SOLUTION BRIEF

LACEWORK.

Cloud security for health IT

Protecting your patients from cyberattacks and your health IT from compliance issues

From Mobile Health (mHealth), telehealth, health informatics, or eHealth, to hospitals and clinics, the growing influence of cloud networks is reshaping the IT landscape. According to recent data, over 325,000 mHealth apps are available for Apple and Android smartphones.

With the pandemic boosting an already booming acceptance of telemedicine and mHealth, the sector is quickly becoming overrun with the need to provide newer, easier, and faster ways to improve the level of care and access to key health data points such as blood sugar, pulse ox levels, blood pressure, temperature, and more.

According to the United Healthcare Consumer Sentiment Survey, over a quarter of Americans use mHealth apps as a primary source of health information.

Yet, when it comes to patient and health security, the battle lines are drawn. HIPAA section 164.402 defines a breach as the acquisition, access, use, or disclosure of protected health information in a manner not permitted, which compromises the security or privacy of the protected health information (PHI).

Processes and tools that worked well in traditional data centers do not translate easily to the cloud, exacerbating cyber vulnerabilities for healthcare systems in a way that can lead to the following HITECH infractions:

- A lack of safeguards of PHI
- An absence of administrative safeguards for electronic PHI
- Insider threats that potentially exfiltrate PHI data

> “Lacework Polygraph®, within minutes of the attack occurring, was able to detect something that the other solutions were not. It outperformed everything we’ve been doing.”
>
> MARIO DUARTE, VICE PRESIDENT OF SECURITY, SNOWFLAKE

From a HIPAA perspective, top compliance rules include:

- Administrative security measures such as regular risk analysis, appropriate security measures for risk management, sanctioned policies aimed at enforcing compliance, and regular review of log entries containing information about the actions performed
- Technical security measures around audit management such as the implementation of mechanisms for recording and researching any activity in a system that contains PHI, as well as authentication of a person or object that also includes developing ways for verifying the identity of those trying to access PHI. More importantly, this HIPAA mandate focuses on securing data in motion and detecting unauthorized PHI modifications during transmission and PHI encryption mechanisms

With 93% of cloud services in healthcare recently categorized as medium to high risk, keeping patient data along with hospital and clinician information safe is challenging without proper cloud security. The right cloud security platform is needed to streamline compliance and security, and eliminate the complexity found within healthcare. It should also help support healthcare in the following ways:

- Migrating legacy healthcare systems to cloud platforms
- Leveraging cloud-based analytics that enable real-time data analysis
- Enabling cloud computing web services and advanced development capabilities that can be applied to physicians, researchers, patients, and support staff
- Utilizing the advancements of automation, parallel computing, virtualization, and utility computing

Streamline healthcare compliance with total visibility

Whether you're working with a new or existing EMR/EHR system, or dealing with a wearable health tech company, the cloud is a focal point of all operations. But not all cloud security solutions are created equal. Lacework is a complete cloud security and compliance platform for your multicloud environments, workloads, containers, and Kubernetes. Not only does Lacework constantly monitor networks for anomalies, but our foundation, Polygraph®, delivers a deep temporal baseline built from collecting high-fidelity machine, process, and user interactions – over a period of time – to drive cloud compliance by:

- Being able to spot IaaS account misconfigurations and achieve compliance for HITECH, PCI DSS, HIPAA, and other cloud compliance and security measures
- Understanding application behaviors by identifying all your users, applications, services, containers, images, pods, etc.
- Creating robust cloud workload protection with deep visibility into all processes and applications within your container and cloud workload environments – all without any rule writing
- Producing total container security by identifying behavioral analysis on anomalous activities across your cloud and containerized environments
- Assessing your cloud security posture by ensuring passwords are complex and multi-factor authentication is enabled

Lacework automation and tooling helps healthcare organizations scale compliance efforts and reduce control failures. From clinics to hospital systems, Lacework helps IT security teams find critical controls that work effectively in their specific environments – like authentication and vulnerability management – and bolsters security policy alignment with healthcare objectives to reflect your specific infrastructure and services.

Boost patient safety with invaluable insights

Over 88% of healthcare organizations experienced a data breach in the past two years and the average healthcare organization uploads 6.8 TB of data to the cloud each month, with only 15.4% of healthcare organizations supporting advanced security capabilities like multi-factor authentication.

Lacework provides cloud and multicloud protection by automating cloud security and compliance across AWS, Azure, GCP, and private clouds while providing a comprehensive view of risks across cloud workload and containers. This security extends to your DevOps security teams, which are empowered by embedded security across the development lifecycle for build-time and runtime operations – enabling continuous security, automation, and the ability to build fast.

