
BCDVIDEO™

# SMARTDEFLECT

Proactive Cybersecurity Made Standard
for Video Recorders & Access Control

**bcdvideo.com**

# CYBERSECURITY IN VIDEO SURVEILLANCE

There's plenty of media attention given to IP digital camera companies building vulnerable devices allowing video networks to be easily hacked from anywhere in the world. These network vulnerabilities are compounded when considering the expansion of the Internet of Things (IoT). As more devices connect to a single network, security is only as strong as the most vulnerable connected device.

Similar to any sensitive data, video surveillance represents an untapped pool of information. Consider the key users of surveillance and the data being stored – defense departments, embassies, hospitals, police departments, etc. Beyond capturing metadata, by hacking into a video network, hackers will be able to view the camera footage, connect the infected device to a botnet, or even convert the device into a bitcoin mine undetected.

According to the FBI, the collective impact of these attacks costs victims billions every year to repair systems with the costliest attacks coming from malicious code and denial-of-service. Consequently, distributed denial-of-service (DDoS) cyber attacks have become an increasingly more common attempt to shut down servers. The role surveillance networks play in these attacks comes from the relatively low-security (default passwords) many IP cameras, DVRs, and NVRs have to combat the malicious code needed to connect the device to a botnet. Once a surveillance device has been infected, it becomes a tool used to take down target servers.

**THE TWO MOST COMMON TYPES OF DDOS ATTACKS:**

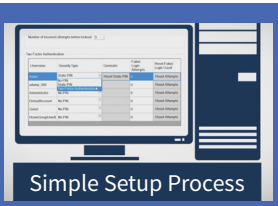
**1. Network-Centric** –Designed to overload a service by using up all the bandwidth

**2. Application-Layer** – Designed to overload a service or database with application calls

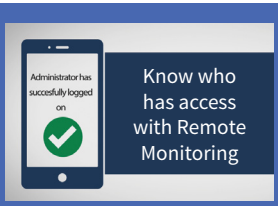

# SMARTDEFLECT CYBERSECURITY

To protect video surveillance systems from hackers, BCDVideo developed SMARTdeflect. An innovative two-factor authentication application designed specifically for BCDVideo access control and video recording servers. The two-factor login process includes a self-generating PIN randomly reassigned every 30 seconds. System administrators will be able to monitor all logins with optional email notifications for every successful or unsuccessful login attempt. Because SMARTdeflect can be accessed on any smartphone, administrators also have the ability to temporarily disable all outside access to a server under attack. Additionally, the easy set-up and customizable system settings give administrators complete control over their servers.

With cybercrime on the rise, providing simple, reliable security with SMARTdeflect to all BCDVideo access control and video recording servers gives security integrators and end users a proactive defense against cyber attacks.








**The hacker in both of these scenarios may have begun as a single person, but the attack is performed by a botnet, potentially comprised of thousands of infected devices, which have been programmed to attack a target server. Vulnerable devices using default passwords like IP cameras, DVRs, routers, and anything connected to the IoT face the possibility of being hacked.**

# FEATURES & BENEFITS

Securing servers from potential cyber attacks requires a proactive solution. That's why BCDVideo developed the SMARTdeflect app. Within the app, system administrators will enjoy several crucial features to remotely safeguard against any threat.

- Pre-Configuration (Optional): Email + SMTP Server
- Easy Set-up Process: Customize settings – email notifications
- Two-Factor Authentication
  - o Secondary PIN uses QR Code (30 sec)
  - o Opt-out to static PIN (optional)
- App iOS, Android, and Windows capable
- Optional mandatory restart for user login beyond set number of failed login attempts per user
- Remotely disable the server (when operator already has access))
- Optional administrator specified PINs for users
- User interface for administrators to adjust basic settings

# SMARTDEFLECT

BCDVideo SMARTdeflect technology ensures system administrators have the protection they need against potential cyber threats. With remote server monitoring and user access control, administrators will receive notifications for every login attempt – successful or unsuccessful. The server can also be disabled remotely by an operator with access to the system if a threat is detected. As the number of cyber attacks increases each year, proactive solutions like SMARTdeflect give system administrators a tool to fight back.