TOSHIBA
Leading Innovation

Toshiba America Medical Systems Network Policy

July 30th, 2015

In keeping with the widespread advancement of Information Technology (IT) within the medical imaging industry, Toshiba recognizes the importance of cyber security and protection of Patient Health Information (PHI). Toshiba offers the latest in medical imaging equipment, incorporating flexible information management and real-time sharing via networks, including integration with Radiology Information Systems (RIS) and Picture Archiving and Communication Systems (PACS). With this integrated connectivity, Toshiba recognizes that it is obliged to provide our customers with secure medical equipment to protect patient information, promote hospital security and to provide malware and virus control.

However, when systems are connected to networks with Internet access, the PCs (including Toshiba products) incorporated in them can become susceptible to malicious software attacks. Therefore all customers must ensure that adequate security measures have been implemented into their network.

The report "Defending Medical Information Systems against Malicious Software," published by the Joint NEMA/COCIR/JIRA Security and Privacy Committee (SPC), indicates that the consensus in the medical industry is that no solution can guarantee 100 percent protection. Toshiba therefore strongly recommends that all the customer's operating systems in a network environment provide the necessary network security measures, including access-control mechanisms, firewalls, Intrusion Detection Systems (IDSs) and user procedures to adequately protect critical medical imaging systems from malicious attacks and thus keep them secure and performing at optimum levels. Manufacturers are not able to control all aspects of network security.

Toshiba's approach to supporting its customers in addressing security threats is as follows.

- All current Toshiba image making devices incorporate McAfee® Solidifier, a whitelist antivirus software.[1] This centrally managed whitelisting solution uses a dynamic trust model and innovative security features that thwart advanced persistent threats — without requiring signature updates or labor-intensive list management.[2]
- All current Toshiba medical imaging systems incorporate Windows 7.[1]
- Selected Toshiba medical imaging systems have the option for advanced security that follows the federal government strict security guidelines of Risk Management Framework (RMF).
- Only authorized Toshiba personnel or Toshiba trained technicians are allowed to install factory released software.
- Toshiba provides software updates from Microsoft® and other applicable companies to maintain and control security threats.
- Toshiba validates all medical imaging system software (including software patches) prior to customer use to ensure safe and reliable performance.

- Toshiba delivers all its products to customers free of infections or malware as of the date of delivery.
- Toshiba offers a malware-checking and restoration service for Toshiba medical imaging systems that have been infected or damaged by malware. A fee is charged for both these services. TAMS' customer engineers are able to run a virus check using their Toshiba laptop. If malware or a virus is discovered, Toshiba will reload the operating system and application software to restore it to the original condition.
- Unauthorized installation of any commercially available antivirus, 3rd party software, or unreleased software in the medical imaging system voids the product warranty. Furthermore, Toshiba will not be responsible for loss of patient safety or any performance issues caused by such installation.

Toshiba eProtect Authentication and Malware Protection Device

eProtect is the quickest, simplest and most secure protection for Toshiba equipment. eProtect is a specially configured network device designed to isolate Toshiba medical products from hospital network traffic.

eProtect will control and limit traffic into and out of Toshiba products to allow DICOM services such as modality worklist, storage to PACS and workstations, structured reports and query & retrieve. At the same time, eProtect restricts unnecessary network traffic from reaching the medical device. This unnecessary network traffic could be, but is not limited to viruses, malware and malicious attacks.

Toshiba has found this to be the best form of malware protection for Toshiba medical imaging equipment. eProtect is provided free of charge to Toshiba warranty and contract customers.

InnerVision with Remote Connectivity Suite

InnerVision is Toshiba Medical's "Remote Support and Diagnostics" suite. InnerVision is a networking technology set up to allow remote service and support via VPN connections to our installed base of medical imaging systems.

Designed along industry standard security guidelines, InnerVision can set up discrete VPN tunnels for each medical imaging device. Toshiba support engineers, In-Touch application specialists and customer engineers may then connect through those secure VPN tunnels to assess, troubleshoot and service issues and application support.

A VPN (Virtual Private Network) is the secure network connection from the customer's site to TAMS HQ. It is the backbone through which InnerVision services operate.

A VPN connection is referred to as a "tunnel". There are various methods of establishing these tunnels. There are two VPN methods (protocols) used by Toshiba depending on the overall setup at the customer's site:

- IPSec (IP Security)
- SSL (Secure Socket Layer)

Contact TAMS security

Please email TAMS-Security@toshiba.com with any questions or concerns.

[1] Excludes Titan 3T, Viamo, and Artida products

[2] http://www.mcafee.com/us/products/application-control.aspx