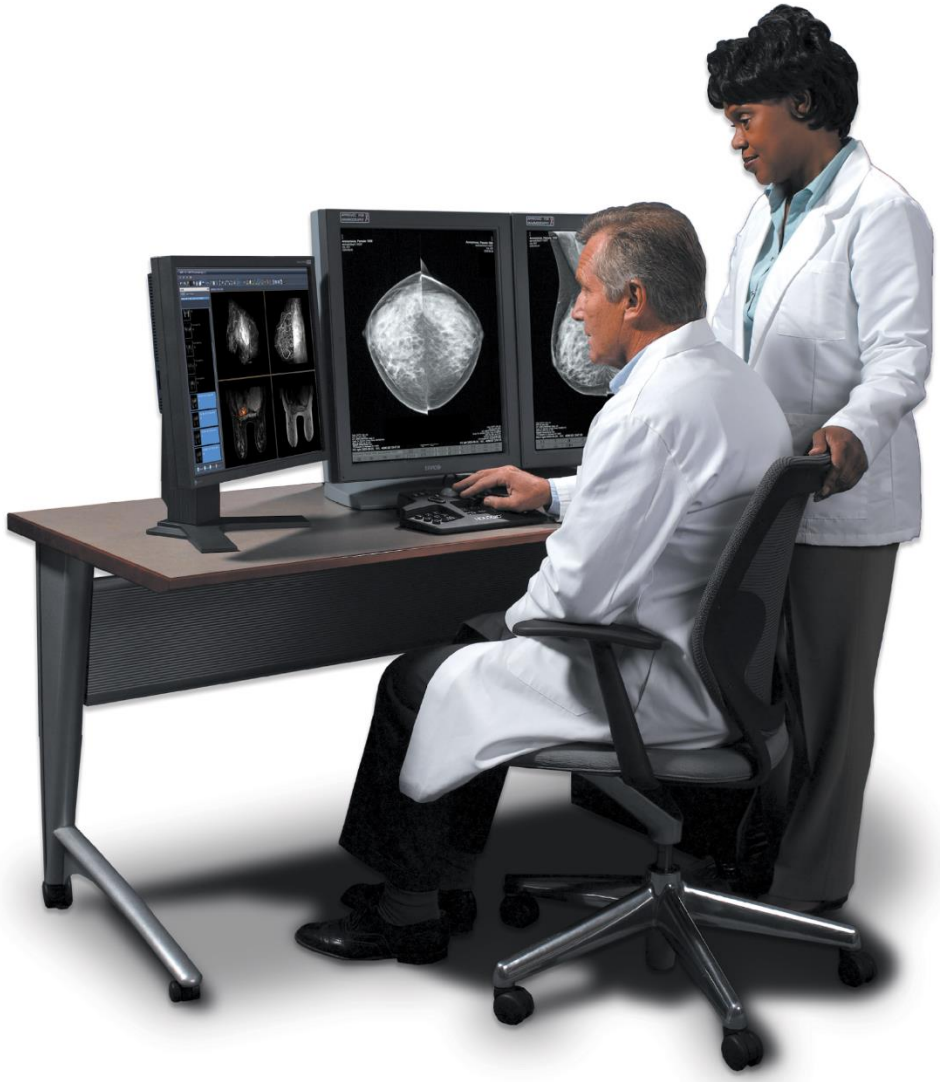
SecurView®

Breast Imaging Workstation



Cybersecurity Product Report

RD-04040 Revision 002

HOLOGIC®

1. Introduction

Hologic is a leading developer, manufacturer and supplier of premium diagnostics, medical imaging systems and surgical products dedicated to serving the healthcare needs of women. Ensuring the integrity of our systems and the business continuity of our customers is a top concern for Hologic. This document is to be used to assist an IT staff in securing their systems and infrastructure where SecurView is deployed.

1.1. Audience

The intended audience includes the systems administrator, network administrator, and/or security personnel. The reader of this document should be familiar with operating systems, networking, and security of computer systems.

2. Cybersecurity

The following sections of this document outline security features and guidelines specific to SecurView workstations. For additional guidance or assistance in implementing security features on SecurView systems, please consult Hologic Technical Support.

2.1. Manufacturer Disclosure Statement for Medical Device Security

For many products, Hologic uses the Manufacturer Disclosure Statement for Medical Device Security (MDS2) to provide HIPAA-related security information about its products. The latest version of the SecurView MDS2 is located in the SecurView Support section of the Hologic website.

2.2. Windows Domain and Active Directory

Since version 8.1, SecurView has supported the use of Active Directory as a mechanism for user authentication. Prior versions did not support this functionality.

2.3. Third-Party Software Packages

2.3.1. Anti-virus

The use of anti-virus software is recommended for SecurView. Installation instructions provided with the anti-virus software product should be used for installation and configuration. If anti-virus software is installed, the following directories[1] should be excluded from real-time scanning as not doing so may affect product performance:

- SecurView-Data-Partition (default F:). The folders in SecurView-Data-Partition are:
  ApplicationEventLog
  DICOM
  DICOMExport
  DICOMImport
  DICOMTemp
  DICOM_Annotation
  DICOM_Spool
  DICOM_SR
  Exports
  Images
  ImagesTemp
  IPCTemp

[1] The paths for these directories may be different for SecurView software-only installation.

Log
MAPTEMP
PrintSpool
ScreenCaptureTmp
ServiceLogfiles
Temp
Thumbnails
TomoImages
Workspace

- Postgres EnterpriseDB-Engine installation folder default:
  "C:\Program Files\PostgreSQL\9.4" (64bit, SecurView 10.x) or
  "C:\Program Files\PostgreSQL\11" (64bit, SecurView 11.0) or
  "C:\Program Files\PostgreSQL\12" (64bit, SecurView 11.1)
- SecurView database folder (default: E:\arcticdata)
- If MultiView Multimodality software is installed, exclude the following folders:

  C:\Program Files\ClearCanvas
  F:\MultiView

2.3.2. Intrusion, Proactive or Network Threat Detection

Real-time intrusion, proactive or network threat detection monitoring software is not recommended to be run when SecurView is active as it may affect performance of the application and greatly impact receipt of and distribution of images in a clustered (manager, client) workstation environment, as well as the communications between manager and client workstations. Intrusion detection could be run in an offline manner on the system when the SecurView application is idle.

2.3.3. Encryption

All new SecurView hardware implements FIPS 140-2 encryption, consisting of AES 256 self-encrypting drives. If encryption is desired, disk encryption is the recommended method for implementing encryption. Software Encryption running on the system may affect the SecurView application's performance. Installation instructions provided with the encryption software product should be used for installation and configuration. Folder encryption can also be employed on the folders listed in section 2.3.1 Anti-virus. It is recommended to consult Hologic Technical Support to better understand the implications of such encryption on performance.

2.4. Operating System Patching

SecurView software versions 10.3 and later run on the Microsoft Windows operating systems: Windows 10 or Windows Server 2016. SecurView software versions 8.x through 10.3 ran on Windows 7 or Windows Server 2008. Microsoft frequently creates patches, service packs, and critical security updates to address potential vulnerabilities in these operating systems.

Due to the fact that vulnerabilities and updates may occur on a more frequent basis and the risk due to vulnerabilities is generally greater than the impact of a fix, customers may implement Automatic Updates for Microsoft Windows. For additional guidance on implementing Automatic Updates, please consult Hologic Technical Support.

Patch release reports of approved patches are available on the Hologic website. It is recommended to have a rollback strategy when applying patches not included in the Hologic patch release reports.