

CompleteView & PowerProtect Enterprise Considerations

Evaluating platform security, uptime and management capabilities.

Salient Systems Corp.
10801 N. MoPac Exp.
Building 3, Suite 700
Austin, TX 78759
Phone: (512) 617-4800

CompleteView Product Summary

Salient Systems is an acknowledged and trusted manufacturer of video surveillance management systems (VMS). Salient Systems CompleteView VMS software is an open architecture platform providing superior scalability and management tools to support large and geographically distributed installations from a single desktop application.

Salient's CompleteView is a hybrid VMS platform allowing for the widest degree of compatibility with video surveillance technology. CompleteView users can take advantage of everything from existing legacy analog equipment up to the latest camera and access control products. The CompleteView VMS platform can be deployed in a number of ways to maximize video surveillance performance while minimizing costs, such as:

1. *Analog*: Use CompleteView with existing cameras to improve forensic investigations and video system management. Analog cameras can be supported using 3rd party Encoders or using the Salient supplied Generation II PCIe video capture boards, which comes included with the CompleteView software.
2. *Hybrid*: Analog and IP cameras can be used on the same platform simultaneously, co-existing on a CompleteView hybrid network video recorder (NVR). In addition, Salient offers the simplest and most cost effect approach to transitioning from Analog camera technology to IP allowing the user to switch camera technology without incurring additional licensing fees.
3. *IP only*: CompleteView supports the latest IP, HD, Megapixel and panoramic cameras from major camera manufacturers.
4. *Cloud*: CompleteView can also be used as a platform for Video Surveillance as a Service (VSaaS) deployments where CompleteView is deployed on infrastructure hosted in the Cloud and provides easy management, multi-tenancy and access to video and recordings anywhere on a variety of platforms (Web, iPhone, iPad, Android etc.).

CompleteView VMS software can be provided on Salient's PowerProtect line of purpose-built Network Video Recorders (NVRs). PowerProtect NVRs are Windows based PC platform servers purpose built for video surveillance recording. Components are selected for high performance and long lifespan. PowerProtect NVRs offer users the option of obtaining the full recording platform from Salient for a single point of support.

A core value of Salient is 'Easy to work with'. This is reflected in the product interface, where features are simple to access, tasks require a minimum number of actions to complete and the product uses consistent themes, terminology and icons to maximize intuitiveness. Our simple, per-camera only licensing model also reflects this value. CompleteView provides unlimited users, unlimited client and server software deployments and the full product feature set with only the purchase of a license per-camera connected to the system. Our US based support and



training provides quick access to answers on the product, troubleshooting support and full online self-paced eLearning training for users at no cost.

Salient's CompleteView and PowerProtect products are made in the United States.



