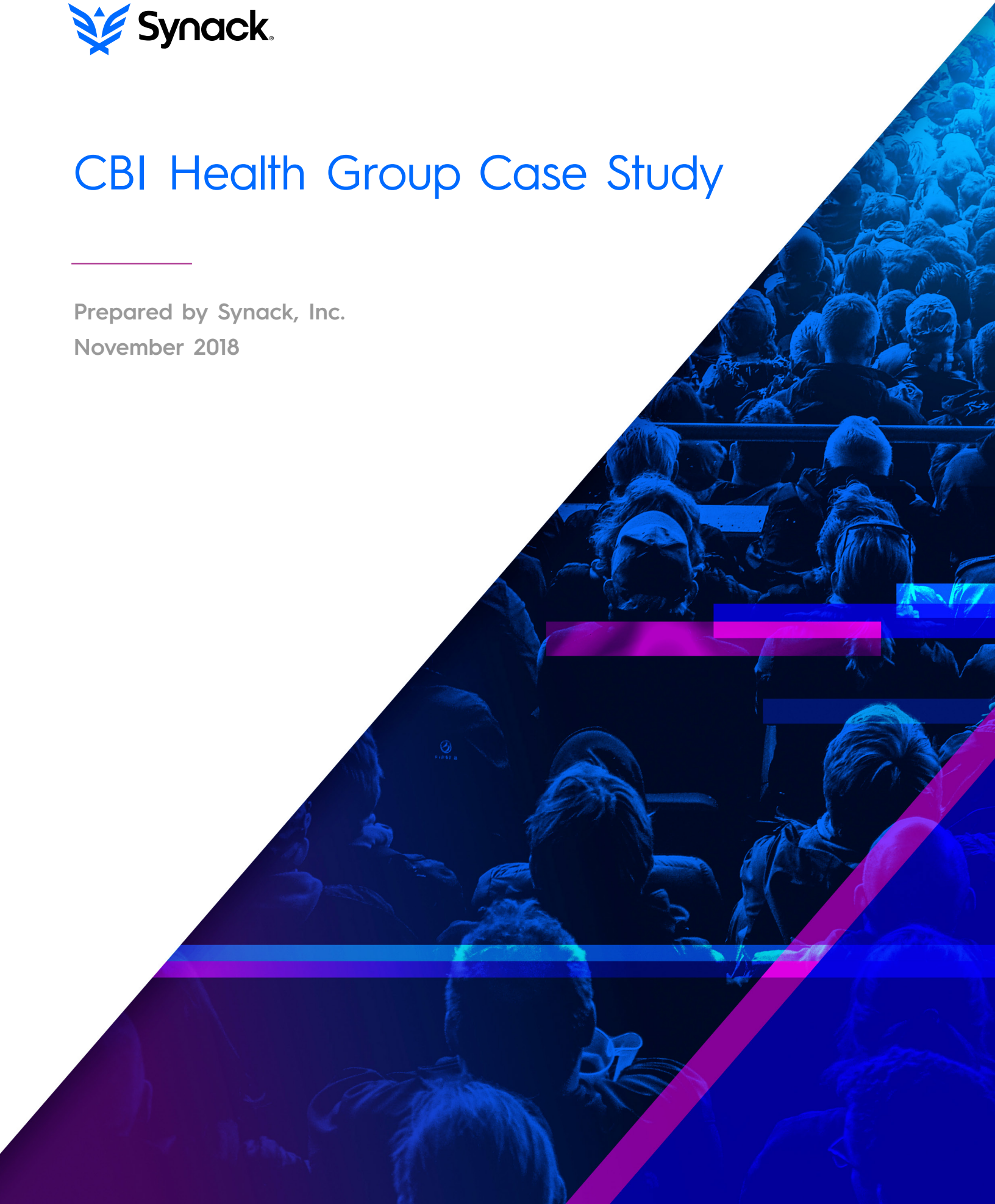
Synack

CBI Health Group Case Study

Prepared by Synack, Inc.
November 2018



Synack CBI Health Group Case Study

Healthcare Means "Data-Care" for Canada's Largest Community Healthcare Services Provider

Security is always top of mind at CBI Health Group, because they know that the world's most dangerous hackers (individual and state-sponsored) have made the healthcare sector their top priority. According to ID Theft Center, 23% of all breaches occurred in the medical/healthcare sectors in 2018.[1]

About CBI Health Group:

CBI Health Group is the largest provider of community healthcare services in Canada. They strive to continually develop new ways of coordinating and delivering care in order to improve access to services and healthcare outcomes.

