Powerful Cloud Security for Top Tier Cloud-Based Care

Powerful Cloud Security for Top Tier Cloud-Based Care

Introduction

The drive to migrate workloads to the cloud has gained momentum in recent years, and shows no sign of slowing down. In 2018, the global healthcare cloud computing market topped $7 billion, and is projected to reach $55 billion by 2025 .

The benefits of cloud-based storage for healthcare organizations are numerous, offering a suite of capabilities that organizations can hardly refuse. However, despite the fact that cloud computing offers across-the-board advantages, vicious cyberattacks routinely threaten to destroy its utility. The top security issues jeopardizing healthcare organizations include the lack of role-based-access control, inadequate malware prevention, and insufficient encryption. In this brief, we'll discuss the insidious nature of these cloud security threats, and present effective mitigation strategies.

> In 2018, the global healthcare cloud computing market topped $7 billion, and is projected to reach $55 billion by 2025.[1]

[1] "5 Things Made Possible in Healthcare Thanks to the Cloud," HealthTech, Andrew Steger, September 12th, 2019.

The rationale behind cloud adoption in healthcare are multifold.

1. **The scalability and flexibility of cloud systems holds wide appeal.** Scalability and flexibility enable healthcare organizations to easily partner with third-party groups or other healthcare or hospital facilities in order to better serve clients. In addition, as organizational needs expand or shrink, the cloud can accommodate fluctuating demands for service.

2. **You only pay for what you need.** Amidst continual healthcare spending and budget cuts, capital-intensive investments aren't in vogue. The pay-for-what-you-need cost structure enables organizations to allocate resources more effectively than ever before.

3. **Artificial Intelligence (AI) and Machine Learning (ML) improve workforce management strategies.** Since patient data requires extensive management, another profound advantage to cloud computing is the ability to use AI and ML to organize records. With cloud services, organizations can pull information from prescriptions, notes, audio and radiology reports, and add information to patient files. This significantly reduces the administrative workload, allowing healthcare organizations to make better use of employees' time. However, despite the obvious benefits, storing healthcare data in the cloud is also an operational risk.

Powerful Cloud Security: Role-Based-Access Control

Another notable reason that accounts for why cloud computing appeals to hospitals is the convenience of cloud-based Electronic Health Record (EHR) systems. When hospital physicians, nurses and technicians can quickly exchange patient information through a connected EHR system, they can provide faster-paced, higher quality patient care. At the same time, these systems are at risk. In a global industry survey, nearly 70% of respondents reported that unauthorized access represented their main cloud security concern.[2]

Employing a role-based-access-control system can help safeguard the integrity of patient data. Dynamic access leases can provide temporary privileges to those who require them in the short-term, while permissions can also be configured to permit long-term access. This avoids the danger of giving widespread admin access to highly sensitive environments. Regional data locks serve as an added safeguard, ensuring that cyber criminals cannot move data beyond certain regional or national borders.

---

[2] "Few Hospitals Have Experienced Healthcare Cloud Security Incident," HIT Infrastructure, Fred Donovan, May 30th, 2019

Malware

In 2017, healthcare providers represented a top target for malware threats. WannaCry disrupted the UK's NHS system, NotPetya ravaged EHR transcription services worldwide, and Locky upended outdated hospital operating systems.[3] In 2019, research indicates that malware continues to represent a major concern for healthcare and hospital systems.[4]

Prevent your cloud from serving as a point of entry for malware attacks. Once in the cloud, malware easily spreads and can take down an entire system.

WannaCry disrupted the UK's NHS system, NotPetya ravaged EHR transcription services worldwide, and Locky upended outdated hospital operating systems.[3]

Healthcare and hospital groups should invest in malware threat protection that stops incoming malicious files, identifies malicious malware signatures, prevents access to malware infested websites, and offers up-to-the-minute malware intelligence. For the best prevention and protection, ensure that you're able to view malware activities and trends on a consolidated dashboard.

Encryption

A Check Point Software cyber security survey reveals that 72% of cyber security professionals prioritize encryption when it comes to securing the cloud.[5] Encryption is a particularly relevant issue for healthcare and hospital systems, as data that's continually in motion is easy for hackers to intercept with Man-in-the-Middle attacks.

First, safeguard your data with full-disk and local file encryption. Then, choose a cloud service provider that offers encryption for data at rest and in-transit. While HIPAA does not mandate encryption, failure to take this basic security precaution can lead to stolen data and corresponding HIPAA fines.[6]

Get cloud security that can help enforce encryption and that can detect unencrypted cloud components. This offers an additional layer of security for optimal business data protection. Increased compliance measures means turning security breaches into a thing of the past.

While HIPAA does not mandate encryption, failure to take this basic security precaution can lead to stolen data and corresponding HIPAA fines.[6]

[3] "How the Worst Cyberattack in History Hit American Hospitals," Slate, Andy Greenberg, November 5th, 2019
[4] "Top Cloud Security Risks for Healthcare," InformationAge, Kayleigh Bateman, April 18th, 2018
[5] "Cloud Security: 2016 Survey," Check Point Software
[6] Why Encryption is Crucial to Your Organization," HealthcareITNews, Tim Maliyil, July 31, 2014

Protecting Against Top Threats

When it comes to scalability, increased cost-savings and better workforce management, cloud computing is an attractive choice. However, pernicious threats could make quick work of your cloud computing assets. At the present moment, cyber threats are surging due to cloud-based infrastructure transitions and new remote working configurations. Your organization is not immune. Taking steps to prevent the top cloud threats from toppling systems is essential. Invest in comprehensive cloud security with role-based-access-control, advanced malware protections, and strong encryption policy enforcement to secure your threat environment. Securing your cloud is synonymous with securing your business continuity and renewing your commitment to patient health.

Amidst the coronavirus pandemic, you've shown unwavering dedication to patients and their families. While it may come across as a lesser priority, ensure that infrastructure and data receive the same quality treatment as your patients.

Among healthcare and hospital systems, cyber attacks are increasing exponentially. "We're in the midst of the most urgent health crisis in modern history, and these attacks threaten all of humanity," stated Peter Maurer, president of the International Committee of the Red Cross. Protect your organization.[7]

For more information on securing your cloud architecture, read our cloud security white paper or reach out to your local Check Point representative.

[7] "Cyber Attacks Against Hospitals Must Stop, Says Red Cross," ZDNet, Danny Palmer, May 26, 2020

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com
U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233
www.checkpoint.com