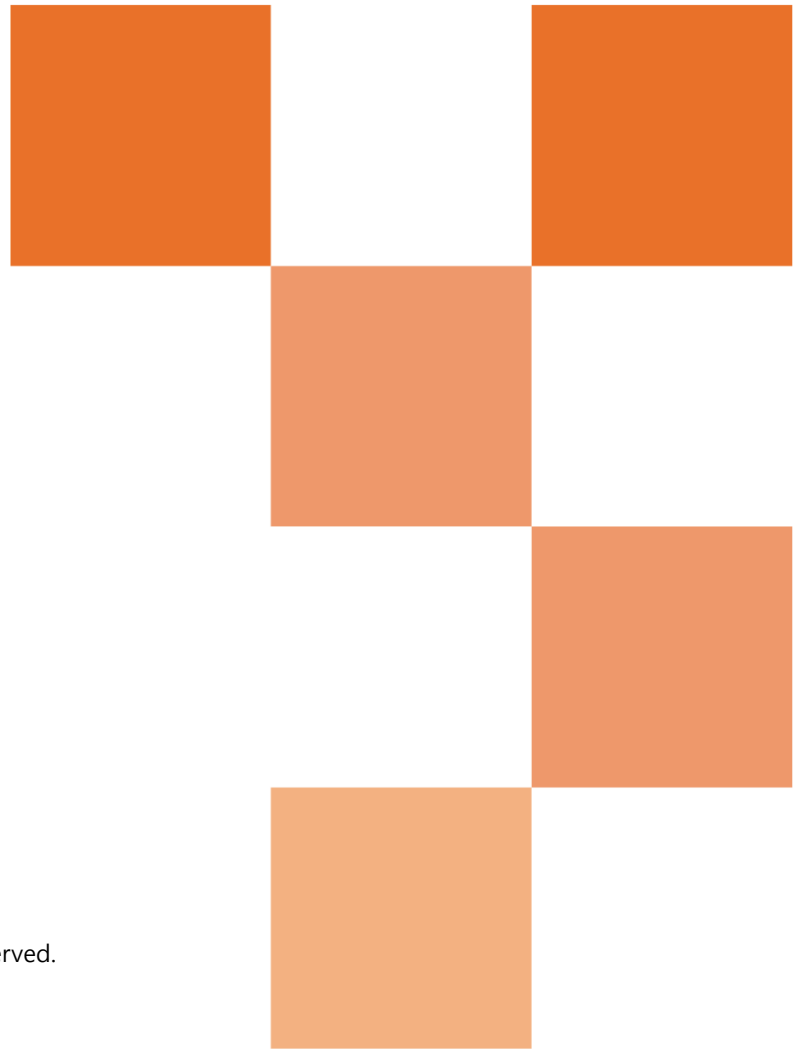
Hanwha Vision

White Paper

BLAZE Cyber Security

March 2026



Contents

1. Introduction

This white paper is intended for security administrators, system users, and video operators, explaining the cybersecurity technologies and response strategies of the BLAZE system. Hanwha Vision designs its software products to provide a high level of protection against various internal and external cybersecurity threats. This document defines the most common types of cybersecurity threats and describes the technical and procedural methodologies Hanwha Vision applies to protect BLAZE systems.

2. Background

A cyber-attack refers to a malicious and deliberate attempt by an individual or organization to breach the information system of another individual or organization. According to Cisco's 2024 Cybersecurity Readiness Index, more than half of the organizations that experienced a cyberattack suffered financial losses of at least $300,000, with 12% reporting massive damages exceeding $1 million. The primary motivation for these attacks remains financial gain through ransomware. Attacks also occur in the form of "Hacktivism," aimed at disrupting or causing confusion in normal business operations. Since the motives and actors behind cyber-attacks are diverse and primarily target vulnerable business systems, cyber-attacks in the IP video security field frequently occur as attempts to cover up criminal acts captured or recorded by the system. Therefore, cybersecurity in the video security sector is considered even more critical.

3. Cyber-Attack Types and Defense

The types of cyber-attacks are very diverse, with the most representative types including malware, phishing, man-in-the-middle (MITM) attacks, DDoS, SQL Injection, and zero-day exploits. While it is important to understand these attack types and establish defense measures, video security personnel who are well-versed in these types can quickly recognize and establish defense strategies when a cyber-attack occurs.

3.1. Malware

Malicious software installed by exploiting vulnerabilities in operating systems or software. It can be used to intercept user credentials and video streams, and poses a potential risk of degrading system performance due to interference with system or network resources.

