Achieving Safe and Compliant Financial Services in the Cloud

Financial Services in the Cloud Generation

The Financial Services sector is among the most targeted groups for financially motivated cyberattackers. Over 90% of attacks on financial services, which often include FinTech companies, are financially motivated. It's getting worse, with attacks on financial institutions increasing by 238% from the beginning of February to the end of April.

Adding to the distress IT security teams face within the financial services sector is the massive attack surface and subsequent attack vectors that come from supporting a large mix of tailored customer services. There is also a growing complexity that regulatory requirements force on a banking infrastructure that includes an always-on and global payment system.

Whether you're a Fintech, a large or community bank, a wholesale bank or working within Capital Markets, chances are you need to report the nuances of your IT security and prove the safety of consumer and client services to Federal and State authorities. It's a precarious game of alphabet soup dealing with the FFIEC, GLBA, PCI DSS, FINRA, OCC, FDIC and/or FRB. But it can have serious consequences. Explaining to the board of directors why you received a dreaded Matter Requiring Attention (MRA) notice from officials at the Federal Reserve Bank or the Office of the Comptroller of the Currency is akin to admitting you failed to understand the nuances of your IT infrastructure in order to prove you operate a safe environment.

For the most part, being able to prove that your organization maintains the highest level of security, metric reporting and documented accountability will keep you out of the woods. But don't mistake compliance with true security. Even after proving compliance, you still need to combat an onslaught of cyberattacks, especially given the challenging environment we face today.

For example, credential stuffing, which is one of the most common challenges banks face today, targets the personal data of banking customers by using stolen account credentials. Attackers gain unauthorized access to user accounts by employing automated large-scale login requests and stolen information, which can then be used to bombard websites and servers in order to gain access to critical IT infrastructure.

Yet there are powerful tools at your disposal that can help.

> **It took four clicks, you wait five minutes, and boom, the account are recognized. Lacework starts ingesting all of the cloud trail data. It was mind-blowing.**
>
> **Gary Tsai,**
> **Application Security Engineer**
> at Marqeta

Galvanizing Cloud Security with Total Visibility Is Key

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, PolygraphTM, delivers a deep temporal baseline built from collecting high-fidelity machine processes and user interactions – over a period of time – to drive cloud compliance by:

- Being able to spot IaaS account misconfigurations and achieve compliance for PCI DSS, the GLB Act's financial privacy provisions and other compliance and security measures.
- Understanding application behaviors by knowing 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.

Lacework automation and tooling helps financial organizations scale compliance efforts and reduce control failures. Regardless of your size and client base, 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.

Get Started Today

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 workloads and containers. This security extends to your DevOps Security teams which are empowered by embedded security across the development lifecycle for build-time and run-time 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 are able to review historical event data across their infrastructure to understand where breaches have occurred and 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.

- Lacework alerts you only when there are new or anomalous events, eliminating alert fatigue.
- With automated workload detection, Lacework saves time by removing the need to write and maintain error-prone rules. Lacework also removes the need to constantly maintain rules.
- Gain the advantage of a cloud security solution that also drives compliance and visibility for DevOps and security teams – all from a single, unified platform.

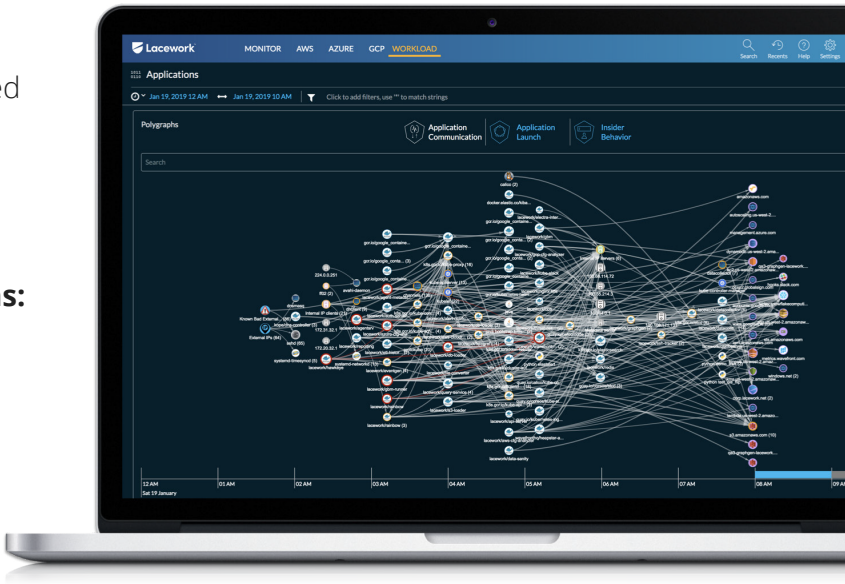
You can't secure what you can't see.

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, the 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, the 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.

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



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

- Capturing behavior at process/container-level
- Separating interactive and non-interactive traffic
- Alert generation at the analysis group-level
- Advanced deductive analysis that does not rely on heuristics

What Makes the Polygraph Work?

Lacework recognized early on the 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. The Polygraph itself is a graphical representation of how we ingest, analyze and understand behavioral data at ridiculous scale.

Every hour we build a Polygraph 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 than 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. Lacework Polygraph takes your alert noise down to a whisper with fewer than 2 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 & security best practices the could put your company at risk.

Lacework™

About Lacework

Lacework delivers security and compliance for the cloud. The Lacework Cloud Security Platform is cloud-native and is SaaS-based (Software-as-a-Service); delivering build-time to run-time threat detection, behavioral anomaly detection, and cloud compliance across multicloud environments, workloads, containers, and Kubernetes. Customers significantly drive down costs and risk by freeing themselves from the burden of unnecessary hardware, rule writing, and inaccurate alerts. Lacework is trusted worldwide by enterprise companies at the forefront of embracing the cloud.

Find out more at www.lacework.com