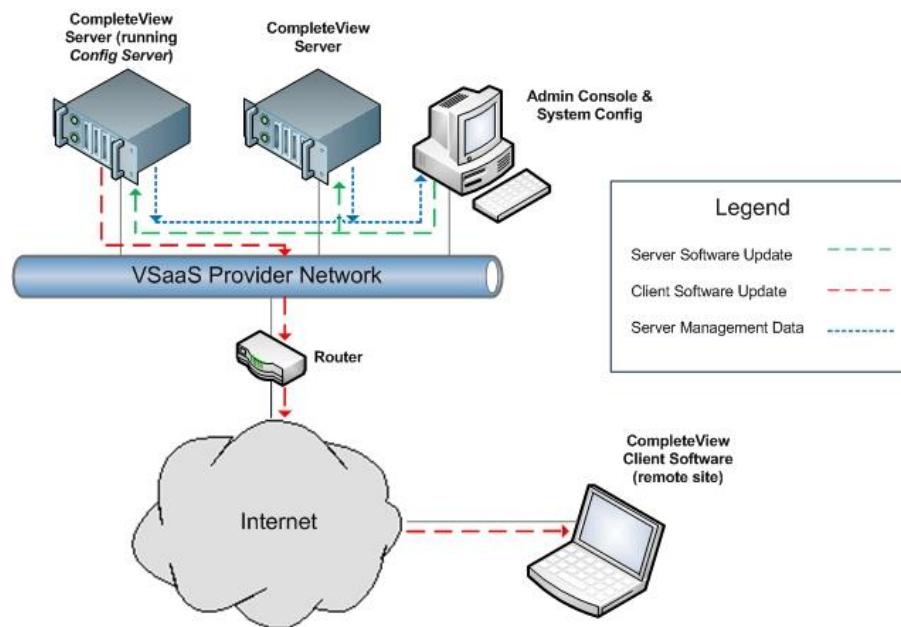
CompleteView Architecture

CompleteView uses a Client / Server application architecture. The server component, CompleteView Server, records video from IP or analog cameras and simultaneously streams live or recorded video to clients. CompleteView also includes a variety of Client applications. Client applications display live video streamed from the CompleteView Server and therefore do not connect directly to cameras.

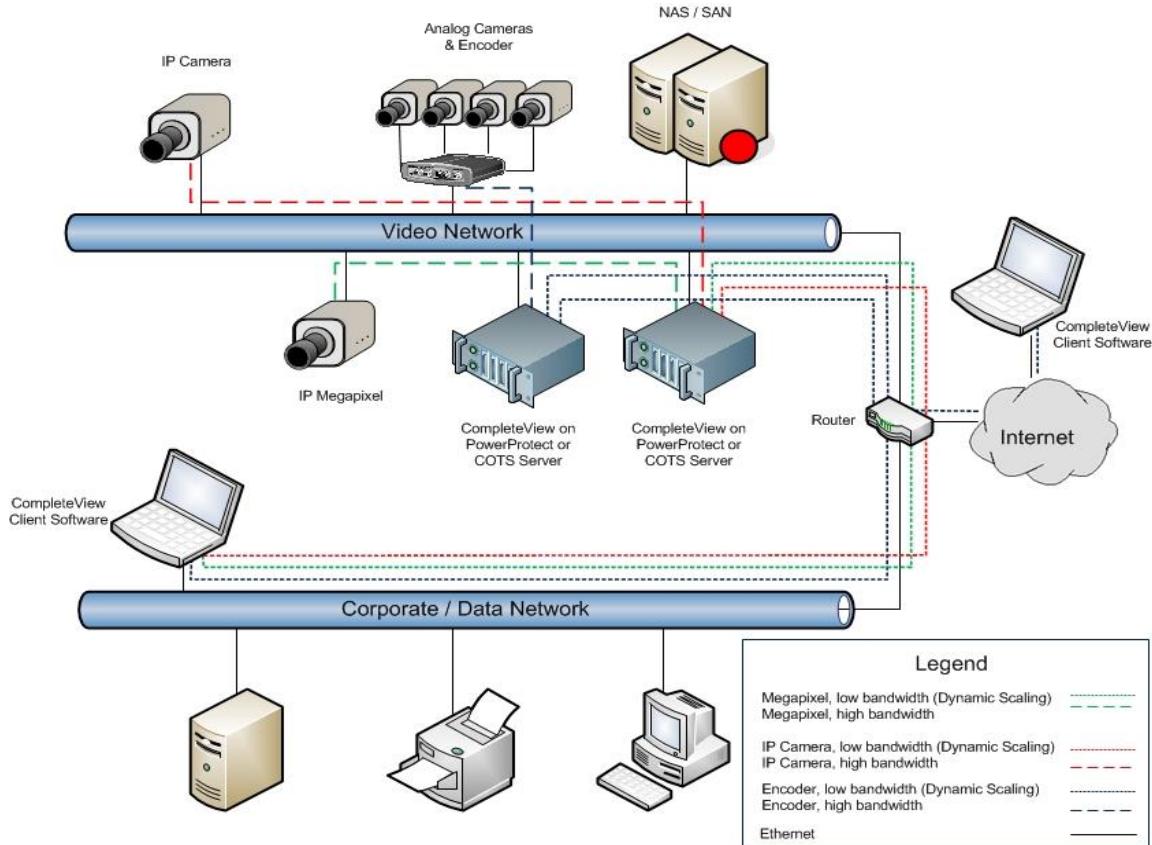
Multiple CompleteView servers have a peer relationship in that no central management server is required. This simplifies deployment and provides for no single point of failure which could cause the system to become inaccessible.

