Cybersecurity

An Essential Priority within the Mindray Patient Monitoring Network

Preparedness & Mitigation

www.mindray.com

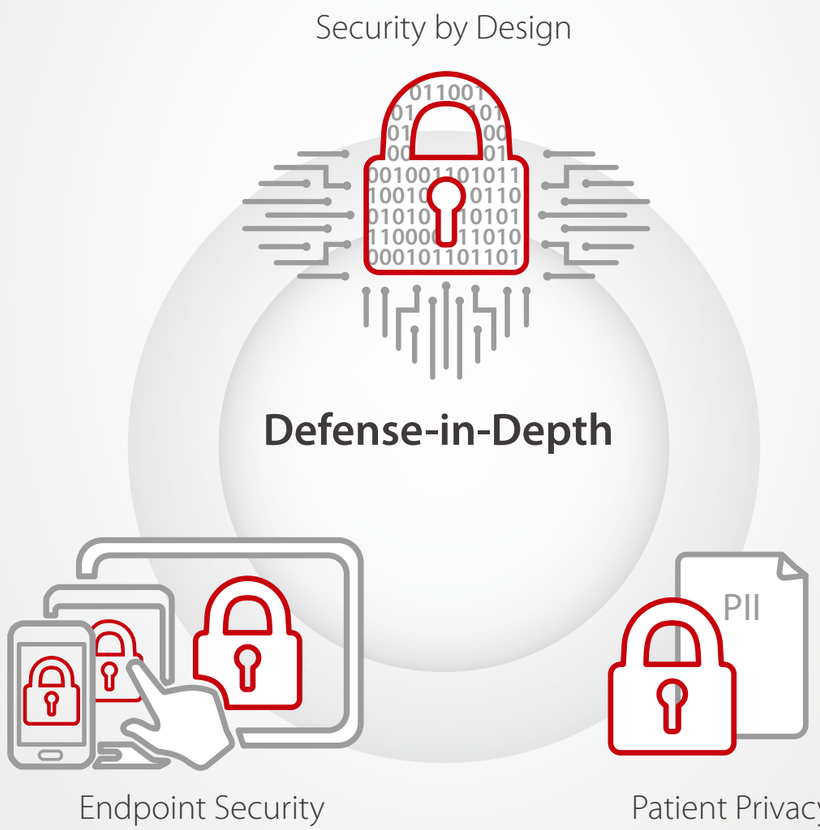
P/N:ENG-Cybersecurity-210285X8P-20210107

healthcare within reach

The development of the Internet has brought us a lot of convenience in our daily life. Also the world of cyber risk continues to develop and expand. Medical data, which attracts a large number of attackers to try to steal and sell for profiteering.

In order to protect patient data, assuring patient safety and privacy, medical device manufacturers should pay more attention to cybersecurity.

Mindray is committed to protecting patient data and assuring privacy. We promote and shape deeply embedded partnerships with our customers to assist in driving the adoption and implementation of strategies that will proactively mitigate cybersecurity risk.



There are three main areas of focus that we target to achieve cybersecurity, Endpoint Security, Patient Privacy and Security by Design. And the sum of Mindray's multifaceted cybersecurity strategies can be described as Defense-in-Depth.

Endpoint Security

Endpoint security focuses on minimizing the threat of unauthorized access through devices such as laptops, workstations, mobile and bedside medical devices. Mindray provides Endpoint security coverage for Mindray devices deployed within the Mindray Patient Monitoring Network.

Mindray reduces the network attack surface by segmenting the network, eliminating unnecessary pathways, and restricting access to communications on the network. Finally, locking down and securing these medical devices is the definitive and core component of Mindray Endpoint Security.

Measures for Endpoint Security

Component	Description	Device
Whitelist	A program that acknowledges and allows predefined and preapproved applications to access a particular service.	CMS, eGateway
Anti-Virus	A program that monitors a device to identify all major types of malware and prevent, detect and remove them.	eGateway
OS Hardening	Disable USB write and startup, disable non-essential ports and services.	All devices
Firewall	A barrier that restricts external access and other applications.	CMS, eGateway
Wi-Fi Encryption	All Monitors with 2.4/5G Wi-Fi module supports WPA2-PSK and WPA2 Enterprise encryption mode.	All monitors
Protocol Encryption	All private protocol data is encrypted by xxTEA or TLS1.2(AES-256).	All devices

Patient Privacy

Mindray patient monitoring system utilizes features such as user access controls and customized screen configurations to support patient confidentiality. When deployed in the hospital, these various strategies prove effective in supporting patient privacy.

