12 Security Camera System Best Practices – Cyber Safe

Technical White Paper

Introduction

Security camera systems are increasingly Internet connected, driven in great part by customer demand for remote video access. The systems range from cloud-managed surveillance systems, traditional DVR/VMS/NVRs connected to the Internet, and traditional systems connected to a local network which in turn is connected to the Internet.

With cyber-attacks accelerating, physical security integrators and internal support staff must keep up-to-date on cyber security attack vectors which can impact the camera video management systems they sell and/or support. These systems require the same level of protection from cyber security vulnerabilities given to traditional IT systems.

This white paper focuses on the best practices for Internet-connected security camera systems. Many of these practices may be also applied to other physical security systems.

Table of Contents

1. Physical Security a Dangerous Door for Cyber Attacks

Security Camera Systems are increasingly Internet connected, driven by the desire for remote access and control, integration, and drastically reduced cloud storage costs.

In addition to the growing number of cloud-managed surveillance systems, most traditional security camera system are connected to the Internet for remote access, support, and maintenance, or they are connected to the local network which in turn is connected to the Internet.

In parallel, cyber-attacks continue to escalate. Reading about millions of breaches in the news headlines are becoming commonplace. Liabilities for damages are great risk to companies.

Thus, it is critical that security camera systems get the same level of attention to, and protection from, cyber security vulnerabilities that is given to traditional IT systems.

Physical security integrators, and internal support staff must to keep up-to-date on cyber security attack vectors which can impact the camera video management systems they sell and /or support.

This white paper focuses on the best practices for Internet-connected security camera systems. Many of these practices can also be applied to other security camera systems.

2. Major Attack Vectors for Security Camera Systems

Five major cyber-attack vectors for surveillance camera systems are:

1. Windows OS
2. Linux OS
3. DVRs, NVRs, VMS
4. Endpoints (Cameras)
5. Firewall Ports

We will discuss these attack vectors in context of applicable best practices which can be destroyed to protect your surveillance system against them.

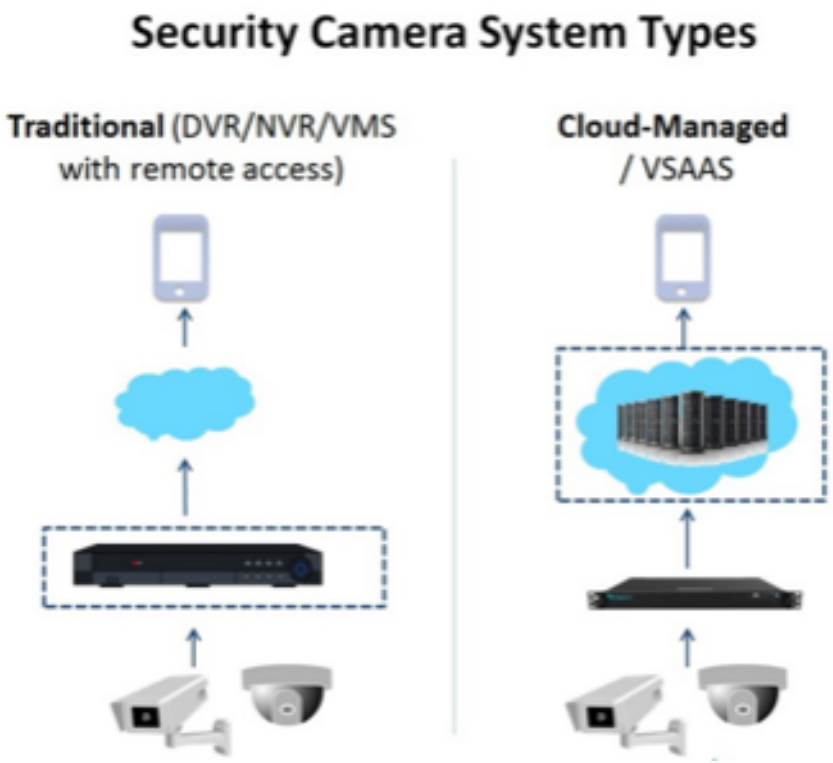
3. Best Practices Differ Based on Surveillance System Type

The terms ‘cloud video surveillance’ and ‘cloud system’ are used inconsistently. Thus, it is important to check with your provider to see exactly how they achieve Internet access, as it will impact which steps you must take to ensure your system is secure.

