Hospital IT Team Gains Insightful Visibility with IoT Guardian

Thinking Outside the Security Box

Bear Valley Community Hospital (BVCH) provides a diverse set of health care offerings — including not only in-person care but also telehealth services — that ensure the well-being of the residents and seasonal visitors of Big Bear Lake, California. The staff at BVCH seeks to deliver the highest quality care as efficiently and effectively as possible to its entire community.

At a multi-faceted facility like BVCH, locating and protecting various types of data and devices is critical to ensuring a seamless and safe environment for patients and care providers. When the security team at BVCH first engaged with Zingbox, they were confident that they had secured the health care facility’s various end points and security perimeter, but they still did not have visibility into the network-connected devices that were left open to risk. There was no standardized system for alerting the IT and facility teams when a new device was activated in the network, leading to “tribal knowledge,” as Bear Valley Community Healthcare District IT Director Jon Booth says, where information about devices was decentralized and quickly lost when individuals left the organization.

BVCH’s security team knew that without identifying, locating, and securing such devices, they were leaving their entire network open to attackers. It would take only one unmanaged, unmonitored, or unmaintained device to instigate a breach of data or network disruption that could raise operational and staff costs, damage BVCH’s standing in this tight-knit community, and, worst of all, erode patients’ trust in the facility and its providers. It was time to think outside the security box.

An Eye-Opening Experience

After a seamless Proof of Concept (POC) and fast deployment of IoT Guardian, Jon and his team began to see the solution’s benefit on their security management capabilities right away. With an interface that was not only intuitive but also intelligent, Zingbox’s platform helped the hospital’s IT team identify endpoints that they knew existed but couldn’t previously classify or locate. Prior to implementing IoT Guardian, unless devices self-reported or self-identified, the team had no way of knowing details about these devices — such as the name of its manufacturer. “With Zingbox, we found between 10 and 15 percent more network connected devices than we expected,” Jon says. “It was a very eye-opening experience.”
Zingbox gave BVCH a clear picture of security across the entire hospital, finally answering instead of creating questions. At last, BVCH’s IT and facilities teams were on the same page, agreeing with information presented across one comprehensive security dashboard.

**Technology That Never Sleeps**

In addition to identifying each device and revealing its location on the hospital network, IoT Guardian gave BVCH decisive and automatic protection against emerging security risks. Through machine learning and three-tier profiling techniques that baseline acceptable behaviors and create the unique “personality” of each device, IoT Guardian knows not only the kind of device — for example, a boiler control — and whether it is online, but also the typical days and times it is used, who uses it, and many other details unique to each device's utilization. When a device is acting abnormally or communicating outside the network through unauthorized means, Zingbox self-reports issues immediately to users.

Leveraging this technology helped BVCH discover that a recent deployment of medical storage devices were communicating in an insecure way and that a device was running unrecognized antivirus software from Eastern Europe. BVCH’s IT team also uses Zingbox to validate their device inventory data on a regular basis.

One of the clearest examples of Zingbox’s benefit on BVCH’s operations is demonstrated through a simple yet powerful metric: Sleep. With Zingbox’s always-on, always-learning technology continuously monitoring the network for potential vulnerabilities, Jon says that he and the other members of his IT team now sleep more soundly at night. “Zingbox is unforgiving. If something’s messing around, it’s going to catch it,” he says.

In a world where the threat environment changes on a moment-to-moment basis, it’s crucial to have technology that never sleeps so IT teams can.

**A Security Solution For Any Organization**

Like many organizations, BVCH was challenged with securing a wide range of data and devices with limited staff and resources. Zingbox provided BVCH with real-time visibility into the security of their entire network. From a community hospital like BVCH to a large medical system, healthcare organizations often don’t have the means to address complex IoT security concerns. And Zingbox’s solutions have an impact beyond healthcare — no matter which industry, gaining instant clarity on the security of connected devices is fundamental to driving down costs, protecting brand and reputation, and ensuring consumer trust.

---

“With Zingbox, we found between 10 and 15 percent more network connected devices than we expected. It was a very eye-opening experience.”

— Jon Booth, IT Director