How Location-Based IT Could Re-Invent Healthcare Security

healthitoutcomes.com/doc/how-location-based-could-invent-healthcare-security-0001

By Christine Kern, contributing writer

One pharmaceutical company has implemented endpoint security to protect users.

Ninety-one percent of all healthcare organizations suffered at least one data breach in the past two years, with an average cost of $2.2 million per hack. Additionally, more than 60 percent of hospitals have no breach response plan in place, ***according to the Ponemon Institute***.

The dangers of breaches have been well reported — from the immediate costs of down time, to secondary costs of loss of reputation and recovery costs, to the potential tertiary and expensive costs of legal repercussions. As attacks against healthcare organizations increase there is increasing pressure from both the federal government and the private sector to bolster information security programs.

For healthcare organizations like Aspire Pharmaceuticals that handle valuable medical records and consumer information, it is imperative healthcare adopt context-aware security policies. This means, above all, understanding where and how data is being used. ***A recent case study*** demonstrates how Aspire was able to implement endpoint security to help re-invent its security protocol and ensure the protection of its data and users.

According to Roman Foeckl, co-founder and CEO of endpoint security and data loss prevention provider, CoSoSys, healthcare organizations should be sure they implement the following context-aware policies to keep their sensitive data safe:

- **Indoor Mapping**. With augmented reality paving the way, Apple and Google have made major strides in enabling localization indoors. Security applications are endless.
- **Beacons**. By transmitting information in a certain range, doctors can have relevant information appear on their tablet depending on where they are in hospital. Conversely, the moment they are out of range of the beacon, data can automatically be removed or encrypted — ensuring data does not leave a designated area.
- **Geofencing**. Can be used both to keep information in by restricting access to devices or applications while inside a specified perimeter, and out by making it impossible for devices outside the perimeter to access the network.

Doug Copley, Senior Security and Privacy Strategist at Forcepoint also reinforced the need for end-to-end protection of data. He told *Health IT Outcomes*, “There are many things healthcare organizations should be doing,” says Copley. “When I sit down with healthcare CISOs, I counsel them to have strong, comprehensive

security mechanisms which include robust controls at entry and exit points to the network, as well as strong insider controls to protect data coming and going off endpoint devices such as PCs, tablets, and mobile phones. Data can leave these devices via memory cards, printers, Web email and programs like OneDrive and Dropbox."

As the Aspire case study points out, since the pharmaceuticals company must secure an extensive range of confidential data, they needed a solution that would add additional security while also closely monitoring employees' activity and related data transfers. Key features of a solution included granular control of the policy and the speed of updates to both server and client when access level is changed at any given point. And the solution had to be cost-effective.

Aspire turned to the Endpoint Protector 4 Hardware Appliance from CoSoSys to meet these needs. As Accounts Manager Jay Patel explained, "We chose Endpoint Protector because it met all of our criteria in the most cost-effective way. The deployment via the user interface is straightforward. Our company was set up within hours and the support and service offered by CoSoSys are excellent."