



TITLE: SuperSonic MACH40 v2.X Security Statement	DOCUMENT # RD.DD.489	Rev. A
		Page 1 sur / of 5

Date: May 13, 2020

SuperSonic MACH40 v2.X Security Statement

DOCUMENT CONFIDENTIEL

Les informations contenues dans ce document sont confidentielles et sont la propriété de SuperSonic Imagine (SSI). SSI met en place ce document dans l'attente qu'il soit gardé strictement confidentiel et ne doit pas être utilisé pour tout autre but que celui qui lui est défini. Aucune portion de ce document ne doit circuler, être citée ou reproduite pour une distribution extérieure à la société sans autorisation préalable écrite de SSI.

CONFIDENTIAL DOCUMENT

The information contained in this document is confidential and proprietary to SuperSonic Imagine (SSI). SSI provides this document with the understanding that it will be held in strict confidence and will not be used for any purpose other than the intended purpose. No part of the document may be circulated, quoted, or reproduced for distribution outside the organization without prior written approval from SSI.

TITLE: SuperSonic MACH40 v2.X Security Statement	DOCUMENT # RD.DD.489	Rev. A
		Page 2 sur / of 5

Table of content

1. Introduction	3
1.1. Scope	3
1.2. Audience.....	3
2. Cybersecurity documentation	3
2.1. Manufacturer Disclosure Statement for Medical Device Security	3
2.2. Software BoM	3
3. Cybersecurity functions	3
3.1. User Authentication	3
3.2. Emergency Access.....	3
3.3. User Restriction	3
3.4. Asset at rest Protection	4
3.5. Communication Encryption.....	4
3.6. Automatic Logoff.....	4
3.7. Authorization.....	4
3.8. Configuration of Security Features	4
3.9. Personal Data De-Identification.....	4
3.10. Data Backup and Disaster Recovery	4
3.11. Physical Security.....	4
3.12. Software Integrity	4
3.13. Cybersecurity Product Upgrades	4
3.14. Antivirus and Malware Detection / Protection	5
4. Cybersecurity contact	5

DOCUMENT CONFIDENTIEL

Les informations contenues dans ce document sont confidentielles et sont la propriété de SuperSonic Imagine (SSI). SSI met en place ce document dans l'attente qu'il soit gardé strictement confidentiel et ne doit pas être utilisé pour tout autre but que celui qui lui est défini. Aucune portion de ce document ne doit circuler, être citée ou reproduite pour une distribution extérieure à la société sans autorisation préalable écrite de SSI.

CONFIDENTIAL DOCUMENT

The information contained in this document is confidential and proprietary to SuperSonic Imagine (SSI). SSI provides this document with the understanding that it will be held in strict confidence and will not be used for any purpose other than the intended purpose. No part of the document may be circulated, quoted, or reproduced for distribution outside the organization without prior written approval from SSI.

TITLE: SuperSonic MACH40 v2.X Security Statement	DOCUMENT # RD.DD.489	Rev. A
		Page 3 sur / of 5

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.

1.1. Scope

This Security Statement applies to SuperSonic MACH40 version V2.X.

1.2. 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 documentation

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 SuperSonic MACH40 MDS2 is in the SuperSonic MACH40 Support section of the Hologic website.

2.2. Software BoM

A Software Bill of Material is available at the end of the SuperSonic MACH40 MDS2 document

3. Cybersecurity functions

3.1. User Authentication

User are logged in using the standard Pluggable Authentication Module (PAM). Applicative users are separated from Operating System user by storing applicative user information in a dedicated PostgreSQL database.

3.2. Emergency Access

An Emergency account is available to enable image acquisition even if an operator cannot login.

3.3. User Restriction

Each user is attributed a role (Admin, User, Emergency). Limitations are implemented based on this role to protect access to configuration and exams.

DOCUMENT CONFIDENTIEL

Les informations contenues dans ce document sont confidentielles et sont la propriété de SuperSonic Imagine (SSI). SSI met en place ce document dans l'attente qu'il soit gardé strictement confidentiel et ne doit pas être utilisé pour tout autre but que celui qui lui est défini. Aucune portion de ce document ne doit circuler, être citée ou reproduite pour une distribution extérieure à la société sans autorisation préalable écrite de SSI.

