TOSHIBA MEDICAL

Made For life

TAMS Detailed Response to Protection of Toshiba Manufactured Image Making Devices

Toshiba America Medical Systems (TAMS) takes protection of PHI, PII, and security of Toshiba medical devices very seriously. With the recent release of Ransomware that has crippled many healthcare facilities across the globe, TAMS is committed to providing our customers with certain security solutions to minimize any security vulnerabilities.

The type of security offered on Toshiba medical devices vary depending on the Operating System (OS) and application software version. The tables below will assist with configurations and availability of enhanced security.

GREEN: System is protected or has the ability to be protected at no cost
YELLOW: System is protected with optional hardware appliance to be installed by TAMS or facility
WHITE: System Information
GREY: System Information or item is Not Applicable
RED: System is not protected and requires installation of any item under the Solution column

CT

Aquilion Version	Windows OS	Windows Firewall (Default Setting)	McAfee Application Control	Risk Management Framework (RMF)	Solution		Ransomware Blocked
					Service Contract / Warranty	Time and Material	
V1.x	Win2000	n/a	n/a	n/a	SP-Firewall or TVR	Purchaseable Option: eProtect (Part #: RB450G)	No
V3.x	Win2000	n/a	n/a	n/a	SP-Firewall or TVR	Purchaseable Option: eProtect (Part #: RB450G)	No
V3.x	WinXP	OFF	n/a	n/a	SP-Firewall or TVR	Purchaseable Option: eProtect (Part #: RB450G)	Yes *
V4.x	WinXP	OFF	n/a	n/a	SP-Firewall or TVR	Purchaseable Option: eProtect (Part #: RB450G)	Yes *
V5.x, V6.x, V7.x	WinXP	OFF	n/a	n/a	SP-Firewall or TVR	Purchaseable Option: eProtect (Part #: RB450G)	Yes *
V5.x, V6.x, V7.x	Win7	OFF (Enabled only with RMF)	ON	Purchasable Option available (CSAS-001A/1A)	SP-Firewall or TVR	Purchaseable Option: eProtect (Part #: RB450G)	Yes *

*SMBv1 has been disabled

MR

MR Model/Version	Windows OS	Windows Firewall (Default Setting)	McAfee Application Control	Risk Management Framework (RMF)	Solution		Ransomware Blocked
					Service Contract / Warranty	Time and Material	
Vantage 1.5T (GP Platform)	WinXP	n/a	n/a	n/a	SP-Firewall or TVR	Purchaseable Option: eProtect (Part #: RB450G)	No*
Titan V1.x, 2.x (Mpower Platform)	WinXP	OFF	n/a	n/a	SP-Firewall or TVR	Purchaseable Option: eProtect (Part #: RB450G)	No*
Titan V3.x (Mpower Platform)	Win7	OFF (Enabled only with RMF)	ON	Purchaseable Option available	SP-Firewall or TVR	Purchaseable Option: eProtect (Part #: RB450G)	Yes **

*Disabling of SMBv1 is expected
** With Risk Manage Framework enabled

UL

UL Model/Version	Windows OS	Windows Firewall (Default Setting)	McAfee Application Control***	Risk Management Framework (RMF)	Solution		Ransomware Blocked
					Service Contract / Warranty	Time and Material	
Aplio XG/MX & Xario XG	WinXP	OFF **	n/a	n/a	n/a	n/a	Yes *
Xario 100/200	Win7	ON **	Purchasable Option available (USSM-X200A)	Purchasable Option available (USSM-X200A)	n/a	n/a	Yes *
Aplio 300/400/500 V5.x or earlier	WinXP	OFF **	n/a	n/a	n/a	n/a	Yes *
Aplio 300/400/500 V6.x or later	Win7	ON **	Purchasable Option available	Purchasable Option available	n/a	n/a	Yes *
Aplio i-series	Win7	ON **	Purchasable Option available (USSM-AI900A)	Purchasable Option available (USSM-AI900A)	n/a	n/a	Yes *

*SMBv1 has been disabled
** TCP/IP port filtering function that blocks port 445 as default setting.
*** McAfee Application Control is installed as default on productions systems September 1st, 2017

VL

VL Model/Version	Windows OS	Windows Firewall (Default Setting)	McAfee Application Control	Risk Management Framework (RMF)	Solution		Ransomware Blocked
					Service Contract / Warranty	Time and Material	
Infinix-I V5.x or earlier	WinXP	ON	n/a	n/a	SP-Firewall or TVR	Purchaseable Option: eProtect (Part #: RB450G)	Yes
Infinix-i V6.x or later	Win7	ON	ON	Purchasable Option available (XIDF-SEC802 Infinix) (XIDF-SEC702 AWS)	SP-Firewall or TVR	Purchaseable Option: eProtect (Part #: RB450G)	Yes

TOSHIBA AMERICA MEDICAL SYSTEMS
2441 Michelle Drive, Tustin, CA 92780 / 800.421.1968 / medical.toshiba.com

Canon
CANON GROUP

	XR Model/Version	Windows OS	Windows Firewall (Optional Setting)	McAfee Application Control	Risk Management Framework (RMF)	Solution		Ransomware Blocked
						Service Contract / Warranty	Time and Material	
X-Ray	Radrex V3.6 or earlier EPS+	WinXP	Off	n/a	n/a	SP-Firewall or TVR	Purchaseable Option: eProtect (Part #: RB450G)	No
	Radrex V4.1	Win7	Off	Off	n/a	SP-Firewall or TVR	Purchaseable Option: eProtect (Part #: RB450G)	No
	Harmony V1.31 or earlier	WinXP	ON	n/a	n/a	SP-Firewall or TVR	Purchaseable Option: eProtect (Part #: RB450G)	Yes *
	Harmony V1.5 or later	Win7	ON	Off	n/a	SP-Firewall or TVR	Purchaseable Option: eProtect (Part #: RB450G)	Yes *

*SMBv1 has been disabled

InnerVision is a TAMS proprietary device that provides 1-1 Network Address Translation (NAT) that is included at no additional charge within all applicable Toshiba medical equipment under warranty or service agreements. This isolates the medical equipment on the customer's network and is one of the strongest protection devices available. The only network traffic allowed to communicate with the modality is the IP address and port number that is configured on the hardware device. All other traffic is prevented and not allowed to make it to the modality.

eProtect provides the same hardware firewall capabilities of InnerVision. eProtect is purchasable device to TAMS Time & Material (T&M) customers.

Risk Management Framework (RMF) is a stringent security vulnerability guideline adopted by the Federal Government including the Department of Defense (DoD) and Veteran Affairs (VA). http://csrc.nist.gov/groups/SMA/fisma/framework.html

McAfee Application Control is a Whitelist that blocks unauthorized executables on a proactive basis. Should a malicious attack occur and get installed on the medical device, McAfee will prevent that program from being executed.
https://www.mcafee.com/us/products/application-control.aspx

TAMS Network Policy:
https://medical.toshiba.com/service-and-support/enterprise-integration/network-security-policy/

TAMS PHI Policy:
https://medical.toshiba.com/service-and-support/enterprise-integration/phi-removal-policy/

For security questions or comments: TAMS-Security@tams.com