For purposes of this white paper, I will distinguish between system types as follows:

- Traditional System: a DVR, NVR, or VMS with an Internet connection, typically for the purpose of remote video access.
- Cloud-Managed System: (aka VSaaS) with a cloud-managed system, though there may be an onsite device, the video is recording and managed from the cloud.

There are differences within each of these categories that impact features and functions, however, this top-level distinction will offer clarity in how you can apply cyber security best practices, as well as what questions to ask your provider.



4.1 Cyber-Safe Best Practices for Security Camera Systems

Vulnerability

It is estimated that 1 in 5 web users still use easy-to-hack passwords. Below are the top 10 passwords of 2018, according to Splash Data:

1. 123456
2. password
3. 123456789
4. 12345678
5. 12345
6. 111111
7. 1234567
8. sunshine
9. qwerty
10. iloveyou

Almost all cameras sold today have a web-based graphical user interface (GUI), and come with a default username and password which is published on the Internet.

Some installers don't change the password at all and leave the same default password for all cameras.

Very few cameras have a way to disable the GUI, so the security vulnerability is that someone can attempt to hack into the camera via the web GUI to guess a password.

The hacker must have network access to do this, but the cameras are often on a shared network, not a physically separate network or VLAN.

Best Practice

Both: Traditional System & Cloud-Managed System

The ideal best practice is to assign a unique, long, non-obvious password for each camera. Such a meticulous process takes time to set up, is more difficult to administer, and very hard to track. Therefore, many installers unfortunately use a single password for all cameras in an account.

To allow for this challenge, an acceptable best practice is:

- Public Network: Different strong password for each camera
- VLAN or Physical Private Network: have the same strong password for all cameras

4.2 Port Forwarding

Vulnerability

Most end users now demand and expect video access from remote mobile devices.

This feature is normally delivered by exposing the DVR, NVR, or VMS to the Internet in some way.

This typical exposure to the Internet of an HTTP server is extremely dangerous, as there are a large number of malicious exploits that can be used to obtain access. Machines open to the Internet are typically scanned more than 10,000 times a day.

One example of this vulnerability was the Heartbleed OpenSSL exploit in 2014; many manufacturers had to ask users to reset their passwords.

Best Practice

Traditional System

Ideally, do NOT connect your unprotected server to the Internet. If you do expose your system to the Internet, then “port forward” as few ports as possible and utilize a next generation firewall which analyzes the protocol and blocks incorrect protocols sent over the wrong port. In an ideal situation, also deploy an IDS/IPS for further protection.

Cloud-Managed System

The more secure cloud-based systems do not have port forwarding, so no vulnerability exists, and no incremental protection action is required. Ask your integrator or provider to verify this for any system you own or a\considering acquiring.

4.3 Firewalls

Vulnerability

As stated above, any on-premise DVR/NVR/VMS should have a firewall for protection, especially if you are going to expose it to the Internet for any type of remote access.

Firewalls can be very complex, with thousands of rules. The next generation firewalls are even more complex because they analyze the protocols going over the ports and verify that proper protocols are being used.

Best Practice

Traditional System

It is best to assign a professional network security expert to verify and configure a modern firewall.

It is crucial to have clear documentation on the firewall configuration, and regularly monitor and implement any necessary changes to the firewall configuration.

Cloud-Managed System

For a cloud-based solution without port forwarding, an on-site firewall configuration is not needed. Speak with your integrator or system manufacturer to confirm this.

4.4 Network Topology

Vulnerability

Mixing the cameras on a standard network without separation is a recipe for disaster.