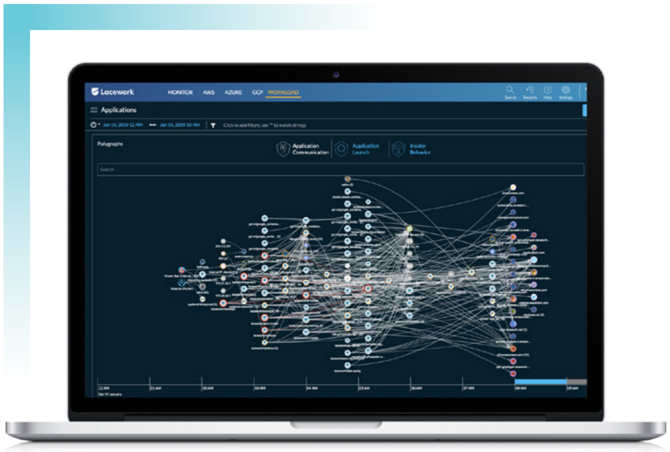
Lacework's approach uses automation and unsupervised machine learning. Security teams are able to deploy the Lacework agent across multiple cloud platforms, within application orchestration environments like Docker, Kubernetes, and even in hybrid workloads. Because they deploy the Lacework platform in a SaaS model, organizations can review historical event data across their infrastructure to understand where breaches have occurred and can identify risk areas. Lacework will:

- Always alert you on new activity so that you are given a chance to investigate any behavior within your environment that could potentially be malicious

- Alert you only when there are new or anomalous events, eliminating alert fatigue within your health IT groups

- Use automated workload detection, which saves time by removing the need to write and maintain error-prone rules, allowing you to focus on securing your patient information

Lacework provides cloud and multicloud protection by automating cloud security and compliance across AWS, Azure, GCP, and private clouds while providing a comprehensive view of risks across cloud workload and containers.



You can't secure what you can't see

The power of Polygraph®

Our foundation is based on the patented Polygraph technology, a context-rich baseline built from collecting high-fidelity machine, process, and user interactions over time. This technology dynamically develops a behavioral and communication model of your services and infrastructure that understands natural hierarchies (processes, containers, pods, machines, etc.) and aggregates them to develop behavioral models at scale. Together with a behavioral model, Polygraph is able to monitor your infrastructure for activities that fall outside the model and dynamically update as behaviors change over time.

Using this information, Polygraph detects anomalies and generates high-fidelity alerts appropriate to your unique environment. Polygraph maps the truth of your cloud instance and helps users quickly visualize the who, what, where, and how far of an event, speed investigation, and triage issues, saving organizations time and money.

Polygraph uses deviation from a temporal baseline to detect changes in behavior, resulting in meaningful alerts. Alerts are either due to a desired change, misconfiguration, or malicious activity. Polygraph then scores the alerts based on severity and threat.

Polygraph is more precise and accurate because of key technology innovations, including:

- Capturing behavior at process/container-level
- Separating interactive and non-interactive traffic
- Generating alerts at the analysis group-level
- Using advanced deductive analysis that does not rely on heuristics

What makes Polygraph work?

Early on, Lacework recognized that the challenge of cloud observability, compliance, and security were all big data problems. And it's that challenge that Lacework was built to take on. Polygraph itself is a graphical representation of how we ingest, analyze, and understand behavioral data at ridiculous scale.

Every hour, Polygraph builds a report of activities and behaviors in your account. Lacework then compares the behaviors found in the data to well-understood behaviors we have derived from every previous hour. The differences in behaviors are what drive our event generation.

This approach is fundamentally different from any other cloud security product on the market. Rather than applying rules and policies against what we "think" might happen, we can now generate events based on what we know to be "normal" and the deviations from what behaviors we understand.

The outcome of using this approach is that Lacework generates significantly higher quality events in terms of context and significantly lower quantity false positives. Polygraph takes your alert noise down to a whisper with fewer than two alerts generated per day, on average. And a Lacework alert is all signal, no noise.

The rewards of securing enterprise cloud infrastructure

The positive outcomes benefit the entire enterprise:

Security Visibility

Get deep observability into and across your cloud accounts, workloads, and microservices to give you tighter security control.

Threat Detection

Identify common threats that specifically target your cloud servers, containers, and IaaS accounts so you can take action on them before your company is at risk.

Anomaly Detection

Detect and resolve anomalous changes in behavior across your workloads, containers, and IaaS accounts that represent a security risk or an IOC.

Host Compliance

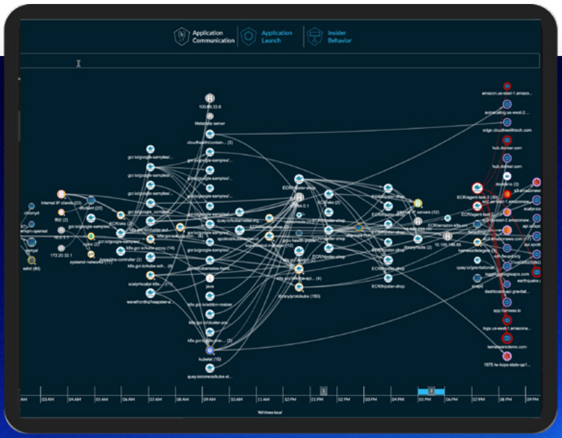
Achieve compliance for SOC 2, PCI DSS, HIPAA, and other compliance measures that require host intrusion detection (HIDS).

Configuration Compliance

Spot IaaS account configurations that violate compliance and security best practices that could put your company at risk.

Ready to chat?

Request a demo



LACEWORK