Arthrex Synergy Vision™ Console Product Software Security

Introduction

Arthrex strives to design and develop secure products by following the Secure Product Development Framework (SPDF) approach. The SPDF process contains the suggested steps and best practices for addressing security and privacy throughout the software product lifecycle, including during the design, development, production, distribution, deployment, and maintenance of an electronic medical device or software produced by Arthrex.

Building Security Into Arthrex Products
The effort to build security into Arthrex products is driven by industry standards, best practices, and premarket and postmarket regulatory guidance. During the SPDF process, the Product Development Security Engineering group works with the Development, Product Management, Integrations, and Support teams to promote a comprehensive, security-conscious approach and culture to foster the delivery of secure products.

Secure Development Lifecycle
As part of every product's SDL the following tasks are required where appropriate:

- **Security training:** Role-based training specific to product security and privacy
- **Security Planning:** Integrating security in the design and development processes
- **Cybersecurity risk analysis:** Identifying and analyzing cybersecurity risks in the product design
- **Threat modeling and risk analysis:** Identifying product-specific cybersecurity threats
- **Software bill of materials (SBOM):** Identifying vulnerabilities in software components for open-source software and third-party software validation
- **Static code analysis:** Using automated tools to detect defects and security flaws in code
- **Vulnerability scanning:** Using automated tools to detect security vulnerabilities in running systems
- **Penetration testing:** Attempting to circumvent security controls and uncover vulnerabilities in running systems
- **Product security review:** Examining the results of the SPDF activities
- **Production monitoring:** Surveilling software and systems for new threats or issues using automated tools and customer feedback

Conclusion

Arthrex is dedicated to building secure products that Help Surgeons Treat Their Patients Better® by establishing oversight procedures that identify and mitigate potential product security risks through the software product life cycle and creating programs and practices that drive software security initiatives and awareness across the company.

Technical and Organizational Measures

Technical and organizational measures are implemented to ensure protection of the security and privacy of processed data. These measures are designed in accordance with data protection laws and take into account state of the art, the costs of implementation, and the nature, scope, context, and purposes of the processing. Risks, including those to the rights and freedoms of natural persons, are also considered. These measures help prevent accidental or unlawful destruction, loss, alteration, and unauthorized disclosure of or access to the transmitted, stored, or otherwise processed data.

Technical and organizational measures include:

- Safeguarding physical access to buildings and facilities in which IT systems used for personal data processing are operated
- Preventing unauthorized persons from accessing or using hardware for processing personal data
- Ensuring access to systems and personal data is limited to authorized personnel acting within the scope of their authorization
- Confirming personal data cannot be read, copied, altered, or removed without authorization during electronic transfer or transport
- Securing personal data against destruction or loss
- Safeguarding the integrity of personal data

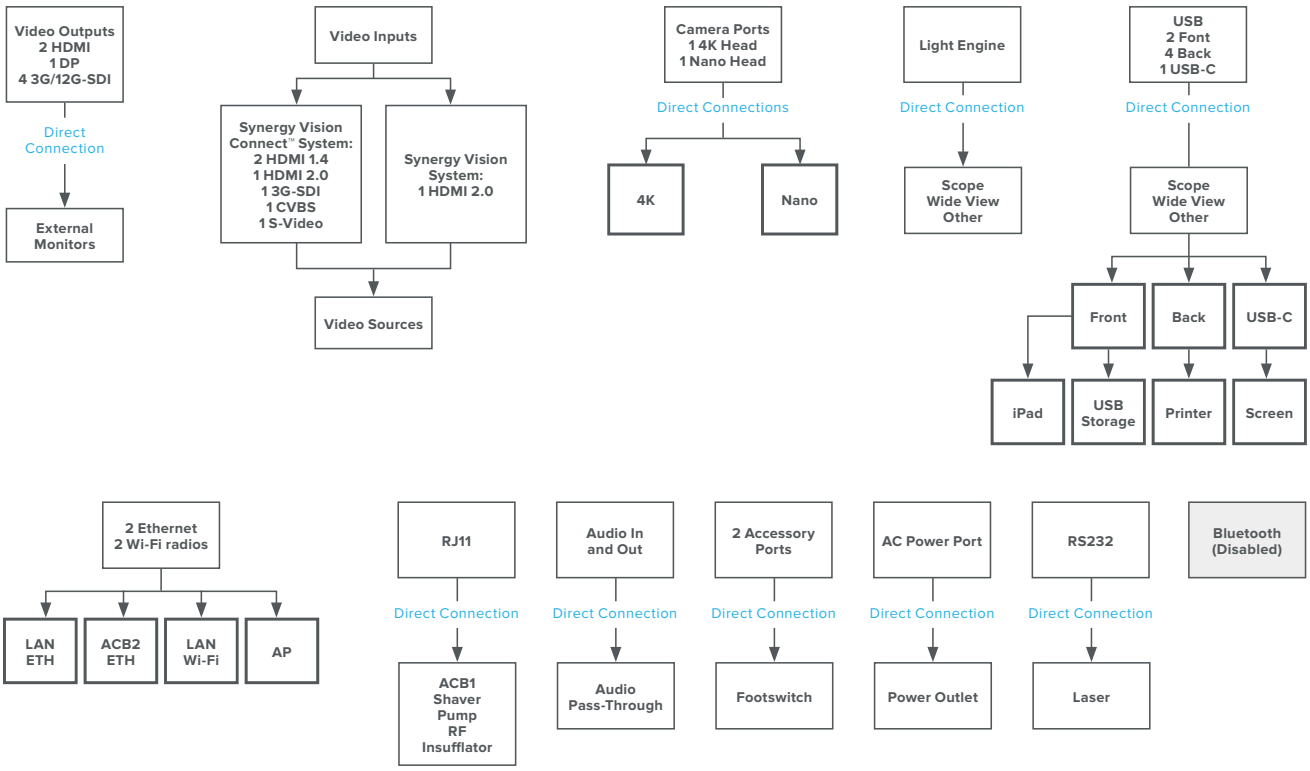
Please find more information about Arthrex privacy policies at link: privacy.arthrex.com/our-commitment-to-privacy/toms.html

