WISENET 7

Nuevo Chipset AI

Hanwha Techwin
WISENET 7
Made in Korea

Lleva la **Seguridad Cibernética** al siguiente nivel

Hanwha Techwin

Descripción general de Wisenet7

- Wisenet7 SoC

- 4K (8MP) 30fps, 4MP 60fps
- Calidad de imagen mejorada
  - WDR extrema
  - Procesamiento de imagen con poca luz.
  - LDC
- Ciberseguridad de ultima generación
- Soporte AI
- Soporte multicanal (máx. 4 canales)
  - en un solo chipset

De seguridad física a ciberseguridad

- La seguridad física añade una capa de protección que le puede ayudar a mantener protegidos y seguros a sus empleados, activos y sus propiedades.
- El nivel de seguridad y gastos que se invierten en un sistema es proporcional al valor de los activos a proteger.
- La naturaleza de las amenazas ha cambiado.

La amenaza

16/03/2021 15:3

BOULEVARD MAGA

"La cib

conve

EITB MEDIA

Los ciberdeli
pandemia. Ar
nuestras emp

Cyber

Hac

Car

By Willia

9 de mar

c|net | Home

FEATURED | HOME SECURITY | HOME INTERNET | SMART HOME | KITCHEN & HOUSEHOLD

Yes, your security camera could be hacked: Here's how to stop spying eyes

Following the recent conviction of a technician for spying on customers' camera feeds, protecting your privacy is more important than ever.

David Priest, Taylor Martin Feb. 11, 2021 5:00 a.m. PT

LISTEN - 08:13

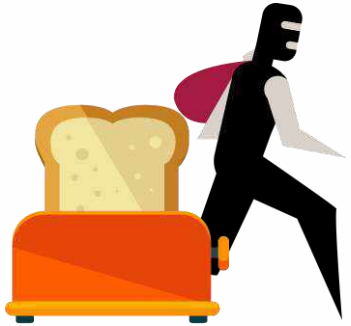
rity

pitals

Los riesgos de nuestro mundo interconectado

- Le llevó 1 minuto a un ladrón robar un auto al usar la señal inalámbrica de la llave de la víctima. Todo lo que necesitaba era un dispositivo relé.

- **http://www.bbc.com/news/uk-england-birmingham-42132689e**

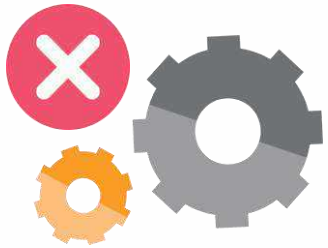


Una falsa tostadora de pan fue conectada a internet con un puerto abierto en una red que no es segura. Les llevó menos de **1 hora** a los hackers para vulnerarla.

http://www.bbc.com/news/uk-england-birmingham-42132689

Los ataques cibernéticos son despiadados

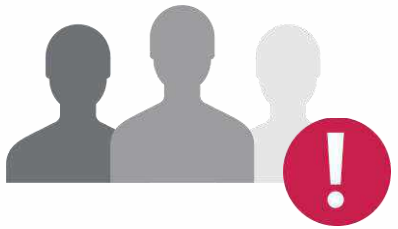
Pérdida de datos privados



Interrupción de las operaciones

Daños a la reputación

Multas y demandas legales



Personas expuestas a peligros

Ciberseguridad / Definición

Def. Ciberseguridad, También conocida como seguridad informática, es el conjunto de políticas, procesos y herramientas de hardware y software, que se encargan de proteger la privacidad, la disponibilidad y la integridad de la información y los sistemas en una red.

, **Def**. La ciberseguridad es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. También se conoce como seguridad de tecnología de la información o seguridad de la información electrónica.

Ciberseguridad de ultima generación

Wisenet7 ofrece seguridad de extremo a extremo con los niveles más altos de política de ciberseguridad de la industria que cumple con los estrictos estándares de UL CAP. Hanwha Techwin estableció su propio sistema de emisión de certificados de dispositivo para incorporar certificados en el producto no solo en el progreso del desarrollo sino también en el progreso de la fabricación.

Ciberseguridad de ultima generación

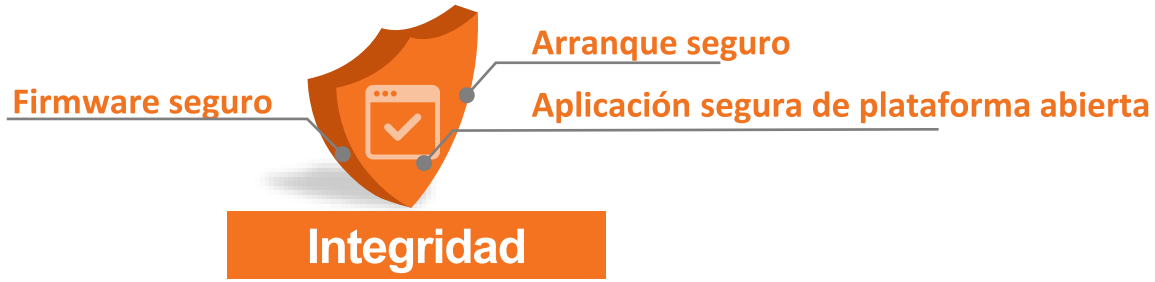
- **Malware**

El malware es una categoría general que engloba el software perjudicial que puede afectar a los dispositivos conectados de un usuario, normalmente sin que este lo sepa.

