Product Brochure

Prevent Successful Cyber Attacks and Simplify Operations

IDIS Cybersecurity

In the modern environment, the threat of cyberattacks against a video surveillance system has increased, making cybersecurity a top area of concern for customers and operators. Beyond traditional local and hardware security measures, the integrity, confidentiality, and accessibility of video surveillance data must be protected during recording, retrieval, and while in-transit. Users now look to manufacturers and the leveraging of modern technology, best practices, and features to meet these challenges.

IDIS, South Korea's largest surveillance manufacturer, has consistently and aggressively considered cybersecurity concerns from R&D through customer installation, developing a rich and comprehensive set of technologies and features to ensure maximum protection for end users of their popular end-to-end line of hardware and software solutions. In addition to educating installers and integration partners on the importance of designing and implementing a physically separate network (or partitioning an isolated VLAN on shared network equipment), IDIS IP surveillance features a comprehensive, layered, and multi-pronged approach to ensuring maximum cybersecurity for users. This approach focuses on three main areas: secure data access, secure data transmission, and secure data recording.

Secure Data Access

DirectIP®

Firewalls on NVRs

Two-Factor Authentication

Secure Data Transmission

Transport Layer Security (TLS)

FEN Security

Secure Data Recording

iBank

Chained Fingerprint

Edge Encryption Recording

IDIS® One Solution. One Company.

IDIS Cybersecurity

IDIS DirectIP®

Network security through a powerful mutual authentication system

IDIS DirectIP plug-and-play technology mutually authenticates all IDIS IP products. When IDIS IP cameras are connected to an IDIS NVR, both devices mutually authenticate each other automatically. This ensures both sides identify and recognize who they are communicating with before the communication session is established. The authentication data is stored and protected on both the IP camera and the NVR.

In addition, DirectIP mitigates against human error by eliminating the need to manage multiple IP addresses and associated passwords during implementation and maintenance.

Firewalls On NVRs

IDIS Firewalls on NVRs utilizing IP and port authentication

IDIS NVR products have their own firewall installed that monitors and controls incoming and outgoing network traffic based on a predetermined set of security rules, including IP, MAC address, and port authentication. The firewalls on IDIS NVR products are designed and pre-configured to prevent unauthorized access.

Two-Factor Authentication

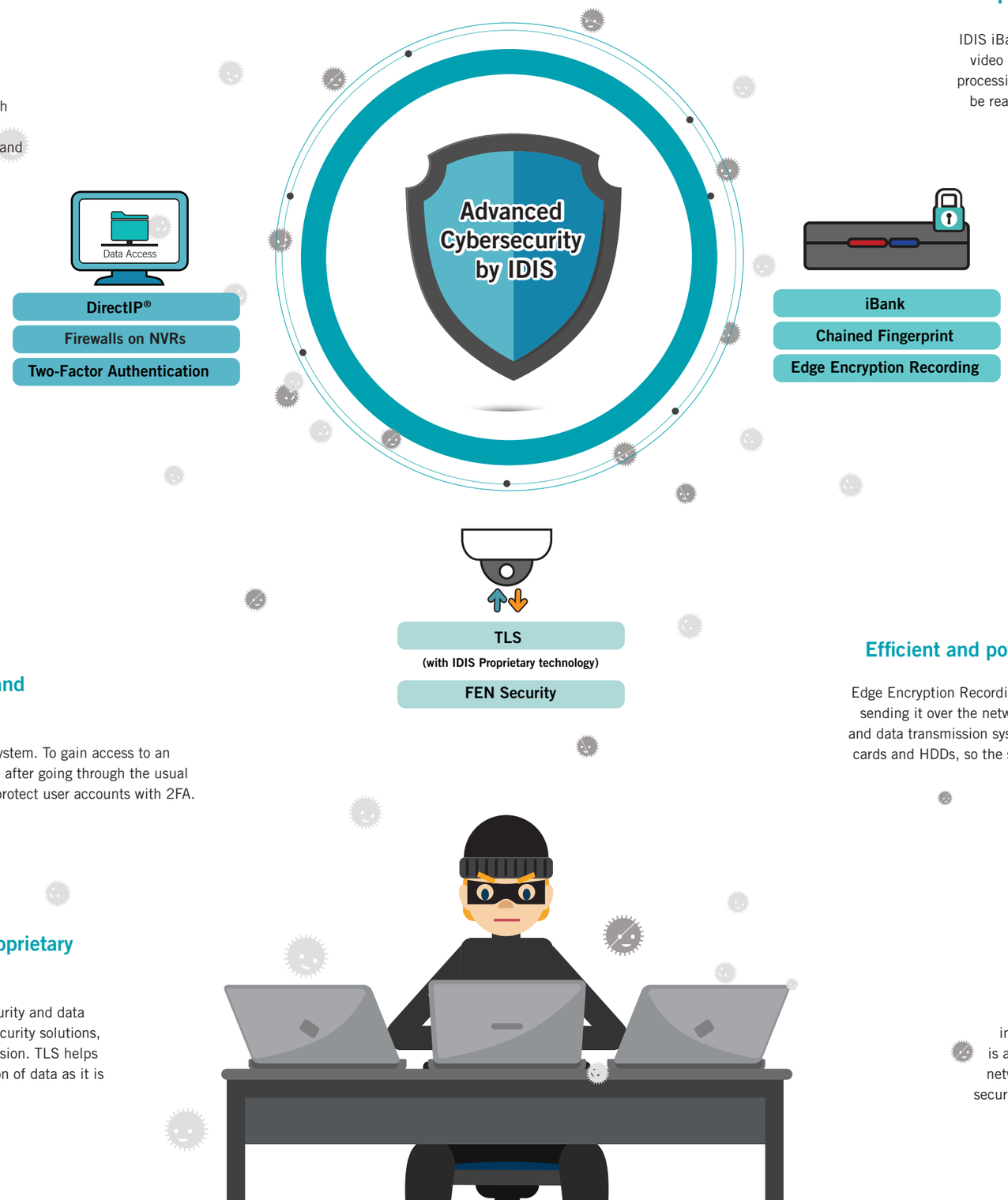
Multi-factor authentication utilizing user accounts and a registered mobile app

