State-of-the-Art Security for Medical Devices

Christoph Hiltl, Karl Stortz

Christoph Hiltl

Since its beginnings in 1945, Karl Stortz has established itself worldwide as an international and highly regarded company in the production and sale of medical instruments and devices. Headquartered in Tuttlingen, Germany, the enterprise has been developing its product range of endoscopic equipment for human and veterinary medicine for more than six decades and has become a world leader in this field. Medical instruments and appliances are invariably the product of teamwork, in which medical practitioners and specialists from various disciplines work in close collaboration.

Challenge

Hospitals are complex environments. Infrastructure may be networked at some locations while in others it may not. Systems are increasingly interconnected and what occurs in one may affect another – both beneficially and negatively. Additionally, systems are frequently left unattended giving ample opportunity for unchallenged access by unauthorised users– be it staff, patients, visitors, or someone just passing by. It is also vital that devices remain operational 24 hours a day, seven days a week, leaving little time for software updates.

To ensure the safety and reliability of mission-critical medical equipment, software is playing an increasingly important role in product development. Protecting devices from unauthorised software is essential to maintain patient safety as it can – unintentionally or maliciously – seriously affect the performance of the sophisticated equipment.

While Karl Stortz had addressed this individually in its previous developments, the 2010 IEC 800001 'Application of risk management for IT-networks incorporating medical devices' standard called for a more comprehensive and reliable solution. For the manufacturer it was essential to develop devices that would provide security and risk management for its Windows-based SCB, OR1 and Aida platforms without affecting the operation and functionality of the system. Equally, it was paramount to find a solution that would keep maintenance and service requirements to a minimum.

Solution

When during this evaluation process a Swedish customer asked for Cryptzone's SE46 Application Whitelisting to be incorporated into all its equipment, Karl Stortz soon recognised that this solution would meet its wider security requirements. Alternative technologies such as anti-virus software work by application black-listing however this means it requires extensive and daily updating to ensure it remains current and, even then, it may still not guarantee a secure system that prevents infections. When a patch is released, for example by Microsoft, to satisfy the FDA regulation it would need to be extensively tested to ensure the patch would not adversely affect the device before it can be passed to the customer to install. In the meantime the vulnerability exists and the device is left exposed.

The principle behind application whitelisting is simple: only allow completely necessary and authorised code and processes to run, denying all others, irrespective of whether the process is known or not.

Application Certificates are electronic ID-cards created and assigned to software programs. Just like an electronic ID can identify a person, an Application Certificate uses the same principle to identify a specific program and all its components. During any attempt to execute code, the software component will be compared to information within an Application Certificate. So, instead of looking for hundreds of thousands of known threats, the software looks through a list of all known approved applications, if no match is found the program will be prevented from starting. This list will always be shorter than one containing identified threats, so much less processing power and memory is used, and will also remain up-to-date, particularly important to secure medical equipment.

Using the principle of "Default Deny" any file that is not part of an authorised application is treated as undesirable and never permitted to start. The result is that any virus or unauthorised software is completely blocked and therefore can never pose a threat.

As the software does not require new signatures or updates, the device remains operational 24 hours a day, seven days a week, vital in a hospital environment. By only permitting authorised software, files and applications to run with the use of digital certificates, critical systems are provided with smart protection against malicious code without affecting the functionality of the system. While previous solutions required resource intensive simulations and behavioural analysis, which put high demands on memory and bandwidth, this technology was easy to implement without impacting systems performance.

The endoscopic equipment manufacturer did require some adjustments to meet the complex needs of medical environments. For example, some hospitals want and need the ability to install software themselves without affecting their warranty. While the software was initially based on online certificates, the medical device manufacturer needed its devices to work independently and locally. To deliver this requirement Cryptzone designed and developed a local whitelist manager to create local certificates on a local system. This allows for the software to be configured by two issuers, with the hospital and Karl Stortz each having their own Certificate Studio to certify software. When used in this way it is simple to create an undisputable audit trail of who has done what, and when a key element for compliance with FDA regulation is updated.

This means that, when a customer wants to install new software or even a printer driver that is not already included in the whitelist, an authorised user can locally create and add certificates then lock the list again.

Christoph Hiltl, Product Manager Aida/OR1 at Karl Stortz explained: "To ensure the security of our devices we were looking for a partner who was on a par with us and would truly understand the needs and concerns of Karl Stortz and its customers. With our previous experience within the aviation and military industries we knew we had found a partner who was competent in developing highly sophisticated and dependable software that our customers could rely on."

In close collaboration, the software and medical device manufacturers developed a solution that could be installed in the factory with minimal need for after-sales servicing and updates. This has not only minimised the time and effort it takes to roll out the new technology, but also considerably reduces downtime due to maintenance and servicing once in operation at a hospital. Operators are now able to make changes and adjustments to the devices without compromising security or affecting compliance as this type of technology only allows 'safe' software into the system.

"With the whitelist manager we can offer our customers active, complete protection that will ensure security, efficiency and reliability for their devices – which not only crucially means higher safety for patients but also keeps maintenance and downtime to a minimum," said Hiltl. "Security can be managed without the need for regular external updates which, if not managed properly, has the potential to adversely affect the performance of our systems."

The Future

With the first devices incorporating the technology complete, further ranges will follow. For the two companies this is only the beginning: "Together, we are continuing to advance our technologies to ensure we will be able to deliver ever more sophisticated, secure and operator-friendly solutions across all our systems," said Hiltl. "Cryptzone is an integral partner in our strategy to mitigate IT security risks to ensure we can continue to provide the quality and reliability our customers can depend on."

Benefits

Secured System

Active protection and compliance through Application Whitelisting that prevents unauthorised system modifications and blocks unauthorised hardware and ports.

Fast and simple installation

Pre-installed and delivered as part of the device to the end customer with minimal CUP and disk space usage.

Stand-alone solution

Stand-alone solution that requires no hook-up to an external server for updates, but works locally, creating local certificates.

Less Downtime

Customer needs to spend less time maintaining and servicing the system and requires less third-party support, saving time and expense.

Easier management

Role-based access through local, enterprise and service keys. Operators can easily make adjustments and changes to the devices without compromising security, compliance or warranty.