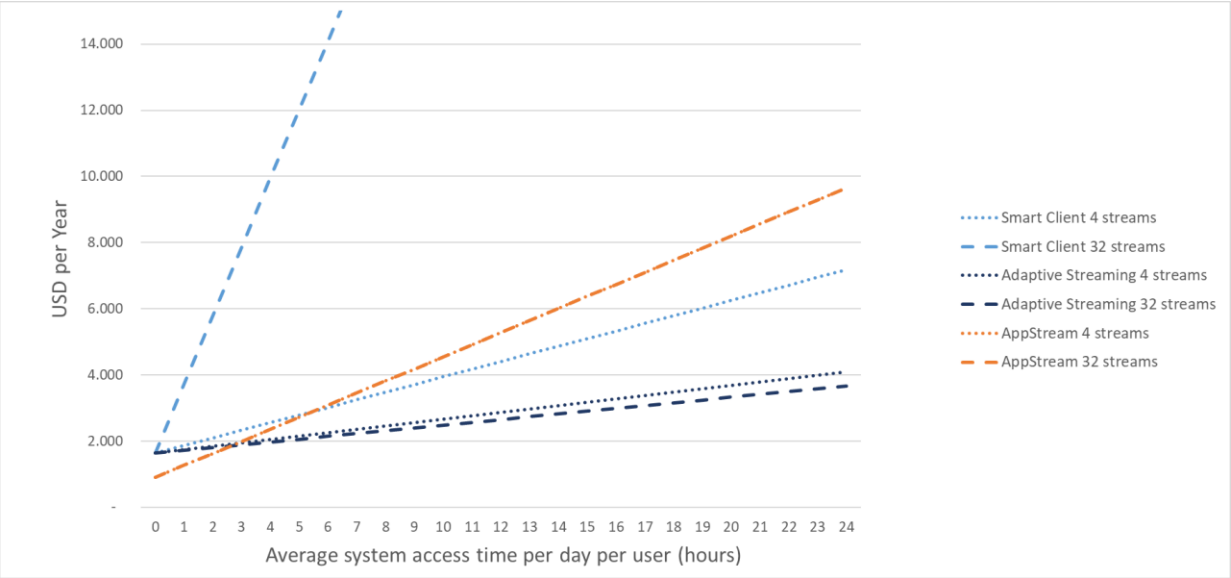


Figure 13. Accumulated yearly user access cost for different user access methods at different levels of average daily usage. The cost includes VPC data egress costs US East (N. Virginia) and workstation hardware costs[3], and presented for 4 and 32 H.264 streams at original stream size of 4 Mbit/s

The graph shows that the yearly cost is a linear function of how many hours a user accesses the system. While the cost grows dramatically when using non adaptive stream access, the adaptive streaming feature keeps the data egress cost at a reasonable level, even when the usage is extensive measured both in number of access hours a day, and number of viewed cameras. Amazon AppStream 2.0 is a viable alternative.

Amazon AppStream 2.0

With reference to the section above and Figure 13, running the Smart Client as a hosted client application in AppStream 2.0 can be a viable and attractive alternative to running the full client on the end customer premises. Especially in deployments with infrequent occasional usage patterns where the average access time per user is less than 3 hours a day.

AppStream 2.0 is priced though three principal parameters:

- Number of enabled unique users
- Duration of usage
- Used EC2 instance type in the AppStream Fleet

[3] The hardware cost is based on a 3-year depreciation period.

While the use of AppStream imposes additional AWS service costs, there is no data egress costs for the data transmitted as a part of the AppStream client streaming session. In addition to this, AppStream has the potential to unlock additional savings on workstation hardware and reduced desktop IT administration effort.

AWS service optimization

Dimensioning server and storage infrastructure for a video surveillance installation is complex, involving numerous assumptions around degree of recording, image complexity, user access patterns, just to mention a few. With the many assumptions that need to be made, there is an evident risk for errors resulting in system overprovisioning. In a physical deployment surplus hardware is sunk cost, but in a cloud deployment there are unlimited opportunities for post deployment optimization, and thus cost reductions.

It is therefore important to emphasize that even though the dimensioning of an AWS deployed XProtect system needs to follow the same principal design steps as a traditional on-premises system, the consequences of an error in the assumptions or in the actual design calculations are far for as fatal and in the physical deployment. When deploying a XProtect system on AWS, there are wide range of opportunities optimize and finetune the design when the system is in production, as a part of a post deployment optimization.

Additional costs

In addition to the AWS service charges one should add the Internet access service provided by the regional Internet Service Provider or network carrier, and the on-premises router equipment needed. The internet access costs are difficult to estimate, as there are major regional differences in availability, up-link speed, and pricing.

General AWS pricing logic

Readers who are not familiar with AWS general pricing policies are advised to study these on AWS website https://aws.amazon.com/pricing/. AWS also provides a full set of price calculators for their service range: https://calculator.aws/#/.

There are however some of the fundamental AWS pricing concepts that can be relevant to point out when using AWS as infrastructure platform for XProtect:

- Region used

  Prices on AWS services vary between Regions, dependent on availability and other factors. Although the differences are not significant, one should make sure to apply the specific Region in which the XProtect BYOL CloudFormation is to be deployed.

- Service pricing logic

  Each of the AWS services that are relevant for the XProtect deployment have their own pricing logic and pricing parameters. All though, most services are priced on a specific time unit (per hour or per month), some services are priced on additional parameters such as throughput, number of connections etc. System integrators and end-customers are recommended to study the pricing mechanisms for the relevant services used by XProtect.

- Saving plans

  AWS offers a wide range of saving plans for its different services. The most relevant for deployments of XProtect on AWS is the Reserved Instance (RI) plan for the EC2 instance used for the XProtect deployment. As video surveillance installations in most cases are intended for long-term continuous usage considerable savings can be obtained by making either a one or a three-year reservation of the EC2 instance. AWS offers different RI Classes, where the Standard provides enough flexibility to shift EC2 instance, when and as the installation grows or is optimized.

Maintenance

AWS shared responsibility model

Security and Compliance is a shared responsibility between AWS and the end-customer. This shared model can help relieve the customer's operational burden as AWS operates, manages, and controls the components from the host operating system and virtualization layer, down to the physical security of the facilities in which the service operates.

