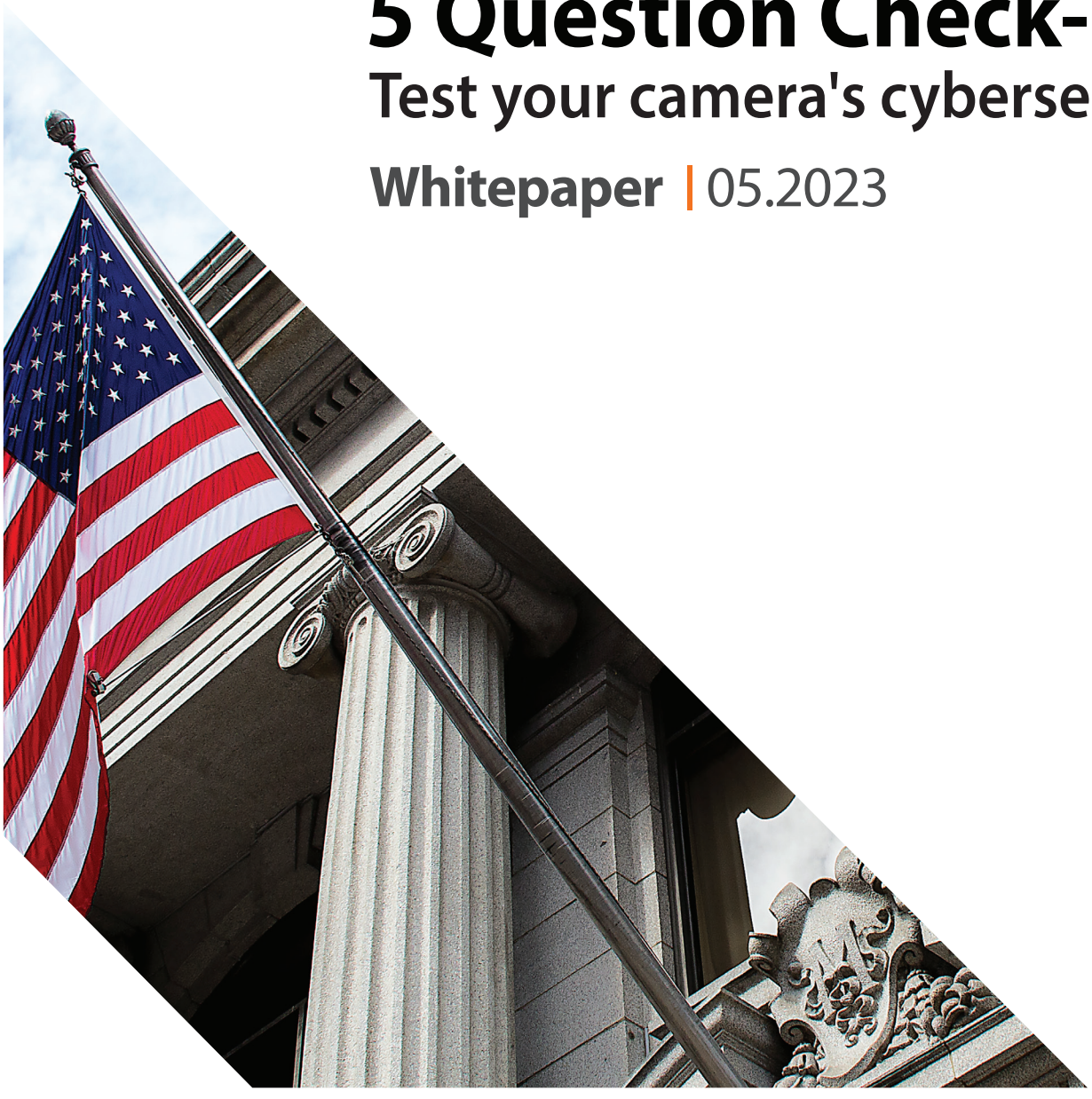
Hanwha Vision

5 Question Check-up:

Test your camera's cybersecurity

Whitepaper | 05.2023



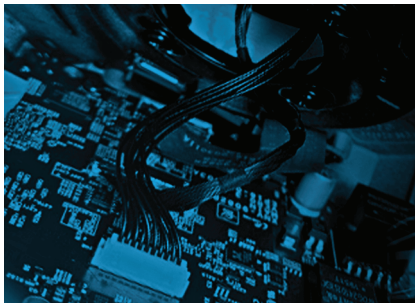
5 Question Check-up:
Test your camera's cybersecurity

Introduction: The critical role of video cameras in physical security systems

The critical role of video cameras in physical security systems cannot be overstated. Video data provides new levels of awareness and visibility into today's enterprises, in addition to video's historical role as a forensic investigations tool.

However, badly designed IP video cameras can also be vulnerable to cybersecurity attacks, inadvertently serving as an entry point to the larger enterprise network. To avoid such a calamity, camera manufacturers must work relentlessly to strengthen the cybersecurity capabilities of their products. Robust functions and technologies also enable equipment to conform with government standards and compliance relating to cybersecurity.

Concerns about the ability of hackers to access live video images or retrieve recorded video surveillance images are timelier than ever. But how can customers know which cameras provide the best cybersecurity?



Following are **5 Questions** customers should ask when shopping for an IP video camera that provides the highest level of cybersecurity. The answers to those questions, including insights from camera manufacturer Hanwha Vision, can guide the search for a camera with stronger cybersecurity and less vulnerability.