System management is performed with an administrative client application called Admin Console. Admin Console connects directly to CompleteView servers to perform configuration, software updating and to collect system information for reporting.

Updating Servers and Client applications is easily accomplished using Admin Console. To perform a system update an administrator selects all CompleteView servers targeted for the update. Next the administrator chooses the update file provided by Salient which is then transmitted to all selected servers simultaneously. After the servers are updated, the next time a client connects to the server (if configured to do so) the client will check it's version against what the server has installed and automatically download and install the update without any further user or administrator intervention.



The graphic below depicts the typical flow of data in a CompleteView VMS deployment. In this example, high resolution and high bandwidth video is being downloaded to the CompleteView server for recording. Dynamic Resolution Scaling reduces the bandwidth necessary to transmit the video to client viewing stations which are located both on the corporate network and over the Internet. In addition, video from multiple CompleteView servers is being viewed simultaneously on a client workstation.



Flow of video data in CompleteView

CompleteView System Management

System Management is accomplished using the Admin Console, which is the administrative client application in CompleteView. Administrators can deploy Admin Console on any computer with network access to the CompleteView servers being managed. All CompleteView servers or a subset of CompleteView servers can be managed by different Admin Console deployments which allows server management to be easily delegated or centralized.

Admin Console opens with a side-by-side view displaying all currently monitored CompleteView servers in a list with a series of tabs corresponding to monitoring information and administrative functions. Administrators can monitor data points such as:

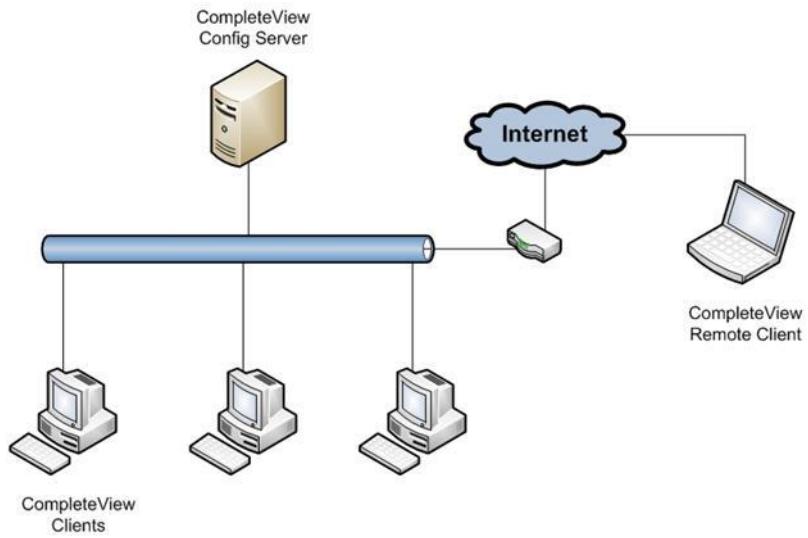
- Currently connected users
- User, camera and system log activity
- Recording volume status and details
- Camera status and details
- View live or recorded video from any camera or recording volume
- System details include CPU, memory usage, installed version, server name and address platform type (32 or 64 bit) and more.
- Server uptime

Administrators can export all or any subset of log events to CSV files.

Admin Console can provide detailed automated email event notification configurable on a per-system basis for events such as server offline, server online, camera offline, camera online and volume offline. Admin Console can also be run as a service so it will automatically restart and begin provide email notification if the Admin Console computer shuts down unexpectedly.

Full server configuration to any server can be accessed and changed remotely using Admin Console. Multiple CompleteView Pro or Enterprise servers can be displayed in Server Configuration at the same time allowing for simultaneous configuration access.