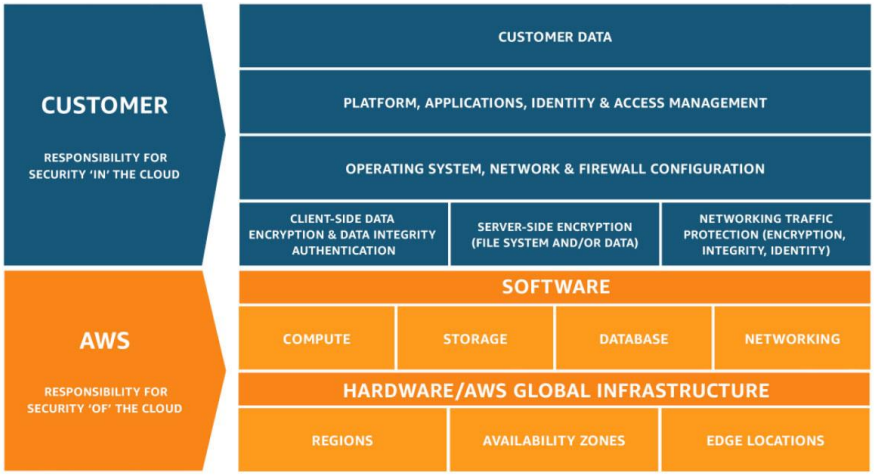


Figure 14. AWS shared responsibility model

AWS is responsible for protecting the infrastructure that runs all the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services, and include all AWS services used in a XProtect VMS deployment. The customer assumes responsibility and management of the Windows operating system (including updates and security patches), the XProtect VMS software, as well as the configuration of the AWS provided security group firewall.

Technical Support

While AWS provides technical support on the infrastructure services provided by AWS under the AWS agreement, Milestone will provide technical support on the XProtect VMS software through the Milestone channel partner, from whom the XProtect software license was obtained.

XProtect VMS upgrade

End customers with XProtect VMS deployed on AWS can upgrade to newer versions of XProtect at any time once a newer version becomes available. An upgrade of an AWS deployed XProtect system is handled in the same way as a traditional on-premises installations. This implies that the XProtect SLC shall be

upgraded via the Milestone channel partner. The upgrade of the XProtect VMS software is made through an upgrade of the individual EC2 instance, or instances, used for the deployment, normal upgrade procedures. It is currently not possible to upgrade an existing deployment via AWS Marketplace.

Customers with Care Plus service coverage can upgrade to the latest version of the XProtect VMS software without any additional charge, in the same way as when the software is deployed on a physical infrastructure on the customer's premises.

Milestone Care services

Milestone Care services are applicable to XProtect VMS products deployed on AWS, in the same way as for traditional on-premises deployments. That means that end customers can purchase Care Plus, Care Premium and Care Elite service coverage for their XProtect VMS product(s). The Care services are obtained through the Milestone distribution channel together with the XProtect VMS software licenses.

Summary

XProtect on AWS is a perfect mix of scalable video management software and an elastic, redundant and secure infrastructure- and service platform. In this paper we have described how cloud deployment reduces friction that is normally encountered in an on-premises deployment. The paper has further explained how the cloud elasticity enables customers to both grow their installations with their needs, but also how it allows for post deployment optimization to optimize cost and eliminate any over provisioning.

The paper has explained how the CloudFormation template ensures instant and predictable deployment of XProtect, and how the default deployment easily can be extended to include customer specific AWS services. Thanks to the elastic scalability in the compute layer, we have concluded that a system can be cost-efficiently scaled from 10 to 500 cameras[4] on a single AWS EC2 instance with server-side motion detection applied, where GPU enabled EC2 instance types provide excellent price performance ratio.

With a range of storage options for long term video archiving, AWS FSx provides a secure and managed video storage. FSx can be configured in a multi availability zone configuration, where video is archived into two separate datacenters to obtain high level of redundancy. Besides FSx, S3 is also a viable option. But as it is a object storage, it needs a 3rd party Surveillance Bridge of Tiger Surveillance to be used.

Deploying XProtect on AWS opens a wide range of possibilities including flexible user access using both XProtect clients, Amazon AppStream 2.0, and the ability to apply a centrally managed video surveillance solution for geographically disperse sites. Deploying XProtect on AWS, customers can apply hybrid architectures, with some XProtect services running in the cloud, and some on-premises.

XProtect on AWS is ideal for organizations and enterprises with a cloud first strategy, which allows them to deploy and manage their XProtect in the same way as any other businesses systems, leveraging their existing AWS infrastructure and IT competences.

[4] 4Mbit/s, H.265 stream with 30 FPS.

Terms and Abbreviations

AWS cloud services

The AWS cloud infrastructure- and service platform includes the following key components that are of relevance for hosting XProtect on AWS:

AWS SERVICE	DESCRIPTION
AMI	An Amazon Machine Image (AMI) is a special type of virtual appliance that is used to create a virtual machine within EC2. It serves as the basic unit of deployment for services delivered using EC2. Milestone is to build an AMI including XProtect and related components. The AMI is instantiated for different customers in runtime operation.
Amazon AppStream 2.0	Amazon AppStream 2.0 is a fully managed application streaming service. It is used to centerally manage desktop applications and securely deliver them to any computer. In the case of Milestone, AppStream 2.0 will provide relayed access to the XProtect Management Client and the Smart Client. https://aws.amazon.com/appstream2/
AWS CloudFormation	AWS CloudFormation provides a common language for modeling and provisioning of AWS and third-party application resources in a cloud environment. AWS CloudFormation allows for automated scripted provisioning of all resources needed for an application deployment across all regions and accounts. This gives end-customers a single source of truth for your AWS and third party resource https://aws.amazon.com/cloudformation/
AWS Direct Connect	AWS Direct Connect is a cloud service solution that makes it easy to establish a dedicated network connection from your premises to AWS. AWS Direct Connect enables private connectivity between AWS and the end-customers' premise, which in many cases can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections. https://aws.amazon.com/directconnect/
AWS EBS	Amazon Elastic Block Store (EBS) is an easy to use, high performance block storage service designed for use with AWS EC2 for both throughput and transaction intensive workloads at any scale. https://aws.amazon.com/ebs/
AWS EC2	Amazon Elastic Compute Cloud (EC2) is a service that provides secure, resizable compute capacity in the cloud. https://aws.amazon.com/ec2/
AWS S3	Amazon Simple Storage Service (Amazon S3) is an object storage service offering industry-leading scalability, data availability, security, and performance. Customers of all sizes and industries can store and protect any amount of data for virtually any use case, such as data lakes, cloud-native applications, and mobile apps. With cost-effective storage classes and easy-to-use management features, you can optimize costs, organize data, and configure fine-tuned access controls to meet specific business, organizational, and compliance requirements. https://aws.amazon.com/s3/
AWS FSx	Amazon FSx for Windows File Server provides fully managed, highly reliable file storage. It is built on Windows Server, delivering a wide range of administrative features and integrates with Microsoft Active Directory (AD). It offers single-AZ and multi-AZ deployment options. https://aws.amazon.com/fsx/windows/
AWS Site-to-Site VPN	AWS Virtual Private Network (AWS VPN) is a secure private tunnel solution between the end-customers' premise and AWS global network. AWS VPN is an alternative to AWS Direct Connect suitable for smaller customers, and customer sites. https://aws.amazon.com/vpn/

