MEDIGATE

Clinical Cyber Hygiene

Reduce device risks and optimize device availability

At a Glance

No organization can manage what they cannot see, which is why so many healthcare delivery organizations (HDOs) struggle to manage their device risks. A lack of visibility into pertinent device details coupled with possible disruption of patient care by active device scanning makes it extremely difficult for HDOs to understand the attack surface area of their connected devices. To understand and manage medical and IoT devices' risks to ongoing HDO operations, a systematic approach is needed.

Key benefits:

- Device risk factor visibility and breach likelihood
- Streamline vulnerability management planning and execution
- Safely scan and act to reduce risks and optimize device availability

Medigate's Clinical Cyber Hygiene

The Clinical Cyber Hygiene (CCH) module from Medigate analyzes, maps, and aggregates threats posed by unmanaged endpoints to help HDOs understand and reduce their device risks. With CCH, effective vulnerability management and orchestration strategies allow HDOs to quickly prioritize risks within their connected endpoints and implement effective vulnerability management and orchestration strategies to optimize their device availability and risk reduction.

How it Works

Medigate deep dives into every device, using deep packet inspection (DPI) techniques to provide visibility of important device characteristics. CCH then applies its unique risk assessment framework to address the individual factors that affect the probability and severity of a compromised device. In the context of the clinical setting, it assigns each device a relative risk score. CCH allows HDOs to focus

on what matters most, enabling them to prioritize the patching or segmenting of devices with known security vulnerabilities and protect their entire operations availability and integrity. With CCH, HDOs get:

- **Customized risk framework:** Individual HDOs can tailor the structure of Medigate's device risk score framework, which looks at device attributes, network connectivity, common vulnerabilities and exploits (CVEs), among other factors.
- **Risk score simulation:** Calculate the benefit or risk of hypothetical device configurations and remediation activities to ensure no disruptions and no surprises.
- **Vulnerability scanning orchestration:** Identity-aware scanning information supports the appropriate inclusion/exclusion of IoT and IoMT devices in vulnerability management scans to ensure critical operations and patient care aren't interrupted.
- **Remediation recommendations:** Clinically aware fixes and patch recommendations for IoT/IoMT devices enable HDOs to know where to focus their resources.

Conclusion

Most HDOs struggle to understand and address the risks their connected devices pose to their operations. Medigate has learned the unique languages of clinical devices and does not guess what they're saying through AI or Machine Learning. Instead, those techniques are used to deliver advanced insights from device data. With Medigate, the data available in all of your connected devices are unlocked, trusted, and the HDO can connect with confidence to improve the availability and quality of care while safely accelerating their real-time healthcare initiatives.