

HOLOGIC®

OSTEOPOROSIS ASSESSMENT

QDR Cybersecurity Best Practices



QDR XP Cybersecurity Best Practices
MAN-00462

HOLOGIC®
CLARITY OF VISION

Table of Contents

1.0	OVERVIEW	4
2.0	INTRODUCTION	5
2.1.	AUDIENCE	5
2.2.	REMARKS	5
2.3.	DEFINITIONS, TERMS AND ABBREVIATIONS	6
2.4.	REFERENCES	6
3.0	NETWORK SECURITY	7
3.1.	ACTIVE DIRECTORY	7
3.2.	IP ADDRESS ASSIGNMENT	7
3.3.	SEGMENTATION.....	7
3.3.1	VLANs	7
3.3.2	Firewall segmentation.....	7
3.4.	EGRESS FILTERING	7
3.5.	NETWORK MONITORING.....	8
3.5.1	Types of IDSs	8
3.6.	REMOTE ADMINISTRATION	8
4.0	HOST BASED SECURITY	9
4.1.	ANTI-VIRUS PRODUCTS.....	9
4.2.	HOST BASED FIREWALLS	9
4.3.	SYSTEM LEVEL AUDITING.....	9
4.4.	INTERNET USAGE.....	9
4.5.	AUDITING.....	10
4.6.	SYSTEM PATCHING	10
5.0	PHYSICAL SECURITY.....	10
5.1.	DESKTOP SECURITY.....	11
5.2.	ONSITE VENDORS	11
6.0	SECURING WINDOWS®	11
6.1.	NULL SESSIONS	11
6.2.	DISABLING SERVICES	11
6.3.	PASSWORD SECURITY	12
6.4.	ACCOUNT LOCKOUT POLICY	12
6.5.	SECURING DEFAULT SHARES	13
7.0	MAINTENANCE	13
7.1.	VIRUS ALERTS	13
7.2.	SPYWARE	13

7.3.	UNAUTHORIZED ACCOUNTS	13
7.4.	HIGH CPU USAGE OR LOW HARD DRIVE SPACE	14
8.0	FURTHER ASSISTANCE	14

Microsoft, Active Directory, XP and Windows are registered trademarks of Microsoft Corporation. Unix is a registered trademark of The Open Group. Realsecure is a registered trademark of Internet Security Systems Inc. Pcity anywhere is a registered trademark of Symantec. VNC is a registered trademark of AT&T Laboratories. Cisco is a registered trademark of Cisco Systems Inc. Netdetector is a registered trademark of Niksun. Snort is a registered trademark of Sourcefire Inc. IEEE and 802 are registered trademarks in the U.S. Patent & Trademark Office, owned by the Institute of Electrical and Electronics Engineers, Inc.

1.0 Overview

Hologic, Inc. develops and markets a full line of Bone products including the QDR system. 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 lifecycle. Additionally, this document outlines the most common cybersecurity vulnerabilities and the appropriate methods for securing our products.

Hologic currently uses Microsoft XP operating systems in its QDR 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 performed in a laboratory environment and have undergone extensive testing. Adherence to these security recommendations will minimize the risk of cybersecurity threats. An experienced IT professional should be able to follow these instructions with minimal difficulty.

2.0 Introduction

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 a risk analysis to determine the potential consequences of cyber attacks. Additionally, the risk analysis will assess the potential consequences for actively mitigating the threat by inducing a product change. Any necessary product change Hologic induces to reduce cyber attacks, must be validated to ensure continual operation of our products.

Hologic also has an on-going maintenance program for the entire life cycle of our products. The on-going maintenance program consists of:

- Periodic Vulnerability Assessments
- Penetration testing
- Laboratory evaluation of Anti-virus 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. By following the Cybersecurity Best Practices below and incorporating them into your facilities security policies and protocols, your cybersecurity risk and vulnerabilities will be minimized.