Table 2. Key AWS services relevant to an XProtect deployment on AWS

Abbreviations

AD	Active Directory
AMD	Advanced Micro Devices
AMI	Amazon Machine Image

AWS	Amazon Web Services
AZ	Availability Zone
BYOL	Bring Your Own License
CAPEX	CAPital EXpenditures
CPU	Central Processor Unit
CUDA	Compute Unified Device Architecture
EBS	Elastic Block Store
EC2	Elastic Compute Cloud
ENI	Elastic Network Interface
FedRAMP	Federal Risk and Authorization Management Program
FISMA	Federal Information Security Management Act
FPS	Frames per Second
FSx	File Storage for Windows File Server
GbE	Gigabit Ethernet
Gbps	Gigabits per second
GiB	Gibibyte (corresponding to 1.073741824 GB)
GPU	Graphical Processor Unit
HD	High Definition
HDD	Hard Disk Drive
HIPAA	Health Insurance Portability and Accountability Act
HTTPS	Hypertext Transfer Protocol Secure
IKE	Internet Key Exchange
IOPS	Input/Output Operations Per Second
IoT	Internet of Things
IPsec	Internet Protocol Security
ISO	International Organization for Standardization
IT	Information Technology
LAN	Local Area Network
MBps	Mega Byte per second
MIP SDK	Milestone Integration Platform Software Development Kit
OS	Operating System
PC	Personal Computer
PCI DSS	Payment Card Industry Data Security Standards
RDS	Relational Database Service
RI	Reserved Instance
S3	Cloud Object Storage
SAS	Statement on Auditing Standards
SLC	Software License Code
SOC	System and Organisation Controls
SQL	Structured Query Language
SSAE	Statement on Standards for Attestation Engagements
SSD	Solid-State Drive
TB	Terabyte
TiB.	Tebibyte (corresponding to 1.099511627776 TB)
UHD	Ultra-High Definition
VMD	Video Motion Detection
VMS	Video Management Software
VPC	Virtual Privat Cloud
VPN	Virtual Privat Network

Appendix A – Milestone XProtect VMS

This appendix introduces Milestones XProtect VMS products and their principal architecture.

Milestone XProtect VMS system architecture

The XProtect VMS software is a scalable video management software that combines high performance video processing and recording with advanced video management functions delivered through a reliable and secure software implementation. To enable seamless scaling and meet different customer needs, the system architecture is divided into a number of Windows system components. This allows the XProtect VMS software to scale from a single server installation serving 10 camera devices, to a fully distributed installation serving the thousand, or more devices.

Figure 15 below provides a principal overview of the XProtect system architecture and its main system components when deployed in a distributed configuration. Please note that that not all components are needed in all installations but can be installed if the functionality they offer is needed. For example, failover recording servers (not depicted in the system drawing) and mobile server for hosting and providing access to both the XProtect® Web Client and XProtect® Mobile client.

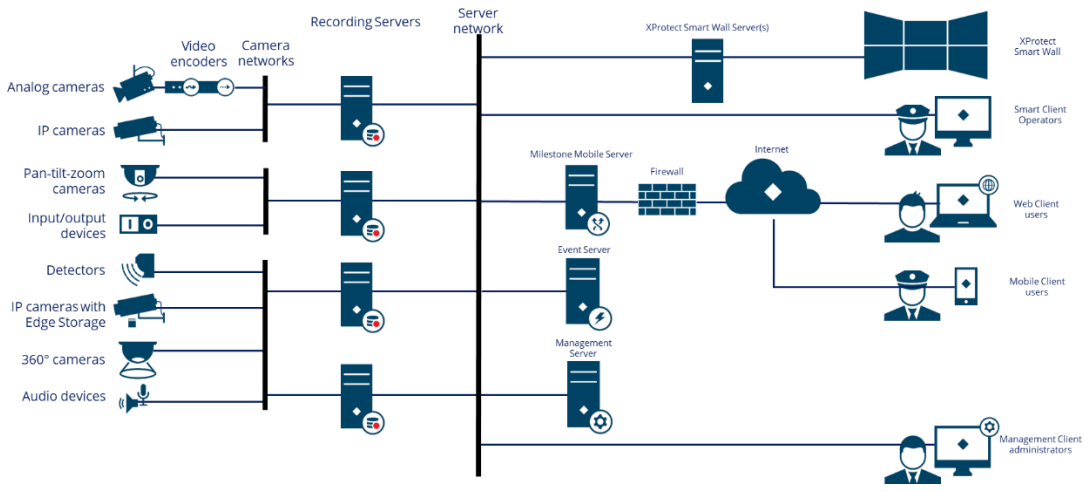


Figure 15. The principal XProtect VMS architecture with server components and client applications

The table below provides a brief description of the key server components and client applications in the XProtect VMS system architecture. Please note that this list is not exhaustive, please refer to the following white paper: XProtect VMS system architecture document, for a complete technical introduction to Milestone XProtect VMS system.

