



Cybersecurity Best Practices
MAN-00363

Table of Contents

1.0	OVERVIEW	3
2.0	INTRODUCTION.....	4
3.0	AUDIENCE	4
4.0	REMARKS	4
5.0	DEFINITIONS, TERMS AND ABBREVIATIONS	5
6.0	DEFENSE IN DEPTH STRATEGY	6
7.0	WINDOWS DOMAIN & ACTIVE DIRECTORY	6
8.0	NETWORK SECURITY.....	7
8.1.	IP ADDRESS ASSIGNMENT	7
8.2.	SEGMENTATION	7
8.3.	VLAN.....	7
8.4.	FIREWALL	7
8.5.	NETWORK MONITORING (INTRUSION VS. EXTRUSION)	8
8.6.	TYPES OF INTRUSION DETECTION SYSTEMS (IDS)	8
9.0	ANTI-VIRUS AND ANTI-MALWARE PRODUCTS.....	9
10.0	ENDPOINT SECURITY MONITORING SECURITY & AUDITING.....	10
11.0	INTERNET USAGE.....	10
12.0	PHYSICAL SECURITY	11
12.1.	MEDICAL DEVICE SECURITY	11
13.0	ONSITE VENDORS	11
14.0	FURTHER ASSISTANCE	12
15.0	REFERENCES.....	12

Microsoft, Active Directory, NT, 2000, 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. pcAnywhere 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. 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 provides a “best practices” guide to assist our customer IT staff in securing their general network infrastructure where Hologic medical products are in use.

Hologic uses commercial off the shelf (COTS) products that include Microsoft Operating Systems and UNIX based Operating Systems in its portfolio of computer based medical products. Hologic takes cybersecurity seriously by taking a number of actions and measures in an effort to make our products safe from software vulnerability and exploits. However, due to the ubiquitous computing and interconnected nature of today’s world coupled with the fast changing landscape of cyber threats, this volatile condition poses a significant risk to the security of medical devices on a daily basis.

These Cybersecurity Best Practice recommendations are intended to increase the overall security posture of the environment where Hologic medical products are installed and operated. Adherence to these security recommendations will minimize the overall risk of cybersecurity threats to your computer based assets by reducing their exposure surface.

2.0 Introduction

Hologic monitors the information security industry on an ongoing basis, to assess potential new cybersecurity vulnerabilities that are discovered on an almost daily basis that may affect our products. Hologic takes appropriate countermeasures to deal with the threats in the interest of protecting our customers at large. Each Hologic product is assigned a specific Cyber Level of Concern (CLOC), 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 a successful cyber attack. Hologic may offer solutions in the form of a software patch or design change, or suggest a compensating control that is external to the product such as configuring a network firewall device to block the malicious traffic. If a design change is called for, then a subsequent risk analysis will assess the potential consequences of that change. Any patch or product change that Hologic introduces to mitigate software vulnerability or exposure must be validated to ensure optimal patient care and the continual operation of our products.

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

- Periodic Vulnerability Assessments
- Laboratory evaluation of anti-virus software or other products that may improve the security of our products
- Laboratory evaluation of software security patches
- Ongoing monitoring of the industry for new vulnerabilities and exploits

Hologic is committed to the cybersecurity maintenance program for our products. Successfully combating the emerging threats that our products may face in your network environment requires cooperation from you, our customer. We put forth some of these general cybersecurity best practices gathered from the information security and Information Technology industry to assist our customers. We believe when our customers incorporate these industry best practices into their overall existing security plan, policies, procedures, and processes, it will increase the overall security posture of their organization. Ultimately the customer is responsible for the security, confidentiality, integrity, and the availability of their network and computing resources within their organization.

3.0 Audience

The intended audience includes the systems administrator, network administrator, or security personnel. It is intended to aid in securing the customer's network infrastructure and network environments where Hologic products are deployed. It is also for people who have an interest in learning about the many challenges of keeping computer systems safe from malicious software and users.

