Where securing data means saving lives

The growing need for effective cloud security in healthcare and HealthTech

LACEWORK

1. Introduction

There has been a revolution in healthcare and HealthTech. Digital transformation, a global pandemic, and an increased focus on global connectivity and rapid innovation have pushed more organizations to the cloud – and data security has never been more important.

In this industry, ransomware and other cyber attacks are on the rise, resulting in critical systems being compromised. This could mean unauthorized access to life-saving Protected Health Information (PHI) or, in some cases, having that data held hostage until a price is paid.

The stakes are high when it comes to handling health data. And achieving proper cloud security can seem overwhelming or out of reach. This eBook openly discusses the unique challenges facing healthcare and HealthTech organizations around maintaining a secure cloud infrastructure. But it also explores a data-driven, automated approach that can provide the visibility and insights needed to expand and maintain healthy and compliant security programs.

In this industry, ransomware and other cyber attacks are on the rise, resulting in critical systems being compromised.

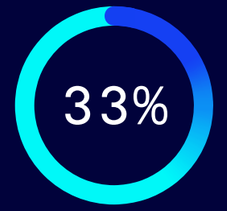
2. A pessimistic diagnosis

One would hope that healthcare would be exempt from cyberattacks, considering its life-saving work. However, sadly, that's not the case; in fact, it's quite the opposite. Because of the heightened stakes, healthcare organizations are increasingly becoming a primary focus for attackers. Ransomware and other healthcare-related data breaches hit an all-time high in 2021 with more than 45 million individuals affected[1].

At the same time, IT departments are severely short-staffed. There are currently over 400,000 open cybersecurity jobs in the U.S. alone[2]. Faced with limited resources, IT departments are forced to deprioritize standard security measures in favor of "fire drills" and often allow breaches to go undetected until it's too late.

Healthcare and HealthTech businesses of all sizes can be crippled by a cyber attack. The weight of penalties, fines, lawsuits, settlements, and loss of critical patient data can be devastating to the organization. Insecure cloud environments put an organization's reputation and revenue at risk — not to mention the lives of its patients.

Alarming 2021 trends



of third-party breaches targeted healthcare organizations[3]

million health records exposed as a result of ransomware attacks[4]

increase in hacking incidents at outpatient/ specialty clinics[5]

3. In search of the cure

With so much at stake, healthcare and HealthTech organizations must invest in modern cybersecurity tools. Traditional rules-based security products — tools which require manual programming to detect known threats — aren't capable of protecting the growing amount of unknown threats like zero-day exploits.

There were a record 80 zero-day exploits in 2021 — nearly triple the number from 2020[6]. Additionally, a rules-based approach creates lots of false positive "noise," drowning the alerts that indicate a true risk. This creates a sizable gap in your cloud security that attackers can exploit.

Short-staffed security teams simply don't have the time to configure, implement, and fine-tune rules. This approach requires teams to write new rules or edit existing rules, all while facing an unending queue of low priority (or outright false) security alerts — alerts created by those very same rules. It's a vicious cycle for healthcare and HealthTech security teams, who are already operating in an extremely high pressure and fast-paced environment.

Many healthcare providers are now shifting from a fully on-premise approach to technology and IT infrastructure to a hybrid or fully cloud-based approach. This cloud migration brings about increased risk and heightens the need for more security controls to maintain compliance.

Cloud-native HealthTech companies continue to build and expand their offerings and often find themselves struggling to meet strict compliance standards and limit their attack surfaces.

4. Prevention is the best medicine

Attacks on healthcare providers and HealthTech businesses are only increasing. At the same time, there are unprecedented talent gaps in cybersecurity. Traditional rules-based security approaches simply aren't sophisticated enough. Here, in an industry where data compromise could carry the highest cost, is it even possible to fully secure a cloud environment given these challenges?

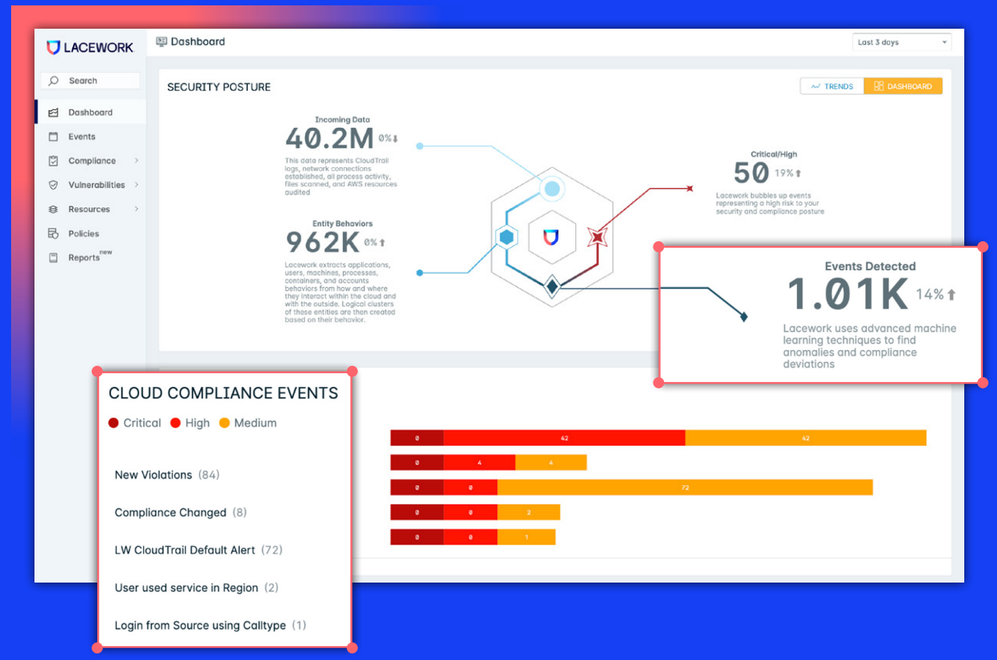
Prevention is key to maintaining good physical health. Likewise, proactive cloud security is the best way to ensure organizations are secure and compliant. With the fast pace of healthcare and HealthTech, nobody has time to manage multiple point security tools. These organizations need a modern security approach that uses their own data to their advantage. Through integration and automation, organizations can reach a new level of security and operational efficiency that scales up or down with their cloud environments.

