A CheckVideo Technical White Paper

How Secure is Your Video Security System ?

Over the past decade, video security systems have migrated from older analog technology to IP cameras that are connected to the enterprise network. These cameras are used for security investigations, loss prevention and increasingly for operational insights. Consequently, the number of cameras on the network continues to grow at a rapid pace.

With this proliferation of cameras, often across multiple floors, buildings, or cities, the video network can include a variety of devices such as cameras, recorders, servers and viewing PCs. These devices bring assortment of embedded firmware, operating systems, databases and web servers to the network. This presents a significant challenge to securing the network, while allowing seamless and ready access to authorized users who increasingly prefer to access video from their mobile devices.

Best practices that are commonly used to secure IT assets such as PCs, printers and network endpoints certainly apply to video devices as well, but present their own unique challenges. We cover the three most common challenges and methods to overcome them.

1. **Authorization and Credential Management**

   Authorization and credential management in enterprises is typically done using Active Directory, LDAP or similar protocols. Access to file shares, network resources and PCs are controlled by a user's authorization level which can be configured centrally. These credentials are unique to a user, and authorization can be granted, modified or changed for multiple devices without having to log into each device.

   IP video cameras have an embedded web server and cameras ship with the web server enabled with a default login and password. Typical enterprise video deployments use video management software (VMS) that manages these cameras and user credentials. The VMS connects to the camera's web server using each camera's credentials.

   The expectation is that legitimate users of the video system log into the VMS server to access cameras. Unfortunately, the web server on the camera is still available for someone that wanted to bypass server authorization. With tens or hundreds of cameras on the network, it is typical to have the same credentials for "root" or superuser access, because it is too cumbersome to manage it otherwise.

Furthermore, these camera credentials are never changed for the life of the camera, which could easily exceed 5 years. This creates a vulnerability that can be easily exploited to gain access to the camera or worse, use the camera as a host or vector.

CheckVideo cameras do not include a login and password for every camera. In fact, there is no way to log into a CheckVideo device. All authorization and credential management is done through the CheckVideo VMS that truly acts as an agent to grant access to a camera. It brings centralized management without compromising security.

2. **Upgrades and security patches**

While servers and PCs are routinely updated with newer release or hotfixes and patched to address vulnerabilities, IP cameras are rarely, if ever updated in practice. Every IP camera runs firmware that can be updated through the camera's configuration pages. This can get quite cumbersome to deploy manually across multiple cameras.

As part of CheckVideo's managed service, software updates and patches are automatically pushed to cameras and servers with zero touch. This ensures that the latest firmware is available as soon as it is released, and any new vulnerabilities that are discovered are patched immediately. This is done in a manner that preserves all settings and minimizes downtime to ensure that no mission-critical video is lost.

3. Federated Management

It is common to have cameras in remote areas of a property that are not directly connected into the main management server. Branch offices and locations may have a few cameras each which can total tens of cameras across all branches. These offices typically do not have staff dedicated to maintaining servers.

Enterprise video systems also have multiple users that require access to different groups of cameras. For instance, department managers may require access to specific but not cameras across multiple offices, e.g. the IT room cameras or parking lot cameras. The local manager generally needs access to all cameras at their location.

Often, such usage requires users to log into the server at a remote site to view cameras from that site. This creates an additional task to propagate user authorization and credentials to each server and keep it current as user roles change or as staff arrive or leave.

Some systems also require per-user licensing with a limit of users per server with the base license. That encourages generic (not user specific) logins and shared passwords, which is a risk it itself.

CheckVideo does not use site servers. It is a federated system that allows unlimited users with no per-user license fees. Management of user credentials is centralized through a web-based administration tool. Users can be allowed arbitrary access to cameras across sites and this access can be modified or revoked from a central location.

Historically, one way to mitigate and address these challenges has been to lock down the camera network, and only allow access to cameras from specific PCs or named IP addresses. In today's distributed and mobile world, that is a severe limitation, which greatly restricts the full potential of an expensive investment. Furthermore, in the event of an emergency, it is unlikely that the viewing PC is accessible because the site may be in lockdown. Video is most often used forensically for investigations of incidents or break-ins. Having access to the video system minutes after an incident is reported almost makes it necessary to provide the flexibility to view it *securely* from a mobile device or from a remote location. The good news is that security does not have to come at the expense of flexibility. With CheckVideo managed solutions, you can rest assured that the video network is secured, and will stay secure with no extra effort required!