	VMS SERVICE	DESCRIPTION
SERVER COMPONENTS	Recording Server	The recording server is responsible for all communication with devices (cameras, video, and audio encoders, IoT devices such as input/output (I/O) modules, metadata sources, etc.). It records received media and metadata streams and makes both live streams and recorded streams available for viewing in the XProtect client application and other applications integrated via the Milestone Integration Platform Software Development Kit (MIP SDK). The recording server is responsible for a wide set of functions related to device and event handling and can be configured to conduct motion detection on received video streams. The motion detection analysis includes video decoding using hardware (GPU) accelerated decoding and/or software (CPU) decoding.
	Management Server	The management server is the central component of the VMS and is responsible for handling the system configuration, distributing configuration to other system components, such as recording servers, and for facilitating user authentication. The configuration data is stored in a standard Microsoft SQL server installed either on the management server itself or on a separate dedicated server. It can also be in Amazon RDS.
	Event Server	The event server handles various tasks related to events, alarms, maps, and third-party integrations via the MIP SDK.
	Mobile Server	The mobile server is responsible for hosting the XProtect Web Client and for providing access to the VMS for the XProtect Web Client and Milestone Mobile client users.
CLIENT APPLICATIONS	Smart Client	XProtect Smart Client is the Windows based main client for XProtect VMS offering a full set of advanced video surveillance and incident management features. The XProtect Smart Client is designed to be run remotely on the operator's computer and decodes video streams and renders them on the Smart Client workstation using hardware (GPU) accelerated decoding and/or software (CPU) decoding.
	XProtect Web Client	The XProtect Web Client is the client designed for the occasional or remote user that needs easy access to the VMS system, including live monitoring, playback, investigation, export, and light alarm management.
	XProtect Mobile Client	XProtect Mobile provides a flexible way of accessing a XProtect VMS for users on-the-go using smartphones and tablets. The application provides all essential functions for live viewing, playback, and incident management. The application is available for both Android and iOS devices.
	Management Client	The management client is a Windows based client administration interface for all parts of the VMS.

Table 3. Description of key XProtect VMS system components and client applications

Milestone XProtect VMS product variants

Milestone XProtect VMS software is available in five products, each designed to match the needs and requirements for specific market segments:

- XProtect® Essential+

  XProtect Essential+ is a full-featured version of Milestone's market-leading video management software (VMS) at no cost. With support for up to eight cameras and devices, XProtect Essential+ is the perfect match for smaller businesses who want basic video surveillance to protect employees and assets.

- XProtect® Express+

XProtect Express+ is designed for smaller, single-site companies with a light need for live video monitoring. Supporting up to 48 cameras and the ability to integrate with existing operations, such as access control and people counting, XProtect Express+ is the perfect match for retail shops, parking lots or office buildings.

- XProtect® Professional+

  XProtect Professional+ is IP video management software (VMS) designed for mid-sized businesses, supporting an unrestricted number of cameras, devices, and servers. Including multi-layered maps and full alarm management capabilities operators have a complete overview of the entire installation making it the ideal choice for institutions such as schools, retail chains, and production plants.

- XProtect® Expert

  Designed for mid-size and large-scale installations, XProtect Expert ensures end-to-end protection of video integrity while maximizing hardware performance. Central management, access through failover recording servers and an optional video wall make it ideal for installations with active live monitoring such as warehouses and stadiums.

- XProtect® Corporate

  Designed for large scale high security installations, XProtect Corporate ensures end-to-end protection of video integrity while maximizing hardware performance. Central management, built-in video wall and support for failover recording servers make it ideal for mission-critical installations such as airports and cities.

Appendix B – XProtect BYOL CloudFormation Template

The figure below shows the CloudFormation template that is used to orchestrate the default deployment of the XProtect BYOL product.

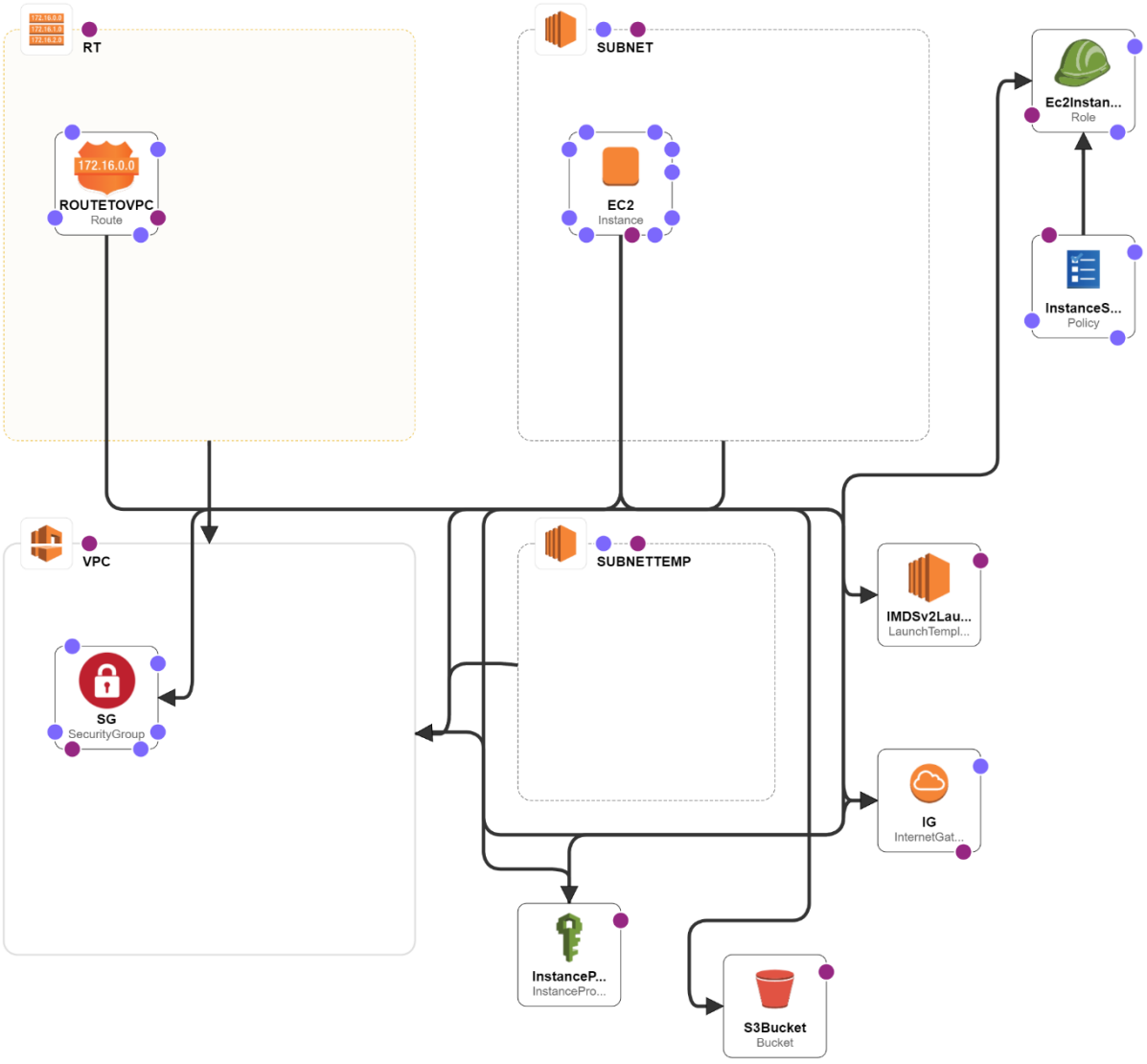


Figure 16. XProtect BYOL CloudFormation Template

Appendix C – EC2 performance

Milestone XProtect VMS is a Windows workload with high to extreme demands on data throughput and compute resources for video decoding. As discussed in the section About XProtect VMS on page 7, XProtect VMS application is made up of different Windows services, where the recording server service is the most critical service to dimension correctly from a compute, network and storage perspective.