2.1. Audience

This document contains information related to the Hologic QDR XP system. It is intended to aid in securing the customer's network infrastructure and network environment that incorporates Hologic products.

The reader of this document should be familiar with the OSI model, networking, and network security.

2.2. 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
- Methods of auditing
- Disaster Recovery Plans / Business Continuity Plans
- Password reset policy
- Perimeter security (e.g., firewalls, 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 its organization.

2.3. Definitions, Terms and Abbreviations

802.1q: The IEEE standard for VLAN tagging

ACL: Access control list

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

IP: Internet Protocol

ISL: Inter-switch link protocol

LAN: Local Area Network

Layer 3: Any device that utilizes the 3rd layer of the OSI model (AppleTalk, IP, etc)

IDS: Intrusion Detection System

OSI model: Open Systems Interconnection Reference Model

VLAN: Virtual LAN

TCP/IP: Transmission Control Protocol/Internet Protocol suite

TFTP: Trivial File Transfer Protocol

2.4. References

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

3.0 Network Security

3.1. Active Directory

Many companies 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.

3.2. IP Address Assignment

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

3.3. 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.

3.3.1 VLANs

VLANs (or Virtual LAN) 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 of segmenting a LAN would be using a physical interface off of a firewall.

3.3.2 Firewall segmentation

Many hardware firewalls are equipped with a 3rd interface. This interface is typically used as a DMZ in small to mid size. However, this 3rd interface may also be utilized to create a dwelling for machines that need increased security.

3.4. Egress Filtering

It is recommended that you employ egress filtering on your network. This will reduce the chances of external data theft and/or loss. In the beginning stages of a system compromise, one of the first

things an attacker will do is TFTP or FTP to a remote server that stores privilege escalation tools. Implementing proper egress filtering will reduce the chances of this occurring.

3.5. 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).

3.5.1 Types of IDSs

IDSs come in two flavors:

- Network based
- Host based

Implementing a Host Based IDS is not recommended, as it may compromise system stability on the host.

For the purpose of this document, we will focus on network-based IDSs. 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 IDSs involve looking at the packets on the network as they traverse the sensor. The sensor can only see the packets that happen to be carried on the network segment it's attached to. Packets are considered to be of interest if they match a signature or previous baseline capture.

Network-based IDSs come in two forms:

- **Signature based** - Sniffers that filter captured network traffic through signatures or patterns of known attacks
- **Anomaly Based**-Captures network traffic and compares it to traffic that has been previously captured to determine if there are unusual patterns

3.5.2 Brands of IDSs

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

- RealSecure
- Cisco's IDS
- Snort (open source)
- NetDetector

3.6. Remote Administration

Hologic does not allow the installation of remote monitoring programs like PCAnywhere or VNC on the QDR System. Any administration that needs to be accomplished should be done physically at the PC. Alternatively, you can contact your local service representative for assistance.

4.0 Host Based Security

4.1. Anti-virus products

It is recommended that you employ anti-virus software to protect your QDR system. While there are several "All in one" anti-virus products available on the market, Hologic does not recommend using these as they may compromise system stability. These "All in one" anti-virus products usually include: an Antivirus engine, Anti-spy ware and stateful firewall. These can significantly raise CPU usage and memory usage during regular usage, which may result in:

- System hangs
- Performance degradation
- Potential data corruption

Hologic recommends that anti-virus products be configured for "on-demand" scanning and not "real-time protection." On-demand scanning can significantly raise CPU usage and memory usage which may result in problems during image acquisition.

Hologic currently maintains a list of products that are supported for the QDR system. This list is available at <http://www.hologic.com/product-support/bone-densitometry/discovery/>. If you would like to use a different Anti-virus product or have any general questions, please contact us for assistance.

4.2. Host based firewalls

Hologic does not allow the installation of 3rd party host based firewalls on our systems. Some 3rd party host-based firewalls are vulnerable to denial of service attacks and if improperly configured, may let an intruder gain system level access to the system. The QDR comes shipped with XP's built in firewall enabled.