Measures for Personally Identifiable Information (PII) Protection

Component	Description	Device
PII Protection	All PII is encrypted on the device and logs. And PII on the displays and reports allow the user to customize.	CMS, eGateway, N series
Secure Data Deletion	Support completely erase all facility data.	CMS, eGateway, N series
Password Management	Supports the use of strong and editable passwords, roles, access timeouts, as well as integration into the hospital Active Directory.	All devices
Access Control	Supports integration into the hospital AD to provide access to managed user account, permissions and password policies.	Monitors, CMS

Security by Design

This strategy of Security by Design is indicative of the critical emphasis Mindray places on the security of the BeneVision Patient Monitoring Network and all its associated devices.

Measures for Security by Design

Component	Description	Device
Security Testing	Fuzz and penetration testing for testing application stability.	All devices
Code Analysis	Automated analysis of source code looking for common implementation issues which lead to vulnerabilities.	All devices
Risk Management	Identification and mitigation of security risk before development and after product release.	All devices
Patching Policy	An ever-vigilant approach to monitoring Microsoft Patch release to shore up vulnerabilities in the Microsoft Operating System.	All devices
Redundancy	System redundancy and data backup.	CMS, eGateway
Backfilling	Retransmit patient data during the network disconnection.	All devices

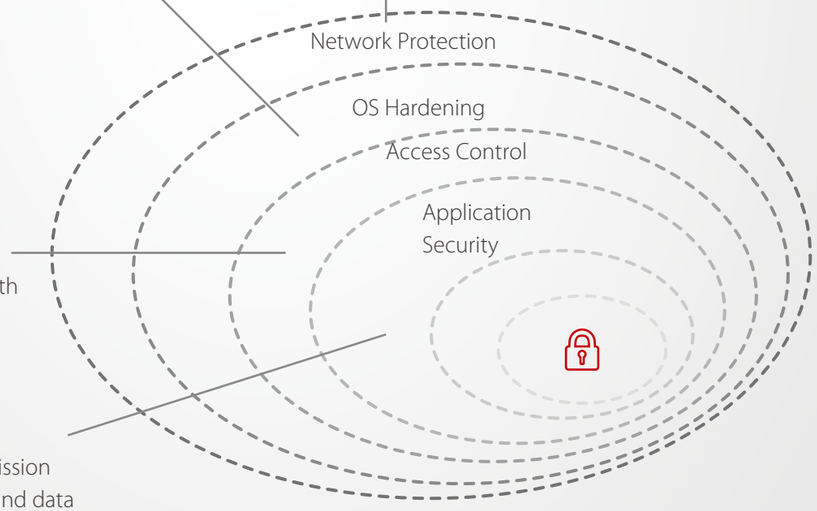
Defense-In-Depth

The sum of Mindray's multifaceted cybersecurity strategies can be described as Defense-in-Depth. There is no one single solution for cybersecurity, but rather a series of measures working together in unison to have a net positive effect. All of the strategies described here are methods which complement existing institutional efforts to reduce the incidence of cybercrime.

Mindray, in partnership with our valued customers, proactively implements these measures and techniques to combat cybersecurity threats and better protect patient privacy.

- Update OS patches regularly
- McAfee white list
- Support hospital antivirus strategy
- Disable USB write and startup
- Disable non-essential ports and services

- Firewalls restrict external access and other applications
- Wi-Fi Enterprise
- Protocol Encrypted by TLS1.2(AES-256)



- Local password
- MLDAP integrated with hospital AD

- Offline data retransmission
- System redundancy and data backup

Fuzz testing/penetration testing/security risk assessment/source code analysis, etc

The network should be designed to keep the Mindray monitoring equipments and traffic as isolated as possible from the rest of the hospital's network.

To protect the entire healthcare system against hacking, hospital also needs to realize a defense-in-depth strategy. Multiple layers of defense should be implement to protect the hospital network from internal and external cyber-attack. You should pay attention to the following network strategies.

- Boundary and Internal Network Security
- Wireless Network Encryption
- Network Isolation
- Patch and Update Policy
- User Behavior and Permission Management
- Disaster Recovery
- End-user Education
- .....