BlackBerry | CYLANCE

CASE STUDY

Phoenix Children's Takes on Cybersecurity

The Company

Phoenix Children's Hospital (PCH) is Arizona's only children's hospital recognized by U.S. News & World Report's 2018–2019 Best Children's Hospitals. For 35 years, PCH has provided world-class inpatient, outpatient, trauma, emergency, and urgent care to children and families in Arizona and throughout the Southwest. As one of the largest children's hospitals in the country, PCH delivers care across more than 75 pediatric specialties. Recognized specifically for its patient-focused innovation, medical education, growth, and research, PCH was named Large Business of the Year and Exceptional Innovator by the Greater Phoenix Chamber in 2018.

The Situation

PCH's Chief Information Security Officer, Daniel Shuler and his team are responsible for preventing threat actors from thwarting the hospital's mission to render quality care to its young patients. The security policies they implement must be sufficiently rigorous to protect an extremely large attack surface without preventing hospital staff, referring physicians, patients, and their families from collaborating and exchanging the information necessary for effective diagnosis and treatment.

When he took the helm in 2016, Shuler knew that PCH would be an attractive target for cyber criminals seeking unauthorized access to the massive troves of sensitive data the hospital routinely collected from its electronic medical records (EMR) and clinical applications, billing and payment systems, and the network of specialized medical devices it utilizes to diagnose and treat patients. Therefore, he moved swiftly when he recognized the need to upgrade the hospital's aging signature-based antivirus system.

"Our incumbent antivirus vendor was continually barraging us with signature update files we would have to install, manage, and audit on thousands of devices," said Shuler. "This was a huge management headache and a serious drain on our IT and security team resources. In addition, we found the reporting and auditing features difficult to access when we were away from the main hospital building, because the antivirus was hosted on a dedicated on-premises server. It was clear to us that our reactive, signature-based approach to cyber defense had become untenable and that we needed an endpoint protection platform that was much easier to manage."

Industry

Healthcare

Challenges

- Protecting a complex distributed attack surface from adversaries attempting to ransom patient data and disrupt hospital operations
- Identifying and closing gaps in the hospital's security policies, processes, and procedures

Solution

- Implementing a prevention-first security posture by operationalizing CylancePROTECT® on all hospital endpoints
- Engaging BlackBerry Cylance red team consultants to assess and minimize cyber risks

PHOENIX CHILDREN'S®

The Process

Shuler considered a number of endpoint protection platform (EPP) solutions before inviting BlackBerry Cylance and two other vendors to participate in a one-month proof of concept (POC). According to Shuler, "We'd assumed that all three next-gen products would demonstrate similar efficacy, so our testing criteria focused primarily on endpoint resource utilization, reporting capabilities, ease of deployment, and management capabilities." Almost immediately, however, the CylancePROTECT solution began detecting malware the other products had missed entirely. "This was totally unexpected," said Shuler. CylancePROTECT also ticked all the boxes for performance and management efficiency. When the POC ended, Shuler and his team selected BlackBerry Cylance as the hospital's new EPP provider and retained a ThreatZERO™ services team to manage the transition from the incumbent antivirus to CylancePROTECT.

Every ThreatZERO engagement proceeds through an efficient and field-proven process methodology that begins with enabling CylancePROTECT's malware detection capabilities in alert-only mode. Once all necessary exceptions have been defined and incorporated into security policies, malware protection is enabled in auto-quarantine mode. Next, the ThreatZERO team moves on to define and enable policies for device control, script control, memory protection, and application control. Because it's an objectives-based process, a ThreatZERO engagement does not conclude until CylancePROTECT is running with all security controls fully enabled. When that milestone occurs, the client has achieved a prevention-first security posture.

The Results

CylancePROTECT was initially deployed in-line with the incumbent antivirus system, which served as the first line of endpoint defense. If the incumbent failed to detect or contain a threat, the suspect file would be passed on to CylancePROTECT, which would prevent it from executing and generate an alert to its cloud-based management console. The incumbent antivirus was decommissioned as soon as the transition to CylancePROTECT was complete. According to Shuler, "All of our locations are required to run CylancePROTECT. That includes our inpatient and outpatient facilities, the main hospital, our data center, every clinic, as well as all of our vendor-provided devices."

Since its deployment, CylancePROTECT has repeatedly proven its efficacy. Soon after the ThreatZERO engagement concluded, CylancePROTECT stopped a ransomware attack that could have disrupted patient treatment by preventing hospital staff from accessing critical EMR data.

With robust endpoint defenses in place, Shuler was ready to address his next set of security priorities. "During that first year, I had identified several other serious gaps in our security program. For example, our password policy was weak, and we were still running old, unpatched versions of Windows on many machines. However, there were too many unknowns for me to feel confident that these were the only issues of concern. I decided to bring in a third-party red team to probe our infrastructure and provide us with a baseline risk assessment."

PCH strives to provide patients and providers alike with convenient and highly secure access to sensitive healthcare information. Physicians can refer patients and view their electronic medical records through a HealthPoint application portal on the hospital's website. The hospital also offers a FollowMyHealth™ application portal that allows parents and patients 13 years and older to view lab results and other medical information. Shuler wanted the red team to assess how easily external-facing systems like these could be compromised.