The scaling of recording service is constrained by two primary resources:

- Data throughput, which is dependent on the number of connected cameras, the bandwidth of the video streams from these cameras and the degree of recording and archiving.

- Compute resources for decoding of streamed video formats such as H.264, which is needed when applying server-side video motion detection (VMD) analysis. XProtect VMS can utilize GPU resources available with some EC2 instance families.

The recording server performance is also determined by the performance of the storage used for media and archive databases. The throughput and IOPS performance can influence the scaling of the recording server, for more information about storage performance, refer to: Appendix D – Media storage dimensioning, page 53.

In this appendix we discuss Milestones recommendations with regards to EC2 dimensioning.

AWS EC2 recommendations

Leading up to the publication of the XProtect on AWS, Milestone has done extensive large-scale performance testing in differ instance families and instance types, including the t3, m5, m5a, c5, g3s, g4dn and i3 families.

The primary purpose of these tests has been to provide system integrators and end-customers with guidance on which EC2 instance type to deploy the XProtect CloudFormation on. Based on this testing, Milestone recommends the EC2 instance types presented in Table 4 below, when operating with different degrees of recording[5].

[5] Degree of recording refers to how much the VMS system is recording during a day. 10% recording thus corresponsive to 2 hours and 24 minutes recording per day.

INSTANCE TYPE	DEGREE OF RECORDING				RECOMMENDED MAX. AVG.. CPU LOAD
	100%	50%	25%	10%	
t3.large	7	7	8	8	35%
c5.large	16	17	17	18	50%
c5.xlarge	36	38	39	40	50%
c5.2xlarge	92	94	95	96	70%
g4dn.xlarge	97	106	110	113	50%
g4dn.2xlarge	133	242	268	275	70%
g4dn.4xlarge	427	468	480	480	70%

Table 4. Validated maximum cameras per XProtect recording server, for recommended EC2 instance. Measurements are based on H.264 video streams with 1080p resolution and 30 FPS, with a constant throughput of 4,0 Mbps per camera. Server-side VMD[6] is applied on all streams and all recordings are archived to AWS FSx storage.

To help system integrators and end-customers select the most optimal compute-infrastructure for their XProtect deployment Figure 17 presents the price performance ratio for the recommended EC2 instance types listed in Table 4 above. The dark blue line and the gray line lists the annual cost per camera for US East (N. Virginia) and Europe (Ireland), respectively at maximum recommended utilization, at 25% recording, and archiving to AWS FSx storage.

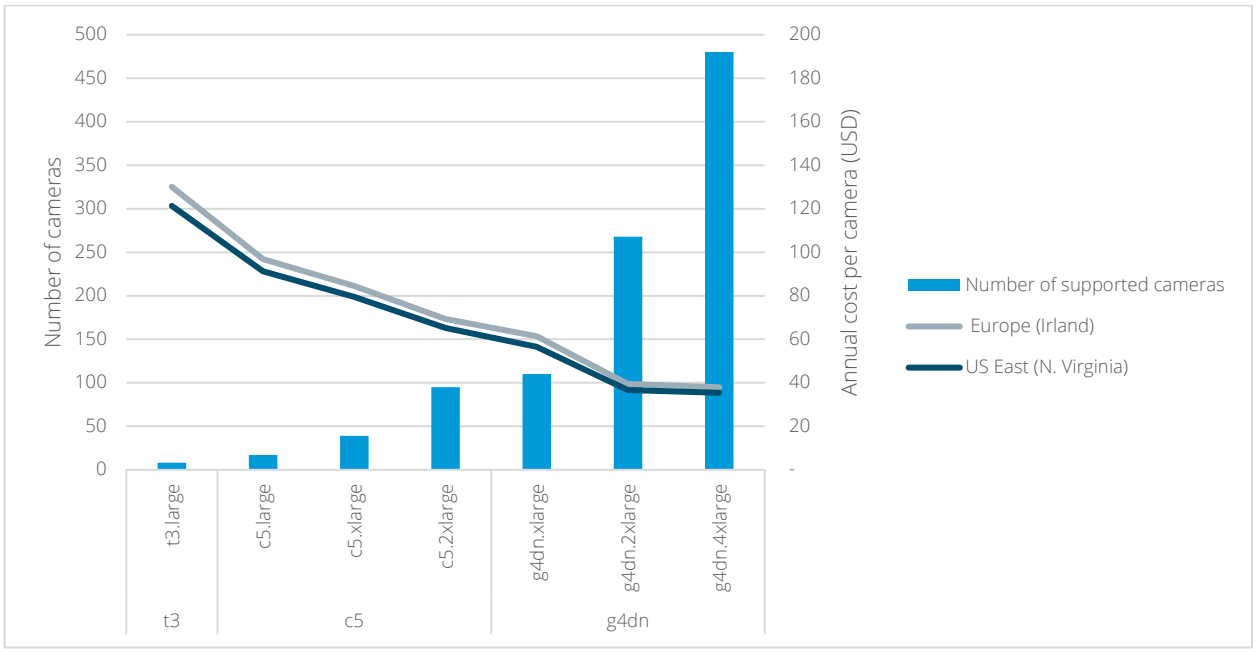


Figure 17. Price-performance ration of recommended EC2 instances for deployments with H.264 video streams with 1080p resolution and 30 FPS, with a constant throughput of 4,0 Mbps per camera. Server-side VMD is applied on all streams, with 25% recording, and archiving to AWS FSx storage.

Impact of Video Motion Detection

[6] Tests results apply to XProtect product variants supporting GPU based video decoding, i.e. XProtect Expert and XProtect Corporate.