Fuente: https://www.avg.com/es/signal/cyber-security-terms

Ciberseguridad de ultima generación

1. Pueden tener los hacker acceso a mi red contaminando mis dispositivos?

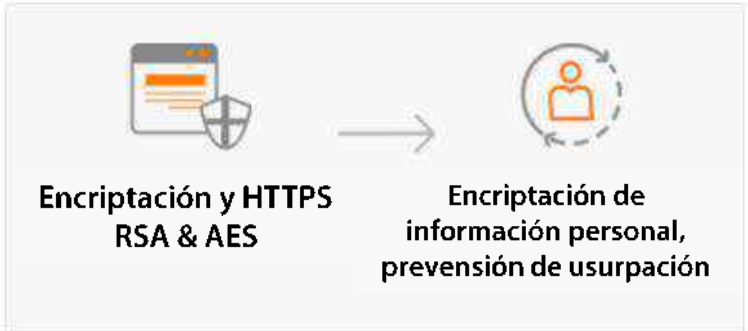


R: La seguridad Avanzada de los Productos Hanwha impide que se ejecuten firmware modificados maliciosamente gracias a su Sistema Seguro protegiendo así su información confidencial

Protección de datos & Ciberseguridad

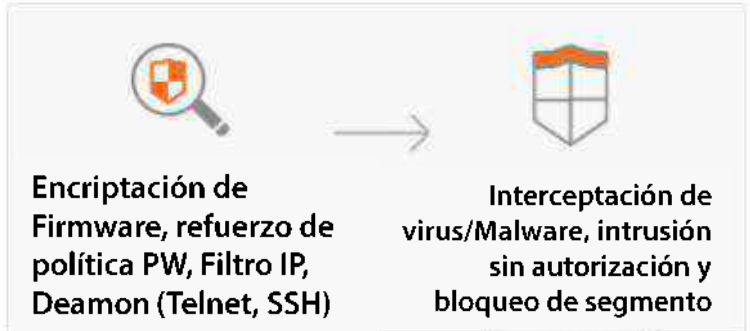
Los delitos que extraen y explotan la información de los clientes de los productos de seguridad han aumentado recientemente. Nuestros productos protegen los sistemas y la información del usuario a través de las siguientes tecnologías de seguridad de vanguardia:

- El protocolo HTTPS y las características de certificado privado para la protección de la información de autenticación del usuario (ID de usuario / contraseña)
- Las últimas tecnologías de seguridad en múltiples dispositivos de seguridad aplicados para la protección contra desvíos de seguridad no autorizados
- Autenticación de usuarios y adquisición de información de imágenes en cada componente del producto.
- Filtrado de IP a través de firewall y eliminación de vulnerabilidades de seguridad de bypass y puertas traseras a través de derechos de administrador.



Protección de credenciales de usuario

Protección de datos de video



Protección de credenciales de usuario

Ciberseguridad de ultima generación

- **Spyware**

Como cualquier buen espía, el spyware está diseñado para pasar desapercibido e infiltrarse en su sistema. ¿Y qué hace cuando se ha introducido? En los casos graves, puede apoderarse de sus datos personales, incluida la información bancaria.

Fuente: https://www.avg.com/es/signal/cyber-security-terms

Ciberseguridad de ultima generación

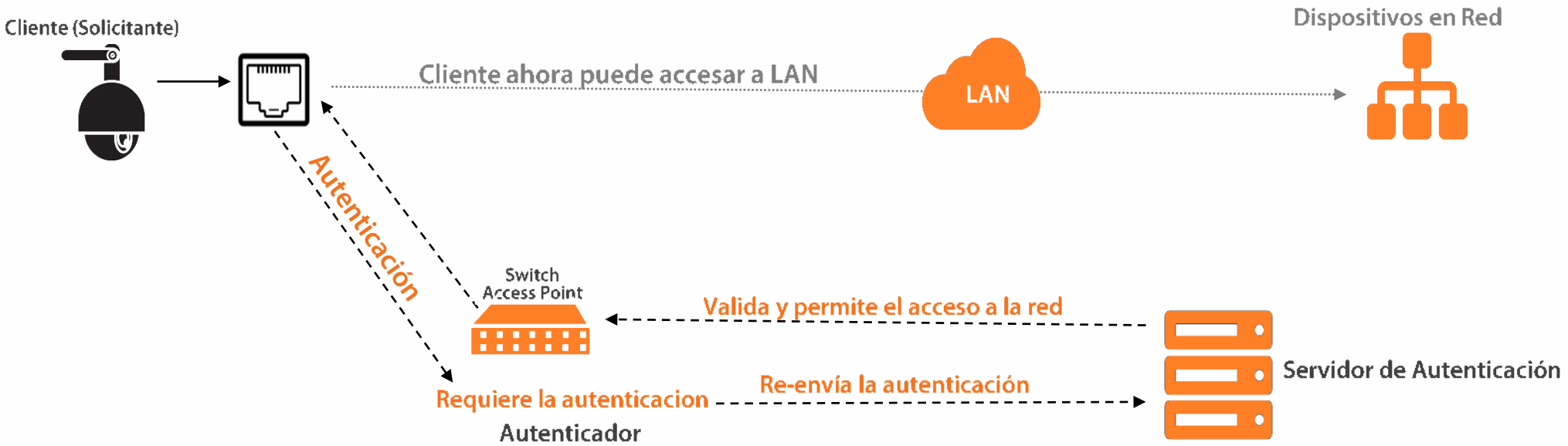
2. ¿Existe la posibilidad de fuga de datos durante la comunicación entre dispositivos de video vigilancia interconectados (por ejemplo, Cámara - Servidor)?

