cloudcover®

Safeguarding Network Security and Prioritizing Data Privacy in the Healthcare Industry

A multi-campus hospital system protects its patient records against phishing and other cyberattacks with the help of CloudCover's CyberSafety CC/B1 Platform™

Prevalence of tech and lack of funding contribute to cybersecurity challenges for hospitals and healthcare systems

Cyberthreats are a growing issue for hospitals and healthcare systems. According to the Healthcare Information and Management Systems Society (HIMSS) 2020 Health Security Survey, 70% of healthcare organizations say they had a significant network security event in 2020, with an additional 57% reporting being the target of a phishing attack (Landi, 2020).

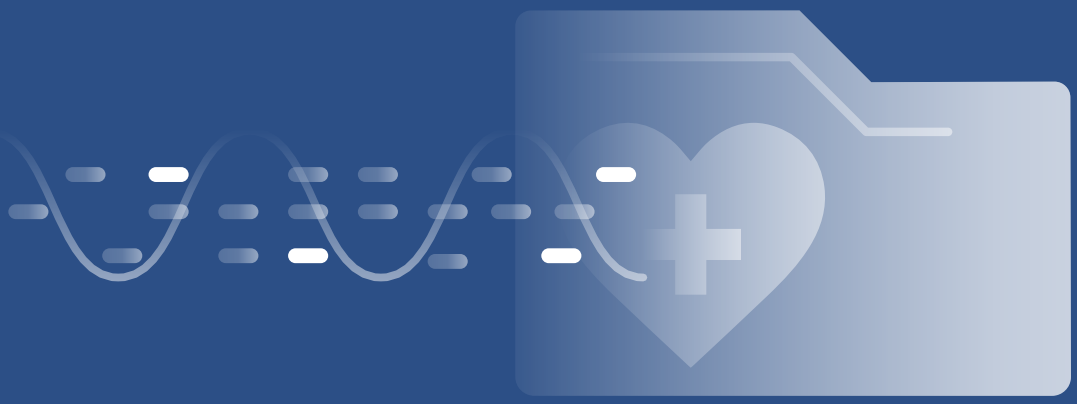
Healthcare entities are especially vulnerable to cyberattacks because of the sheer volume of information they possess — information that's of high monetary and intelligence value. This data usually includes a patient's protected health information, financial information — credit cards and bank account numbers — and other personally identifiable information. Stolen health records are worth up to 10 times that of stolen credit cards on the dark web — and they can cost more to contain. One stolen health record can cost $408 — compared with a non-health record's price tag of $148 (Riggi).

In addition to this incredible amount of high-value data, there's a complexity to healthcare organizations that can make data security challenging:

- **Patient care:** Similar to other industries, hospitals are technologically saturated environments that struggle to manage the devices, software, and platforms needed for patient care, including BYOD (bring your own devices) and medical devices that aren't regulated by an IT administration network.
- **Legacy systems:** Those environments often rely on legacy systems — Windows 7, Windows XP, and Windows Server 2008 — that are no longer supported by manufacturers (Landi, 2020).
- **Resource availability:** There's uncertainty when it comes to resource availability, both with budget for cybersecurity initiatives and available IT talent. According to the HIMSS 2020 Health Security Survey, only 6% of an organization's budget is dedicated to cybersecurity (Landi, 2020).
- **Specializations:** Individual departments and specializations mean a variety of workflows and functions.
- **Compliance:** Healthcare entities also have strict compliance requirements in place due to the sensitive nature of patient data.

The loss of data is staggering on its own, and there are other repercussions in terms of:

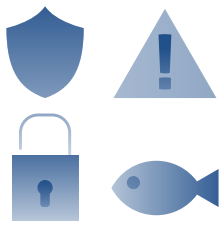
- **Cost:** Hospital network security breaches have the potential to cost a single hospital as much $7 million in fines, litigation, and reputation damage (Jalali and Kaiser, 2018).
- **Patient care:** Compromised medical records may mean disruptions in care, including access to lifesaving medical devices. This is especially true if cyberattackers intentionally, or unintentionally, alter a patient's records.



The challenge

Multi-campus healthcare system searches for proactive solution to network security breaches

Even with new, more sophisticated cyberthreats emerging, healthcare organizations tend to get hit with the most common ones, including:



- **Malware and ransomware:** Cyberattackers use these to shut down individual devices, servers, or entire networks.
- **Cloud threats:** While there are many benefits to cloud computing, the platforms are typically less secure and not properly encrypted, making them a ripe target for hackers.
- **Phishing attacks:** Emails being sent out from sources that seem reputable in an effort to obtain personally identifiable information.
- **Misleading websites:** Cyberattackers will duplicate a website to look identical to a reputable site, making a simple change to a web address that a user wouldn't catch.
- **Employee error:** Weak passwords, unencrypted devices, and other failures of compliance can all lead to data breaches ("Cybersecurity, How Can It Be Improved In Healthcare?", 2020).

These repercussions — specifically data privacy concerns about endpoint solutions and zero-day protection with ransomware attacks-prompted a medium-sized hospital system to begin a partnership with CloudCover® for its cybersecurity needs. The entity had satellite clinics and nursing facilities dispersed through five campus environments, and the lack of holistic network security was making the IT department uneasy.

The solution

CloudCover's CC/B1 B100 Platform — configured with an eye toward ransomware and phishing attacks

After performing an audit of the system's existing network security, CloudCover knew its CC/B1 Model B100 H/A would be the right fit. The CC/B1 Platform functions as an advanced AI-based security operation center (SOC), collecting and analyzing an organization's data with patented SOAR (security orchestration, automation, and response) technology. This real-time learning creates an automated N-SOC (no security operation center) that safeguards data without the need for human intervention.