If your security camera system is connected to your main network, you are creating a doorway for hackers to enter your main network via your surveillance system, or to enter your physical security system through your main network.

Some DVRs can even be shipped with a virus.

Best Practice

Both: Traditional System & Cloud-Based System

Ideally, place the security camera system on a physically separate network from the rest of your network.

If you are integrating with a sophisticated IT environment, it is not always possible to separate the two systems physically. In this event, you should use VLAN.

4.5 Operating Systems

Vulnerability

Your on-premise VMS, DVR, NVR or recording system will all have an operating system. The cameras all have an operating system.

All operating systems have vulnerabilities, both Windows-based and Linux-based.

Window OS vulnerabilities are so well-accepted that IT teams monitor them regularly. Recently it has become more and more apparent that Linux has many vulnerabilities also, such as Shellshock (2014) and Ghost (2015), which made millions of systems vulnerable.

In theory, your system manufacturer would have a high-quality security team that is responsive in providing you with security updates. The reality is that many vendors don't do this on a predictable basis.

Best Practice

Traditional System

To ensure your system and network are protected from malicious exploits, you should track and monitor known operating system vulnerabilities, and then make sure that your OS is up-to-date with all the security patches.

If it's a Windows-based system, there are a lot of vulnerabilities and a lot of updates need to be applied. And though they are less frequent, Linux vulnerabilities must also be tracked and addressed quickly.

IT security professionals typically understand which ones are relevant and which ones you can skip, but this can be an extremely daunting task without the proper training and experience.

You can also proactively contact your DVR/NVR vendor to find out which OS your NVR/DVR is using (Linux, Windows) and also the OS versions and the versions of the additional modules that sit on the OS (e.g. Microsoft IIS webpage server) so you can understand which security vulnerabilities will impact you.

Then track vulnerabilities to that OS and contact your OS vendor to see what patches are needed.

The best practices for a VMS is to make sure that the machines are under the domain of the IT department and that the IT department has the responsibilities and staff assigned to do the proper patching, upgrading, modifications, and has processes in place to make sure the machines are secure.

Also, make sure your camera vendor is patching for security issues, and that you are upgrading your camera firmware as soon as new versions are available.

Cloud-Managed System

Best practice here is to inquire with your integrator or cloud vendor if the cloud vendor has a dedicated, experienced security team which monitors vulnerabilities.

Also confirm whether the cloud vendor will automatically send security patches/updates through the cloud to any on-premise appliance. If so, no action is required from the end user to do operating system security monitoring, patching, or upgrading.

4.6 Operating System Passwords

Vulnerability

As with camera passwords, a weak system password can create an opportunity for cyber-attacks on the surveillance system and the network.

Unfortunately, in many OS environments, the root password or the administrator password is shared among all the admins, spreading the security ris. Empllyee turnover, either through attrition or a change of roles can create unexpected security holes.

Best Practice

Traditional System

Set high quality, long passwords for the operating system.

Additionally, establish policies and procedures for changing passwords. For example, the root admin password should be changed every time an employee with password access leaves the company or changes roles.

Cloud-Managed System

No action required. True cloud systems do not have separate passwords for OS access. They only have system passwords which are for individual accounts (see below) which are explicitly deleted when employees leave or their roles change.

4.7 Video Surveillance System Passwords

Vulnerability

Unauthorized access to your security camera system leaves both the surveillance system and network connected to it vulnerable.

Best Practice

Both: Traditional System & Cloud-Managed System

Change your surveillance system passwords on a schedule. Enforce security quality with the same stringency as your company standard. Long, strong passwords are best.

4.8 Connection Encryption

Vulnerability

A surprising number of DVR/NVR/VMSs use connections which are not encrypted with SSL or equivalent.

This risk would be identical to logging into a bank or doing online shopping without https. It creates password vulnerability and allows potential for privacy and eavesdropping breaches.

Best Practice

Traditional System

It is imperative that the connection be encrypted with SSL or equivalent.

Ask your vendor how they handle this. Only choose vendors who encrypt their connections.