R: La autenticación mutua de productos entre los dispositivos permite una comunicación segura, mientras que la emisión de certificaciones privadas por dispositivo puede defender el sistema de las amenazas a gran escala.

Comunicación certificada / Ciberseguridad

La implementación de la comunicación basada en certificados garantiza que los puntos finales del dispositivo con los que está interactuando no solo son dispositivos seguros pero válidos en su red.

Solicitud de acceso a la Red



Ciberseguridad de ultima generación

- **Filtración de datos**

La información expuesta puede tratarse de inicios de sesión, contraseñas, números de tarjetas de crédito y hasta números de la seguridad social. Eso significa que una filtración de datos puede desembocar en un robo de identidad, aunque sus fines varían

Hanwt Techwin

Ciberseguridad de ultima generación

3. ¿Puede un tercero leer o alterar mi video?

R: Todo el proceso de transferencia de datos, almacenamiento y respaldo es cifrado, salvaguardando con esto los datos de video personales.

Ciberseguridad de ultima generación

Troyanos

A menudo, los troyanos (o caballos de Troya), se ocultan en descargas de software. Son un tipo de malware que descarga otro malware. Uno de los tipos más peligrosos es un troyano de banca móvil.

Janeleiro, troyano bancario que tiene como objetivo usuarios corporativos en Brasil

11 abril, 2021 Por Alejandro Parras — Leave a Comment

Desde 2019 ESET ha estado investigando este troyano bancario que apunta a usuarios corporativos de distintas industrias en Brasil, viéndose afectados sectores como ingeniería, salud, retail, manufactura, finanzas, transporte y gobierno.

Ciberseguridad de ultima generación

4. ¿Puede software malicioso entrar en mis dispositivos de seguridad a través del firmware o abrir y ejecutar aplicaciones en el sistema de Open Platform?

R: La firma electrónica adaptada al firmware y a las aplicaciones de Open Platform puede garantizar la integridad de los datos y bloquear el funcionamiento de software malicioso.

Ciberseguridad de ultima generación

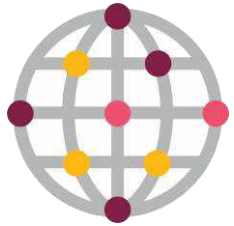
Ransomware

Software malicioso que al infectar nuestro equipo le da al ciberdelincuente la capacidad de bloquear un dispositivo desde una ubicación remota y secuestrar nuestros archivos. Los rescates normalmente se pagan con bitcoins. Algunos de los últimos ataques de ransomware más famosos son los de Petya, WannaCry y Cryptolocker.

Ciberseguridad de ultima generación

Ransomware WannaCry

Operaciones interrumpidas en hospitales, empresas de envíos, fabricantes de carros, empresas de telecomunicaciones y universidades.



Afectó a más de 230k computadoras en más de 150 países

>$1.000 millones en costos por daños en los primeros 4 días

Ciberseguridad de ultima generación

5.¿Podemos confiar en los productos que, según se afirma, cumplen con los estándares de seguridad del propio fabricante?

S-CERT & External Monitoring
Security Vulnerability Response Team
Monitoring via CVE, ICS-CERT, KISA

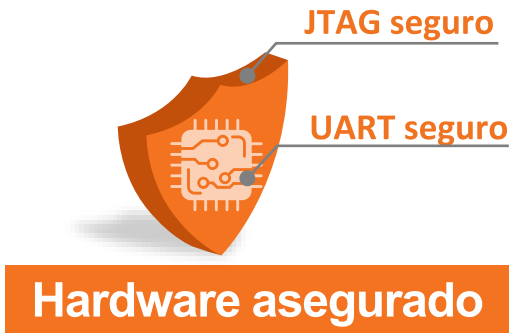
Other Certificates
TTA Public IP Camera Certificate
KISA Intelligent CCTV Solution Certificate

Cyber Essentials
3rd Party accreditation
UK Government backed accreditation scheme

R: Los productos de Hanwha techwin cumplieron con el estándar de seguridad más alto de la industria al obtener certificaciones de autoridades de ciberseguridad reconocidas en la industria.