3.2. Phishing (Social Engineering)

An attack method where an attacker impersonates a trusted source to steal login credentials, often via phishing emails. BLAZE mitigates the risk of credential theft by separating authentication methods.

Local administrator access is strictly controlled, requiring re-initialization if lost, while cloud portal accounts for BLAZE Cloud services provide a secure, email-based password recovery process. This allows legitimate users to safely regain access even if targeted by phishing.

3.3. Man-in-the-Middle (MITM)

An attack where an attacker intervenes between two communicating parties to intercept sensitive data. BLAZE is designed to counter this via secure communication features, including TLS-based encryption and HTTPS[1] communication[2].

[1] When using HTTPS, TLS employs a combination of cryptographic algorithms—including key exchange, encryption, and hashing techniques—to secure the traffic.

[2] Video encryption is implemented via TLS between the Server and Client; SRTP is not currently supported.

3.4. Distributed Denial of Service (DDoS)

This attack causes excessive traffic to a system, server, or network to exhaust resources, paralyzing the system's ability to function normally. BLAZE's server status monitoring feature detects abnormal conditions such as sudden traffic spikes or high system resource consumption in real-time. This enables operators to quickly recognize and respond to potential availability threats, including DoS/DDoS attacks.

3.5. SQL Injection

Occurs when a malicious actor inserts code into a server running an SQL database to force the server to reveal information. BLAZE utilizes OWASP standards to prevent SQL Injection attacks and applies rigorous input validation and data sanitization techniques.

3.6. Zero-Day Exploit

Occurs after a vulnerability is discovered but before a patch or solution is implemented. Hanwha Vision operates S-CERT, a professional team dedicated solely to product and service security. This team identifies and manages risks proactively by performing precision security tests and diagnostics (Vulnerability Assessments) to find potential flaws before attackers do. They also continuously scan and audit open-source components and the latest CVE (Common Vulnerabilities and Exposures) databases to ensure all libraries are secure and up-to-date. Furthermore, a dedicated response strategy minimizes exposure time by monitoring global security intelligence and issuing CVEs alongside emergency patches upon the occurrence of a zero-day vulnerability. Release notes specify the application of security patches, while detailed vulnerability info, affected models, and fixed versions are provided in separate CVE reports.

3.7. Password Cracking

In password-based attacks, hackers use software and Brute Force Attacks to access secure accounts. BLAZE implements account lockout policies (to prevent brute force), enforces password complexity requirements, and uses secure authentication for BLAZE Cloud-connected systems.

4. BLAZE Cybersecurity Defense Framework

BLAZE is continuously being sophisticated to respond to cybersecurity threats. This defense framework is implemented through a strategic combination of security technologies and rigorous processes.

4.1. Device Discovery & Registration

BLAZE utilizes a credential-validated discovery mechanism to prevent security threats from aggressive automatic discovery. Unlike indiscriminate background scanning, BLAZE is designed to go through appropriate authentication during the discovery phase, preventing device conflicts (such as lock-outs) and ensuring secure connectivity.

4.2. User Rights Management

BLAZE operates on the Principle of Least Privilege. User permissions are strictly managed so individuals can only access resources and data essential for their duties. Specifically, it uses Role-Based Access Control (RBAC) and license verification. RBAC allows administrators to set granular permissions for each user or group to limit access to specific cameras, features, or system settings. License integrity verification ensures only authorized instances are activated via hardware unique values (Appliance) or the Sales Hub (Software).

4.3. API Security

To protect system interfaces from unauthorized manipulation, BLAZE applies strict security measures to all API interactions, consisting of token-based authentication, input validation, and privilege separation. Token-based authentication strictly performs user authentication and permission checks for all API requests. Input validation filters malicious data to prevent injection attacks. Privilege separation ensures users cannot escalate privileges or access unauthorized endpoints.

4.4. Audit Trail

BLAZE maintains comprehensive logs of all security-related events and user activities. This includes integrity assurance to protect logs from unauthorized modification or deletion, privacy masking to exclude sensitive information from logs to prevent data leakage, and cyclic logging to ensure continuous monitoring by sequentially overwriting old logs when storage limits are reached.

4.5. Authentication Security

BLAZE applies a multi-layered authentication scheme designed for rigorous identity verification. By combining industry-standard hash algorithms for credential storage, strict policies for local management, and secure session management protocols, BLAZE minimizes the risk of unauthorized access.

4.6. Password Security

BLAZE utilizes industry-standard encryption algorithms to protect user credentials. Hashing ensures user passwords are treated with strong algorithms, providing resistance against rainbow table attacks. The Strict Admin Recovery Policy prioritizes security over convenience; lost administrator passwords cannot be reset and require a full re-initialization of the software or appliance. Brute Force Defense enforces account lockout policies to block repeated login attempts.

