LOGIPIX'S COMPREHENSIVE APPROACH TO CYBERSECURITY

INTRODUCTION TO CYBERSECURITY

In today's digital age, the importance of cybersecurity cannot be overstated. With the increasing prevalence of cyber threats and attacks, safeguarding sensitive data and systems has become paramount. In this landscape, Logipix offers effective cybersecurity measures to protect its systems and components throughout their entire lifecycle.

FOUNDATIONAL CYBERSECURITY MEASURES

Logipix's commitment to cybersecurity begins with a foundation of basic protections that are always active. One of the fundamental elements of our security architecture is the implementation of proprietary encryption similar to SSL/TLS for all communication. This encryption utilizes asymmetric strong 2048 bit RSA certificate, integrated into the license key, ensuring authentication of endpoints and fostering secure, private communication resilient against spoofing attacks.

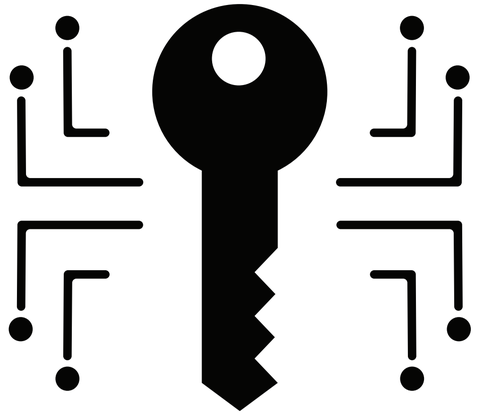
ADVANCED SECURITY FEATURES

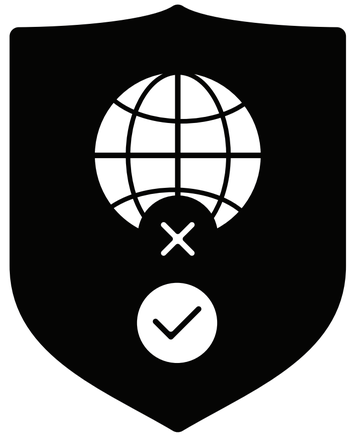
Logipix separates the camera network from the server/client network by default, a proactive measure that blocks attacks directed towards recording. Further protection is ensured as Logipix disables SSH/HTTP(S)/Telnet access and limits system integrators' interaction to use Logipix Management Software components.

Tamper-protected storage and the utilization of cryptographic keys add another layer of defense against unauthorized access. Additionally, Logipix implements anti-DoS protection mechanisms, mitigating the risk of denial-of-service attacks that could disrupt system functionality.

PROTECTING RECORDED DATA

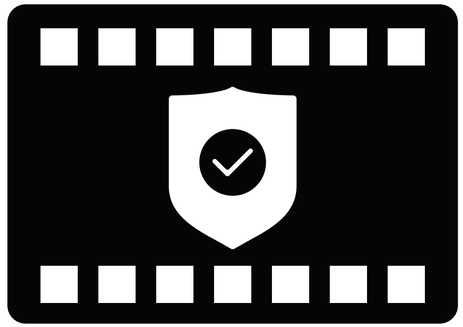
To prevent unauthorized access to recorded data, Logipix employs stringent measures such as binding NVR HDDs to the NVR and formatting disks upon insertion into another NVR, stopping attempts to steal recordings. Recordings are secured by cryptographic binding of HDDs to their designated NVRs, preventing unauthorized use of drives elsewhere.





CRYPTOGRAPHIC EXPORT

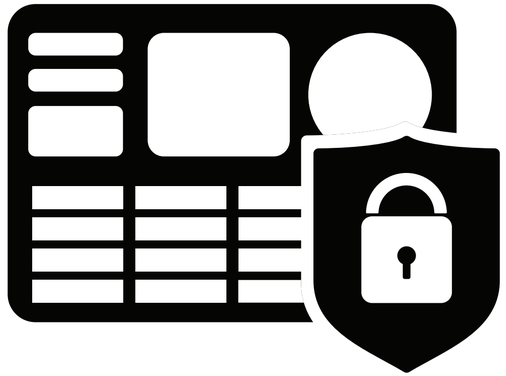
The option for cryptographic signing of exported recordings empowers users to enhance data integrity and authenticity, further bolstering their cybersecurity posture.



CYBERSECURITY ENHANCEMENTS

Logipix also offers enhanced cybersecurity features, such as full encryption of raw video streams and recordings, ensuring end-to-end protection of sensitive footage. Devices are bonded to the system, requiring a full factory reset before they can be repurposed. A security measure ensures data remnants are effectively erased, including video encryption keys, during the reset process, rendering recordings on disks unrecoverable.





PRIORITIZING DATA RESILIENCE

All configuration parameters of a certain device is automatically generated by the Logipix configuration service based on a system level configuration stored in an SQL database. The SQL database is running on a server computer in a secured server room environment.

Logipix prioritizes data resilience by implementing daily backups of the SQL database, a proactive measure that can mitigate data loss in the event of a ransomware attack or other catastrophic incidents.

FIRMWARE UPDATE VERIFICATION

Logipix digitally signs its firmware update files. This signature is verified by the device's firmware before it can be processed further.

SECURE BOOT

The SoC in the Logipix system provides a tamper resistant hardware environment for running the FPGA hardware, the operating system and the application. The SoC has an internal, secure and tamper proof storage area to store device specific keys for the internal AES/HMAC decryption/signature engine. The boot loader reads the firmware from an external flash memory, and uses the internal AES/HMAC decryption/signature engine to decode the encrypted firmware.

COMPREHENSIVE SOURCE CODE VALIDATION

The firmware source code is analyzed using various static analyzers and compiled with hardening options, providing runtime protection against certain types of attacks.

VULNERABILITY ASSESSMENT AND PENETRATION TESTING (VAPT)

Before every new release, Logipix undergoes rigorous Vulnerability Assessment and Penetration Testing (VAPT) to ensure the robustness and security of its systems. This proactive approach aims to identify and address potential weaknesses in the software and hardware components, reducing the risk of exploitation by malicious actors.

The VAPT process includes a comprehensive assessment of the entire system, including network infrastructure, software applications, and firmware. This assessment involves scanning for known vulnerabilities, misconfigurations, and weak security controls that could be exploited by attackers.

Using a vulnerability manager software, ports are scanned and tested against a broad database of 300k+ software and 160k+ network vulnerabilities. The software also categorizes vulnerabilities by severity and recommends mitigation.

VULNERABILITY REPORTING

Despite comprehensive cybersecurity measures, vulnerabilities may occasionally arise. When a potential weakness is detected, Logipix maintains an open and accessible reporting channel to ensure prompt action. Reports can be submitted via a monitored email mailbox, allowing anonymous disclosure while encouraging identification to enable effective communication and timely resolution.





CONCLUSION

In essence, Logipix's approach to cybersecurity encompasses both foundational and advanced measures, addressing threats at every stage of the product lifecycle. By integrating robust encryption, network segmentation, access controls, and data resilience strategies, Logipix ensures that its systems and components remain resilient against cyber threats, providing peace of mind to its users in our ever-evolving digitized world.