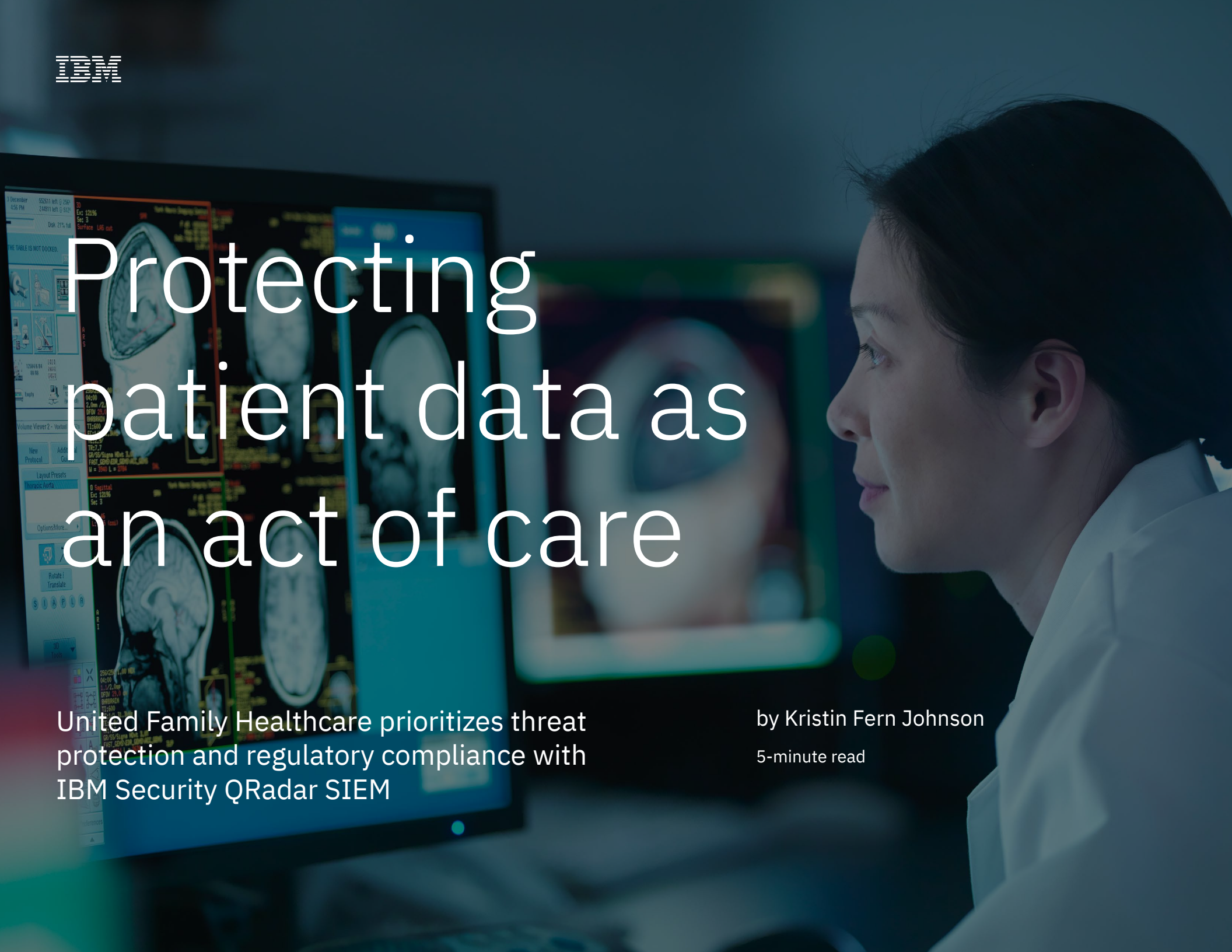


Protecting patient data as an act of care

United Family Healthcare prioritizes threat protection and regulatory compliance with IBM Security QRadar SIEM

by Kristin Fern Johnson

5-minute read

Patients are always top of mind at United Family Healthcare (UFH). In fact, patient-centered care is a core piece of the company's mission: to operate at international standards, pursue excellence in medical healthcare, provide patient services with warmth and care, put people first, tend to community residents, strive for continuous improvement and advance developments.