4.3. System level auditing

Hologic's products are shipped with auditing enabled to track security events. This is to provide accountability and to help diagnose potential problems that may arise. Please do not attempt to disable auditing. It is recommended daily review of the logs be completed to ensure the integrity of the system.

4.4. Internet usage

Please do not allow any users or staff to access the Internet from any of the QDR XP systems. This exposes your systems to a plethora of vulnerabilities such as:

- Viruses
- Spyware
- Trojans
- Hostile code (embedded into webpages)

Hologic's products are considered medical devices; therefore you are not permitted to install unauthorized software on your own. Peer to peer software can expose your entire hard drive to any individual running the same type of software.

4.5. Auditing

We at Hologic depend upon auditing to provide for accountability and to track system changes. It also assists us with diagnosing potential problems that may arise. Hologic has tested the QDR system with auditing enabled and determined that proper operation is not compromised.

To enable auditing:

1. Click START > run and type gpedit.msc.
2. Browse to Computer Configuration > Windows® Settings > Security Settings > Local Policy > Audit Policy.
3. Define every object for both "Success" and "Failure."
4. Browse to Control Panel > Administrative Tools > Event Viewer.
5. Right click on "Security" and select properties.

Browse to Control panel > Administrative Tools. Double click "Event Viewer." In the right pane, right click "Security" and select properties. Ensure that auditing is set to overwrite as needed. Maximum log size should not be smaller than 1000Kb. Failure to ensure this setting is enabled may prevent access to the machine should the event log become full.

NOTE: It is important the clock on your system is set correctly. If the time is set incorrectly, it will not provide proper accountability in the event of a system compromise. Hologic recommends using an in-house NTP server to synchronize the clock on all your systems (including all network based monitoring devices)

4.6. System patching

Hologic's products are considered medical devices, therefore you are not permitted to upgrade the operating system or apply service packs that have not been validated by Hologic. Hologic periodically performs regression testing on critical patches and service packs. The patches that have been validated and that you may install are listed in the QDR Cyber-Security Product Report.

5.0 Physical Security

It is recommended you employ some method of physical security when dealing with our systems. This ensures 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

5.1. Desktop security

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

- Log out of system when not in use
- Utilize a form of close captioned monitoring
- Physically segment the systems in a secure room

5.2. 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).

6.0 Securing Windows[®]

6.1. 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 isn't in place. Windows XP is protected against null sessions by default. However, improper configuration can resurrect this vulnerability. To ensure your machine is protected against Null Sessions, perform the following:

1. Open up Administrative tools (via control panel).
2. Double click Local Security Policies.
3. Expand Local Security Policies and highlight "Security Options."
4. Locate the parameter titled "Do Not Allow Anonymous Enumeration of Sam accounts."
5. Ensure this is set to "Enabled."
6. Perform the following for "Do Not Allow Anonymous Enumeration of Sam accounts and shares."

Additionally, disabling Netbios over TCP/IP and Unbinding File and Print Sharing will remove all SMB based protocols in the QDR XP system. This will effectively thwart all SMB based password attacks.

6.2. Disabling Services

Browse to Control Panel>Administrative Tools>Services

Locate the following services. Set the services to a "stopped" and "disabled" state.

- Remote Registry
- Netmeeting
- Wireless Zero Configuration
- Task Scheduler

6.3. 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 that a set of protocols be adhered to.

- Choose a password between 7-10 characters (choosing a password 15 characters or greater ensures the password is not stored as LmHash).
- Use special characters in the password (ie: @ % &).
- Do not share your password.
- Do not base your password on a pet, loved one or dictionary name.
- Do not write down your password.
- Make your password alphanumeric. This can trick a potential attacker (some tools only crack passwords upper-case).
- Examine the back of your QDR system 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).