4.0 Remarks

At Hologic we strive to make every Hologic medical system that we sell as secure and user friendly as possible before it leaves our factory. However, the primary functions of the devices we sell are first and foremost for medical uses that save women's lives. They are not security devices by design.

We periodically validate OS security patches released by vendors such as Microsoft, and publish the result as a product report. Any patches listed in the cybersecurity product report are safe to install on our systems to the best of our knowledge based upon our testing. Due to the break-neck speed in which software vulnerabilities are discovered on a daily basis, speedy patching becomes impractical and ultimately a knee-jerk reactive security. Therefore we expect our customers to take vigilant approaches to security in their day-to-day operations. We expect our customers to have a resilient environment with a sound security architecture design that incorporates proactive security mechanisms to deal with emerging new zero-day vulnerabilities and exploits.

A successful overall organization IT security strategy consists of comprehensive security plan, policies, and best practices that utilize a combination of effective physical, administrative, and technical controls. These should address at least the following. This list is by no mean exhaustive. It is meant only as a general guidance.

- Defense in Depth strategy that incorporates layered defenses
- Timed access control
- Centralized logging and auditing
- Disaster Recovery Plans / Business Continuity Plans
- Data backup and recover strategy
- Authentication and password security
- Perimeter security (e.g., firewalls, IDS/IPS, proxy servers, anti-virus gateway)
- Internal security (e.g., network monitoring, intrusion detection and extrusion detection, log review process, scan of network)
- Physical security (e.g., biometrics, locks, cameras)
- User Security Awareness Training focusing on safe computing practices
- Technical network defense design and control

Ultimately security is a people problem and there are limits to what a technology solution can accomplish in the face of a “cat-and-mouse” game. Security is only as strong as its weakest link and unfortunately people remain the weakest link. It is the customer’s responsibility to ensure the confidentiality, integrity and availability of the information technology resources and medical devices within their organization.

5.0 Definitions, Terms and Abbreviations

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

COTS: Commercial off the shelf (i.e. Microsoft Windows Operating System)

DAC: Discretionary Access Control

DHCP: Dynamic Host Configuration Protocol

DMZ: Demilitarized zone

Egress: Traffic destined outbound from an organization’s network

FTP: File Transfer Protocol

IDS: Intrusion Detection System

Ingress: Traffic destined inbound to an organization’s network

IP: Internet Protocol

IPS: Intrusion Prevention System

LAN: Local Area Network

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

Malware: Malicious software such as computer viruses, worms, rootkits, Trojans, data stealing, or any other malicious intents that are programmed by its author(s)

MIMS: Mammography Information Management Solution (Hologic's departmental image archive and connectivity product)

OS: Operating system

OSI model: Open Systems Interconnection reference model

TCP/IP: Transmission Control Protocol/Internet Protocol suite

VLAN: Virtual LAN

6.0 Defense in Depth Strategy

Defense in Depth is an Information Assurance strategy in which several layers of defense are put in place to protect a computing resource such as an information system. It is designed to address security weaknesses in personnel, technology and operations for the duration of the system's life cycle. In a simple analogy, a belt is good and suspenders are good, but having both suspenders and a belt is better. The idea behind this layered defense is to defend a system against any particular attack using several different methods. It is a layering tactic originally conceived by the National Security Agency (NSA) as a comprehensive approach to information and electronic security.

In terms of computer network security, Defense in Depth measures should not only prevent security breaches, but also mitigate the impact of a breach. It is about proactive security versus reactive security. Defense in Depth strategy buys an organization time to detect and respond to an attack from zero-day vulnerabilities and exploits on their terms rather than the attacker's terms. Resilient network defense involves incorporating the "[Nine principles of security architecture](#)".

