DornerWorks

Embedded Systems Engineering

Secure your Medical IoT with a Firewall

Key Benefits

- IT can manage all connected devices from a single, secure portal
- Firewall takes advantage of known traffic patterns on a per-device level, easily blocking threats
- Respond to 0-days without waiting for vendors to issue patches by remotely filtering packets or quarantining infected devices
- Built for stringent requirements of medical environment (compliance/privacy/security)

A Worst-Case Scenario

Infected by malicious Petya ransomware, the Princeton Community Hospital in West Virginia was unable to access its own data, and forced to replace its entire network. Countless medical documents were lost.

The Healthcare and Public Health sector is ironically one of the least immune from cyber attack, with more security incidents reported in 2015 than any other critical area infrastructure. Added to that, expensive legacy equipment, newer, often incompatible devices to manage, and strict compliance requirements are often all seemingly working against medical IT professionals as they attempt to keep a variety of software and OSs secure from the latest threats.

It doesn't have to be that way.

DornerWorks is developing a **specialized firewall** that can be installed **inline with connected medical devices**. This new technology works out-of-the-box with minimal configuration or oversight, is a breeze to maintain at scale and is backed by a service that provides safe, automatic OTA updates to effectively battle tomorrow's cyber threats.

Or Long-Term Security, *and Immediate Freedom*

With the **IoT Medical Firewall** developed by DornerWorks, internet-connected devices would be instantly protected. Stored medical device profiles could be used to effortlessly apply proactive rulesets to firewalls. Rudimentary metrics could be accessed from any connected device, giving IT pros insight into network utilization. And as a bonus, the firewall could provide wireless freedom as a WiFi bridge.

Contact us to learn more
www.DornerWorks.com
sales@dornerworks.com
616-245-8369

Let's Talk

Together, we will determine a customized solution that fits your needs.

Or

Buy a Quick Start Package

A Quick Start Package includes all the essentials to get your project off the ground.

DornerWorks, Ltd. 3445 Lake Eastbrook Blvd SE, Grand Rapids, MI 49546 USA

A Safer Alternative

The damage Petya caused could have been easily avoided were a firewall device placed in front of the Princeton Community Hospital's legacy computers (e.g., ones running older versions of Windows) or those with critical functions. The device could have subsequently blocked ports for unused services by default, like SMB, which Petya leveraged to infiltrate the network.

More importantly, IT staff could have rapidly deployed configuration changes from the central web portal to isolate infected machines and *protect un-infected machines*.

Perimeter firewalls and Network Intrusion Detection can only do so much in diverse networks, but individual firewalls can be tailored for the device they protect, potentially learning their normal behavior and quickly identifying threats. The level of security can also be tailored to the medical device being protected, imposing more strict constraints on legacy devices that pose a bigger threat.

Future Add-ons

- **Optional debug port connectivity** – connecting the firewall to a medical device's debug port -- could enable additional remote monitoring or maintenance issues and OTA upgrades.
- **Machine learning** could further augment the firewall's protection algorithms so that new threat vectors could be automatically blocked as they emerge.
- **Security upgrade features** could interpret and upgrade insecure communication from a medical device automatically (e.g., DNS to DNSSEC, HTTP to HTTPS, etc.).
- **VPN** could pipe all traffic from insecure devices through a secure network or DMZ to external networks without the need to established expensive two-network solutions.

Security Highlights

The **IoT Medical Firewall** developed by DornerWorks has no open ports and all of its own command and control communication is encrypted with TLS. Among other benefits, this technology offers:

- A web service that meets industry-standard security standards
- Defense-in-layers approach (e.g., even trusted devices and double-authenticated users would have limited access)
- Regular monitoring and updates to address any new threats
- External auditing/testing so as to be sure we're not introducing new attack surfaces into the network
- Guided by the NIST Cybersecurity Framework for critical infrastructure
- HIPAA compliance through a carefully constructed policy, enforced at the data acquisition level

Ease of Use

Provisioning for the IoT Medical Firewall can be streamlined, as the device works right out of the box. An accompanying app would allow even more advanced field-provisioning options, when needed. The devices are designed to be centrally managed through a web portal and could be updated in batches based on the device they protect.

And, updates to the firmware would be safe and automatic – ***no maintenance required***.

The IoT Medical Firewall will continue to work and provide a level of protection even when the supporting service contracts end. On-premise management options could be available through licensing if there is interest.