Understanding Cybersecurity Challenges in Video Surveillance

A D SECURITY SYSTEMS

Your video surveillance system is a target of cybercriminals, and any network-connected surveillance system—on-premise or cloud—is at risk.

The right cloud surveillance system, though, should secure your video and data and provide cybersecurity protections beyond what is expected of a traditional on-prem system.

Traditional Surveillance System Vulnerabilities

Login credentials
Weak or factory-default passwords make for easy system access for cybercriminals.

Outdated software
The operating system, web server, and application software must be updated with the safest available software.

Open ports
Cameras have accessible, unsecured inbound and outbound connections to the internet and network.

Malware infections
Hardware components can contain malware that was added in the supply chain.

The global average cost of a data breach is over

£3 million

(Source: IBM Security's annual "The Cost of a Data Breach Report")

Global cyberattacks grew by

38%

YoY in

2022

(Source: Security Magazine, "Global cyberattacks increased 38% in 2022," Jan 20, 2023.)

Purpose-Built VS General Purpose

Purpose-built video surveillance systems can and should provide bank-level security to protect system and data:

Many traditional surveillance systems lack specifically designed hardware and software.

Purpose-Built		General Purpose
• Automatic security updates • Software designed for system security • Hardware blocks inbound connections • Encryption protects video transmission and data • Authentication protocols for authorised users	VS	• Software requires manual, on-site updates • Components not designed for video surveillance • Data transmitted/stored unencrypted by default • Cameras connect directly to the internet • Open ports allow inbound connections

Eagle Eye Networks and Cybersecurity

The Eagle Eye Cloud VMS (video management system) is a fully managed cloud video surveillance solution, delivering an end-to-end solution with hardware and software designed and maintained to provide unmatched security and accessibility.

Camera isolation

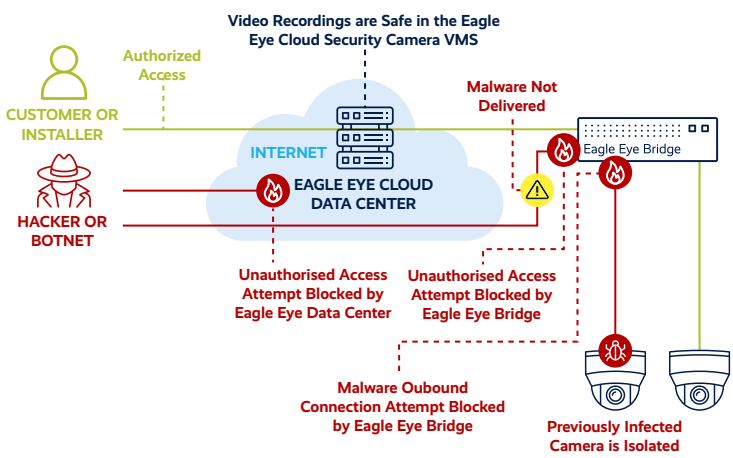
Eagle Eye Bridges/CMVRs are designed as "locked down" devices. These on-site appliances isolate cameras from the internet, blocking inbound and outbound connections.

Data encryption

The Eagle Eye VMS uses two layers of encryption: one for the data itself, and another for the transmission of data. Only authorised users can access decrypted video and data.

How Eagle Eye Protects Customer Video and Data

Even though the cameras have password and other vulnerabilities, hackers and botnets cannot connect to cameras, so have no impact. Previously infected cameras cannot connect to botnet servers.



Get in-depth insights into cybersecurity best practices and learn more about how you can secure your video surveillance system against hackers.

ACCESS THE FULL GUIDE

CONTACT
operations@adsecuritysystems.co.uk
01277 215 679

EAGLE EYE NETWORKS