OPTIVIEW

How to create a more secure Security System

Cybersecurity is more than just a buzzword: it's something that pertains to every device that is connected to the internet. IP-based video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations from Optiview on how to create a more secure security system.

1. Update Firmware.
   Keep your NVR, DVR, and IP camera firmware up-to-date to ensure the system is current with the latest security patches and fixes.
2. Change Passwords and Use Strong Passwords. This should go without saying, but the number one reason a system gets "hacked" is due to weak or default passwords. Optiview recommend never using a default password and choosing a strong password whenever possible. A strong password is at least 8 characters and is made up of a combination of special characters, numbers, and upper- and lower-case letters.
3. Change Passwords Regularly. Regularly change the credentials to your devices to help ensure that only authorized users are able to access the system.
4. Disable UPNP. UPNP will automatically try to forward ports in your router or modem. Normally this would be a good thing. However, if your system automatically forwards the ports, and you leave the credentials defaulted, you may end up with unwanted visitors. By default, UPNP is disabled on our DVR and NVR.
5. Disable P2P, if you are not using the feature. P2P is used to remotely access a system via a serial number. The possibility of someone hacking into your system using P2P is highly unlikely because the system's user name, password, and serial number are also required
6. Disable SNMP. If you are not using the SNMP with your DVR or NVR, disable the feature. By default, this setting is already disable on all our DVR and NVR. If you are using SNMP, you should do so temporarily while tracing and testing only but disable it as soon as you are finished.
7. Enable HTTPS/SSL. This will require you to create an encrypted digital server certificate at the DVR/NVR and download/install CA Root certificate on your client computer that will need to view your security appliance, DVR and NVR.
8. Change ONVIF Password. On older IP Camera firmware, the ONVIF password does not change when you change the system's credentials. You will need to either update the camera's firmware to the latest revision or manually change the ONVIF password.
9. Enable IP Filter. This feature allows you to create a list of specific trusted IP address allowed to access your security system.

   Note:

   - If you enabled trusted sites, only the IP in the trusted sites list can access the device.
   - If you enabled blocked sites, the IP in the blocked sites cannot access the device.
   - System supports add MAC address.

10. Change the factory default HTTP and TCP ports. The two ports used by the DVR and NVR has already been changed by Optiview from its factory default port numbers. These ports can be changed to any set of numbers between 1025-65535. Avoiding the default ports reduces the risk of outsiders being able to guess which ports you are using.

11. Check the Log. If you suspect that someone has gained unauthorized access to your system, you can check the system log. The system log will show you which IP addresses were used to login to your system and what was accessed.
12. Disable Auto-Login on Optiview Video Management Software. If you are using Optiview VMS to view your system and you are on a computer that is used by multiple people, make sure auto-login is disabled. This adds a layer of security to prevent users without the appropriate credentials from accessing the system.
13. Isolate NVR and IP Camera Network. The network your NVR and IP camera resides on should not be the same network as your public computer network. This will prevent any visitors or unwanted guests from getting access to the same network the security system needs in order to function properly.
14. Implement limited rights and permissions on surveillance account. If your system is set up for multiple users, ensure that each user only has rights to features and functions they need to use to perform their job.

Optiview takes security on their surveillance equipment seriously. Just to provide an overview of its security model, below are graphic presentation of the security model used for Optiview DVR and NVR systems.

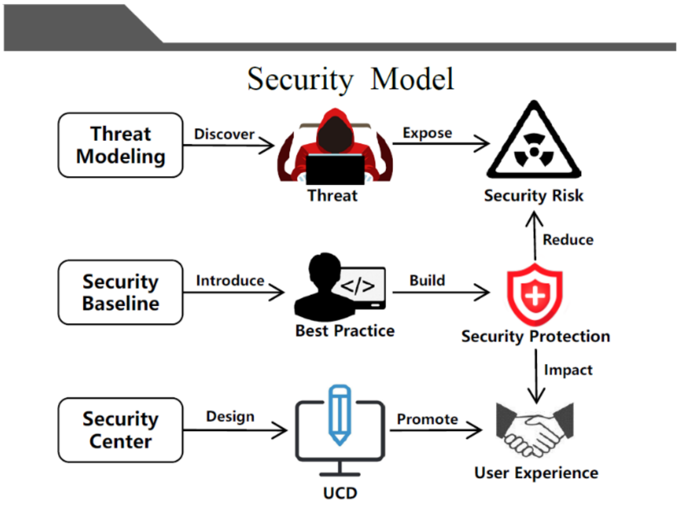
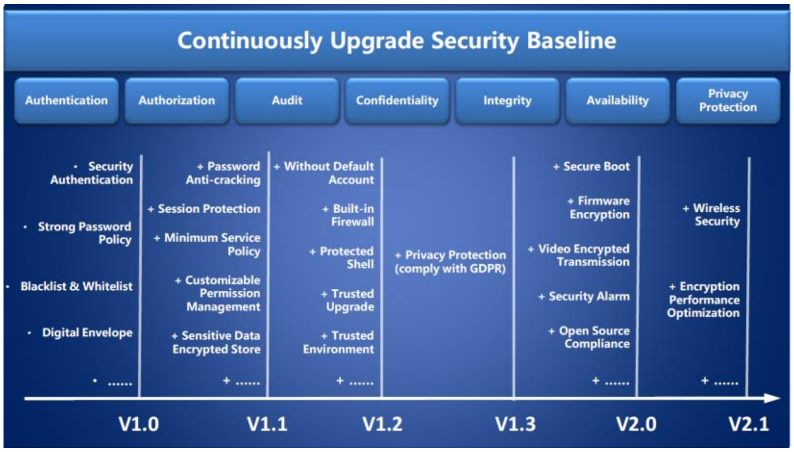


Figure 2-1 Product Security Model



Continuously Upgrade Security Baseline

Authentication | Authorization | Audit | Confidentiality | Integrity | Availability | Privacy Protection

V1.0
- Security Authentication
- Strong Password Policy
- Blacklist & Whitelist
- Digital Envelope
- ......

V1.1
+ Password Anti-cracking
+ Session Protection
+ Minimum Service Policy
+ Customizable Permission Management
+ Sensitive Data Encrypted Store
+ ......

V1.2
+ Without Default Account
+ Built-in Firewall
+ Protected Shell
+ Trusted Upgrade
+ Trusted Environment
+ ......

V1.3
+ Privacy Protection (comply with GDPR)

V2.0
+ Secure Boot
+ Firmware Encryption
+ Video Encrypted Transmission
+ Security Alarm
+ Open Source Compliance
+ ......

V2.1
+ Wireless Security
+ Encryption Performance Optimization
+ ......