4.7. User Enumeration Detection

To prevent attackers from guessing valid usernames, BLAZE does not reveal whether a login failure was due to an incorrect username or an incorrect password. A consistent error message is displayed regardless of the reason.

4.8. Session Management

BLAZE uses token-based authentication for stateless, secure session management. It also utilizes Token Security by synchronizing the refresh token lifespan with session timeouts. Client-side credentials for auto-login are stored in an encrypted database (not plaintext) to protect auto-login.

5. BLAZE Cybersecurity Implementation Cases

5.1. Data Protection at Rest

To maintain system integrity, protecting stored data is paramount. BLAZE employs a multi-layered access approach to safeguard both system configurations and recorded media. This is achieved by implementing security for system settings and credentials, along with comprehensive protection for media and video data.

5.1.1. System Configuration and Credential Security

BLAZE uses advanced database encryption to protect sensitive system data from theft. Important data, including device passwords, cloud credentials (tokens), and configurations, are subjected to industry-standard strong encryption. It also implements a hierarchical key management strategy, separating Data Encryption Keys (DEK) and Key Encryption Keys (KEK).

5.1.2. Media and Video Data Protection

Strict security controls are applied to prevent unauthorized access to video data. Internal recordings are protected by OS-level access control, restricted only to authorized BLAZE services. Exported video data is secured using cryptographic hashing and digital signatures (Archive and Backup Integrity), ensuring any tampering can be detected immediately.

5.2. Secure Communication

To prevent data interception and tampering during transmission, BLAZE enforces encryption by default across critical network channels. From client-server interactions to cloud connectivity, robust TLS protocols are utilized to ensure that sensitive control commands and video data remain confidential while in transit.

5.2.1. Encryption Standards:

Supports only TLS 1.2 or higher and prohibits the use of obsolete algorithms (e.g., TDES, ECB mode). Encryption keys utilize high bit-strength to ensure resistance against modern decryption attacks.

5.2.2. Security by Communication Segment:

No intrusion is tolerated across the connections between Client, Server, Cloud, and Camera. Between the Client and Server, all Command-and-Control traffic is encrypted via HTTPS. Video streams are protected using TLS-based encrypted RTP and RTSP, ensuring that unauthorized third parties cannot intercept live or recorded footage. Security between the Cloud and Server is managed by using MQTT over TLS and HTTPS for communication with the cloud portal. Communication between clustered Servers is established using HTTPS and WSS (WebSocket Secure), which guarantees secure data synchronization and system integrity. For Camera and Server connections, BLAZE supports HTTP, HTTPS, and RTSP protocols. We recommend enforcing HTTPS for secure device management. For sensitive data, authentication tokens and personal information are never transmitted in plaintext.

5.2.3. Cloud Connectivity:

Utilizes a Cloud Connector architecture. The system initiates outbound connections to the cloud using unique identifiers, eliminating the need for inbound port forwarding (Port Mapping) and reducing the attack surface.