"Healthcare is under siege and the barrage of attacks is never-ending. The healthcare industry is perceived as being particularly vulnerable, and organizations who have IT on premises (like CBI), are seen as much easier targets," says Cameron Chojnacki, Director, National I.T. Operations, Information Technology, CBI Health Group, Toronto. "We hired Synack to enable our security transformation because as good as we are, no one is perfect, and every organization needs outside expertise. Our goal was to get an adversarial perspective."

Of course, CBI wants its healthcare professionals—such as nurses and clinicians—focused exclusively on their patients and the clinical outcomes, while recognizing strong passwords and ransomware detection are typically the last thing on patients' minds. As a result, CBI must be hyper-vigilant and protective because the majority of its employees and patients are not, and never will be, cybersecurity experts.

"A further security transformation was in order because a breach would be catastrophic and detrimental to our business affecting everything from our patients' and employees' trust in us to our finances and daily operations," says Chojnacki. "We could be subject not only to fines ranging from the hundreds of thousands to millions of dollars, but it could also jeopardize our government contracts and relationships, hurting Canadians' health even further."

Fortunately, CBI was well into its contract with Synack when a fellow Canadian healthcare provider suffered a significant data breach of healthcare information. As a result of that breach, and likely others, the Office of the Privacy Commissioner of Canada instigated a nationwide call with a large group of Canadian healthcare providers just a few months before launching its inaugural breach-reporting law in November 2018.

CBI reported on Synack's penetration and missions testing, each of which was proving effective and efficient, as well as the results being achieved to further transform its security. For example, Synack's elastic platform scales the security team's efforts, while Hydra scanning helps researchers automate and accelerate repeatable tasks.

> "If we take our foot off the gas for even a moment, our patients' and employees' private, personal information could be compromised. Synack's perpetual testing ensures CBI Health Group's employee and patient data is secure."
>
> —Cameron Chojnacki, Director IT Operations, CBI Health Group

[1] https://www.idtheftcenter.org/wp-content/uploads/2018/09/2018-August-Monthly-Category-Summary.pdf

"On that call, CBI was able to directly and publicly address our proactive, leading-edge security strategies with Synack with the government office that funds, governs and monitors companies like ours," says Chojnacki. "Our partnership with Synack further enhanced the perception of CBI as a true leader when it comes to leveraging innovation and technology to further transform our security and protect our network."

By the Numbers:

Vulnerabilities Found: 37

% High/Severe: 62%

Reports Filtered Out by Synack: 45

Researcher Hours: 918

Most Common Category: Authentication

CBI has no interest in adopting innovative technologies just for the sake of being bleeding edge. CBI's goal is just to efficiently protect our customers and our business and appreciates Synack's truly leading-edge security which provides comparable benefits with the control, efficiency and reduced workload that are typically lacking with pioneering strategies. Synack's forward-looking security strategies keep CBI more than one step ahead of the rest without the generally-accepted disruption and chaos. In Chojnacki's eyes, Synack is known for thinking well outside the box when addressing the many ways a network could be penetrated.

"Synack offers a new, very sophisticated paradigm in penetration testing and really leverages the many benefits of crowdsourcing," says Chojnacki.

Synack achieves compliance and security through a combination of structured (checklist-based) and unstructured (mimics a real attack) testing. Its dynamic, incentive-based model, which includes bounties and other compensation, rewards white-hat hackers only for the vulnerabilities found to maximize motivation.

CBI Group recognized and appreciated Synack's highly strategic approach to security and wanted to leverage its strong methodology and absolute dedication to protecting the very clients it has been hired to hack.

