



Guardicore

CASE STUDY

Beckman Coulter Safeguards Patient Data, Meets Complex Compliance Demands with Guardicore

The Client

Beckman Coulter is a leading global manufacturer of medical laboratory diagnostic equipment. Its customers include the world's largest healthcare systems. More than a quarter of a million Beckman Coulter instruments operate in laboratories around the world, supplying critical information for improving patient health and reducing the cost of care.



The Challenge

Preventing Product and Data Tampering While Demonstrating Compliance to Global Regulators

As medical devices have become more sophisticated, they are also increasingly interconnected, delivering data to cloud-based analytics, both to make more precise and timely patient diagnoses, and aggregate data to advance scientific research. Though they have supported great advances in patient care, networked medical devices are prime targets for hackers and cyber-thieves.

"Healthcare data has every element of personal information that someone can use for identity fraud," points out Scott T. Nichols, Beckman Coulter's director of global product privacy and cybersecurity. "The data we have is more valuable on the dark web than credit card numbers."

What's even more important, Nichols says, is patient safety. "Cybersecurity can impact patient safety. For example, there have been reports of vulnerabilities regarding infusion pumps and, if someone were to alter frequency or dose, this could have life-or-death consequences for a patient." Product availability is also critical, as providers need accurate diagnoses quickly to make proper treatment decisions.

Medical devices are highly regulated by the United States Food and Drug Administration, and must also comply with global regulations governing patient privacy and restricting the movement of data across borders. In Beckman Coulter's case, these include HIPAA in the U.S., the European Union's General Data Protection Regulation (GDPR), and Canada's PIPEDA and FIPPA. Beckman Coulter's technology is also considered part of critical infrastructure in the U.S., and thus falls under Department of Homeland Security Coordinated Vulnerability Disclosure (CVD) processes.

Simply put, Beckman Coulter has a responsibility to protect patient safety and data, ensure clinical performance for its customers and then prove to regulators that it is effectively doing so.

Challenges in the Cloud

Beckman Coulter has now launched some cloud-based products and has more planned in the near future. "Some of these are analytics-based, collecting data from our instruments to provide different kinds of usage analyses for our customers," Nichols explains. "We have regional clouds, including public clouds utilizing Amazon Web Services (AWS) infrastructures, and private clouds hosted within our own data centers."

The company's cloud initiatives have brought a host of new challenges, Nichols says. "The key challenge is obviously protecting the data, but it's also having visibility into that data, knowing where the data is flowing, who's accessing it and what types of threats could be present."

Another challenge is convincing customers that their data is secure in Beckman Coulter's cloud instances. "We have a shared responsibility with customers to make sure that our medical devices are secure and not susceptible to privacy breaches. That's true on-premise, but all the more so now that we're taking their data and putting it into a cloud. They need reassurance we have the proper protection and visibility to help prevent cyberattacks, malware or ransomware."

Importantly, Nichols knew Beckman Coulter needed to put those protections in place before launching. "I did not want to go live in the cloud with any of these products and services and be blind."


The Solution

Guardicore Centra™ Security Platform

Nichols learned about Guardicore through a value-added reseller (VAR) with whom he had partnered extensively.

"He understood my needs surrounding product security and privacy, and he suggested I talk to Guardicore." Coincidentally, Nichols also read a favorable write-up about Guardicore in a prominent cybersecurity industry publication.

On the face of it, the Guardicore Centra Security Platform seemed to meet a number of Beckman Coulter's cloud-security requirements, with a built-in visualization tool for mapping data flows, and automated breach detection and response capabilities. Before making a decision, however, Nichols and his Bangalore-based security team undertook a proof-of-concept



(POC) study with Guardicore. “We actually put Centra into our staging environment, which replicates our production environment, to see how it would behave,” Nichols recalls. “Our applications have certain Service Level Agreements, and we needed to make sure that it wouldn’t impact performance. We also wanted to really see what kind of data we could collect on the security of our environment.”

The test was extremely very convincing. “Even in the POC, we were already seeing a surprising amount of bot activity. But we also saw a full visualization of traffic occurring within our cloud infrastructures, and that was exactly what I was looking for—that level of visibility and transparency, and the ability to take action on it. That was very eye-opening.”

It was clear Guardicore Centra aligned perfectly with the security team’s intentions. “That was a very successful POC,” Nichols reports, “which is why we moved forward with production and purchased the product.”

The Benefits

Since implementing Guardicore, Nichols has noted four key capabilities that stand out.

Visibility: “Visibility, to me, means being able to see the traffic patterns, the communication flow between the systems, and knowing what’s going on in the cloud. That’s really what I saw as the strength in Guardicore Centra. I also didn’t realize how many bots were constantly hitting our infrastructure. They aren’t getting through, but just the amount of activity makes

it even more important to have that protection surrounding our different systems.”

Guardicore’s deep visualization capabilities enable operators to set microsegmentation security policies around specific applications and prevent unauthorized process-level communications. “If we know that server A only talks to server B, but we start seeing it talking to server C, that’s not a normal behavior,” Nichols says. “Having the 3D visualization that Centra displays gives you a better perspective on what’s happening.”

Threat intelligence: “Guardicore has the built-in capability to identify malicious activity. It knows how to flag various types of anomalies.”

Automation: “I like having the flexibility to really define the types of behavior that are allowed. It can either alert us or actually take action, spinning out decoys on suspicious activity.”

Forensics: “We have very tight breach-notification windows, and we don’t want to be sending out false-positives to our customers. Guardicore Centra lets you dive in very quickly and determine whether a threat is real or not, or requires further investigation. So the forensic ability has been very beneficial. And I really love the interface.”

The People Behind the Product

The implementation of Centra went very smoothly, Nichols says. “What really impressed me was that a lot of our team was in Bangalore, and Guardicore was able to accommodate the time difference and work within hours that were convenient for our team. That is unique in my experience.”

The working relationship did not end with the sale, either. “The follow up has been incredible,” Nichols says. “A lot of times a company will sell a product, and you don’t hear from them again until the renewal is up. That certainly hasn’t been the case here. Guardicore has been proactive through the whole process, and I’m really impressed with the technical flexibility of the staff.”

Guardicore Centra is now part of Beckman Coulter’s rollout plans for regional data centers and cloud installations around the globe. Above all, Guardicore has enabled Beckman Coulter to attest to its customers and to the regulators that it has the proper controls in place to protect patient data from cyberthreats, ensure product performance and reliability, and adhere to privacy and cross-border restrictions. “The protections and visibility that Guardicore provides to us we believe are very reassuring to our customers,” Nichols says.

About Guardicore

Guardicore is an innovator in data center and cloud security that protects your organization’s core assets using flexible, quickly deployed, and easy to understand micro-segmentation controls. Our solutions provide a simpler, faster way to guarantee persistent and consistent security - for any application, in any IT environment.

www.guardicore.com