7.0 Windows Domain & Active Directory

Many organizations have migrated to Windows® Active Directory® for the ease of centralized administration of their network resources. While Active Directory has several great benefits for general IT purpose computers, we do not recommend adding Hologic medical devices into your domain as they do not require it to function properly. In fact they perform better in a workgroup mode. Any software changes on medical devices need to be tested per FDA quality and safety systems procedures, to insure these changes do not have adverse effects on the device that may ultimately impact optimal patient care. Depending on how an Active Directory (AD) environment is configured and managed, pushing down untested software packages or policy rules to medical devices may cause unintended side effects.

However, if your organization insists on having our medical devices join your Windows Domain infrastructure then you do it at your own risk. Hologic cannot support any issues that result from this action. In an event of system corruption, Hologic will restore the medical device to its default factory state and bill for time and materials. If you decide to proceed despite this warning then we strongly recommend the following actions:

- a) Create a separate OU just for Hologic medical devices and do not apply any intrusive policies to it.
- b) Join one device into the domain at a time and run it through a series of tests, to insure the device still functions as intended without any adverse impact before joining a second device, etc.
- c) Block policy inheritance from anything above it like another OU or site, etc.
- d) Any software or program that is not made by Hologic is NOT to be pushed down to any Hologic medical device. Watch out for auto logon scripts, or any applications which the user's account is allowed access that are tied to their Windows domain account.

- e) Do not allow any Windows Domain user or administrator to logon interactively to any Hologic medical device either locally or remotely, as non-Hologic software could be contained within a roaming profile, etc.
- f) Be very careful about any policy applied to the Hologic OU as it may adversely impact the device's performance or functionality, especially an intrusive policy such as firewall, etc.

8.0 Network Security

8.1. IP Address Assignment

For several reasons, the IP address of a Hologic device should be assigned statically, rather than dynamically by a DHCP server. First it ensures the IP address records that our service technicians maintain are accurate. Second, it can prevent a certain form of denial of service attack in the event that a rogue DHCP server is deployed in your network.

It also goes without saying that medical devices should not be assigned a publicly addressable IP address. They should be assigned to a private IP address space based on RFC 1918. Medical devices should not be Internet facing without strong technical safeguards in place.

8.2. Segmentation

Separating medical devices from the rest of your general network helps to increase the security of these life-saving devices as it keeps them safe from the general user population. It also protects medical devices in an event a user within the general network accidentally downloads malware such as viruses or worms off the web or from an email attachment, where the malware attempts to spread itself to other computers on the same network. For security and privacy reasons, it is prudent to have a separate physical network designed just for the needs of medical devices that is not exposed directly or indirectly to the Internet. If a separate physical network is not feasible then implement a logical or virtual separation using VLAN, firewall, or a router. A medical network, whether partitioned off physically or logically, should not be reachable from the Internet or have Internet access without proper security protection in place to filter out and block malicious traffic.

8.3. VLAN

VLAN (Virtual Local Area Network) is a way to create several different broadcast domains on a single switch regardless of their physical location. It is a way to create multiple virtual networks within a single physical network mainly for improved network performance, where security is an ancillary benefit. VLAN is a feature of modern switches that is not designed with a purpose of security in mind. VLAN does not maintain true isolation as it depends on software and configuration, which are inferior to that of an actual physical isolation or air gap isolation. There are known attack vectors that exploit the weakness of VLAN, so proper configuration is extremely important to minimize the likelihood of a successful attack. Proper configuration includes using a non-default VID value, and trunk ports specifically configured for trunking. The great benefit of VLAN is the ease with which network reconfiguration can be accomplished through software, instead of having to relocate the devices physically as in years past.

8.4. Firewall

"A firewall is an integrated collection of security measures designed to prevent unauthorized electronic access to a networked computer system. It is also a device or set of devices configured to permit, deny, encrypt, decrypt, or proxy all computer traffic between different security domains based upon a set of rules and other criteria." – Wikipedia.org

A firewall plays a crucial and integral role in any successful technical security measures to protect a given network and devices contained therein from cybersecurity threats. Therefore the importance of a properly configured and well run firewall cannot be understated. A properly configured and maintained firewall goes a long way toward providing good protection not only from external threats

from the Internet, but also from insider threats from malicious employees, contractors, etc. A firewall is not a “set it and forget it” technology if you want continuous and effective protection. It needs to be updated frequently to retain its relevance in the network it is tasked to protect. A good firewall solution is a critical part of your Defense in Depth strategy.

