Cutting through the Cloud Clutter

Elevating Security Past the Complexities of Cloud Computing

Why is cloud security an uphill battle? The short answer is popularity. Every company needs cloud platforms to deliver results. This popularity and subsequent proliferation have historically made application security take a back seat to application development and application delivery functions in the cloud. As a result, we start to notice complexity growing exponentially when organizations attempt to instill cloud security, particularly while simultaneously optimizing and speeding-up the delivery of cloud-built applications. We also see the same complexity double as organizations drive more application development lifecycles within cloud platforms.

These challenges highlight flaws from compounding complexity in cloud security as well as vulnerabilities relying on cloud native security platforms which all result in new attack surfaces previously unseen from on-premise data centers. Continuous migration of computing resources to cloud environments and the increase of cloud-born application development leads to security issues.

It is also important to note that cloud data breaches often look different to the typical IT security team or Security Operations Center (SOC) analyst – especially when compared to traditional physical attacks and breaches. There are simply more options open to prospective attackers which leaves most cybersecurity teams protecting cloud networks scrambling to keep data safe. They also tend to become exhausted due to constantly chasing ghosts.

But there is hope. The first step is understanding the top things to consider when evaluating your cloud security program. This step includes better understanding the other challenges facing your cloud security. The second step is understanding how perfect visibility and actionable insights from an effective cloud-native security application helps mitigate security issues.

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, Snowflake Computing

Not Your Traditional Attack

Cloud attacks often have a common progression. Although each data breach incident may develop differently, a cloud-native attack breach often starts from a compromised user account which then develops into account reconnaissance, privilege analysis, resource exploitation and finally data exfiltration.

95% of cloud security failures are a customer's fault.

Within a cloud environment, there are resources that were previously located outside of an organization's perimeter and out of control of system administrators. In the cloud, they can be accessed from anywhere in the world. Workload security, therefore, is defined by the people who can access those workloads and the permissions they have. In effect, your permissions equal your attack surface.

SIEMs can be costly, especially when handling AWS CloudTrail data.

Ignoring logs or placing raw data into a SIEM is often a bad move. AWS CloudTrail is a service that enables governance, compliance, operational auditing and risk auditing on AWS accounts. And CloudTrail provides event history of AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools and other AWS services. CloudTrail logs can be exceptionally noisy for Internet of Things (IoT) security teams. In fact, Security Boulevard in 2019 reported that the signal to noise ratio in a typical CloudTrail is 1 to 25,000. The burden falls to each organization to quickly sift through CloudTrail data and understand what is useful and actionable information versus excessive noise.

Two costly approaches to handling AWS CloudTrail data are either ignoring logs or placing the raw data into a SIEM. However, pre-filtering CloudTrail logs prior to importing them over to a SIEM or another analysis tool can significantly reduce storage and analysis costs. Yet reviewing CloudTrail log data is essential to protecting the cloud and providing early warning signs of an attack.