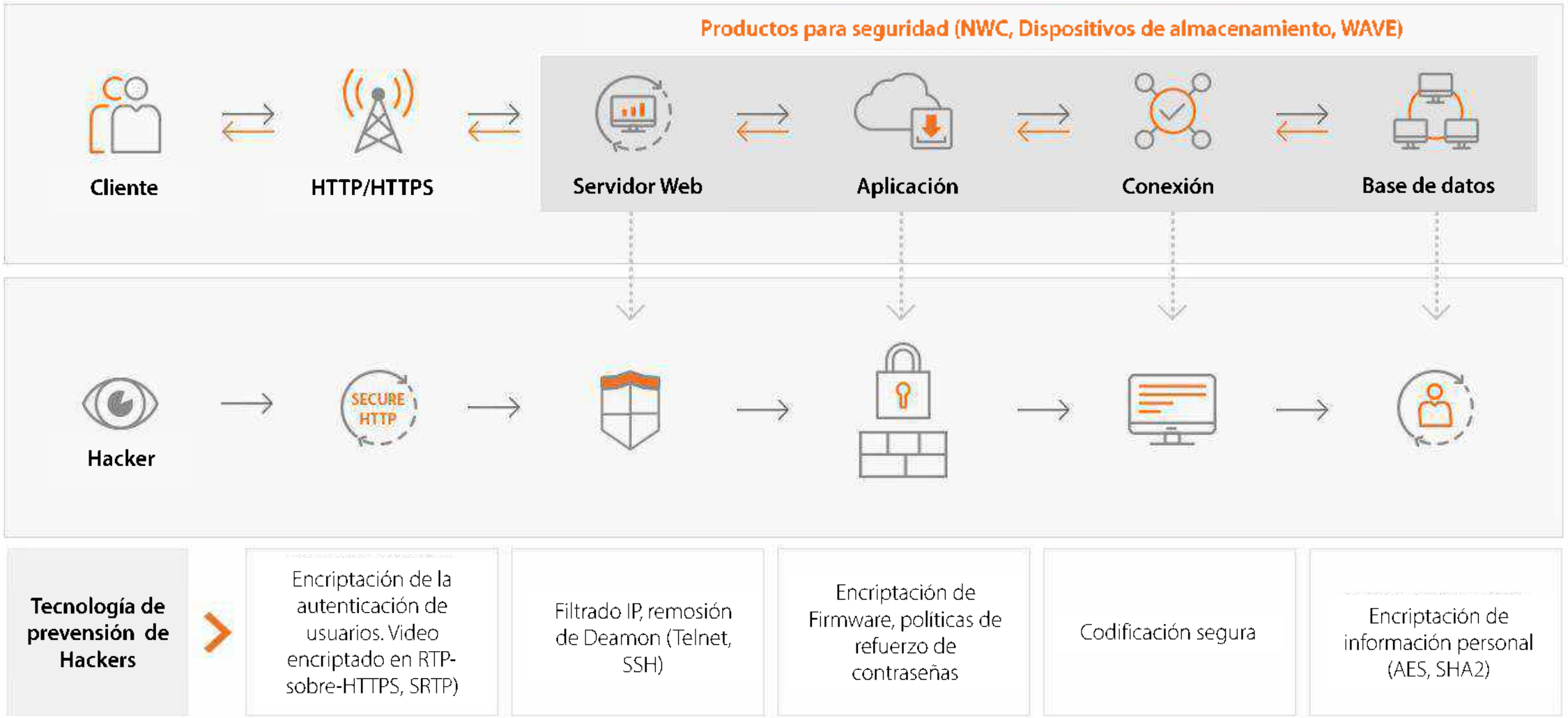
Ciberseguridad de ultima generación

6. ¿Tengo que configurar el producto por mi cuenta para que sea seguro?



R: Con el fin de brindar protección a los productos desde el inicio, Hanwha Techwin ofrece una sólida seguridad por defecto implementada en su equipamiento.

Protección por diseño / Ciberseguridad



Ciberseguridad de ultima generación

7. ¿Qué puedo hacer en caso de encontrar una vulnerabilidad de seguridad en el producto?

R: Cuando detecte una vulnerabilidad de seguridad, puede informar secure.cctv@hanwha.com. El departamento de ciberseguridad de Hanwha Techwin, S-CERT, reaccionará de inmediato a la vulnerabilidad de seguridad.

Actividades para mejoras en Ciber seguridad

Hanwha Techwin cuenta con un equipo de respuesta a la vulnerabilidad en la seguridad (S-CERT) para prevenir fracturas de seguridad ilegales o no autorizadas desde Fuentes externas, y para prevenir fallas internas de seguridad.

Con el objetivo de mejorar la calidad de la seguridad del producto, S-CERT analiza la seguridad del producto en la etapa de desarrollo y realiza pruebas de penetración periódicamente por agencias especializadas. Si un problema de seguridad es encontrado, el equipo S-CERT lo analiza para dar una respuesta en el menor tiempo posible.