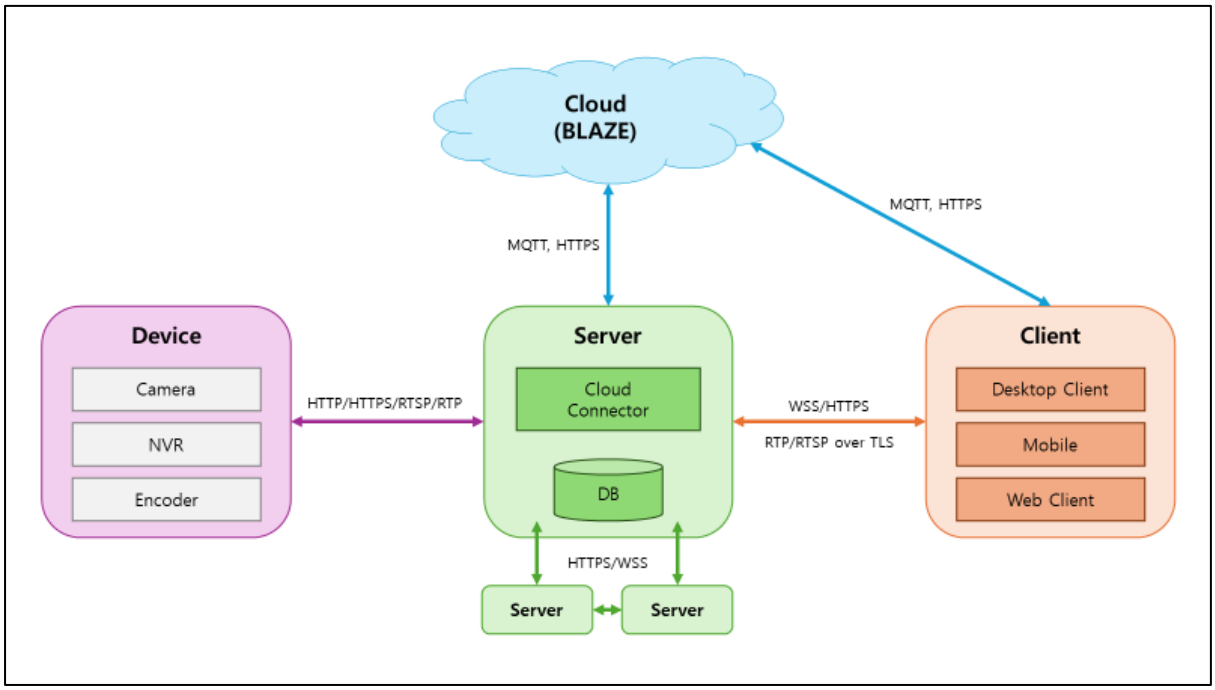


Figure 1: BLAZE Secure Communication Architecture

5.3. Mobile and Client Security

Security extends beyond the server to the edge. BLAZE mobile and client applications implement platform-specific encryption standards and memory protection techniques to ensure that user terminals do not become vulnerable paths for system penetration.

5.3.1. Secure Mobile Storage

BLAZE mobile apps utilize platform-specific hardware security modules (e.g., Android Keystore, iOS Keychain) for native OS-level encryption.

5.3.2. Client-Side Protection:

UI Masking prevents "shoulder surfing" by masking sensitive info like passwords. Sensitive data is strictly managed in memory or secure storage and is never saved as plaintext on the client device.

5.4. Risk Prevention and Management

BLAZE was designed based on a proactive security framework. Hanwha Vision minimizes the attack surface and ensures the integrity and trustworthiness of all software components through a rigorous Secure Development Lifecycle (SDLC), continuous vulnerability monitoring, and code signing.

5.4.1. Secure Coding

BLAZE is developed using a rigorous Secure Software Development Life Cycle (SSDLC). All input data is validated against a strict whitelist, and input validation is performed through processes such as data sanitization to prevent SQL Injection and XSS attacks. Hardcoded credentials and debug backdoors are strictly prohibited, and unnecessary services and ports are disabled by default.

5.4.2. System Integrity and Updates

All software packages are digitally signed to ensure their origin and integrity. Appliance firmware (OS/BIOS/SW) is packaged and encrypted to prevent tampering, and digital signatures are applied using code signing to verify the integrity and legitimacy of update files. This fundamentally blocks file tampering and Man-in-the-Middle (MITM) attacks. Updates are securely conducted through either an online method via the Hanwha Vision update server or a local method via direct upload.

Software Package	Digital Signature
Windows	Code Signing
macOS	Notarization & Hardened Runtime
Linux	GPG Signing

5.4.3. Continuous Security Evaluation

Hanwha Vision operates continuous security evaluation programs, including an Internal Bug Bounty Program to encourage responsible reporting of flaws and Third-Party Penetration Testing performed bi-annually (twice a year) for objective validation against the latest threats.

6. Conclusion

Hanwha Vision's BLAZE effectively thwarts cyber threats through a multi-layered security architecture that incorporates over TLS 1.2 based communication encryption, continuous vulnerability monitoring by the S-CERT team, and the principle of least privilege. By providing technical and procedural responses to diverse attack types—ranging from malware to zero-day exploits—it ensures the confidentiality, integrity, and availability (CIA) of video security while maximizing customer operational efficiency.

Going beyond a simple Video Management System (VMS), BLAZE is evolving into a security solution that embodies "Secure by Design" principles throughout its entire lifecycle, from development to deployment. It minimizes the attack surface through innovative designs such as API token authentication, database-level encryption (DEK/KEK), and outbound cloud connectors, while maintaining robust security through compliance with OWASP guidelines, input validation, and code signing (GPG, etc.). Hanwha Vision remains committed to building global trust by preemptively addressing future threats through continuous security enhancements and protecting the digital assets of its customers.

Hanwha Vision Co.,Ltd
13488 **Hanwha Vision** R&D Center,
6 Pangyo-ro 319-gil, Bundang-gu, Seongnam-si, Gyeonggi-do
TEL 070.7247.8771 **FAX** 031.8018.3715
www.HanwhaVision.com