System Introduction

The Synergy Vision™ console is a next-generation endoscopic imaging system that integrates high-definition camera technology, minimally invasive camera technology, LED lighting, and an image management system into a single console.

Synergy Vision™ System's Back Panel

System Diagram



System Controls Information

System Access and Use Overview	The Synergy Vision™ console is most often located in a surgical operating room. Surgeons interact with the system using attached arthroscopic cameras. Surgical staff interact with the system via the touchscreen panel.
Operating System	Custom Linux-based OS built on the Yocto Linux framework leveraging version 4.0, also known as kirkstone.
System Data Classification	Protected health information
Data Storage	Data is stored on internal NVMe storage physically secured within the device. Users may elect to store data outside the system on a network share, PACS/VNA, EHR, or external USB device.
Data Security	Sensitive data at rest is protected by industry standard encryption methods. The Synergy Vision console employs LUKS2 encryption to encrypt the contents of the storage volumes for data at rest. LUKS2 uses an AES-256-GCM cipher in XTS mode with a key size of 512 bits. Data in transit is protected by TLS v1.2 when sent to Synergy.net™ data integration software.
Data Export	Data can be exported to the Synergy.net data integration software or to an EHR repository (HL7) or USB drive.
Data Deletion	The system will automatically delete data either when a high watermark threshold is achieved for remaining storage or when a facility-defined number of cases (between 1 and 200 cases) are stored on the device. The system also supports a manual purge of all data if needed.
Retention	Facilities can choose the number of cases they want to retain on the device. This varies between a single case and 200 cases. Once the set threshold for cases is met, the system will automatically purge the oldest case stored on the device each time a new case is created.
Network Security	Secure connections using TLS 1.2 encryption or SSH are required for the encryption of data in transit.
Certificates	Arthrex uses commercially available certificates for software signing and system support.
Authentication	Authentication requires a unique username and password on the system. Authentication may occur locally using complex passwords or may occur via Active Directory.
Authorization	Role-based access control (RBAC) is used.
Audit Logging	Logs of all user accounts are kept. Additionally, any time a record is created, viewed, modified, or deleted, a log is made to ensure the record's chain of custody is maintained. All entries in the audit logs are stamped with the time and date.
Accountability	Arthrex is responsible for releasing patching and assisting with upgrades to the device. Customers are responsible for scheduling and requesting patch deployment.
Software Patching/Upgrade	Arthrex is the sole developer of the Synergy Vision console and maintains software patches and upgrades for the system. Standard patches for the Synergy Vision console are issued via signed system updates and are distributed through field service upgrades. Emergency patches for the Synergy Vision console are issued via signed hot-fix updates and are distributed through field service upgrades and emergency field notifications.
Support	Support for the Synergy Vision console can be obtained through telephone or email.
Ports, Protocols, and Services	Please reference the Manufacturer Disclosure Statement for Medical Device Security (MDS2) document.

Note: MDS2 is maintained where applicable and contains additional important end-user-recommended cybersecurity controls.

arthrex.com