Hanwha Techwin

Built-in Cybersecurity

Making a case for government compliance

Built-in Cybersecurity

Making a Case for Government Compliance

The global business landscape is complex, especially as organizations and operations grow increasingly connected. We are all spending more time online as the workday now consists of video calls with colleagues, customers, and partners all around the world. This increase in network activity, heavy streaming and content sharing makes companies attractive targets for cyber-criminals.

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

Cybersecurity is now top of mind, whether it is for protecting personal identities online, safeguarding confidential business communications or complying with regulations governing content and rights management. News outlets regularly report the latest network intrusion, ransomware hack or identity theft. However, cybersecurity -- one of the most potentially devasting threats to the global economy -- is also one of the most preventable, provided the right steps are taken and organizations become pro-active rather than reactive.

Cybersecurity has also 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.

For Hanwha's partners and customers, 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.

A Smooth Path to Security Compliance

Hanwha Techwin is committed to complying with all government and international trade regulations. Hanwha Techwin supports NDAA-compliancy 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.

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 Techwin manufacturing facilities are located in Vietnam and South Korea; making them compliant with the Trade Agreements Act (TAA) terms and qualifying Hanwha products 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.

Security is also Hanwha's business, so we're intimately 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).

Hanwha's SoC already included key cybersecurity enhancements such as "secure by default," meaning a camera's out-of-the-box settings are already the recommended ones for use. With Wisenet 7, Hanwha went even further to secure the hardware and deliver everything the market needs.

Hanwha added more than a half dozen new features exclusively 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 entire 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 you're assembling a completely new architecture, and not using somebody else's chipset.

Now, essentially there are two different operating systems running. 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.

Supply Chain of Trust

Customers can count on the Hanwha Techwin "Supply Chain of Trust," based on the fact that the company 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.

Hanwha has a complete view into not just cybersecurity, but also quality control and software development. It's a much different scenario from other manufacturers who OEM their components. They simply can't do what Hanwha can from a cybersecurity perspective.

Compliance is Key

Why is all this important? There is such heightened awareness of the security manufacturing process: What's going into a chip? Who is building this part of a chip? Where are they based? Who's doing what behind the scenes? When you add in the requirements for NDAA, FCC and TAA compliance, the stakes are raised even higher.

An Industry Seal of Approval

As cybersecurity grows more complex and attracts more industry attention, industry standards also become more important. The UL is a well-recognized institution worldwide and they developed a standard for certifying a company's level of security in its technologies. The work that went into developing Wisenet 7 resulted in Hanwha Techwin recently receiving UL CAP (Cybersecurity Assurance Program) certification for its recently launched range of IP cameras featuring the new chipset. It's an intense process that looks at how coding is done. It tests the strength of encryption cipher algorithms. It tests against known databases of vulnerabilities and what versions of software are being used. It's really an industry stamp of approval that Hanwha can show to customers and partners to validate its stringent cybersecurity processes.

Each Hanwha Techwin location is ISO 9001-certified for design, development and production – and each 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 like encryption algorithms are properly used. Hanwha also ensures that it's using proper levels of encryption and that all software is validated and vetted for use by the federal government.

Whether you are a small business that entrusts video surveillance solutions to protect its assets, people, and property or you are a government agency, it is a requirement to keep confidential data secure.

Hanwha Techwin continues to work relentlessly on strengthening the security capabilities of its products with built-in cybersecurity to help make a case for government compliance by offering robust security functions and technologies that are unmatched.