451 Research

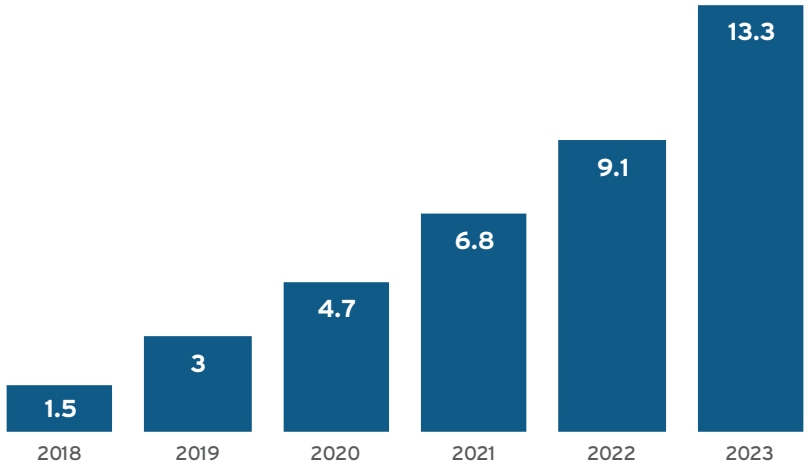
Business Impact Brief

Growth in Connected Medical Devices Furthers the Need for Authentication

The 451 Take

Connected medical devices continue to improve patient outcomes and reduce treatment costs both in hospitals and personal environments. 451 Research's Global IoT Market Monitor projects that the number of connected medical devices, including those found in healthcare facilities, personal monitoring devices and hospital beds, will grow from 1.5 million to 13.3 million between 2018 and 2023, representing an average 154% CAGR. By 2023, we predict that healthcare facility devices and hospital beds will collectively make up 64% of total devices, with personal monitoring devices making up the remaining 36%. As the number of devices continues to grow, so too does the attack surface. This increases the already critical need for more robust medical device security, including strong authentication capabilities. This is further evidenced by 451 Research's Voice of the Enterprise: Organizational Dynamics 2017 survey, in which 64.3% of respondents identified the poor authentication capabilities of IoT endpoints as their primary security concern.

Total Connected Medical Devices (in Millions)



Source: 451 Research Global IoT Market Monitor

The safety risks of weak device authentication are real; the ability to remotely manipulate a medical device poses a direct threat to patient health whether in a hospital or at home. For example, in a hospital, a ransomware attack such as WannaCry could easily spread among medical devices that lack methods of validating data and device integrity. The British National Health Service was among the organizations hit hardest by WannaCry, which took down surgical instruments and other devices for extended periods, delaying life-saving surgeries and putting patient health at risk. The safety concern associated with these devices is so great that in 2017, Abbott Labs recalled nearly half a million pacemakers for an update after the discovery of a safety-critical vulnerability.

In addition to the safety risks, stakeholders face extensive financial risk because of poorly secured devices – the impact of extended downtime on a hospital's revenue and the impact of device recalls on that of an OEM. This risk is exacerbated by the fact that connected medical devices interoperate with a variety of resources on the network including electronic medical record (EMR) systems. Without a way to cryptographically authenticate a device's identity or the integrity of its communications – e.g., through PKI-based methods such as X.509 certificates – these devices provide attackers with a foothold in the network to exfiltrate patient medical history from the EMR or conduct reconnaissance for more sophisticated attacks to steal financial and insurance information.

Business Impact Brief

The 451 Take (continued)

Despite these risks, devices are often manufactured without the specialized hardware necessary to perform essential functions such as establishing root of trust, performing secure boot, validating updates and authenticating commands. Part of the reason for this is that the FDA requires manufacturers to submit any material device changes for regulatory review to ensure they will continue to function, which is a long and expensive process. There are also no enforceable regulations in place requiring strong cryptographic authentication on medical devices. In 2014, the FDA issued a premarket cybersecurity guidance for medical devices suggesting that manufacturers avoid the use of hard-coded passwords and authenticate firmware and software updates, although it did not specify acceptable authentication methods. The FDA also issued post-market guidance on security management for medical devices in 2016, as well as a separate guidance in 2018 on securing devices with off-the-shelf software. However, no updates have been made that supersede the premarket guidance in terms of security controls recommended in manufacturing. While guidance is a step in the right direction, it lacks the enforceability necessary to force manufacturers to strengthen their devices' authentication. GDPR, on the other hand, could have a material impact on hospitals and manufacturers as weak authentication exposes patients' private information.

There are methods available to hospitals that recognize the need for stronger authentication on medical devices. Gateways deployed on the hospital network can act as a trust broker between devices too constrained to store and exchange their own credentials, including certificates. Hospitals can also limit the ability of a compromise to propagate throughout the network by applying the principle of least privilege, revoking a device's access to any systems it does not explicitly require for normal functions based on that device's cryptographic identity.

Business Impact

MONITOR THE REGULATORY ENVIRONMENT FOR MATERIAL CHANGES TO SECURITY REQUIREMENTS. The FDA's emphasis on authentication in its premarket cybersecurity guidance could be indicative of stricter regulations, and GDPR is likely to impact the measures taken by both device manufacturers and hospitals to protect sensitive patient information. Implementing cryptographic authentication methods can help manufacturers and hospitals remain compliant through the shifting regulatory landscape.

SIGN FIRMWARE TO VALIDATE DEVICE INTEGRITY. Code signing validates that the device's executables were written by the authorized manufacturer. By only allowing software to execute that has been signed by a designated certificate authority, hospitals and OEMs can limit an attacker's ability to inject and execute malicious code on a medical device and inhibit an attack's ability to spread throughout the network.

CONDUCT SECURITY ASSESSMENTS OF ALL NEW DEVICES BEFORE PURCHASE. To prevent exposing themselves to unnecessary risk when deploying new medical devices, hospitals should determine whether a given device possesses the proper hardware to perform critical security functions. If not, the hospital needs to weigh whether the improved care from connected devices outweighs the potential safety, financial and privacy risks.

Looking Ahead

With the advent of stricter global privacy regulations and an increasing focus by consumers on protecting their personal information, it is only a matter of time before the focus turns to improving medical device security. Long device replacement cycles may slow down the adoption of medical devices in the short term, but measures such as using gateways to perform authentication for older endpoints will serve as a stopgap during the interim. As the use of cryptographic authentication grows in medical environments, scalability becomes an increasingly important factor, and proven PKI-based methods could lead the way.