We realize some organizations use a host-based firewall on their endpoint devices. In fact some advanced anti-malware software comes with a built-in firewall. There are many security benefits to having a host-based firewall installed and running on the host. It may require some care and feeding from knowledgeable staff, especially when you utilize advanced features and have devices being added to and removed from your network regularly. However, a host-based firewall is not recommended on certain Hologic devices, as it may have adverse effects on functionality, usability, and cross-device compatibility, depending on configuration and setup. A network firewall is recommended provided the customer IT staff supports and maintains it. Hologic does not provide firewall support as every solution and environment is unique.

8.5. Network Monitoring (Intrusion vs. Extrusion)

Effective monitoring of your network may detect the initial reconnaissance stages of a potential looming attack. This is vital information to capture, as it may indicate how a system is going to be compromised. Network monitoring typically involves deploying an Intrusion Detection System (IDS) or an Intrusion Prevention System (IPS) at major choke points in your network to gain maximum visibility into your network traffic. It also involves regular systematic reviews of logs from servers, routers, firewalls, gateway appliances, proxy servers, databases, anti-virus management servers, etc., to look for signs of intrusion attempts.

At a minimum it is prudent to employ an intrusion detection monitoring solution at the main choke points of your network traffic, to monitor for malicious payloads and exploits. An IDS provides an early warning system to alert personnel to take actions to protect the network and its connected devices. Monitoring your network allows you to detect and respond to any cyber intrusion attempts against your network and its computing assets. Often you get crucial information in the early stages of an attack from the intelligence your monitoring solution provides, which you can use to neutralize the threat while the problem is still small and before it turns into an incident.

Ideally you should complement your intrusion monitoring (ingress) with an extrusion monitoring solution (egress). This provides a comprehensive visibility into your network, thereby allowing you to detect unauthorized activity by inspecting outbound traffic destined outside your organization. Extrusion detection allows you not only to pick up on malware or crimeware that may phone home to its central Command & Control server, but also to detect malicious insider threats such as an employee or contractor attacking your network from the inside, or using your network to attack another organization.

8.6. Types of Intrusion Detection Systems (IDS)

An Intrusion Detection System typically comes in two flavors:

- Host-based Intrusion Detection System (HIDS)
- Network-based Intrusion Detection system (NIDS)

A HIDS provides protection to the computer on which its service is installed. It provides coverage to the local system. As with any software that is installed on the computer it consumes resources such as CPU, RAM, and disk space. The performance of the computer can be impacted greatly, depending on which settings you turn on or off. As a general rule, the more features you turn on the more resources they consume and the slower the overall performance is going to be. HIDS implementation and administration require advanced computer knowledge to keep it working properly. The installation of a host-based intrusion detection system solution on a Hologic medical device is not recommended, since it can impact the functionality and performance of the medical device adversely depending on configuration and setup. Due the wide array of HIDS solutions and vendors coupled with the fact that each customer situation is unique, it is impractical for Hologic to test and make recommendations.

A NIDS provides protection at the network level. Think of HIDS as protection for a tree and while NIDS protects the whole forest. A NIDS provides several critical detection services to the network by monitoring for malicious activity such as denial of service attacks, port scans, and intrusion attempts. NIDS generally comes in two forms:

- **Signature based** - detection through signatures or patterns of known attacks
- **Anomaly Based**- dynamic detection of network traffic behaviors that deviate from what is considered normal traffic. This involves teaching the NIDS which traffic is normal by putting it into a “learning mode” for a period of time.