Admin Console also allows for remote and simultaneous server and client software updating. The CompleteView Administrator selects any or all servers configured in their Admin Console view and can deploy a new software version to those servers over the



network. Clients are updated the next time the client connects after checking the client version against the installed server software version. Client updates happen automatically if configured to do so, without user or administrator intervention. This capability allows for a updating all CompleteView servers and Video Clients system wide with a single action.

CompleteView also provides a Configuration Server. The Config Server is a Windows server service that runs alongside the CompleteView recording server service. The Config Server acts as a centralized repository of CompleteView client configuration. When users log in, their configuration can be pulled from a config server. This allows for client to roam to different CompleteView client workstations while maintaining their credentials and user experience. More importantly, the Config Server allows administrators to remotely access client configuration, so changes can be made remotely, over the network.

Finally, CompleteView can manage unlimited amounts of storage from almost any type of storage device. NAS, SAN, DAS and other types of storage are supported.

Storage in CompleteView is configured as a 'volume'. A volume is any folder path or UNC path accessible to the CompleteView server. Multiple 'volumes' in CompleteView can be defined on a single or multiple storage devices allowing for maximum configuration capability.

Administrators can define storage configuration on a volume-by-volume basis, including the amount of storage to use on the volume and the number of days to keep recordings for.

Automated archiving or back of recordings can be scheduled in CompleteView. Recordings on a volume can be scheduled to backup (copy) or archive (move) to a designated backup or archive volume. Administrators can specify whether to backup or archive all recordings or any combination of scheduled, motion or alarm recordings.

Storage complexity is removed from the user. When searching for recorded video the investigator does not need to know where the video is stored or whether it has been archived or backed up. All video managed by CompleteView is always available. CompleteView automatically keeps track of recorded clip locations so investigators and users can focus on security related tasks.

CompleteView & PowerProtect Platform Security Features

CompleteView includes a number of built-in security features including those listed below.

- Support for proprietary or Active Directory or LDAP based account credentials.
- A built in web server with HTTPS/TLS encrypted communications.
- User activity and camera access logging.
- Ability to delete default system accounts
- CompleteView's Video Proxy

PowerProtect Network Video Recorders include the following security features and attributes.

- Windows 7 or Windows Server 2012 R2 are installed and patched to the latest available drivers and Windows updates.
- Windows updates are set to automatically install for internet-connected systems.
- Windows Firewall is enabled and CompleteView application specific ports are opened.

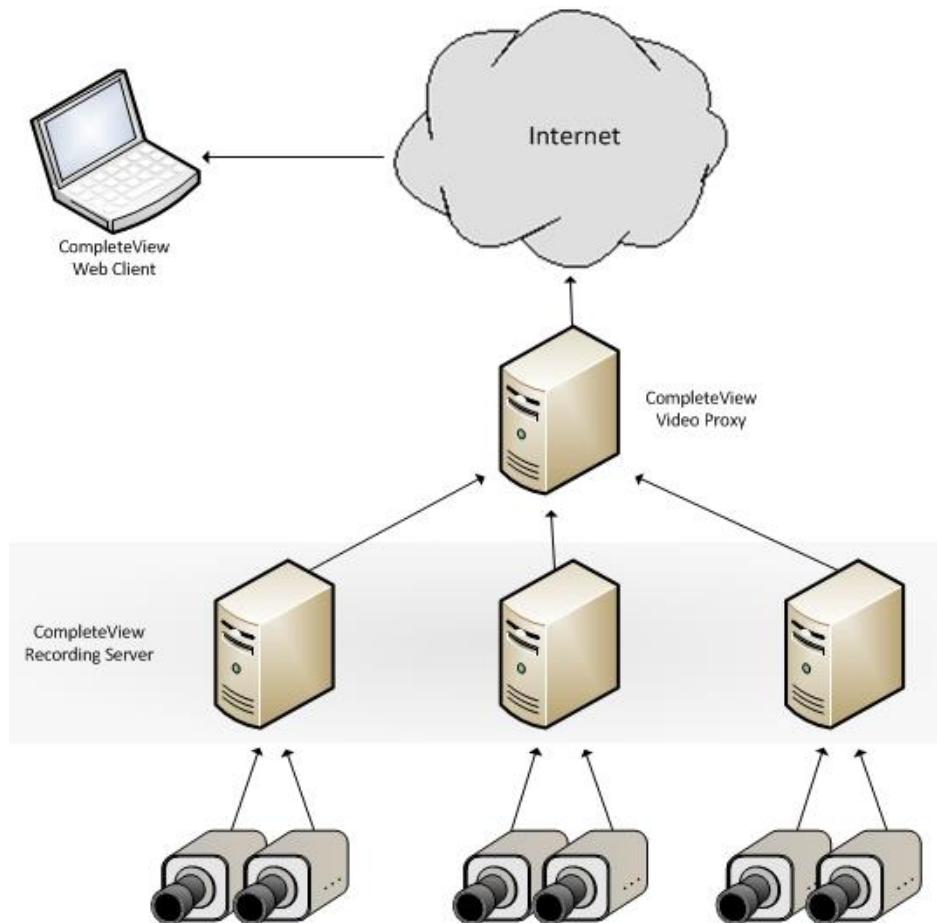
User permissions in CompleteView can be defined according to what cameras can be accessed and the level of access per camera. Individually settable permissions per camera include viewing live video, playback of recorded video, exporting recorded video, taking snapshots, control of camera illumination, control of Pan, Tilt and Zoom camera positions, ability to set or show individual preset positions and PTZ user priority for a camera.

