R2 Cenova™

Cybersecurity Best Practices

MAN-00766 Rev 003

HOLOGIC™

Mammography

R2 Cenova™

Cybersecurity Best Practices

MAN-00766 Rev 003

HOLOGIC™

Technical Support

For support in North America contact:

Toll Free:	+1 866.243.2533 (+1 866.CHECKED)
Email:	**r2support@hologic.com**
Hours:	Monday – Friday, 6:00 AM – 5:00 PM, PT (GMT –8:00)
Website:	**www.hologic.com**

You may also reference our Security Center at:
http://www.hologic.com/cc/netwrksec.htm.

Contents

1.   Introduction

Hologic, Inc. develops and markets a full line of digital mammography products including the R2 Cenova server, the Selenia full-field digital mammography system, and the SecurView family of products. Ensuring the integrity of our systems is a top priority for Hologic. This document provides a guide for user 'best practices' to ensure the integrity of Hologic products through their lifecycles. Additionally, this document outlines the most common cybersecurity vulnerabilities and appropriate methods for securing our products.

Hologic currently uses Microsoft 2000/XP operating systems and various UNIX-based operating systems in its computer-based medical products. Although Hologic performs extensive testing prior to the deployment of our computer systems, ongoing computer security threats may pose a significant threat to the security of these systems on a daily basis.

These Cybersecurity Best Practice recommendations have been developed under controlled conditions and have undergone extensive testing. Adherence to these security recommendations will help minimize the risk of cybersecurity threats. An experienced IT professional should be able to follow these instructions with minimal difficulty.

1.1. Overview

Hologic continually monitors the current state of computer and network security to assess potential threats to our systems. Each Hologic product is assigned a Cyber Level of Concern, which classifies the susceptibility and impact of each product to malicious cyber attacks. Once the concern has been identified and properly classified, Hologic performs risk analysis to determine the potential consequences of cyber attacks. Additionally, the risk analysis assesses the potential consequences for actively mitigating the threat by inducing a product change. Any necessary product change Hologic introduces to reduce cyber attacks must be validated to ensure continual operation of our products.

Hologic also has an ongoing maintenance program for the entire lifecycle of our products. The ongoing maintenance program consists of:

- Periodic vulnerability assessments
- Penetration testing
- Laboratory evaluation of antivirus products
- Critical security updates validation
- Creation of a Cybersecurity team

Hologic is committed to delivering and maintaining our products in the rapidly changing environment of cybersecurity threats. To help minimize cybersecurity risk and vulnerabilities, follow the Cybersecurity Best Practices and incorporate them into your facility's security policies and protocols.

1.2. Audience

This document contains information related to cybersecurity and Hologic's R2 Cenova digital mammography server. It is intended to aid in securing the customer's network infrastructure and environment when they incorporate Hologic products.

The reader of this document should be familiar with the Open Systems Interconnection (OSI) model, networking, and network security.

1.3. Remarks

It is recommended that the customer implement and maintain a set of facility security policies and procedures. These security policies and procedures should address the following:

- Discretionary access control (Who needs access to what?)
- Methods of auditing
- Disaster recovery and business continuity plans
- Password reset policy
- Perimeter security – e.g., firewalls, intrusion detection system (IDS), proxy servers
- Internal security – e.g., network topology monitors, log file review, weekly vulnerability scans
- Physical security (e.g., biometrics, locks, cameras)
- Security awareness

It is the customer's responsibility to ensure the confidentiality, integrity, and availability of the information technology resources in his/her organization.

1.4. Definitions, Terms and Abbreviations

The many abbreviations and acronyms used in this document are listed below:

- 802.1q: The IEEE standard for VLAN tagging
- ACL: Access Control List
- AWS: Acquisition Workstation
- CBAC: Content-Based Access Control
- CLOC: Cyber Level Of Concern
- DAC: Discretionary Access Control
- DHCP: Dynamic Host Configuration Protocol
- DMZ: Demilitarized Zone
- Egress: Traffic destined outbound
- FTP: File Transfer Protocol
- IDS: Intrusion Detection System
- IEEE: Institute of Electrical and Electronics Engineers
- IP: Internet Protocol

- ISL: Inter-Switch Link protocol
- LAN: Local Area Network
- Layer 3: Any device that utilizes the third layer of the OSI model (AppleTalk, IP, etc)
- IDS: Intrusion Detection System
- MIMS: Mammography Information Management Solution (Hologic's departmental image archive and connectivity product)
- NEMA: National Electrical Manufacturers Association
- OSI model: Open Systems Interconnection model
- SAM: Security Account Manager (Windows registry file that stores user passwords in an encrypted format)
- VLAN: Virtual LAN
- VNC: Virtual Network Connection
- TCP/IP: Transmission Control Protocol/Internet Protocol suite
- TFTP: Trivial File Transfer Protocol