He also needed an assessment of the damage an adversary could inflict if they managed to compromise and control a system residing on the internal network. How quickly could they move laterally and infect other machines? What data and systems were most vulnerable? He began looking for a consulting organization with the technical acumen and healthcare industry experience needed to effectively test the hospital's internal and external-facing systems.

Shuler had utilized penetration test providers before, but he'd often found the results to be only marginally useful. "To be actionable, pen test findings must be contextualized in terms of their impact on the business and include specific, prioritized recommendations for reducing cyber risks," he said. "What I usually received was an exclusively technical analysis. That's not what I was looking for this time."

Shuler had been highly impressed by the knowledge and professionalism of the ThreatZERO consultants. "They ensured that the transition from our previous EPP to CylancePROTECT was not only seamless, but also an opportunity to share best security practices with our team," said Shuler. After considering his options, he decided to retain BlackBerry Cylance for the pen testing assignment. The three-month engagement included both external and internal pen tests.

According to Shuler, “I told the red team conducting the first external pen test to shoot as widely and broadly as possible. My goal was to get an overall sense of our risk exposure from an external threat actor’s point of view and to identify the weakest points in our attack surface.” Next, the red team moved on to internal pen testing. “This time I was a bit more directive. In addition to the usual vulnerability scanning and unauthorized access attempts, I tasked the team with evaluating our password policies and documenting gaps between our security controls, processes, and procedures.”

Within two months, the BlackBerry Cylance red team submitted its report and formally presented its findings at a meeting attended by PCH’s Chief Information Officer and executive management. “BlackBerry Cylance provided exactly what we needed,” said Shuler. “They identified three medium-severity issues with our external-facing systems that required immediate attention, then provided clear and concrete recommendations for resolving them.” These included a list of critical systems that needed to be patched and recommendations for improving the efficiency of the hospital’s overall patch management processes.

Next, the red team presented its findings from the internal pen test. According to Shuler, “I knew our password policies were weak, but everyone in the room was shocked by the huge quantity of passwords the red team found in employee Word and Excel documents and on scraps of paper by their desks.” The presenters also demonstrated how an adversary could utilize those stolen passwords to exploit privileged local and user accounts to disrupt hospital operations and access patient data. According to Shuler, “The BlackBerry Cylance red team gave me exactly what I asked for; a baseline security assessment, a prioritized roadmap for strengthening our overall security posture, and the credibility with the executive team I needed to put those plans in place.”

Since then, BlackBerry Cylance pen testing engagements have become an annual event at the hospital. According to Shuler, “Philosophically, I’ve always believed in changing pen test providers every year in order to gain fresh perspectives on our cyber risk profile. But, when I asked the BlackBerry Cylance team to offer up something new, I found their proposal too compelling to pass up.”

The three-month engagement that followed included pen tests targeting the hospital’s clinical systems. According to Shuler, “I wanted to assess the potential impact of cyber threats on our patients and caregivers.” The second BlackBerry Cylance red team engagement sparked broad interest among stakeholders across the hospital. At the presentation of findings meeting, the room was packed with attendees peppering the red team with questions ranging from medical device security to best practices for preventing social engineering exploits.

The BlackBerry Cylance red team returned again for a third time the following year with a new remit from Shuler. “This year, we’ve added deep web research to the mix,” he said. “I want to determine whether any of our user account data has reached the dark web, and if so, how it could be used against us by hackers and cyber criminals. What attacks could they make? Most importantly, how do we stop them?”

Shuler recognizes that there are no panaceas when it comes to cybersecurity. However, there is one constant he has come to rely upon: the hospital’s enduring partnership with BlackBerry Cylance. “Our relationship is unique in my experience,” said Shuler. “When you’re dealing with a complex environment like ours, it’s helpful to have allies who thoroughly understand not only your environment, but also your organizational processes and goals. BlackBerry Cylance has proven repeatedly that they have our best interests at heart and that they share our commitment to provide the best care possible for children and their families.”

For more information about Cylance Consulting Services, visit cylance.com/consulting.

©2019 Cylance Inc. Trademarks, including BLACKBERRY, EMBLEM Design, CYLANCE, and CYLANCEPROTECT are trademarks or registered trademarks of BlackBerry Limited, its affiliates, and/or subsidiaries, used under license, and the exclusive rights to such trademarks are expressly reserved. All other trademarks are the property of their respective owners.

About BlackBerry Cylance

BlackBerry Cylance develops artificial intelligence to deliver prevention-first, predictive security products and smart, simple, secure solutions that change how organizations approach endpoint security. BlackBerry Cylance provides full-spectrum predictive threat prevention and visibility across the enterprise to combat the most notorious and advanced cybersecurity attacks, fortifying endpoints to promote security hygiene in the security operations center, throughout global networks, and even on employees’ home networks. With AI-based malware prevention, threat hunting, automated detection and response, and expert security services, BlackBerry Cylance protects the endpoint without increasing staff workload or costs.

+1-844-CYLANCE
sales@cylance.com
www.cylance.com

MKTG 19-0423-20190725