Configuration of user permissions applies to both CompleteView-proprietary users and accounts imported from Active Directory. Active Directory accounts have the added advantage of higher security as a result of process improvements. With the Active Directory integration in CompleteView, typically groups are imported from AD and the groups are assigned camera permissions. Users of the group in AD can log into CompleteView and gain the camera permissions assigned to the AD group. When a user of the group is removed, commonly because someone left the organization, no change needs to be made in CompleteView for the user to be removed whereas with CompleteView proprietary users, the user needs to be manually removed from CompleteView. If this step is missed, a user could continue to have access to the security system even after they should no longer have that access.

Configuration tools in CompleteView can be installed separately from user tools. This aids in further limiting the possibility of unauthorized system configuration because the system configuration tools are not built into the user client software and can therefore be physically installed only on computers intended for system management tasks.

Web Client connections are served from a purpose-built CompleteView-proprietary web server. The web server has limited functionality, limiting potential security vulnerabilities and preventing most known vulnerabilities with common web servers, such as IIS and Apache, from being used on a CompleteView system.

Video Proxy, a component of CompleteView Enterprise, acts as a central connection point for Web Client and TouchView Mobile client connections. Using the Video Proxy, organizations can easily open access to their video surveillance feeds to external organizations. Exposing the Video Proxy for remote video access provides the benefit of not directly exposing CompleteView recording servers. This provides a management benefit as well as a security benefit. From a systems management perspective there are far fewer firewall rules to maintain as compared to exposing multiple CompleteView recording server for remote access, and remote client systems are configured with just the video proxy, so in the event IP or hostname configuration of a CompleteView recording server changes, remote clients do not require reconfiguration so long as the connection details of the Video Proxy remain the same. From a security perspective the Video Proxy does not perform camera recording and does not have configuration or administrative capabilities over CompleteView recording servers. If anything happens to compromise the Video Proxy recording and internal client access should not be affected.



Finally CompleteView's web server and Video Proxy support HTTPS connections and signed certificates. HTTPS connections are TLS encrypted and the server can be authenticated via a signed certificate. A default certificate is installed for users who do not want to obtain a certificate from a CA. The default certificates are generated for the specific system CompleteView is installed on, further enhancing HTTPS security for users who do not use certificates signed by an authority.

Operating System Platform Security

CompleteView is designed to run on Microsoft Windows operating systems. The currently supported operating systems range from Windows 7 up to Windows Server 2012 R2.

The vast majority of professional Video Management Software platforms also run on Windows operating systems, but a small minority provides support for Linux.

Generally, uptime and security are the primary considerations for OS platform selection as it relates to VMS products.