1 Is the camera compliant with government standards and regulations?

Cybersecurity has been elevated to the level of national security, due to its status as a key element of the recent National Defense Authorization Act (NDAA, effective August 13, 2019), specifically section 889. This section outlines the prohibited use of certain video surveillance, telecommunications services, equipment, and components manufactured by specific vendors.

These regulations can affect international supply chains, GSA contracts and even currently deployed technologies, especially if the customer is a U.S. government-related agency.

Hanwha Vision is committed to complying with all government and international trade regulations. Hanwha supports NDAA-compliance across its product lines and has a full suite of trade-compliant devices, with many currently used in government, defense and a range of commercial applications.

commitment to innovation

Hanwha's top priority is being the best partner to its customers, dealers and system integrators - and that means making it as easy as possible to work with us. Hanwha is compliant with all government and international trade regulations, including the NDAA provisions related to video surveillance equipment including components manufactured by specific vendors.

All Hanwha Vision manufacturing facilities are located in Vietnam and South Korea. Hanwha Techwin products are compliant with the Trade Agreements Act (TAA) terms and qualify for sale under GSA guidelines. Hanwha products no longer use System on a Chip (SOC) technologies from any supplier prohibited under the NDAA. Hanwha will continue that practice for all new product development and will also make every effort to transition its legacy products to NDAA compliance.

2 Is cybersecurity addressed at the foundational level?

Cybersecurity cannot be added to a device after the fact. Rather, cybersecurity must be "baked into" the device at the factory during the manufacturing process.

For its video cameras, Hanwha has added more than a half dozen new features excusively related to improved system and device protection. These efforts included establishing its own device certification issuing system to embed certificates and encryption keys into the chip during the manufacturing process. As a result, Hanwha's "ground-up" security policies ensure comprehensive cybersecurity through the lifecycle of a device and guaranteeing all video is securely stored, encrypted and accessible only by authorized users.

When building chips, Hanwha has adopted an approach common in the laptop market, using a Trusted Platform Module (TPM), which is embedded in nearly every laptop made today. It locks down the BIOS - the foundational level - to prevent tampering or malicious firmware being written.

With Wisenet 7, Hanwha has built a TPM into its cameras, making sure the firmware is signed and encrypted - which is only possible when assembling a completely new architecture, and not using somebody else's chipset.

Now, essentially there are two different operating systems running on Hanwha cameras. If there is an intrusion attempt, someone is only able to access the application side. They don't have access to the raw hardware, or the chip side, which is protected. The TPM will catch any attempts to load unauthorized firmware.

3 Are the camera's components designed to be "secure by default?"

"Secure by default" means a technology comes out of the box with the optimal settings to ensure cybersecurity. Key cybersecurity enhancements are also included from the onset. The term "secure by default" also reflects a heightened awareness of the manufacturing process.

In the case of video cameras, questions include: What's going into a chip? Who is building the chip? Where are they based? Who's doing what behind the scenes?

With Wisenet 7, Hanwha went even further to secure the hardware and deliver everything the market needs. Because security is Hanwha's business, the company is familiar with what customers and partners need to keep their operations protected. Hanwha put that knowledge to use building its own System on Chip, continuing that approach until the company's most recent release: Wisenet 7 System on Chip (SoC).

4 Is there a "chain of trust" in the manufacturing process?

When manufacturing is outsourced or performed in other countries, quality control can be an issue, as can standards of ethics, sustainability and environmental regulation. Manufacturing systems that are not well controlled and documented can also contribute to concerns about cybersecurity.

Hanwha makes its cameras and chipsets, assembles, designs, fabricates and lays out the circuit boards. Hanwha is controlling all those pieces, creating a safer environment for users. The result is a **"Supply Chain of Trust"** that ensures customers the highest levels of cybersecurity.

Hanwha has a complete view into cybersecurity, and also into quality control and software development. It's a much different scenario from other manufacturers who OEM their components to outside factories.

5 Has cybersecurity been confirmed or evaluated by third parties?

As cybersecurity grows more complex and attracts more industry attention, industry standards also become more important. Underwriters Laboratory (UL) is a well-recognized institution worldwide, and they developed a standard for certifying a company's level of cybersecurity in its technologies.

The work that went into developing the Wisenet 7 chipset resulted in Hanwha Vision recently receiving UL CAP (Cybersecurity Assurance Program) certification for its recently launched range of IP cameras featuring the new chipset. Certification is an intense process that looks at how coding is done. It tests the strength of encryption cipher algorithms. It tests against known databases of vulnerabilties and what versions of software are being used. Certification amounts to an industry stamp of approval that Hanwha can show to customers and partners to validate its stringent cybersecurity processes.

In additon, each Hanwha Vision location is certified to ISO 9001 quality standards for design, development, and production - and each location adheres to rigorous quality control and testing procedures.

In addition, many Hanwha products now incorporate the FIPS-142 federal information processing standard from the National Institute of Science and Technology to ensure that elements such as encryption algorithms are used properly. Hanwha also ensures that it is using proper levels of encryption and that all software is validated and vetted for use by the federal government.

Cybersecurity: An essential requirement for video surveillance

For a video camera to be effective, cybersecurity needs to be considered directly alongside physical security to ensure a customer is in the best position to capture key footage that will assist in future forensic investigations.

No longer an option, built-in cybersecurity is an essential requirement for ensuring the highest levels of security in video surveillance devices.

For more information visit us at

HanwhaVisionAmerica.com

Hanwha Vision America
500 Frank W. Burr Blvd. Suite 43 Teaneck, NJ 07666
Toll Free : +1.877.213.1222
Direct : +1.201.325.6920
Fax : +1.201.373.0124
www.HanwhaVisionAmerica.com