Furthermore, your QDR system is configured so any local passwords are not stored as LANMAN. This will thwart most locally based password attacks.

6.4. Account Lockout Policy

Defining an "Account Lockout Policy" ensures a user account will be locked out after a pre-defined amount of failed attempts. This is important to define, as it will protect your user account from being "brute forced attacked."

To enable an Account Lockout Policy, follow the steps below:

1. Click START > RUN and type gpedit.msc
2. When the window appears, browse to Computer Configuration > Windows® Settings > Security Settings > Account Policies > Account Lockout Policy
3. Double click "Account lockout threshold."
4. Enter 5 attempts and click apply.

6.5. Securing default shares

The C\$ D\$ and E\$ is the root of each partition. For a Windows® NT workstation/W2K/2003/XP computer, only members of the Administrators or Backup Operators group can connect to these shares. For a Windows® NT Server/W2K Server machine, members of the Server Operators group can also connect to these shares. The problem with default shares is that they leave the system open to network based password attacks via IPC\$. To mitigate this risk, Hologic has shipped the QDR with several SMB based protocols disabled. No action is required.

7.0 Maintenance

7.1. Virus Alerts

In the event that the anti-virus utility alerts you to the presence of a virus, please take the following steps.

1. Record the virus/Trojan name, time and date from the notification window.
2. Open up your virus utility and view the history log. Export the file to a text document.
3. Exit out of any loaded programs.
4. Run a manual scan of all hard drives and any media in the QDR System. (Ensure definitions are updated prior to beginning the scan.)
5. If no Virus is found during a manual scan, view the anti-virus utility's event log.

7.2. Spyware

In the event that the QDR System becomes infected with spyware:

1. Browse to Control Panel > Add Remove Programs.
2. Remove any unauthorized programs (contact your local service representative if you need assistance determining what is unauthorized).
3. Click Start>Run and type regedit. Browse to HKEY LOCAL MACHINE > SOFTWARE > MICROSOFT® > WINDOWS® > CURRENT VERSION > RUN.
4. In the right pane, delete any keys that are unauthorized.
5. If the spyware persists, contact your local service representative.

7.3. Unauthorized accounts

In the event that unauthorized user accounts are found on the QDR System:

1. Ensure anti-virus "real protect" is still operating.
2. Examine the Event Viewer logs to locate when the account was added. If the logs are cleared, examine the logs of any other logging devices (i.e.: IDS). Look for any recently added services or protocols as well.
3. Examine the anti-virus event viewer logs to ensure "real protect" was not disabled at any time.

4. Examine the following locations for unauthorized entries:
 - HKEY LOCAL MACHINE > SOFTWARE > MICROSOFT® > WINDOWS® > CURRENT VERSION > RUN
 - C:\Documents and Settings\scr\Start Menu\Programs\ Startup
 - C:\Documents and Settings\Administrator\Start Menu\Programs\ Startup

7.4. High CPU usage or low hard drive space

In the event that the QDR System exhibits high CPU usage or low hard drive space during idle or normal usage:

1. Use “Task Manager” to view running processes. (Normal is < 36 processes:). Note the CPU column. Record any process that is consistently using over 05.
2. Ensure anti-virus “real protect” is still operating. Examine the anti-virus event viewer logs to determine if a virus was found or if “real protect” was ever disabled.
3. Complete a full system scan of the QDR System.
4. Examine the drive partitions to determine any unusual files or folders that may be present.
5. Browse to Control panel > Add/Remove Programs. Ensure no unauthorized programs have been installed on your QDR System.
6. Click START > RUN and type cmd. Once the window appears, type netstat –an. Note any foreign addresses that should not be communicating with the QDR System.

8.0 Further Assistance

Hologic is here to help. If at any time you need further assistance or just have general questions regarding the security of Hologic products, please do not hesitate to contact us at 800.321.4659. You may also reference our Security Center at <http://www.hologic.com/product-support/bone-densitometry/discovery/>