An [analysis by GFI Blog](#) of the NIST National Vulnerability Database for the year 2014, the latest data available at the time of this writing, may serve as an objective reference point when comparing operating system platform security. The chart below, taken from the GFI Blog report, shows the number of vulnerabilities of various OS platforms.

Operating system	# of vulnerabilities	# of HIGH vulnerabilities	# of MEDIUM vulnerabilities	# of LOW vulnerabilities
Apple Mac OS X	147	64	67	16
Apple iOS	127	32	72	23
Linux Kernel	119	24	74	21
Microsoft Windows Server 2008	38	26	12	0
Microsoft Windows 7	36	25	11	0
Microsoft Windows Server 2012	38	24	14	0
Microsoft Windows 8	36	24	12	0
Microsoft Windows 8.1	36	24	12	0
Microsoft Windows Vista	34	23	11	0
Microsoft Windows RT	30	22	8	0

The chart data shows approximately 3x higher quantity of vulnerabilities for Linux Kernel as compared to most Windows platforms. [Data for 2013](#) shows a similar ratio of Linux to Windows vulnerabilities reported.

An analysis of specific Linux distributions for 2014 reveals that a commonly used distribution in the security industry, Ubuntu, also has a similar number of total vulnerabilities at 39 as compared to Windows Server 2012 with 38 or Windows 7 with 36.

CompleteView and PowerProtect systems are installed and used successfully in some of the most controlled network security environments. These deployments include government, large financial institutions and some of the largest telecommunications



providers. Using the security controls available in CompleteView and Windows can provide a robust and highly secured video recording platform.

System Uptime

Several factors affect system uptime. The most common circumstances in a video management platform that cause the system to be down are software updates and recording server reconfiguration.

CompleteView is designed to minimize recording downtime, even for planned maintenance and reconfiguration. CompleteView is designed as a platform for cloud-based video recording and some of the cloud platform attributes used to minimize interruption to multi-tenant systems carry over to the traditionally deployed product.

CompleteView's recording server configuration tools do not require a restart of the recording service for most configuration changes. This means when adding or modifying a camera, user account, storage volume or recording schedule the system recording service will not need to restart and recording occurring with already configured cameras will not be interrupted. This reduces or eliminates the need to have reconfiguration related planned outages for most organizations.

CompleteView's recording server does restart when the software is upgraded to a later version. The restart time varies based on hardware platform and number of connected cameras, however the service startup time is minimized. A [video demonstration](#) of a remote, multi-server software update is available on Salient's YouTube channel showing an upgrade of two servers takes 42 seconds. Software updating should be planned for, however the maintenance window for software updates can be minimized as compared to alternative VMS platforms that do not support a remote and centralized push updating capability.

CompleteView deployed on PowerProtect hardware can be reconfigured to allow for better planning of downtime for Windows updates. The default configuration of PowerProtect systems is set so Windows updates are automatically downloaded and applied but the best practice is to configure for manual updates for those organizations that follow regular system update practices. Setting up manual updates provides the opportunity to plan for update intervals and control which Windows updates are applied to NVRs.

ABOUT SALIENT SYSTEMS

Salient Systems offers network friendly, comprehensive IP and analog video surveillance management systems (VMS) built on open architecture. As the recognized transition leader from analog to digital video, Salient Systems' VMS, CompleteView™, is scalable and provides everything needed to manage a multi-server enterprise from a single desktop. Salient delivers simple and scalable security today...and tomorrow. For more information about Salient Systems and CompleteView, visit www.salientsys.com.

ABOUT THE AUTHOR

Brian Carle is the Director of Product Strategy for Salient Systems Corporation. Prior to Salient he worked as the ADP Program Manager for Axis Communications.

For information about this white paper or CompleteView, email info@salientsys.com.

Salient Systems

10801 N. MoPac Expy.
Building 3, Suite 700
Austin, TX 78759
512.617.4800
512.617.4801 Fax
www.salientsys.com



©2012 Salient Systems Corporation. Company and product names mentioned are registered trademarks of their respective owners.