Adicional a esto, S-CERT esta comprometido a desarrollar y encontrar soluciones de seguridad para liderar en el campo de la video vigilancia, así como también se esfuerza para tener diferentes certificaciones para ser reconocido externamente por la calidad de los productos en materia de seguridad.

Actividades para mejoras en Ciberseguridad

Estos son los cuatro actividades que Hanwha Techwin constantemente evalúa para la mejora de los equipos en materia de seguridad:

- Actividades de respuesta ante vulnerabilidad de seguridad
- Actividades de mejora del producto en seguridad
- Actividades de desarrollo de soluciones de seguridad
- Actividades para la adquisición de certificados de seguridad

*CVE: Common vulnerabilities and exposures. https://cve.mitre.org/about
*KISA: Korea Internet Security Agency

Ciberseguridad – Certificaciones internacionales

S-CERT & External Monitoring
Security Vulnerability Response Team
Monitoring via CVE, ICS-CERT, KISA

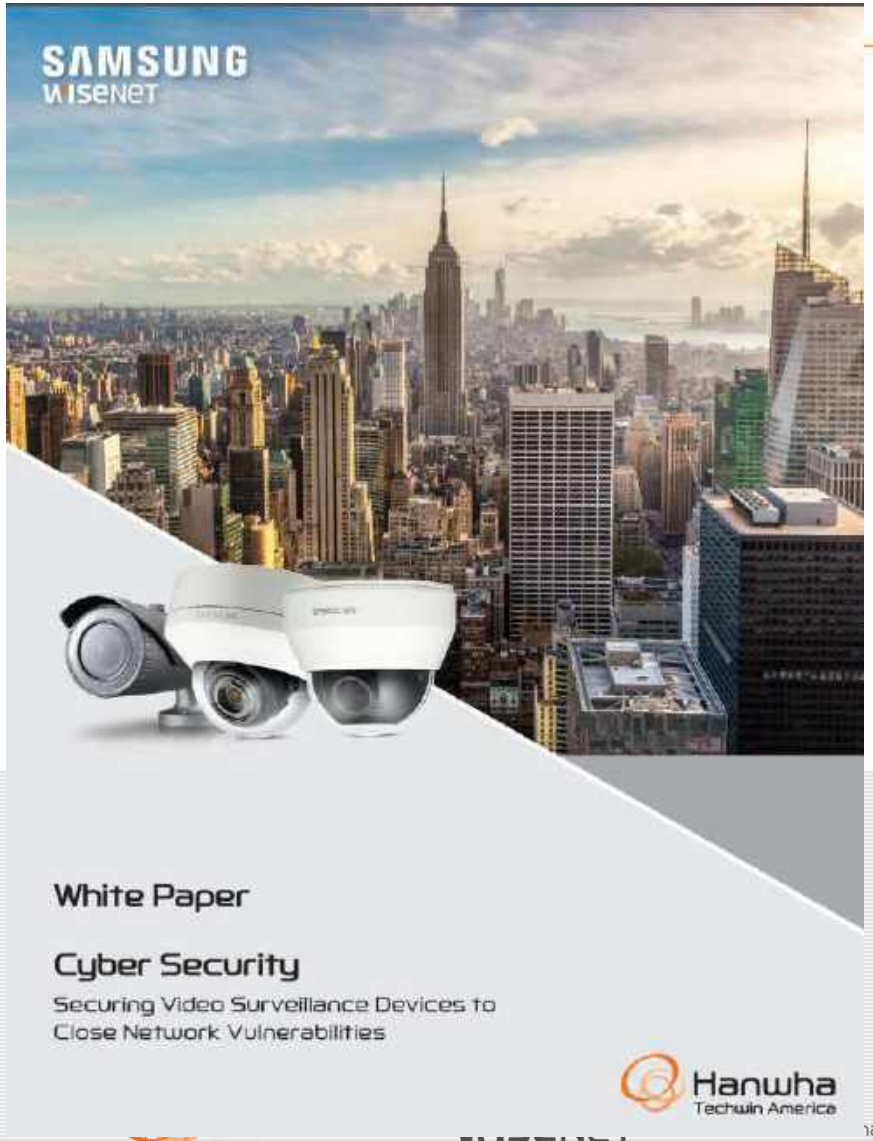
Hardening
Practical setup guide, detailed guide for 4 levels of security implementation

Disclosure
Security Vulnerability disclosure policy.
Clear and published policy for sharing vulnerabilities

Cyber Essentials
3rd Party accreditation
UK Government backed accreditation scheme

Other Certificates
TTA Public IP Camera Certificate
KISA Intelligent CCTV Solution Certificate

Hanwha – White Paper de Ciber Seguridad



Introduction

We live in an increasingly connected world, where more and more devices and systems are networked and shared with other systems. Convenience is a main driver behind this trend, as people have come to expect the ability to connect to and control devices and systems anywhere, anytime.