CONFIDENTIAL DOCUMENT

The information contained in this document is confidential and proprietary to SuperSonic Imagine (SSI). SSI provides this document with the understanding that it will be held in strict confidence and will not be used for any purpose other than the intended purpose. No part of the document may be circulated, quoted, or reproduced for distribution outside the organization without prior written approval from SSI.

TITLE: SuperSonic MACH40 v2.X Security Statement	DOCUMENT # RD.DD.489	Rev. A
		Page 4 sur / of 5

3.4. Asset at rest Protection

Asset at rest are stored on an encrypted disk partition (using TPM 1.2).

3.5. Communication Encryption

DICOM communication are encrypted using DICOM TLS. The default profile for communication encryption is BCP 195 TLS Secure Transport Connection Profile

3.6. Automatic Logoff

SuperSonic MACH40 does not allow automatic logoff, but a session is automatically locked after a defined period of inactivity. A locked session can be unlocked by its user or may be closed to allow any other user (including emergency account) to create another exam.

3.7. Authorization

Based on the role they are assigned, user accounts may or may not allow access to the exams stored on the database or to configuration of cybersecurity features.

3.8. Configuration of Security Features

Access to security feature configuration is prohibited to any user not having the admin role

3.9. Personal Data De-Identification

DICOM objects are anonymized in accordance to the “basic profile” from PS3.15 Annex E Attribute Confidentiality Profiles.

3.10. Data Backup and Disaster Recovery

SuperSonic MACH40’s configuration and exam database can be backed up and recovered.

3.11. Physical Security

The system does not come with physical locks. Customers can restrict access to USB ports by applying physical locks.

3.12. Software Integrity

SuperSonic MACH40 use a custom OS based on the Debian 9 GNU/Linux distribution. All packages included in this distribution are digitally signed by Hologic SuperSonic to prevent installation of untrusted software.

3.13. Cybersecurity Product Upgrades

SuperSonic MACH40’s software can be updated remotely or by a technician on site. Upgrades are included in Service Packs (SP) updates.

DOCUMENT CONFIDENTIEL

Les informations contenues dans ce document sont confidentielles et sont la propriété de SuperSonic Imagine (SSI). SSI met en place ce document dans l'attente qu'il soit gardé strictement confidentiel et ne doit pas être utilisé pour tout autre but que celui qui lui est défini. Aucune portion de ce document ne doit circuler, être citée ou reproduite pour une distribution extérieure à la société sans autorisation préalable écrite de SSI.

CONFIDENTIAL DOCUMENT

The information contained in this document is confidential and proprietary to SuperSonic Imagine (SSI). SSI provides this document with the understanding that it will be held in strict confidence and will not be used for any purpose other than the intended purpose. No part of the document may be circulated, quoted, or reproduced for distribution outside the organization without prior written approval from SSI.

TITLE: SuperSonic MACH40 v2.X Security Statement	DOCUMENT # RD.DD.489	Rev. A
		Page 5 sur / of 5

3.14. **Antivirus and Malware Detection / Protection**

SuperSonic MACH40 does not come with an antivirus and no additional software can be installed.

4. **Cybersecurity contact**

The following contact information can be used to report incidents, vulnerabilities or for general inquiries regarding cybersecurity:

cybersecurity@supersonicimagine.com

DOCUMENT CONFIDENTIEL

Les informations contenues dans ce document sont confidentielles et sont la propriété de SuperSonic Imagine (SSI). SSI met en place ce document dans l'attente qu'il soit gardé strictement confidentiel et ne doit pas être utilisé pour tout autre but que celui qui lui est défini. Aucune portion de ce document ne doit circuler, être citée ou reproduite pour une distribution extérieure à la société sans autorisation préalable écrite de SSI.

CONFIDENTIAL DOCUMENT

The information contained in this document is confidential and proprietary to SuperSonic Imagine (SSI). SSI provides this document with the understanding that it will be held in strict confidence and will not be used for any purpose other than the intended purpose. No part of the document may be circulated, quoted, or reproduced for distribution outside the organization without prior written approval from SSI.