MEDIGATE Check Point SOFTWARE TECHNOLOGIES LTD.

INTEGRATION

Protecting the Internet of Medical Things

KEY FEATURES

- Comprehensive and accurate discovery of all connected medical devices
- Clinically-contextual anomalous behavior detection
- Device tagging to create rule-based security policies
- "Single pane of glass" viewing for all Medigate generated content on Check Point's SmartConsole

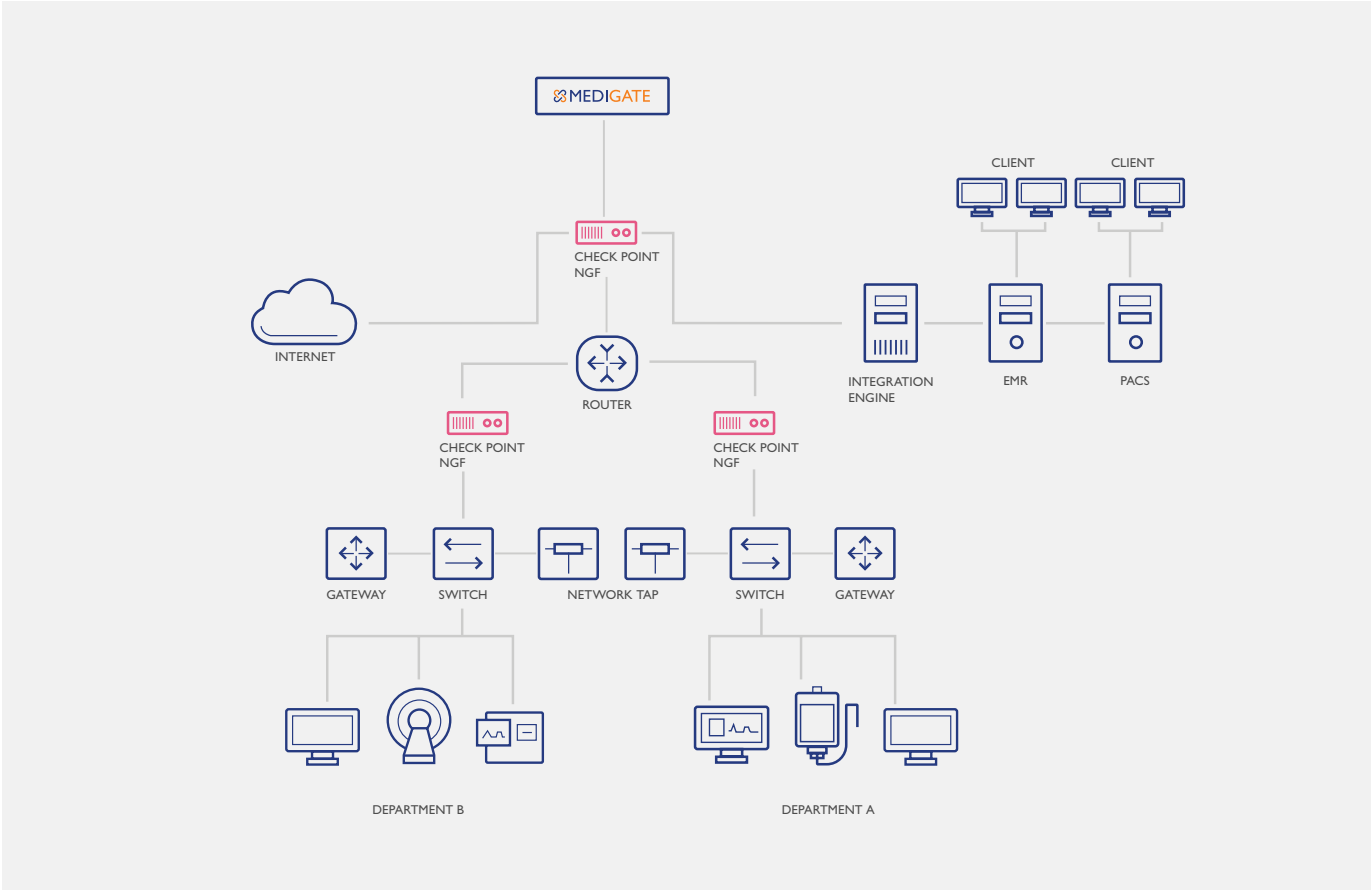
KEY BENEFITS

- 24/7 enforcement of protective and preventative security policies on individual medical devices
- Mitigate security flaws and reduce risk of successful cyberattacks
- Prevent infected medical devices from spreading to other systems
- Gain actionable insights for management of of IoMT and IoT connected devices

Medigate and Check Point are delivering a state-of-the-art IoT and IoMT security solution that addresses the security risks connected devices generate in the clinical network. Combining Medigate's industry-leading, clinically contextual visibility and detection capabilities with Check Point's proven Security Gateway capabilities provides healthcare organizations with a security solution tailored to their unique needs.