1.5. References

1 FDA Guidance for Off-The-Shelf Software Use in Medical Devices, 2005
2 FDA General Principles of Software Validation; Final Guidance for Industry and FDA Staff, 2002
3 NEMA Patching Off-the-Shelf Software Used in Medical Information Systems, 2004

2. Network Security

2.1. Active Directory

Many facilities have migrated to Windows Active Directory for easy, centralized administration of their network. While Active Directory has several benefits when deployed correctly, it is recommended you do not make Hologic's systems a part of your existing domain. This may cause undesirable results and system instability.

2.2. IP Address Assignment

The IP address of the system should be statically assigned. The system should not be a DHCP client in order to ensure that our service technicians' records are accurate. This can also prevent denial of service attacks in the event that a rogue DHCP server is deployed in your network.

2.3. Segmentation

Properly segmenting Hologic's products from the rest of your network can further increase the security of the systems. The goal with segmentation is to prevent unauthorized access to the system(s) by utilizing ACLs.

2.3.1. VLANs

VLANs (or Virtual LANs) are a way to create several different broadcast domains on a single switch. VLAN capability is available on most modern switches.

Utilizing VLANs allows you to apply some level of security (access control lists and CBAC) to protect certain extensions of your network. If implemented correctly, this creates a 'virtual' DMZ.

Resources needed:

- VLAN capable switch
- Layer 3 switch OR existing router capable of recognizing different VLAN tagging (i.e., 802.1q, ISL)
- Knowledge of networking and Cisco products

⚠ **Note:** *VLANs were designed for management purposes and not for security. There are specific cybersecurity threats (attacks) where a user can 'jump' VLANs. A more effective way to segment a LAN is to use a physical interface off of a firewall.*

2.3.2. Firewall Segmentation

Many hardware firewalls are equipped with a third interface. This interface is typically used as a DMZ in small- to mid-sized installations. However, this third interface may also be utilized to create protection for machines that need increased security.

2.4. Egress Filtering

It is recommended that you employ egress filtering on your network. This reduces the chances of external data theft and/or loss. In the beginning stages of a system compromise, an attacker will sometimes TFTP or FTP to a remote server that stores privilege escalation tools. Implementing proper egress filtering reduces the chances of this occurring. Furthermore, modern day Trojans have the capability to turn a machine into a mail relay box.

2.5. Network Monitoring

Effective monitoring of your network may detect the initial reconnaissance stages of a potential attack. This is vital information to capture, as it may indicate how and when a system is going to be compromised. Network monitoring can be accomplished by utilizing an Intrusion Detection System (IDS).

2.5.1. Types of Intrusion Detection Systems

Intrusion Detection Systems come in two flavors, network-based and host-based. Implementing a host-based IDS is not recommended, as it may compromise system stability on the host. For the purposes of this document, we will focus on network-based Intrusion Detection Systems.

A network-based ID system monitors the traffic on its network segment as a data source. This is generally accomplished by placing the network interface card in promiscuous mode to capture all network traffic that traverses its network segment. Network traffic on other segments and traffic on other means of communication (like phone lines) cannot be monitored.

Network-based Intrusion Detection Systems look at network packets as they traverse the sensor. The sensor can only see packets carried on the network segment it is attached to. Packets are of interest if they match a signature or previous baseline capture.

Network-based Intrusion Detection Systems come in two forms:

- Signature-based: Sniffers that filter captured network traffic through signatures or patterns of known attacks
- Anomaly-based: Systems that capture network traffic and compare it to traffic that has been previously captured to determine if there are unusual patterns

2.5.2. Brands of Intrusion Detection Systems

There are several vendors that produce software and hardware Intrusion Detection Systems. Hologic recommends you choose a vendor that accommodates your needs. Some of the more popular vendors are:

- Cisco (many products)
- IBM (RealSecure)
- NIKSUN (NetDetector)
- Snort (open source)

2.6. Remote Administration

Hologic does not allow installation of remote monitoring programs like pcAnywhere on the R2 Cenova server. Any administration that needs to be accomplished should be done through the web-based R2 Cenova control panel. Alternatively, you can contact your local service representative for assistance.