Additionally, organizations that develop code can now empower developers to incorporate security throughout the entire software development cycle. By integrating security practices from ideation to deployment, businesses can ensure code is secure before it is shipped. This approach reduces the friction between security and development teams and results in a faster time to market, reduced downtime, and minimized exploitation risk.

With the fast pace of healthcare and HealthTech, nobody has time to manage multiple point security tools.

Did you know?

The top cause of ransomware is misconfiguration.



5. Treating the sickness, not the symptoms

The Lacework Polygraph® Data Platform utilizes automation to free up time and resources, allowing your security team to focus on only the biggest issues and your developers to build and launch secure code faster. Rather than retroactively plugging holes and fixing problems, Polygraph cures issues early, allowing teams to feel in control and not like they're always catching up from behind.

Machine learning turns millions of data points into meaningful alerts by providing context and reducing excess alert noise – without the manual effort of rule writing.

Our integrated platform allows you to:

- Understand your resources and how they are configured with resource scanning
- Have confidence you are meeting Health Insurance Portability and Accountability Act (HIPAA) guidelines and other industry best practices
- Reduce attack surface and identify risk across the software development lifecycle during build time with vulnerability management
- Avoid delays and identify risks at the source with Infrastructure as Code (IaC) scanning
- Access meaningful telemetry data on your workloads to monitor for early signs of trouble without the cost and hassle of querying SIEM logs with workload protection
- Fix the most meaningful issues quickly through context-rich alerts

6. A healthy security program that can grow with you

The Lacework Polygraph Data Platform empowers you to:

Understand your cloud

Know what's in use across cloud environments and make sense of the interactions between resources, services, and microservices

Gain expert-level security outcomes

Identify signs of trouble in your workloads and cloud accounts, including unknown zero-day threats, and share context across teams

Fix what matters

Prioritize risk and eliminate noise by focusing on actions that fix the biggest risks first, without relying on complex rule sets

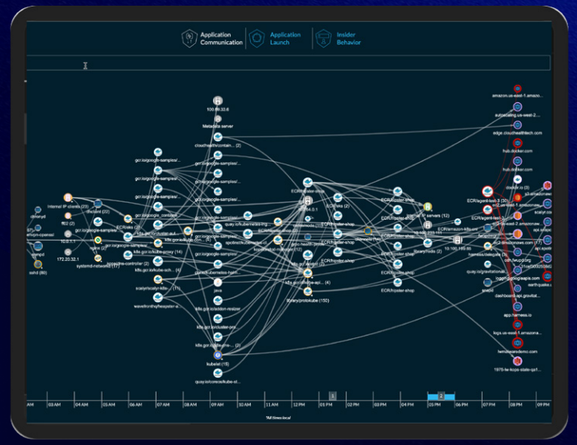
Prove compliance in a fraction of the time

Safeguard regulated healthcare data and achieve compliance with HIPAA, PCI, SOC 2, and other security standards

Lower total cost of ownership

Reduce licensing to labor costs and eliminate silos for streamlined communications that saves time and money

Public cloud platforms offer native tools for containers and orchestration, but they are not enough. These controls are dependent on sufficient runtime visibility into configuration compliance, real-time anomaly detection and alerting, and traceability.



Ready to chat?

Request a demo

Check your HIPAA compliance.

Watch a webinar

LACEWORK®

Lacework is the data-driven security company for the cloud that delivers end-to-end visibility and automated insight into risk across cloud environments. Trusted by enterprise customers worldwide to reduce risk, Lacework significantly drives down costs so you can securely innovate in the cloud with speed.

Sources

1. Heather Landi, Healthcare data breaches hit all-time high in 2021, impacting 45M people, Feb. 2022
2. Meghan McCarty Carino, As companies brace for cyberattacks from Russia, specialists are in short supply, March 2022
3. Security Magazine, 33% of third-party data breaches in 2021 targeted healthcare orgs, January 2022
4. Compliancy Group, 10 Largest 2021 Healthcare Breaches (so far), Dec. 2021
5. Jill McKeon, Cyberattacks Against Health Plans, Business Associates Increase, Jan. 2022
6. Jill McKeon, Zero-Day Exploits Reached All-Time High Last Year Report Finds, April 2022