However, there is a downside to the unprecedented level of convenience provided by the growing number of networked devices, namely increased security risk. Because each device is an endpoint for networks, they introduce the potential to become entry points for hackers and others with malicious intents. In fact, in many of the most high-profile data breaches that have occurred recently, hackers were able to access corporate networks through POS, HVAC and other networked systems that failed to provide an adequate level of security to prevent these types of breaches.

While IP-based video surveillance and other solutions have grown in popularity to become the accepted standard for new deployments and upgrades, security systems are no exception. A hacker does not discriminate among networked devices whether it performs a critical function like security or not. As such, video surveillance cameras and other devices are among the lengthy list of potential network entry points that are continually being probed for vulnerabilities that can be exploited. Therefore, it is essential that organizations take the necessary measures to ensure the highest level of security for their networks and IP cameras, encoders, NVRs and DVRs. There are a number of best practices that should be undertaken to strengthen device security to prevent unauthorized access and protect end users video surveillance systems and their overall network. Hanwha is not only aware of these best practices but has built a number of technologies and capabilities into its products to make it easier for organizations to take these important steps toward improving network security. These items should be reviewed by the owner of security systems, IT personnel, and Systems Integrators installing systems to determine the level of security needed while balancing the ease of use, with acceptable risks.

This guide will show snapshots from network cameras where applicable. Most settings can be configured in batch for multiple cameras using the Wisenet Device Manager Software (Figure 1).