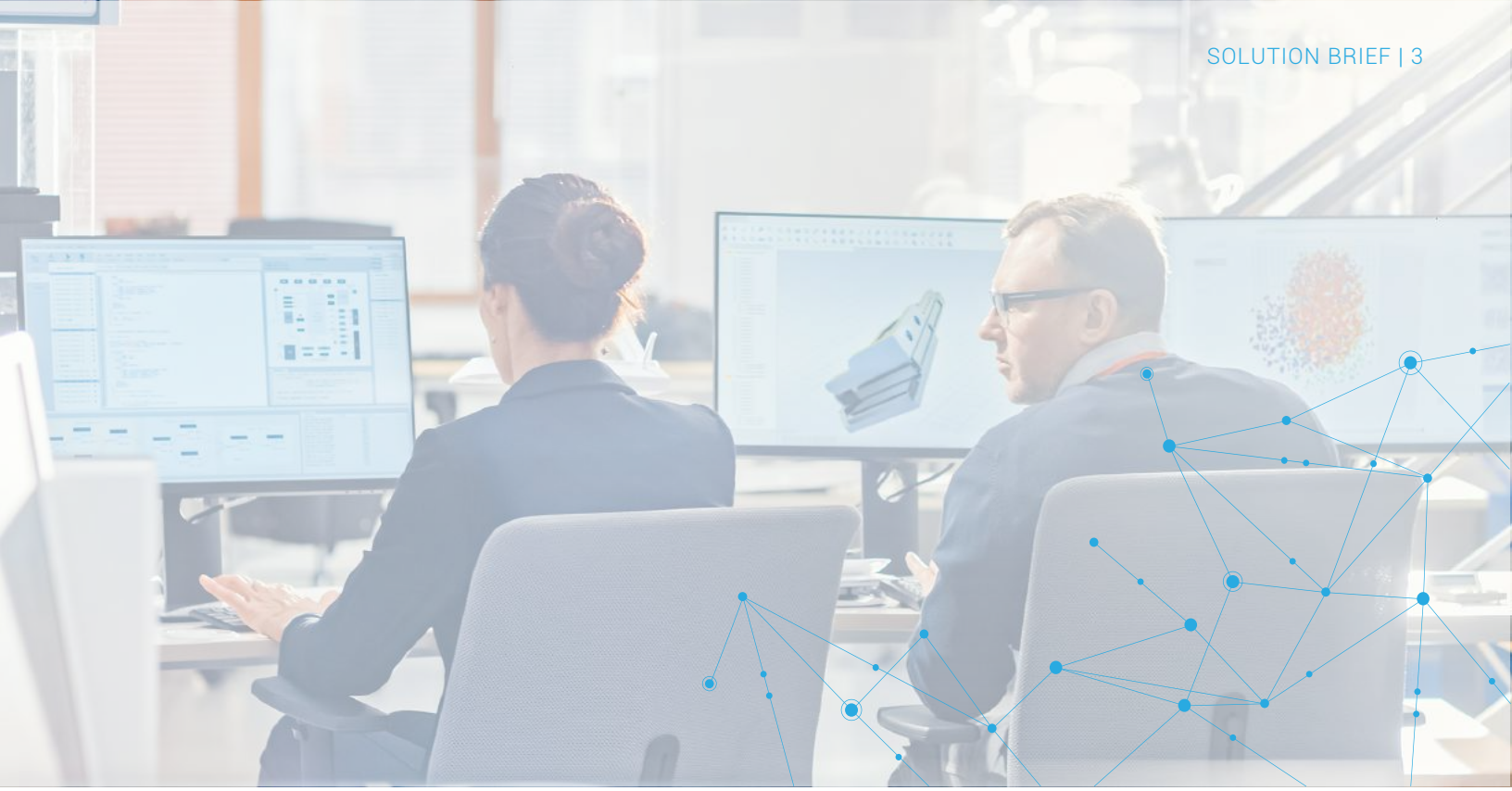
Not Your Traditional Cloud Security

Buying multiple security tools to address your cloud and container visibility gaps is a bad plan. In fact, 53% of security professionals said the excessive number of security tools in place at their organization adversely impacted their security posture.

Organizations facing challenges with cloud native security need partners that can provide cloud and multi-cloud protection using automation and compliance across the spectrum of public and private clouds, including AWS, Azure, and GCP instances.

Insight is the key to successful cloud native security. Lacework's approach uses automation and unsupervised machine learning. Security teams that deploy the Lacework agent across multiple cloud platforms, even within Docker, Kubernetes and hybrid workloads, benefit from a review of historical event data across their infrastructure to understand where breaches occurred and identify risk areas.

- Lacework will always alert you about 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 within your health IT groups.
- With automated workload detection, Lacework saves time by removing the need to write and maintain error-prone rules. Lacework removes the need to constantly maintain rules, allowing you to focus on securing your customers' information.



Lacework provides 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. This empowers continuous security, automation and the ability to build quickly.

Lacework solves the challenge of total cloud security with an approach that involves native support throughout the application lifecycle at every level, with key features that include:

Automated Threat Detection

This includes discovery of every anomaly in and out of containers and clusters to establish baseline behavior that performs continuous monitoring of communications, launches and other cloud runtime behaviors. Machine learning is employed to detect abnormal behavior and issue alerts in real-time.

Deep and Continuous Visibility

By functioning at the process level, Lacework gains deep visibility into container-related events, communication, new connections and images. Deep visibility and security for Kubernetes clusters and communication among the clusters can be further visualized at the namespace and pod levels. The solution exposes threats at all layers, including publicly exposed or unsecured API servers and management consoles.

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