



St. Joseph's Healthcare Hamilton Secures Critical Applications With AI-Powered Cloud Security



INDUSTRY

Healthcare

HEADQUARTERS

Hamilton, Ontario, Canada

COMPANY SIZE

8,000 employees

OVERVIEW

In 1852, the Sisters of St. Joseph's began their work at the docks in Hamilton, Ontario, Canada, treating the victims of a cholera epidemic. Today, the mission continues its service through the physicians, staff, researchers, learners, donors and volunteers of St. Joseph's Health System (SJHS). Since its founding, SJHS has expanded its presence across southern Ontario, with over eight thousand staff serving more than two million people. St Joseph's Healthcare Hamilton (SJHH) is one of SJHS's eight care centers located in the region.

OUR SOLUTION



CloudGuard WAF is a largely set-and-forget solution. It has given us real peace of mind to know our web applications are protected 24/7 with minimal effort.

Shawn Fletcher, Senior Enterprise Architect, St. Joseph's Healthcare Hamilton



CHALLENGE

As a healthcare organization, protecting organizational processes and patient data is a primary concern. Amidst increasingly sophisticated and disruptive cyber attacks, the responsibility of investing in the right security strategies and tools lies with Scott Lowell, chief technology and information security officer; Shawn Fletcher, senior enterprise architect; and their security team.

"We've seen nearby hospitals suffer from cyber attacks, resulting in cancelled surgeries and delayed critical patient care," said Lowell. For a hospital handling life-and-death situations daily, compromising on security is out of the question. "Preventing nightmare scenarios and protecting our patients is our highest priority, and that requires that we make smart cyber security decisions," he said.

Like other healthcare institutions in Canada and abroad, SJHH has transitioned to a hybrid, digital-first environment. Publicly facing websites facilitating an array of patient services are hosted on premises. To manage clinical information and perform administrative functions, the hospital relies on an electronic health record (EHR) software platform that offers applications and online portals for patients and physicians. Because sensitive medical data can be accessed from outside care centers and satellite offices, securing SJHH's digital environment is critical.

SOLUTION

While rolling out their EHR system, SJHH discovered Check Point CloudGuard WAF, an AI-powered cloud-native application security solution, and an integral part of the CloudGuard CNAPP platform. "We found the right product at the right time to secure our primary hospital information system, electronic medical records and expanded patient functionality via patient and physician portals," said Lowell. "It's no secret that healthcare institutions have become prime targets for cybercriminals, as medical data can be more valuable on the Dark Web."

With CloudGuard WAF's hands-off management capabilities, SJHH has struck the perfect balance between security and performance. "We were one of CloudGuard WAF's first customers, and we have no regrets," said Fletcher. "The timing was great for us, as Check Point offered it in an early release program. CloudGuard WAF is extremely transparent, and it has been providing us with excellent app security for four years."

SJHH evaluated other solutions, many of which involved complicated manual processes. Conversely, CloudGuard WAF was fast and easy to deploy. "CloudGuard WAF is largely a set-and-forget solution," said Fletcher. "It has given us real peace of mind to know our web applications are protected 24/7 with minimal effort."

With CloudGuard WAF, the team quickly onboards hosted websites in learning mode to establish a baseline before engaging prevent mode, which leverages contextual AI and machine learning to defend against website defacing, information leakage, digital theft, user session hijacking and other attacks. By differentiating normal and malicious traffic, the solution reduces false positives and eliminates the need for manual fine-tuning of rules when updating a web application or API.

"When the Log4j vulnerability was exposed across the industry, we immediately saw that it was detected and blocked by CloudGuard WAF," said Fletcher. "We were not impacted at all, and to date, we have not seen a breach or exposure with CloudGuard WAF in place." The solution allows his team to easily manage URL inspection on a granular level, investigate logs and send log data to their security information and event management (SIEM) tool to correlate data with other logs. "We can visibly see what's being stopped by this product and customize it to our specific needs in terms of policy and protections."

OUTCOME

Today, SJHH's security team has reached a new level of comfort knowing their critical web-application traffic is monitored and protected. Being able to address website vulnerabilities and exposures, protect patient data and access a holistic view of the hospital's security posture gives the security team added confidence in its ability to ensure the availability of critical services and applications.

The security team continues to add new applications to CloudGuard WAF to support the organization's secure growth. Thanks to the solution's AI-powered capabilities and hands-off maintenance, the team can focus its efforts on high-value tasks. And with minimal overhead impact on users, employees can perform their job functions more effectively, further maximizing the hospital's cybersecurity investment.

ABOUT CHECK POINT

Check Point Software Technologies Ltd. (www.checkpoint.com) is a leading AI-powered, cloud-delivered cyber security platform provider protecting over 100,000 organizations worldwide. Check Point leverages the power of AI everywhere to enhance cyber security efficiency and accuracy through its Infinity Platform, with industry-leading catch rates enabling proactive threat anticipation and smarter, faster response times. The comprehensive platform includes cloud-delivered technologies consisting of Check Point Harmony to secure the workspace, Check Point CloudGuard to secure the cloud, Check Point Quantum to secure the network, and Check Point Infinity Core Services for collaborative security operations and services.

[LEARN MORE](#)

Worldwide Headquarters

5 Shlomo Kaplan Street, Tel Aviv 6789159, Israel | Tel: +972-3-753-4599

U.S. Headquarters

100 Oracle Parkway, Suite 800, Redwood City, CA 94065

www.checkpoint.com