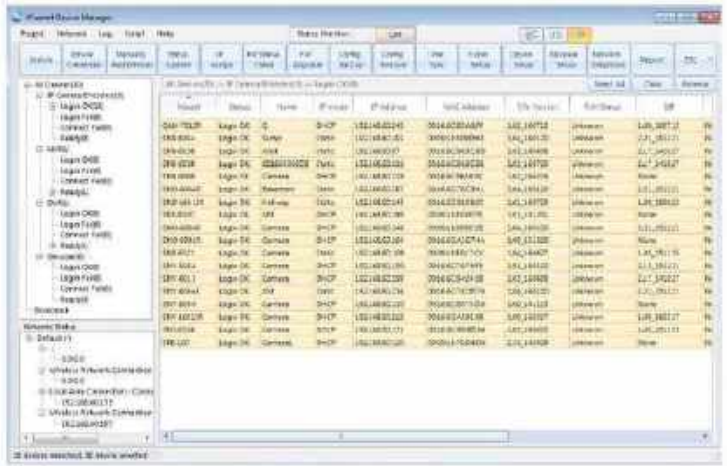


Figure 1

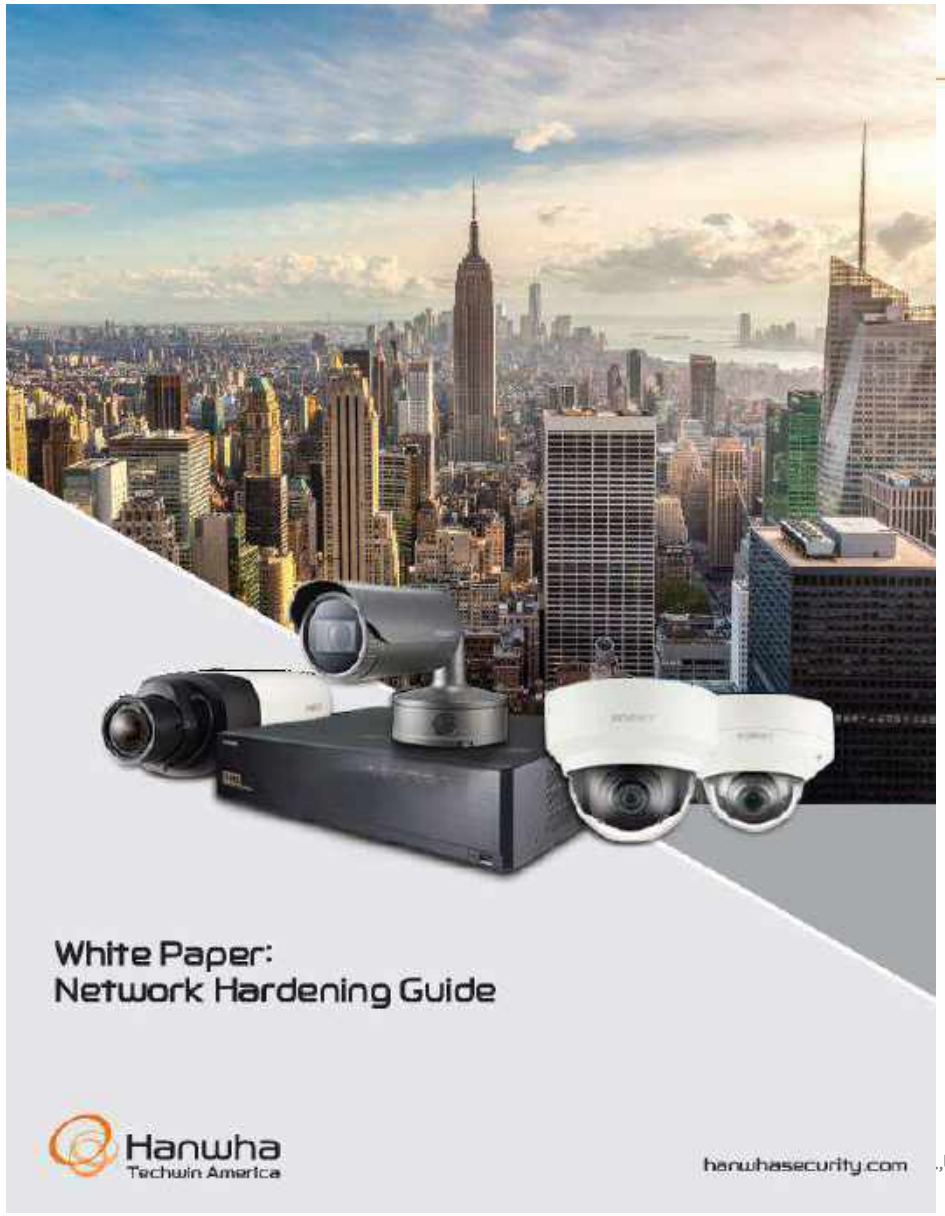
Hanwha Techwin

Summary

The harsh reality in today's connected world is that individuals and groups will continue their attempts to identify and exploit vulnerabilities to breach network security. And while we benefit from the convenience of a growing number of devices accessible via those networks, the reality is that those devices only increase the likelihood of unauthorized network access. Therefore, it is vital that all of these devices are secured to prevent them from becoming an open door for hackers. Employing those best practices not only can prevent networked video devices and systems from serving as entry points, but also ensures the integrity and continued operation of this critical function – ensuring the ongoing safety and security of people and assets. Additionally, many of these steps are also applicable to other devices and systems. Therefore, these best practices serve as a requirement for organizations that recognize the importance of and are serious about securing their networks.

Therefore, these best practices serve as a conversation starter for organizations that recognize the importance of and are serious about securing their networks. Open and informed dialogue between the end user, their IT department, the installer and systems integrator are the key to finding the best solution to fit an individual organization's security needs.

Hanwha Techwin – Guia de fortalecimiento para la Red



2. Definition of Security Levels

This guide defines cyber security levels according to the following criteria, each level building on and assuming the previous level has been implemented.

- The product design level is the level of security that users can achieve with the cyber security product design provided by the device, without any settings.
- The protective level means the level of security that can be achieved with the default settings that initial purchased products have or in the state immediately after the factory initialization.
- The secure level is a level of security that user can achieve by disabling unnecessary features or services as well as keeping it up to date and reviewing system logs.
- The very secure level means the level of security that can be achieved by combining the security features provided with additional external security solutions.

< Table 1 >

Security Level	Hardening features & activity for cyber security	Initial Setting	Recommended Setting
Product Design Level	Forced complex password setting	Default	
	No initial password	Default	
	Input limit for consecutive password failures	Default	
	HTTP Authentication (Digest only)	Default	
	No Backdoor (Telnet, SSH)	Default	
	Configuration file encryption	Default	
	Firmware encryption	Default	
	Watermark & encryption of extracted video	Default	
	Maintained logs after factory reset	Default	
Protective Level	Perform Factory Reset	-	
	Disabling guest login	Disabled	Disabled
	Disabling unauthenticated RTSP connections	Disabled	Disabled
	Disabling unused multicast	Disabled	Disabled
	Disabling unused DDNS	Off	Off
	Disabling unused QoS	Not set	Not Set
	Disabling unused FTP	Disabled	Disabled
	Disabling unused audio input	Disabled	Disabled
Secure Level	Checking the version of firmware and updating	-	
	Setting the correct date & time	Initial value	Change
	HTTPS (Hanwha Techwin certificate)	HTTP	HTTPS (own certificate)
	HTTPS (authenticated certificate)	HTTP	HTTPS (authenticated certificate)
	Changing the default port	Initial value	Change
	IP Filtering	Not set	Set
	Sending E-mail using TLS	Not use	Use
	Disabling unused Link-Local IPv4 address	Use	Not use
	Disabling unused UPnP	Use	Not use
	Disabling unused Bonjour	Use	Not use
	Using SNMP securely	SNMP v2c	SNMP v3
	Disabling unused SNMP	SNMP v2c	Not use
	Creating additional user accounts	-	
	Checking the log	-	
Very Secure Level	802.1 X Certificate-based access control	Not use	Use

Lista de verificación cibernética: un punto de partida para que la discusión fluya entre SI, el usuario final y TI.