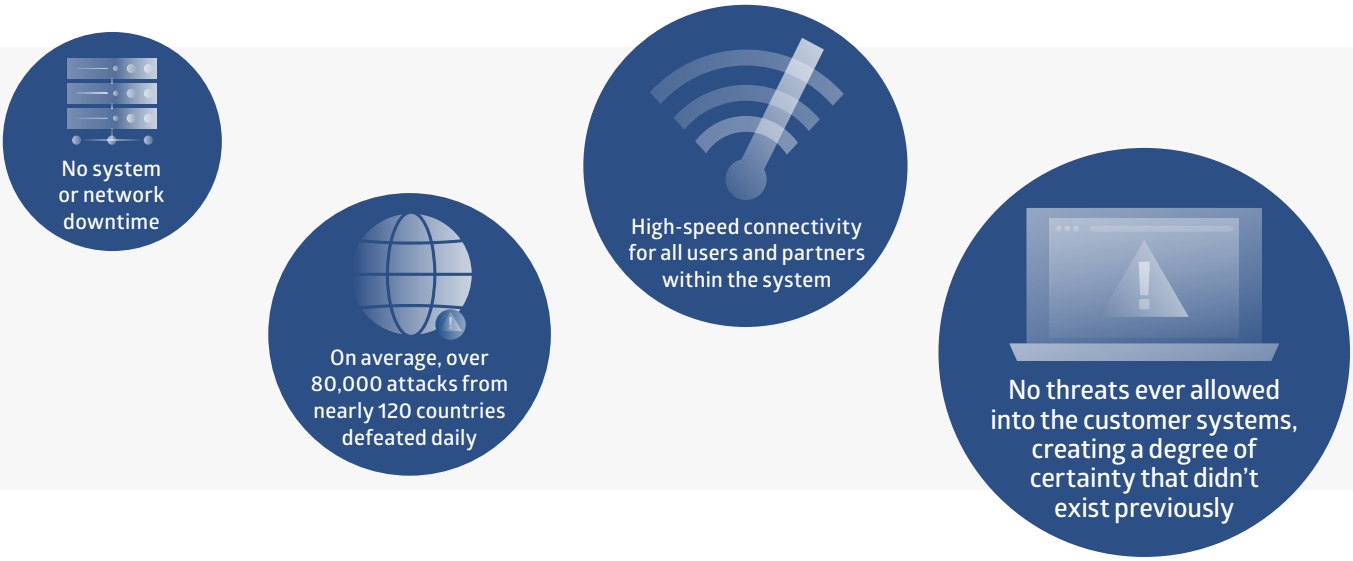
The B100 series is the high-speed, high-demand network solution for reliability, adaptability, and redundancy — ideal for data-intensive organizations such as healthcare entities who are looking to protect their data privacy. The series is also designed for heavy networking, including cloud and telecom carrier use. CloudCover installed and configured CC/B1 Model B100 H/A with these capabilities:

- B1/OS AI-based AWARE/stateful firewall, which includes a deep set of algorithms and over 35,000 sensors to utilize over 54 million risk attributes — making it easy to detect, identify, analyze, and react to cyberthreats in microseconds, with near-perfect accuracy
- Router/network protection
- Multiple internet service providers (ISPs) for redundancy and throughput
- Virtual local area network (VLAN) support
- 120GbS fully inspected network throughput
- .000012 mS network latency in all cases
- Request for comments (RFC) protocol awareness
- Secure sockets layer (SSL)/virtual private network (VPN) configuration to create an easy and secure way for individuals to communicate safely with the hospital's networking regardless of where their connection originates
- Multi-factor authentication to Active Directory and Lightweight Directory Access Protocol
- Anti-virus/anti-spam protection to detect and stop malicious traffic, never-before-seen events, and unsolicited and illegal email messages
- Web content filtering that goes beyond traditional platforms by identifying and inspecting URL sites against CloudCover's database of over 40 million known websites and allowing or blocking user access
- Connections via IPSEC tunnels to 1,024 partner locations
- Dynamic reporting

The results

Network security solved — for five years running

Five years into their implementation of CloudCover's CC/B1 Platform, the hospital is in control of their cybersecurity strategy, reporting:



Mitigate cyberattacks at your hospital system or healthcare organization by taking a look at CloudCover's CyberSafety CC/B1 Platform™ — check it out for yourself or contact us directly to learn more.

References

Jalali, Mohammad S, MsC, PhD and Kaiser, Jessica P, MBA (2018). "Cybersecurity in Hospitals: A Systematic, Organizational Perspective." US National Library of Medicine, National Institutes of Health. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5996174/

Landi, Heather (2020). "Could patients be at risk during a hospital cyberattack? It depends how far hackers are willing to go, expert says." Fierce Healthcare. https://www.fiercehealthcare.com/tech/could-patients-be-at-risk-during-a-hospital-cyber-attack-it-depends-how-far-hackers-are

Riggi, John. "The importance of cybersecurity in protecting patient safety." AHA Center for Health Innovation. https://www.aha.org/center/cybersecurity-and-risk-advisory-services/importance-cybersecurity-protecting-patient-safety

University of Illinois-Chicago (2020). "Cybersecurity: How Can It Be Improved in Health Care?" https://healthinformatics.uic.edu/blog/cybersecurity-how-can-it-be-improved-in-health-care/