Cloud-Managed System

It is imperative that the connection be encrypted with SSL or equivalent.

Many cloud vendors provide connection encryption, but it is variable. Confirm with your cloud vendor how their system handles this.

4.9 Video Encryption

Vulnerability

In addition to insecure connections due to lack of encryption, the same privacy risks apply when the video is not encrypted when stored on the disk or in transit.

Best Practice

Both: Traditional System & Cloud-Based System

For a truly secure system, the video should be encrypted, both when it is stored on disk and when it is in transit.

4.10 Mobile Access

Vulnerability

Password, account deletion and encryption vulnerabilities apply doubly to mobile.

Best Practice

Both: Traditional System & Cloud-Based System

Just as when you run the application on your personal computer, ensure that you have an encrypted connection for the mobile application on the iPhone or Android to the VMS or NVR/DVR.

Set high quality passwords and do password enforcement and account deletion when staff changes.

4.11 Physical Access to Equipment & Storage

Vulnerability

The financial rewards for stealing company data are sufficiently high enough that intruders will also seek to access your network by directly hacking into your onsite physical equipment.

Best Practice

Traditional System

Keep secure: your cabinets; the cables; and the room where the DVR/NVR/VMS, switches and video storage servers are located. Provide secure access control to the room, including video security to monitor it. This practice not only protects your network, but prevents ‘smash and dash’ thefts at your facilities, where the recording DVR/NVR is stolen along with any other items.

Cloud-Managed System

Although the same principles clearly apply to a cloud-based system, there is much less on-premise equipment to protect. The immediate cloud recording also protects against smash and dash theft of the on-site recording.

It is important to inquire of your integrator or vendor what general security measures they take for their cloud servers.

4.12 Video Recording Software

Vulnerability

Video Management Software use a lot of components beyond the operating system, such as Microsoft database applications. As with the operating system itself, these components must be upgraded and secure.

Many VMS's, for example, use Microsoft Access, libraries, as well as the software they have written. New system vulnerabilities can be introduced if the supporting software is not kept up-to-date, including security patches.

If you are passive here, you are highly dependent on the provider sending patches for you to update the system for such vulnerabilities.

Best Practice

Traditional System

Ask you VMS vendor about their policy for keeping the components they use up-to-date and secure. Check for and install regular updates. Be proactive in monitoring the known security vulnerabilities in the industry and contact your integrator or vendor when you learn of new breaches.

It is important to make sure the VMS vendor has a team focused on this an dis sending you updates regularly.

Cloud-Managed System

True cloud managed systems do not have software on-site, so no vulnerability exists here.

However, it is very important to confirm if the system is truly 'cloud-managed' versus Internet-connected before making this assumption, or you risk exposure to a potential vulnerability.

5.0 Video Surveillance Cyber Best Practice Reference Matrix

Below is a summary matrix of the best practices I have discussed. This can be used as a quick reference starting point for your combined end-user, security integrator and system manufacturer security team.

Vulnerability	Best Practice	Best Practice
System Type Description	Traditional System	Cloud-Managed System
1. Camera Passwords	Ideal - Unique long password for each camera. Acceptable - Public Network: Different strong password for each camera VLAN or Physical Private Network: have the same strong password for all cameras.	
2. Port Forwarding	Ideal – Do NOT connect your unprotected server to the Internet. If you do expose system to the Internet, then “Port Forward” as few orts as possible & utilize next gen firewall.	A secure cloud-based system does not have port forwarding, so no vulnerability exists, and no special protection action is required. Verify with integrator or vendor.
3. Firewalls	Assign network security expert to configure & verify a modern firewall. Have clear documentation on firewall configuration. Regularly monitor & implement needed changes to firewall configuration.	For cloud-managed systems without port forwarding, an on-site firewall configuration is not needed. Verify with integrator or vendor.
4. Network Topology	Ideal – Place security camera system on physically separate network from the rest of network. Acceptable – If not possible to separate the systems physically, use a VLAN.	
5. Operating Systems	DVR/NVR – Contact vendor to find out which OS & versions & modules your NVR/DVR is using (e.g. Linux, Windows). Track & monitor know OS vulnerabilities, update OS with security patches. VMS – Have IT department monitor VMS to ensure proper patching, upgrading, modifications, process. Camera – Contact camera vendor to ensure they are doing ongoing security patching;	Ask if cloud vendor has dedicated security team that monitors vulnerabilities and automatically send security patches/updates through the cloud to any on-premise appliance. If yes, no action required from end user.