UFH has a unique approach to applying that care, melding Eastern and Western medical models. The company has grown significantly since it was founded in 1997 in Beijing, China. It now operates more than 10 hospitals in seven cities across China and beyond, staffed by more than 700 doctors, 1,000 experts and 1,500 medical assistants.

Such a large enterprise generates massive amounts of data across UFH's distributed IT environment. That data, and the IT infrastructure behind it, is expected to grow exponentially in the coming years as the company pursues its vision of becoming the leading healthcare provider in Asia.

In 2020, UFH began evaluating its security infrastructure to better protect its data and applications, adhere to compliance regulations and prepare for the coming growth. External threats,

such as spear phishing, malware-backdoors and malware-ransomware, as well as internal security vulnerabilities among the company's 5,000-plus employees, were a concern. Personal computers, social platforms and smart phones created possible exposures, as did password and information sharing among employees.

At the time, the company didn't possess a unified security operations center (SOC) platform. With no centralized view, it was difficult to detect risks or possible breaches or to manage them when they occurred.

UFH needed an SOC platform from which to clearly view and manage security incidents across its many sites and to generate reports that demonstrated compliance with local regulations. In addition, the platform needed to be easy to install, update and use, so the IT staff could manage it without in-depth training.

Can detect, contain and respond to a ransomware attack in

30

minutes, which previously took days

Can complete event processing, sourcing and reporting in

1

day, which used to sometimes take weeks

A unified view of security management

In choosing a solution, UFH conducted proofs of concept (POCs) with security offerings from several top vendors. IBM's security solution, highlighted by IBM Security® QRadar® SIEM, stood out, not only for its capabilities, but for its ease of use.

"We found outstanding strength in IBM's solution over competing products in the testing stage," says Chu Chun Peng, Medical Information Security Manager at UFH. "Specifically, with IBM's solution, we discovered plain-text usernames and passwords in the system, as well as such non-compliant behaviors as sharing accounts among employees."

Support services for the solution were a must. “We don’t have a large number of security operations and maintenance personnel, and IBM’s value-added services can make up for that,” says Peng. “This is a differentiation from other security vendors, some of whom cannot make the software work optimally because they sell products, but do not provide support and services.”

With IBM Security QRadar SIEM, UFH team members with limited formal security training can view prioritized threats and engage in level-one investigations of them. Centralized log management helps UFH manage compliance with local regulatory requirements using automated reporting capabilities that enable internal and external audit report generation at a moment’s notice.

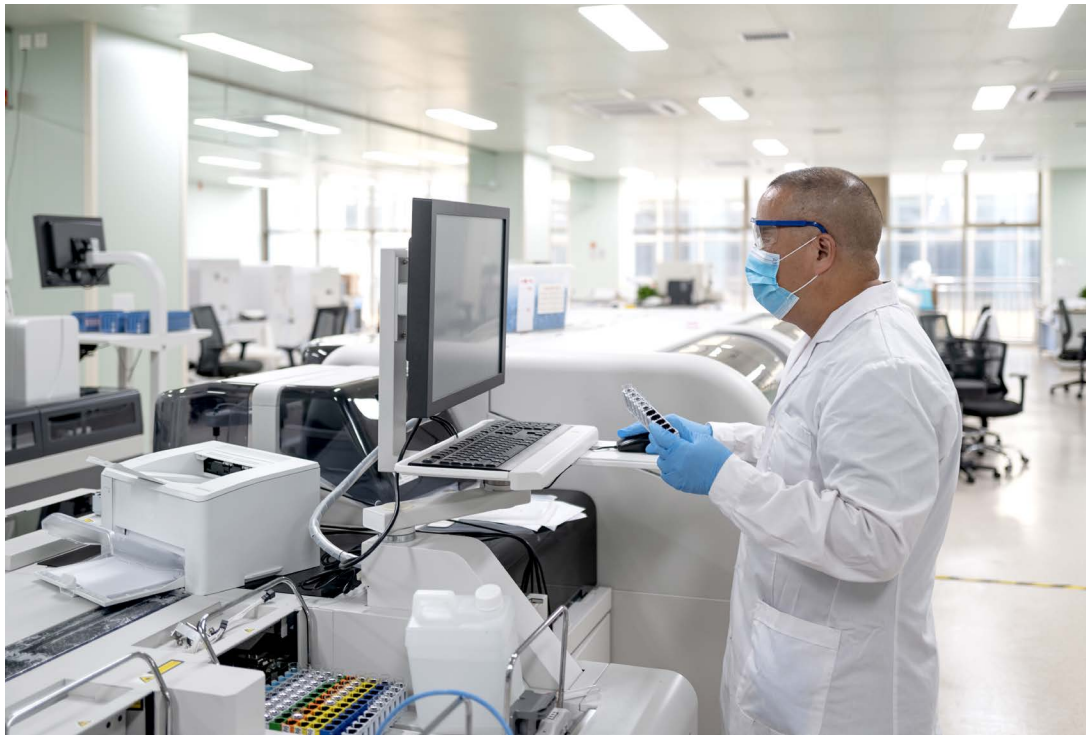
“Many of the preset built-in rules of QRadar are very comprehensive and can detect more risks, such as strong log management and traffic collection capabilities, high compatibility with log sources and ease in making direct correlation analysis,” says Peng. “Overall, it is efficient, time-saving and labor-saving.”