Two-factor authentication (2FA) is a type of multi-factor authentication system. To gain access to an IDIS NVR, the user needs to certify themselves with the IDIS Mobile App after going through the usual login process by typing in a user ID and password. All IDIS NVRs safely protect user accounts with 2FA.

Transport Layer Security (TLS)

Data transmission security combined with IDIS's proprietary technology with TLS

TLS is a cryptographic protocol designed to provide communications security and data integrity over networks. By integrating TLS into IDIS's proprietary data security solutions, there is minimal performance impact on video surveillance data transmission. TLS helps prevent malicious activities such as sniffing, modification, and destruction of data as it is transmitted between devices across a network.



iBank

Protect data using IDIS's proprietary database system

IDIS iBank is a database system, developed and patented by IDIS, specifically for video recording. This system maximizes storage efficiency and enables fast data processing. In addition, storage devices that implement the iBank solution cannot be read by external devices such as PCs, keeping the data safe from forgery and alterations. The iBank system is used in all IDIS's recording systems.

Chained Fingerprint

Preventing data forgery and maintaining data integrity

IDIS's Chained Fingerprint technology extracts distinctive features of recorded video data to create fingerprints for each frame and then embeds each fingerprint into the data of the next frame, connecting each frame together with the next like a blockchain. Video data created with Chained Fingerprint technology can be submitted to courts as evidence since an alteration to any frame is easily and quickly detectable, making it simple to prove the footage is authentic and unchanged. It is a highly efficient technology for ensuring and proving the integrity of users' recorded video data.

Edge Encryption Recording

Efficient and powerful technology for encrypted video data recording

Edge Encryption Recording technology encrypts the video data at the IP camera before storing and sending it over the network. Therefore, additional encryption and decryption processes on storage and data transmission systems are not necessary. The encrypted data is recorded directly to the SD cards and HDDs, so the stored data is safe from unauthorized access and alteration even if the SD cards or HDDs are stolen.

For Every Network (FEN) Security

Access and data transmission security system over a public network

FEN from IDIS is an access and data transmission security system independently developed by IDIS using peer-to-peer (P2P) technology. FEN is an automated network configuration service which simplifies installation of networked surveillance systems. FEN enables the user to setup and configure secure surveillance systems without needing a in-depth knowledge of routers or IP networking.