Medigate's passive platform is easily installed within a hospital's network and integrates with Check Point's R80 management system and Security Gateways. Once connected, Medigate's medical device security platform shares identified device and application information with Check Point's SmartConsole. This enables an all-in-one viewing experience for complete device visibility information generated by both platforms, creating a seamless experience.

How it Works



It all starts with granular visibility of every medical device on the network. Utilizing deep packet inspection, Medigate provides fingerprinting of a device's unique identifiers, including: configuration, utilization, performance and location. Integrating the two systems enables the data from both systems to be displayed within the Check Point SmartConsole, removing the needed to flip back and forth between dashboards.

Until now, Checkpoint's firewall rules relied on network zones, IP addresses, and ranges. Having the ability to tag medical devices by functionality type, vendor and model name enables more granular policy management capabilities. Medigate also makes sure that the tags stay current by constantly monitoring changes in the device's network properties, such as IP address and software version.

Four types of security policies through Check Point's Security Gateways

01

Network Segments Restriction

Authorize and block access between network segments tailored by device types / other device clustering logic (e.g. restrict medical device of a particular manufacturer access to Internet domains).

02

Port Restriction

Leverage Medigate's clinical domain expertise to control a device's authorized ports and enforce only vendor-approved communications.

03

Protocol Restriction

Reach the deepest level of network traffic inspection, authorizing only proprietary device protocols and block threatening communication methods.

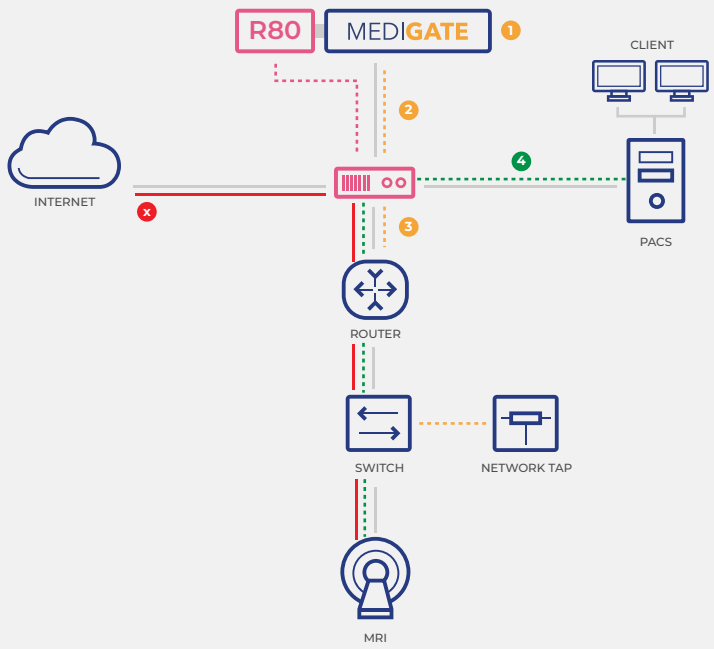
04

Group to Group Restriction

Authorize connections between specific devices, such as an infusion pump and its dedicated gateway and server, while blocking all communication out of manufacturer scope.

For example, if an infusion pump is tagged as such, a provider can control its access to other parts of the network and set it to solely communicate with its dedicated gateway and server. Moreover, with the Port and Protocol Restriction features, it is possible to control which devices the infusion pump communicates with as well as ensure it communicates only with the pre-defined ports and certain protocols set by the manufacturer. In this example, the infusion pump could communicate with its protocol server, while SMB packets would be intercepted.

Diagram of an Exemplary Enforcement Policy Set-up



1. Clinical security policies are preconfigured via Checkpoint's R80 Management System.
2. Medigate Identifies medical device, in this case an MRI device.stem.
3. Medigate attaches the appropriate IP-tags: manufacturer's tag, MRI tag, medical device tag – to the appropriate host on the network.
4. The MRI successfully manages to connect to the PACS.

× A forbidden connection attempt from the MRI to the internet is blocked.

A Security Solution for Today's Healthcare Cyberthreats

You can only protect what you can see. Knowing exactly what's on the network and what it's supposed to be doing is the first step towards securing it. Combining that with Checkpoint's advanced enforcement capabilities, empowers you to confidently expand your inventory of connected devices and receive all of the benefits of digitization while maintaining patients' privacy and safety.