Video motion detection conducted on the server-side by the XProtect recording server represents a significant part of the load on the compute resources available on the allocated EC2. The load caused by the VMD decoding and analysis can represent as much as 80% of the overall CPU load on EC2 instances with no GPU resources, or when using XProtect product variants not supporting GPU based decoding (i.e. XProtect Express+ or XProtect Professional+).

Milestone therefore recommends the XProtect Expert or XProtect Corporate VMS product variants and GPU enabled instance EC2 instance types, where the g4dn family has been verified by Milestone.

If no server side VMD is to be applied, smaller and non-GPU enabled EC2 instance types can be considered.

Appendix D – Media storage dimensioning

As discussed earlier in this white paper, the XProtect VMS software works with a tiered storage architecture with a media database for short-term storage and one or more levels of archives for long-term storage. While the media database is defined as SSD EBS storage, Milestone recommends using HDD storage for the FSx storage or S3 (through third party plugins that enable usage of S3 storage as file system structure) to optimize the storage costs for long-term video storage. In case of using Surveillance Bridge from Tiger Surveillance, it is not needed to use Archiving functionality of XProtect, instead you may configure movement of video to other storage types in Surveillance Bridge configuration page in Management Client.

This appendix discusses the high-level design principles for the storage infrastructure used by XProtect when deployed on AWS.

AWS EBS performance aspects

All EC2 instance types recommended by Milestone (see Appendix C – EC2 performance) are EBS–optimized instances that use an optimized configuration stack and provides additional, dedicated capacity for Amazon EBS I/O. This gives optimal performance for the media database and does as such do not require specific design attention. For details about the dedicated bandwidth to AWS EBS, please refer to: https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/ebs-optimized.html.

It is recommended that the media database is configured to hold 24 hours of video storage in the media database.

AWS FSx performance aspects

The FSx file system is defined with a storage size and throughput capacity. As these definitions cannot be changed at a later stage it is important to dimension the FSx correctly. The effective throughput and IOPS of FSx files storage is dependent on both the network throughput and IOPS towards FSx, and the internal disc throughput and IOPS performance, as depicted in Figure 18.

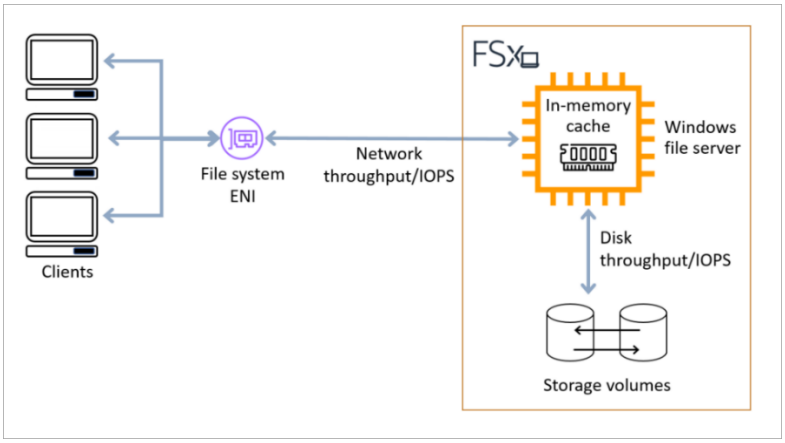


Figure 18. Detailed FSx file storage architecture illustrating the difference between network throughput/IOPS and disk throughput/IOPS

The type and amount of storage capacity impacts the performance of the FSx file system. The FSx storage is defined in steps of 1 GiB with a minimum size of 2 TiB and a maximum size of 64 TiB, where the disk performance for HDD based storage is proportional to the volume size.

PERFORMANCE ASPECT	BASELINE PERFORMANCE
Disk throughput	12 MB/s per TiB of storage
Disk IOPS	12 IOP/s per TiB of storage

Table 5. FSx HDD performance and throughput and IOPS baseline allocation

The graph below illustrates the dependencies between the required FSx storage volume for different retention times (calculated based on the video data volume to be archived), required throughput (yellow line) and required number of IOPS (light blue line), and the allocated disc throughput and IOPS baseline (dark blue line). More specifically this graph represents a deployment with 100 cameras, each generating 4 Mbit/s. The assumption is that the VMS system on average records 10% during a day. This means that the required throughput is 5 MB/s and the required IOPS to write the video data to the FSx disk system is 49 operations per second line.

Given the volume of video data to be archived (5 MB/s) the required storage per retention day is 0,37 TiB (gray area). In this example we assume that the FSx storage definition is fully optimized to match the required storage exactly. Based on the FSx storage definition a disc throughput and IOPS baseline allocation is given, as discussed in Table 5.

