NanoScope™ Product Software Security

Introduction

To design and develop secure products, Arthrex follows the Security Development Lifecycle (SDL) approach. The SDL process implemented at Arthrex includes the steps and best practices for addressing security and privacy throughout the software product lifecycle (eg, the design, development, production, distribution, deployment, and maintenance of an electronic medical device or software).

Building Security Into Arthrex Products

Designing products with security in mind is driven by industry best practices along with premarket and postmarket regulatory guidance. During the SDL process, the Product Software Security 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 Life Cycle

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 during the design process
- **Product Security Requirements Scorecard**: Security standards for the Development team to follow
- **Threat Modeling and Risk Analysis**: Identifying security flaws and risks in the product design
- **Open-Source Software and Third-Party Software Validation**: Identifying and fixing vulnerabilities in software components
- **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
- **Security Review**: Examining the results of the SDL activities
- **Production Monitoring**: Monitoring software and systems for new threats or issues using automated tools and customer feedback

Conclusion

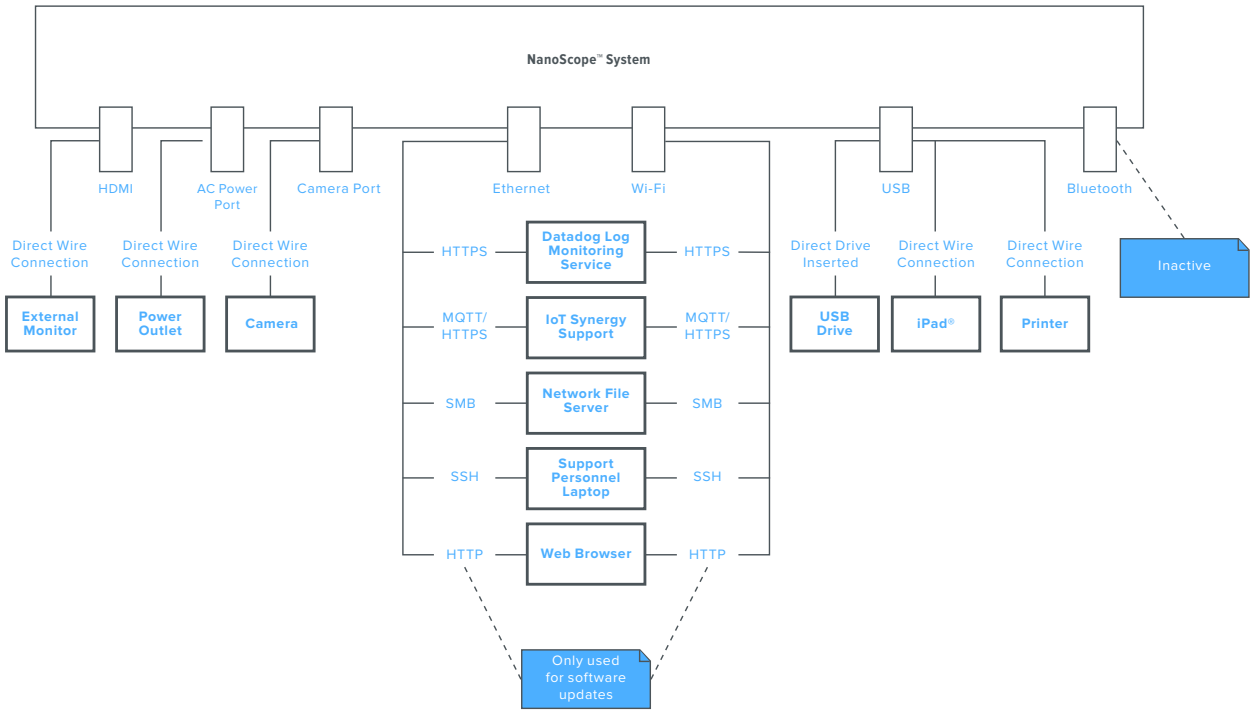
Arthrex strives to build secure products that Help Surgeons Treat Their Patients Better™ by establishing oversight procedures that identify and mitigate potential product security risks during the development and installation of programs and practices that drive software security initiatives and awareness across the company.

System Introduction

The NanoScope system is the first medical-grade, 3-in-1, single-use camera system. The chip-on-tip NanoScope system combines the latest technology in 1 mm imaging sensors, LED lighting, image management, and OR integration with an intuitive touchscreen tablet. An alternative to MRI imaging and second-look arthroscopy, the system provides precise, direct image-guided visualization of injections.

Arthrex helped pioneer operative arthroscopy and continues to innovate with Nano operative arthroscopy. The minimally invasive patient experience and unlimited atraumatic access to joint spaces make the NanoScope system and Nano arthroscopy instrumentation the tools of choice for instant diagnostic imaging and less invasive arthroscopy procedures.

System Diagram



System Controls Information

System Access and Use Overview	NanoScope system is an all-in-one, stand-alone system.
Operating System	Arthrex Linux distribution
System Data Classification	Private health information
Data Storage	Data is stored locally with options for storage on SMB and USB.
Data Security	Device storage is encrypted using an encryption key unique to each device.
Data Export	Data may be exported to an encrypted USB drive or SMB drive on the local network.
Data Deletion	Case files can be deleted from the user interface.
Retention	Data remains on the device until the user deletes the case files or the disk becomes full, at which time the oldest case is deleted first in order to store the new case.
Network Security	Secure connections using TLS1.2 encryption or SSH are required for encryption of data in transit.
Certificates	Arthrex uses commercially available encryption certificates.
Authentication	Uses a default admin password that the installer must change. Password complexity rules (eg, uppercase letter, lowercase letter, number, and symbol) are enforced. User processes are run as a nonprivileged user.
Authorization	Role-based access control (RBAC) is used.
Audit Logging	▪ No GUI log viewing option on user interface. ▪ Logs may be exported to USB from the password-protected admin settings. ▪ Logs may be captured and stored remotely if the device is connected to the Internet.
Accountability	Arthrex is responsible for patching and upgrades.
Software Patching/Upgrade	▪ Arthrex is the sole developer of the NanoScope system and maintains software patches and upgrades for the system. ▪ Updates are cryptographically signed and will only be installed if the signature is correct.
Support	Support for the NanoScope system can be obtained through telephone or email communication.

Arthrex Governance Policies and Practices

- Designated Information Security Manager
- Corporate Information Security Policy (ISO27001)
- Designated Privacy and Compliance Manager
- Corporate Privacy and Compliance Policy (HIPAA-HITECH)
- Incident Response Policy
- Disaster Recovery and Business Continuity Policy
- High-Assurance Agile Software Development Life Cycle

arthrex.com