	upgrade camera firmware for new versions.	
6. Operating System Passwords	Set high quality, long OS passwords. Establish policies & procedures for changing passwords. (e.g. change root admin password every time an employee with password access leaves company or changes roles.	No action required. The cloud does not have separate passwords for OS access, but only VMS system passwords (see below), which are for individual accounts, which are explicitly deleted when employees leave or their roles change.
7. Video Surveillance System Passwords	Change your security camera system passwords on a schedule. Enforce with same stringency as your company standard. Long, strong passwords.	
8. Connection Encryption	Ask your vendor how they handle this. Only choose vendors who encrypt their connections.	Confirm with your cloud vendor how their system handles this. Many cloud vendors offer connection encryption, but it is variable. Only choose vendors who encrypt their connections.
9. Video Encryption	For a truly secure system, the video should be encrypted, both when it is stored on disk and when it is in transit.	
10. Mobile Access	Ensure that you have an encrypted connection for the mobile application. Set high quality password; do password enforcement & account deletion when staff changes.	
11. Physical Access to Equipment & Storage	Keep secure: your cabinets; the cables; and the room housing the DR/NVR/VMS, switches, & video storage servers. Provide secure access control to room, including video security monitoring. This practice not only protects your network, but prevents 'smash and dahs' thefts on the facilities, where the recording DVR/NVR is stolen along with any other items.	The same principal applies to a cloud-based system; however, there is much less on-site equipment to protect. The immediate loud recording also protects against smash and dash theft of the on-site recording. Ask your integrator or cloud vendor what general security measures they gave for their cloud servers.
12. Video Recording Software	Ask VMS vendor about their policy and their designated resources for keeping their software components up-to-date and secure. Check for and	True cloud-managed systems do not have software onsite, so no vulnerability exists here, and no action is needed.

	install regular updates. Be directly proactive in monitoring the known security vulnerabilities. Contac t your integrator or vendor when you learn of new breaches.	However, it is very important to confirm if the system is truly 'cloud-managed' vs. 'Internet-connected' before making this assumption, or you risk leaving a potential vulnerability.

6.0 Conclusion – Video Surveillance Cyber Best Practice Reference Mix

Data breaches continue to accelerate throughout the world. With increasing Internet connectivity, physical security systems are very vulnerable to cyber-attacks, both as direct attacks and as an entrance to the rest of the network. Liabilities for these attacks are still being defined.

To maximize your cyber security, it is critical to define best practices for your own company, as part of your security camera system assessment, as well as its deployment and maintenance.

It is prudent to protect your company and your customers through preventative measures.

About Dean Drako, CEO of Eagle Eye Networks

Dean left Barracuda Networks in 2012 to form Eagle Eye Networks, delivering the first on-demand cloud-based security and business intelligence video management system (VMS) providing both cloud and on-premise recording.

Prior to Eagle Eye Networks, Dean was founder, President and CEO of Barracuda Networks, where he developed the IT security industry's first spam filter appliance. From Barracuda's inception in 2003 through 2012, Drako grew the company to be an IT security industry leader for mid-market businesses, with more than $200 million in annual sales, and 150,000 customers. Barracuda Networks completed its IPO in 2013. In 2007, Drako won the Ernst and Young Northern California Entrepreneur of the Year. Goldman Sachs named Dean as one of the "100 Most Intriguing Entrepreneurs of 2014."

Dean received his BSEE from the University of Michigan, Ann Arbor, and an MSEE from the University of California at Berkeley.