3. Host-Based Security

3.1 Antivirus Products

Use of antivirus software can increase CPU and memory usage, which can cause a slight degradation in the performance of the R2 Cenova server. However, functionality should not be affected.

If you still elect to employ antivirus software, Hologic currently maintains a list of products that have been tested with the R2 Cenova server. This list is available at http://www.hologic.com/cc/netwrksec.htm. If you would like to use a different antivirus product or have any general questions, please contact us for assistance.

3.1. Host-Based Firewalls

Hologic does not allow installation of host-based firewalls on our systems. The R2 Cenova server ships with the built-in XP firewall enabled.

3.2. System-Level Auditing

Hologic's products may be shipped with auditing enabled to allow tracking of security events, provide accountability, and help diagnose potential problems that may arise. Please do not attempt to disable auditing.

3.3. Internet Usage

Using the server to gain access to the Internet exposes your systems to a plethora of vulnerabilities such as:

- Viruses
- Spyware
- Trojans
- Hostile code

Hologic does not permit the installation of any unauthorized software on our systems. Peer-to-peer software can expose your entire hard drive to any individual running the same type of software.

3.4. Auditing

Hologic depends upon auditing to provide for accountability and to track system changes. Auditing also assists diagnosing potential problems that may arise. Hologic has tested R2 Cenova with auditing enabled and determined that proper operation is not compromised.

3.5. System Patching

Hologic's products are considered medical devices, and therefore you are not permitted to upgrade the operating system or apply service packs on your own. Hologic periodically performs regression testing on critical patches and service packs. When these patches and service packs are validated, they are published in the R2 Cenova Cybersecurity Product Report. This document may be found at http://www.hologic.com/cc/netwrksec.htm. A customer validation form is included for patches that have been officially validated by Hologic. Note that service packs cannot be customer installed.

4. Physical Security

It is recommended you employ some method of physical security when dealing with our systems to ensure that only authorized personnel have access to Hologic's products.

There are several vulnerabilities a malicious user could exploit locally. Some examples are:

- Theft of equipment
- Local password cracking
- Installation of hardware keyloggers

4.1. Desktop Security

It is of vital importance to ensure desktop security is addressed in your environment. Some examples of desktop security are:

- Log off of the server when not in use.
- Utilize a form of close-captioned monitoring.
- Physically segment the systems in a secure room.

4.2. Onsite Vendors

If your organization uses vendors to assist in the administration of your network infrastructure, please make them aware of the recently added Hologic products. Ensure they do not make any configuration changes in any network devices. Doing so may adversely affect the performance of our products. It is also advised that you do not permit any outside vendors near our systems unless there is an absolute need (i.e., faulty network drop).

5. Securing Windows

5.1. Null Sessions

Null sessions are a built-in part of Microsoft's operating system. They allow systems and users to view available resources from other servers or domains. This can be useful if you manage a large enterprise. However, there are severe risks with null sessions. Null sessions do not require authentication and leave no trace if the proper auditing is not in place. By default, the software installer used with the R2 Cenova server automatically protects the system against null sessions.

5.2. Disabling Services

During installation of the R2 Cenova server, the following services are automatically disabled:

- NetMeeting Remote Desktop Sharing
- Remote Registry
- Telnet
- Wireless Zero Configuration

5.3. Password Security

In today's world, passwords can be compromised in literally seconds by using a wide variety of tools and techniques. As new automated tools are invented each year, the more trivial it becomes to crack passwords (both remotely and locally). To lower the possibility of a compromised password, it is vital to adhere to a set of protocols.

- Choose a password between 7–10 characters using both alpha and numeric characters.
- Use special characters in the password (e.g., @ % &).
- Do not share your password.

- Do not base your password on a pet, relative, or dictionary name.
- Do not write down your password.
- Examine the back of the R2 Cenova server for hardware keyloggers.
- Do not leave your account logged in.
- Routinely examine the event viewer logs. Under the 'Security' tab, look for failed attempts. This may be a sign of an attack.
- Define an Account Lockout Policy (see below).

5.4. Account Lockout Policy

When installed, the R2 Cenova server is configured with an Account Lockout Policy already enabled.

6. Maintenance

6.1. Virus Alerts

In the event that the antivirus utility alerts you to the presence of a virus, please contact your Hologic service representative.

6.2. Spyware

In the event that the R2 Cenova server becomes infected with spyware, please contact your Hologic service representative.

6.3. High CPU Usage or Low Hard Drive Space

In the event that the R2 Cenova server exhibits high CPU usage or low hard drive space during idle time, please contact your Hologic service representative.