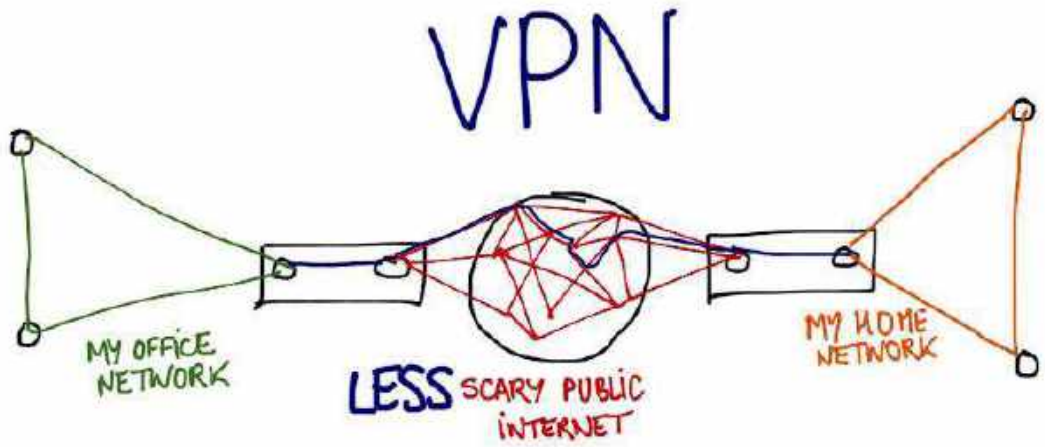
WISENET

Security Checklist

Please refer to these as guidelines of things to think about. Most systems will not use everything listed. Good conversation starter with all partners.

- ☐ Assign static IP addresses
- ☐ Set strong admin password
- ☐ Create user-level accounts with least privileges required with strong passwords
- ☐ Update firmware to the latest version
- ☐ Enable SSL encryption
- ☐ Disable guest login/unauthenticated RTSP connections
- ☐ Update system clock/NTP, DST, time zone
- ☐ Enable multicast only if needed
- ☐ Enable DDNS only if needed
- ☐ Enable bonjour only if needed
- ☐ Enable UPnP only if needed
- ☐ Enable link-local address only if needed
- ☐ Enable FTP only if needed
- ☐ Enable e-mail notifications only if needed
- ☐ Enable QoS only if needed
- ☐ Enable 802.1x certificate-based access control
- ☐ Enable SD card recording
- ☐ Enable tamper detection
- ☐ Enable network disconnect detection if using low voltage power
- ☐ Enable SNMP v3 or disable all versions if not needed
- ☐ Check device logs
- ☐ Ensure cameras are on a separate network from corporate/production network/Int
- ☐ Enable VLANs on network
- ☐ Enable IP Filtering
- ☐ Change default ports from well-known ports to high ports
- ☐ Ensure camera is out of reach, cables are protected
- ☐ Document configuration and create a export a backup
- ☐ Save a snapshot of camera view
- ☐ Place a recognizable setting to indicate tampering/defaulting
- ☐ Utilize VPN for remote access
- ☐ Configure port forwarding for the least number of devices/ports needed
- ☐ Use proprietary video file format for SD recording and exporting video
- ☐ Ensure all network switches, NVRs/VMS, & PoE midspans/injectors are protected by a UPS

Hanwha



Avalados por el Fed. Register USA / Ciberseguridad

FEDERAL REGISTER

The Daily Journal of the United States Government

Rule

Addition of Certain Entities to the Entity List

A Rule by the Industry and Security Bureau on 10/09/2019

PUBLISHED DOCUMENT

AGENCY:

Bureau of Industry and Security, Commerce.

ACTION:

Final rule.

SUMMARY:

This final rule amends the Export Administration Regulations (EAR) by adding twenty-eight entities to the Entity List. These twenty-eight entities have been determined by the U.S. Government to be acting contrary to the foreign policy interests of the United States and will be listed on the Entity List under the destination of the People's Republic of China (China).

DOCUMENT DETAILS

Printed version:
PDF

Publication Date:
10/09/2019

Agencies:
Bureau of Industry and Security

Dates:
This rule is effective October 9, 2019.

Effective Date:
10/09/2019

Document Type:
Rule

Document Citation:
84 FR 54002

BRASIL
DIRECTOR VENTAS: Rodrigo Martini r.martini@Hanwha-wisenet.com

CAM
DIRECTOR VENTAS : Sofia Borelly s.Borelly@Hanwha.com
INGENIERIA: Luis Miguel Davila ldavila@Hanwha-wisenet.com.com

REGION ANDINA
DISTRIBUCIÓN Ivonne Pinzón Ivonne.ínzon@Hanwha-wisenet.com
INGENIERIA: Hernando Chavez h.chavez@Hanwha-wisenet.com

MEXICO
DIRECTOR VENTAS : Ian Juarez i.Juarez@hanwha-wisenet.com
INGENIERIA: Oscar Arrieta oarrieta@Hanwha-wisenet.com

PERU Y BOLIVIA
DIRECTOR VENTAS Manuel Carlos mcarlos@Hanwha-wisenet.com
INGENIERIA: Juan Carlos Yañez jyanez@hanwha-wisenet.com

CONO SUR
DIRECTOR VENTAS Jorge Vallejos jvallejos@Hanwha-wisenet.com
INGENIERIA: Alberto Muñoz alberto.munoz@Hanwha-wisenet.com

WE MOVE with trust

"… Una cadena es tan fuerte como su eslabón mas débil…."

Hanwha Techwin