The best form of NIDS is a hybrid that provides efficient detection of known attacks while at the same time permitting detection of zero-day exploit attacks with as yet unknown signatures. Over the years Intrusion Detection System (IDS) has evolved into Intrusion Prevention System (IPS). IPS is an in-line network security device that provides proactive automated response in real-time against active threats. IPS works by dropping suspected malicious traffic while letting the safe traffic through whereas the traditional NIDS is passive and only alerts the security administrators to suspected malicious traffic. There are hybrid products, such as Sourcefire, which can be configured to be an IPS or IDS at the time of deployment. The customer can initially deploy it as an IDS, to provide passive monitoring benefit until they get comfortable with their network environment, and then later switch over to IPS for the active protection. Deploying a successful IPS solution requires tremendous technical knowledge of one’s network environment and time to roll it out.

There are a lot of security vendors out there producing an array of solutions for customers and organizations of all sizes and budgets. You can find an extensive list of vendors at the below website that is supported by the Department of Homeland Security (DHS):http://cve.mitre.org/compatible/intrusion_detection.html

9.0 Anti-virus and anti-malware products

Running anti-virus software at endpoint devices such as workstations has become a necessity in most organizations these days to combat potential threats from malicious software such as viruses, worms, Trojans, keystroke loggers, etc. Anti-virus generally is a safe product when used as directed. Over the years it has become a “set it and forget it” solution for most organizations. However there are some drawbacks to using anti-virus and anti-malware products. First, depending on conditions of the current threat landscape, which may fluctuate month-to-month, or year-to-year, the detection rate for a given anti-virus can be as low as 20% or as high as 98%. For this reason anti-virus is not *the* solution, but rather part of a larger solution that relies on Defense in Depth strategy. Secondly anti-virus and its anti-malware features can be CPU intensive, thus slowing down overall system performance along with potential for false positives, data corruption, and blocking DICOM or other communication protocols between systems. The more advanced features you utilize, the greater the potential for issues or growing pains until the product is manually tuned to your specific network environment by a knowledgeable local IT staff. At the time of this writing there are about 40 commercially available anti-virus products, some with anti-malware features. Hologic cannot possibly test every one of these, let alone test every major and minor version update from a given vendor. Furthermore each customer has their own approved anti-virus solution dictated by corporate policy.

Hologic has validated several products from industry leaders Symantec and McAfee. We may validate others in the future as time and resources permit. Hologic strongly encourages customers to use only anti-virus products that we have officially validated to insure the continual safety and reliability of our medical devices for optimal patient care. However if you insist on using an untested anti-virus solution you use it at your own risk. In an event the system experiences serious issues, Hologic will restore the system back to its default factory state and bill for time and materials.

10.0 Endpoint security monitoring & auditing

Enabling logging in the OS and whenever possible in the applications can assist in the forensic analysis in an event of intrusion attempts at endpoint devices. Regular audit review of logs is essential to detect intrusions. However as the quantity of enabled logging features increases the general performance tends to decrease, and the complexity of log analysis increases. The trade offs should be considered carefully, especially on medical devices where proper performance is critical to optimal patient care.

Hologic's products are shipped with certain auditing features enabled to track certain events at the OS and application levels. This is to aid our support personnel in diagnosing problems that may arise. These logs are for Hologic use only so please do not attempt to change any settings.

11.0 Internet usage

Please do not allow any users, staff, or contractors to access the Internet from any Hologic medical device for email or general web use. In fact Internet access should be blocked from these medical devices as the Internet is the greatest threat pool for network devices. Web-based exploits and malicious email attachments are two of the most common threats to endpoint devices at the present time. Any device with access to the Internet is potentially exposed to the following threats:

- Viruses
- Spyware
- Trojans
- Worms
- Rootkits
- Keystroke logging
- Identity theft software
- Spam
- Botnet activity
- Spyware
- Drive-by download of malicious code