Taking advantage of those out-of-the-box capabilities for integration and analysis, UFH deployed the SOC solution in less than one month. To identify potential high-risk user behaviors and activities, UFH implemented IBM Security QRadar User Behavior Analytics, a machine-learning add-on application that determines baseline user and peer group behavior to detect suspicious anomalies and send alerts on potential insider threats or compromised hosts. Another add-on, IBM Security QRadar Network Insights, analyzes network traffic to monitor sensitive patient data flow and provides real-time alerts.

A core piece of IBM security technology, IBM Cloud Pak® for Security, is in the process of being implemented and is expected to go into full production in 2023. The unified security management platform integrates with IBM Security QRadar SIEM to bolster security incident detection, investigation and response.

Envisioning future growth

Upon initial implementation in 2020, the new SOC's value quickly became clear. "After the system went online, the results were remarkable," says Peng. "The dashboard made the security management of the entire enterprise visible, so management could view our system's operation status at any time, which was greatly appreciated by our CxOs." The centralized view provides administrators an understanding of the overall security posture in minutes rather than months.



The impact has been positive internally, as well. "Over the past two years, we have seen alarms and risks decrease year by year," says Peng. "Thanks to visible safety management, the department can now discover employees' risky behaviors in a timely way and immediately issue reminders, improving employees' safety awareness and reducing possible risks." Customers are also experiencing the benefits. Not only is their sensitive information protected, but also their sense of security is enhanced.

The effectiveness of the solution has been borne out through testing. “In an emergency drill, ransomware was found on our terminal equipment and an alarm appeared immediately,” says Peng. “Our management personnel disconnected the network at once, controlling the impact of the risk point within 30 minutes. Such action could take a few days or more in the past. In addition, we can complete event processing, sourcing and reporting in a day, which used to take weeks.”

Today, the IBM Security QRadar SIEM solution is running in UFH hospitals and clinics in seven cities and 11 locations throughout China. Further enhancements are in the works. “In the short term, we plan to expand the capacity of QRadar and deploy IBM Cloud Pak for Security into production systems,” says Peng. “In the long run, we strive for a security ecosystem within UFH and continuous cooperation with IBM Security ReaQta endpoint detection and response solution, as well as data privacy solutions from IBM Security Guardium.”

Mutual trust is at the heart of the relationship between IBM and UFH. “This collaboration has created many unforgettable moments, from the POC at the beginning to emergency drills—which have always worked better than expected,” Peng concludes. “IBM continuously works with UFH to build a security system that provides better protection for our customers.”

“After the system went online, the results were remarkable. The dashboard made the security management of the entire enterprise visible, so UFH management could view our system’s operation status at any time, which was highly valued by our CxOs.”

Chu Chun Peng, Medical Information Security Manager at United Family Healthcare

United Family Healthcare (UFH)

UFH (link resides outside of ibm.com) is an international hospital and clinic network headquartered in Beijing, China. Integrating medical models of the East and the West, the company focuses on providing high-quality, patient-centered medical services. It has hospitals and clinics in Beijing, Shanghai, Guangzhou, Shenzhen, Tianjin, Qingdao and Boao, and employs over 700 doctors, 1,000 medical experts and 1,500 trained nurses.

Solution components

- IBM Cloud Pak® for Security
- IBM Security® QRadar® SIEM