As the customer, CBI decides what, where, when and how to test and has access to a Synack-supplied audit trail and technical controls for all testing activity. Synack's coverage analytics also let CBI know which assets have been tested and how rigorously which eliminates false negatives. As importantly, of course, CBI ultimately owns all of the findings.

"We knew we were secure because Synack really controls the test environment and doesn't just throw its clients into a Wild West scenario," says Chojnacki.

For example, Synack's unique approach to bug bounty services doesn't just provide hacking, it provides information about successful hacking. CBI used Synack's LaunchPoint, a secure VPN gateway and analysis tool, to which all Synack Red Team researchers must connect while testing client assets. This provided additional protection for CBI and its customers.

"Synack really thought through the many potential risks that could be associated with a bug bounty service and addressed them very proactively," says Chojnacki.

As importantly, CBI Group, which hires only suppliers it considers partners, soon saw that every action Synack takes is designed to support and entrench long-term relationships. At every point, Synack demonstrated its deep commitment to a mutually beneficial relationship because that's what drives long-term partnerships.

"Everything Synack did showed us the extent to which Synack is on our side and wants to help us protect our organization—it's about doing what's right for our patients and employees. Not selling us a Synack service," says Chojnacki.

In that spirit, CBI and Synack have built a highly productive, collaborative and results-oriented partnership that has uncovered incredibly complex, deeply buried vulnerabilities that CBI's ordinary software tools and methods did not detect. Ultimately, they were unique findings that were beyond the scope of traditional penetration tests and well outside what could be expected of CBI's internal teams and the traditional, widely-accepted automated scans.

CBI's Highlights

Protecting PII through Partnership

- An innovative, outside-the-box model keeps CBI more than one step ahead of the adversaries without the generally-accepted disruption and chaos.

Efficiency through the Platform

- The Synack Red Team augmented their efforts without unnecessary operational burden.
- All submitted vulnerabilities were reproduced, validated, and prioritized by Synack to remove noise from their workstream

Control

- Full visibility into all crowdsourced testing activity.

Not surprisingly, CBI's core infrastructure team initially got a little defensive, but that changed the moment they saw what Synack's team discovered and as importantly, how they'd found it. Synack's results certainly created buzz and Chojnacki's team constantly asked: "What else did they find? Did they catch anything new?" Working with Synack certainly recharged and reinvigorated the CBI team's always-fierce dedication to protecting its network and systems and subsequently, its patients' and employees' most personal, private information.

"The entire team got really curious and was very engaged by the cool stuff Synack was finding," says Chojnacki.

CBI immediately acted on 90% of the Synack-provided remediation recommendations for the various vulnerabilities identified (the remaining 10% had existing compensating controls). Better yet, Synack's Patch Verification ensures that when CBI patches it, the Synack hacker who originally found the vulnerability double-checks the patch. If the hacker can't breach the patch, they report its success and confirm true remediation has been achieved.

"Synack tells us exactly how to address the vulnerabilities and simplifies the actions we take," says Chojnacki. "Figuring out the fixes ourselves would take far too much time, so the remediation recommendations and Synack validating the fix for us is quite exceptional and something we really value."

Fully aware of the fact CBI Health Group will always be the target of everyone from the script kiddie messing around on a computer in a basement somewhere to a state-sponsored attack, CBI has contracted Synack to perpetually test its network.

"If we take our foot off the gas for even a moment, our patients' and employees' private, personal information could be compromised," says Chojnacki, who appreciates the relationships he and his team have developed with Synack, whether they're face-to-face in Toronto or online. "Synack's perpetual testing ensures CBI Health Group's employee and patient data is secure."

The Synack team reacted and responded very positively when Chojnacki pushed hard, and persistently, for the immediate validation of certain internal findings, and ultimately provided a very outcome-oriented, quickly-delivered solution.

When security is top of mind, time is of the essence and ASAP is the mantra, because in Chojnacki's own words, "If you've just started, you're already behind."

Synack, Inc.

855.796.2251 | www.synack.com | info@synack.com