Internet access from a medical device should not be provided unless there is a legitimate business reason along with very good technical security measures in place to block or prevent malicious traffic from reaching the local system on your trusted network. When people think of Internet access, they likely think only of access to the World Wide Web or email. The truth is that web access is just a subset of applications and protocols that fall into the category of Internet access. Some other types of Internet access are file transfer services such as FTP, Instant Messaging (IM), Internet Relay Chat (IRC), Peer-to-Peer such as Bit Torrent, eDonkey etc., and any other applications that utilize the TCP/IP protocol suite. In recent years the greatest threat vector is from the web because of its immense popularity and wide-reaching audience. On the web a user can click on a seemingly innocent link, and malware can be downloaded without user knowledge or consent, which can wreck havoc on the device and other devices on the same network.

Hologic products are FDA approved medical devices. Therefore, you are not permitted to make any unauthorized software changes or modifications to the device, such as installing untested OS patches, service packs, non-approved applications, or upgrading the underlying OS without explicit authorization from Hologic technical support personnel. Any software changes such as installation of service packs, patches, etc. need to be tested first by Hologic to insure the safe and continual

operation of the device. Periodically we validate new security patches and release the result in the form of a cybersecurity product report that is published on our website at www.hologic.com.

12.0 Physical Security

All security starts with physical security and there are no exceptions to the rule. Good physical security is the foundation of any sound security plan as it provides protection on the inside. Even in the high-tech world, if a person with malicious intent can easily gain physical access to device or network attack points, your site has huge exposure to risks such as:

- Theft, tampering, or destruction of equipment
- Theft, modification, or destruction of sensitive and confidential data
- Attacker can install a backdoor access program and use it to further compromise other devices on the network that may be more valuable

Therefore it is absolutely critical that you have good physical security access control over your medical devices and any other critical IT systems, as a security incident may cost your organization in reputation, litigation, and breach announcements in some states.

12.1. Medical device security

It is critical to ensure that medical device security is addressed in your environment. Some examples of good security practices are:

- Log out of the device when not in use or password protect the screen when the device is left unattended for an extended period of time
- Use robust passwords that are more than 8 characters long
- Regularly change passwords at least on a monthly basis
- Do not write down a password and leave it accessible to unauthorized personnel
- Do not give out or share a password with anyone
- Do not use a medical device to email or surf the web or for any other Internet access
- Do not install any non-approved software or make software modifications on Hologic medical devices without specific written authorization from Hologic
- Place the medical device in an environment with good physical security so only authorized personnel can gain access
- Isolate medical devices to their own separate network or isolate using a firewall, router, VLAN, or some other isolation mechanism

13.0 Onsite vendors

If your organization uses vendors to assist in the administration of your network infrastructure, please make them aware of any Hologic products recently added to your network. Ensure they do not make any configuration changes in any network devices that may impact Hologic medical devices. Doing so may adversely affect the performance of our products or create serious issues that may require a Hologic field engineer to visit the site to repair a down device. It is also advisable that you do not permit any outside vendors near our devices unless there is an absolute need (i.e. faulty network drop or other network hardware issues extrinsic to Hologic devices). Always escort and closely monitor a contractor if they need to perform work on any Hologic devices, and do not give out any passwords. Instead, login for him or her and then watch carefully to insure nothing suspicious is going on. In most circumstances there are absolutely no legitimate reasons for other vendors to access Hologic medical devices. If it happens make sure you report any suspicious activities to your manager and Hologic support personnel.

14.0 Further Assistance

Hologic is here to help. If at any time you need assistance with Hologic products please do not hesitate to contact us toll free at 1-800.321.4659.

15.0 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
- ❖ www.wikipedia.org
- ❖ VLAN Insecurity (<http://www.spirit.com/network/net0103.html>)
- ❖ "Nine principles of security architecture" (<http://www.linux.com/articles/49803>)
- ❖ Fundamental Principles of Network Security (<http://www.ptsdcs.com/whitepapers/70.pdf>)