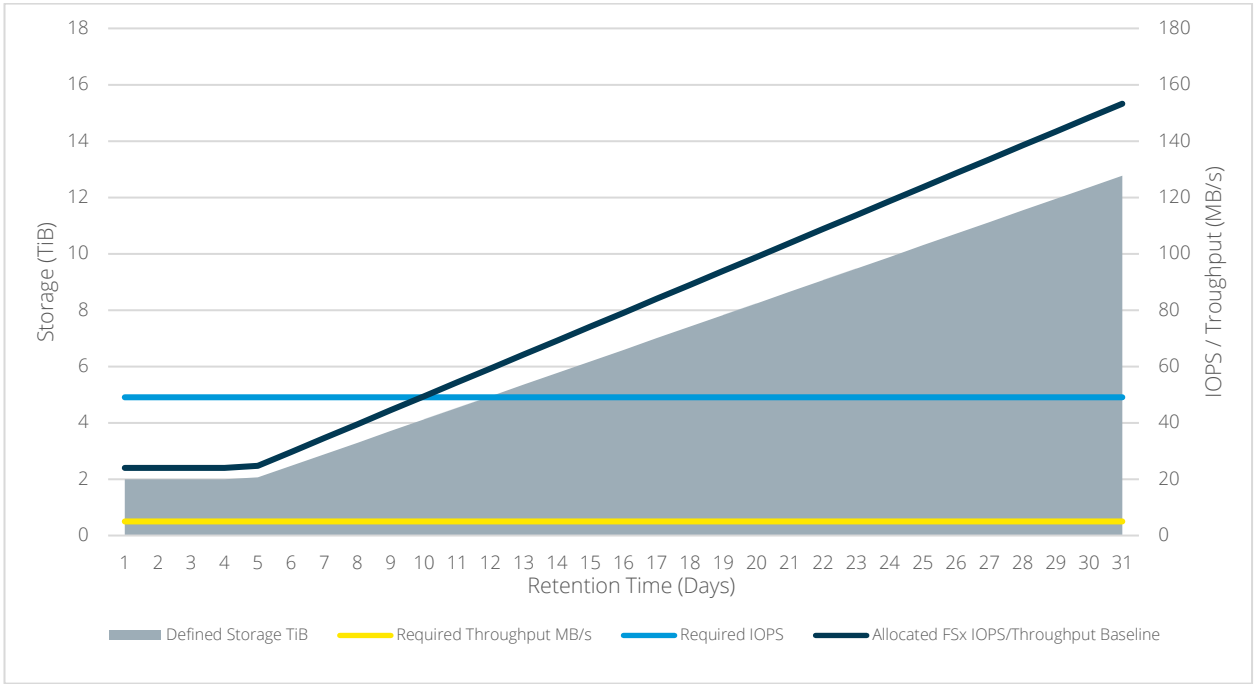


Figure 19. FSx performance at different size definitions, compared with required performance for archiving in a system with 100 cameras generating 4 Mbit/s, with 10% recording

From Figure 19 it can be derived that special care needs to be taken when dimensioning an HDD based FSx file system with short retention times. We can see that the allocated disk IOPS is lower that the required number of disk operations, for FSx storage volumes smaller than 4,12 TiB. This will result in a situation where the media storage on the EBS disc cannot be archived fast enough, which will eventually cause the storage system to overflow where video data will be lost.

To secure a sustained operation in this specific case the FSx storage should in this particular case not be smaller than 4,12 TiB, even for the shorter retention times, to obtain a sufficient IOPS baseline. In a real-life deployment, Milestone of course recommends a reasonable margin on the storage definitions, to not end up with system bottlenecks.

Milestone recommends system integrators and end customers to thoroughly acquaint themselves with the performance dynamics of FSx to ensure correct storage design. For more information refer to: https://docs.aws.amazon.com/fsx/latest/WindowsGuide/performance.html.

AWS S3

Another storage type which is possible to use is S3. S3 is an object type storage and therefore cannot be directly used like a file system that XProtect expects. But there are third party add-ons like Surveillance Bridge from Tiger Surveillance that make it possible to use S3 as medium where video is stored. See appendix.

Appendix E – AppStream 2.0 dimensioning

This appendix covers recommendations and performance related to the selection of EC2 streaming instance types for AppStream Fleets for XProtect Smart Client.

Recommended AWS EC2 instance types

As XProtect Smart Client is a compute and graphic intense application that runs best when utilizing hardware accelerated video decoding, there is only a limited set of EC2 instance types that are relevant for XProtect Smart Client hosting.

Based on extensive performance testing of the various EC2 streaming instance types, Milestone recommends the Graphics G4 family (stream.graphics.g4dn) only. With its native Nvidia Tesla T4 GPU support and reasonable pricing, it supports the Smart Client even in usage situations with views consisting of 50, or more, video streams. Please note that end-customers may need to request access to this EC2 streaming instance family via AWS Support.

Other EC2 streaming instance families are available for AppStream, but not recommended to use with the XProtect Smart Client:

- General purpose, Compute optimized and, Memory optimized instances

  As none of these instance families provides hardware accelerated video decoding, they deliver poor Smart Client performance with few supported simultaneous camera streams.

- Graphics Design instances

  Includes an AMD GPU infrastructure that is not compatible with the XProtect Smart Client.

- Graphics Pro instances

  Although equipped with NVIDIA Tesla M60 graphics cards, current version of XProtect Smart Client is not compatible with the provided Nvidia CUDA platform[7].

[7] Milestone Smart Client requires CUDA version 10.1.

Performance results for EC2 streaming instances

Milestone has done extensive testing of the Smart Client in AppStream, using different user scenarios, with different number of simultaneously displayed camera streams, different resolutions and at different frame rates. These tests are summarized in Figure 20 below. In the testing, Milestone has benchmarked the performance of decoding and rendering 480p, 720p and 1080p H.264 streams at 15 fps and 25 fps respectively.

The smallest instance size in the stream.graphics.g4dn family delivers remarkably good performance, and should be sufficient in most common usage scenarios. With reference to the table the stream.graphics.g4dn.xlarge instance supports decoding and rendering of approximately 49 camera streams at 15 FPS, or 35 streams at 25 FPS. If users view more cameras in a single view, the larger streaming instance types can be considered.

