

Protecting Surveillance from Cybersecurity Threats

Making cybersecurity easy for you,
hard for the hackers



Automated Camera Hardening



Secure Appliance Architecture



Cyber Threat Monitoring

- Block unauthorized IoT devices
- Secure access to cameras
- Protect from cyber attack

- Isolated camera network
- Encryption-ready hardware
- Integrated virus & malware protection

- Real-time security alerts
- Flexible alert management
- Dynamic threat detection

The Security of the Security

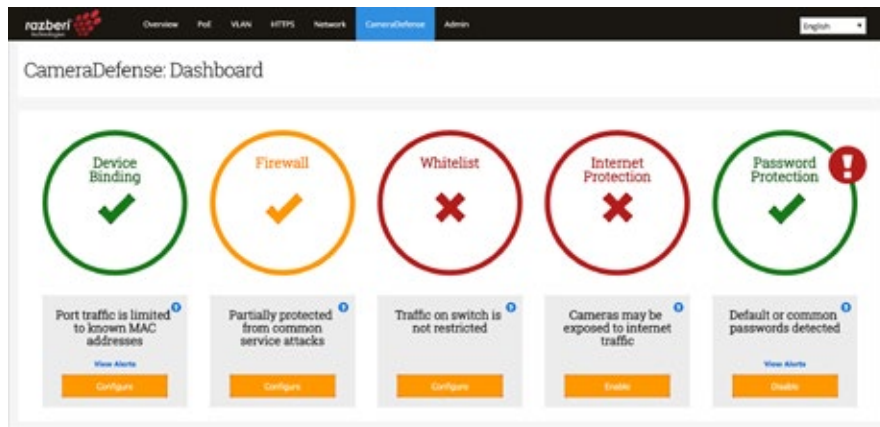
Hackers are relentless. They never stop looking for the next entry point into a network. Ironically, the surveillance cameras installed to protect and lower risk provide yet another window of opportunity. It's keeping security leaders awake at night - but it doesn't have to. With the right technology partner, you can be on the offense and defense to protect the surveillance system and to stop infiltration into the IP network and critical data.

What's at stake is the organization's brand reputation, millions of dollars and personally identifiable information. It's time to make sure that the camera is not a launch pad for attack with the right tools, automation and architecture.

Acting Now to Lower Risks for Good

Camera hardening, secure architecture and threat monitoring

Thinking about cybersecurity in three key pillars, you are already ahead of the game. Razberi CameraDefense™ automates and scales your efforts. First, you'll harden cameras automatically so they don't become a liability. Next, you'll use the unique capabilities of Razberi ServerSwitchIQ™ to isolate cameras in a distributed appliance architecture and set up a VLAN. Then, you'll take advantage of ongoing health monitoring for proactive alerts to act before it is too late. Razberi provides encryption-ready hardware and uses artificial intelligence by embedding CylancePROTECT® to protect against antivirus and malware threats. Razberi makes it easy for you, hard for the hackers.



 Automated Camera Hardening	Solution
Block unauthorized IoT devices	Binds cameras and other IoT security devices to the network, prevents unauthorized devices from using Ethernet ports.
Secure access to cameras	Restricts camera access to whitelisted IP addresses, blocks camera traffic to the public Internet, flags weak passwords.
Protect from cyber attack	Denies un-needed and potentially dangerous camera services with a next generation firewall.
 Secure Appliance Architecture	Solution
Isolated camera network	Separates the camera network from the business network with independent network interfaces and a configurable VLAN.
Encryption-ready hardware	Supports video encryption and trusted system boots with an embedded Trusted Platform Module (TPM).
Integrated virus & malware protection	Protects the video management system by predicting known and unknown attacks to proactively prevent malware execution.
 Cyber Threat Monitoring	Solution
Real-time security alerts	Generates real-time security alerts for incident response.
Flexible alert management	Manages security alerts with Razberi VyneWatch™, Milestone XProtect® and other certified VMS products.
Dynamic threat detection	Evolves with new threats through machine learning.