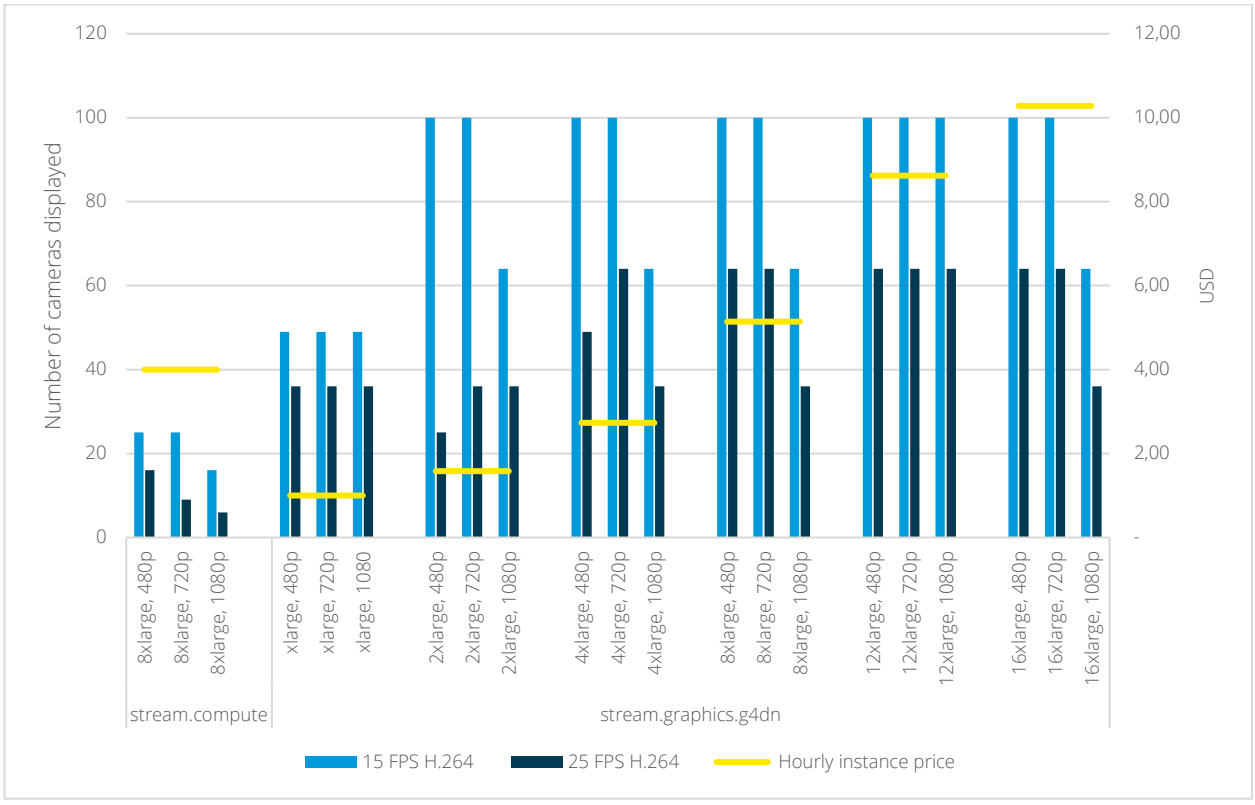


Figure 20. Amazon AppStream 2.0 – Smart Client performance at different user scenarios and different EC2 streaming instances measured on a HD display, and hourly instance price US East (N. Virginia)

Appendix F – Surveillance Bridge from Tiger Surveillance

One of the storage types available in AWS ecosystem is S3. S3 is an object type storage. It does not directly have the file system structure available in file systems like Windows NTFS.

Therefore it cannot be directly used by Milestone XProtect VMS as XProtect expects to write to a file system.

Third party software can be used to facilitiate this and provide a workaround by mapping a file system to S3 storage.

Surveillance Bridge from Tiger Surveillance is an option. Please note that this software requires its own license from Tiger Surveillance. And all the support and help regarding using this software should be sent to Tiger Surveillance directly.

The optional plug-in Surveillance Bridge allows for the extension of EBS storage to S3, resulting in significant cost savings and increased durability of recordings. This feature enables users to leverage the benefits of S3 storage while seamlessly integrating it with their existing Milestone XProtect setup. For long-term retention periods, the plug-in also supports all low-cost S3 Glacier Storage Classes.

You can download Tiger Surveillance information from Milestone Marketplace:

https://www.milestonesys.com/marketplace/tiger-surveillance/surveillance-bridge---xprotect-plug-in/

About Tiger Surveillance

Tiger Surveillance is a software company specializing in seamless data management and data protection for video surveillance. The company is powered by Tiger Technology, an established technology provider of storage, data, user, and media management solutions. The Tiger Surveillance portfolio includes easy-to-deploy software products designed to manage and safeguard surveillance data both on-prem and with any cloud provider.

About Surveillance Bridge for XProtect

Surveillance Bridge is a software-only solution enabling XProtect to utilize S3 low-cost storage classes. For long-term retention periods, data is automatically transitioned to any S3 Glacier tier while maintaining direct access. Organizations can now meet compliance requirements by seamlessly extending data to S3 storage, providing the fastest possible disaster recovery while ensuring the highest data durability.

Enablement of S3 storage

The best way to get started with using S3 storage is through the CloudFormation template that Milestone provides. Milestone provides option to automatically install Surveillance Bridge during the initialization process.

In order to use, you need to refer to Surveillance Bridge user manuals.

You will need two EBS storages, one for Windows and XProtect installations, another one for video data storage. You will not need to use Archiving function of XProtect. Instead for the EBS storage where the media database will be located, Surveillance Bridge will move the files to S3 or other storage classes based on configuration in the Surveillance Bridge software.

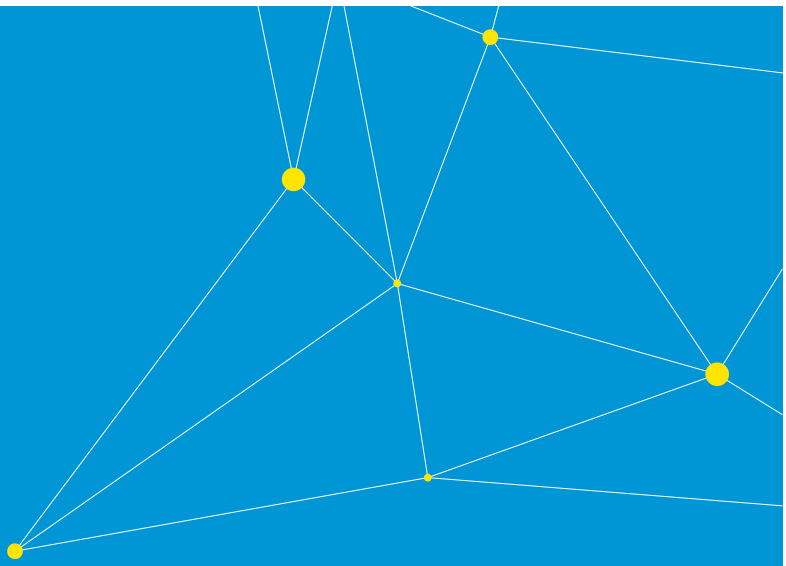
EBS storage for media database needs to be as large as 2-12 hours of media. Please use our calculator in order to dimension properly and calculate the costs. This EBS storage will act as a cache. You need to configure the Surveillance Bridge plugin.

While video data is saved continuously on this EBS storage, in the background it will be moved to S3 storage as configured in the plugin configuration page in Management Client.

If part of video data is requested by XProtect that is not currently in the cache EBS storage, it will be fetched by background service and provided.

It is possible to configure the plugin in such a way that after video data is moved from EBS storage to S3, it gets moved to other storage classes (Glacier, ...).

Please refer to Surveillance Bridge user manual for instructions on how to configure the plugin correctly.



Milestone Systems is a leading provider of open platform video management software; technology that helps the world see how to ensure safety, protect assets and increase business efficiency. Milestone enables an open platform community that drives collaboration and innovation in the development and use of network video technology, with reliable and scalable solutions that are proven in more than 150,000 sites worldwide. Founded in 1998, Milestone is a stand-alone company in the Canon Group.