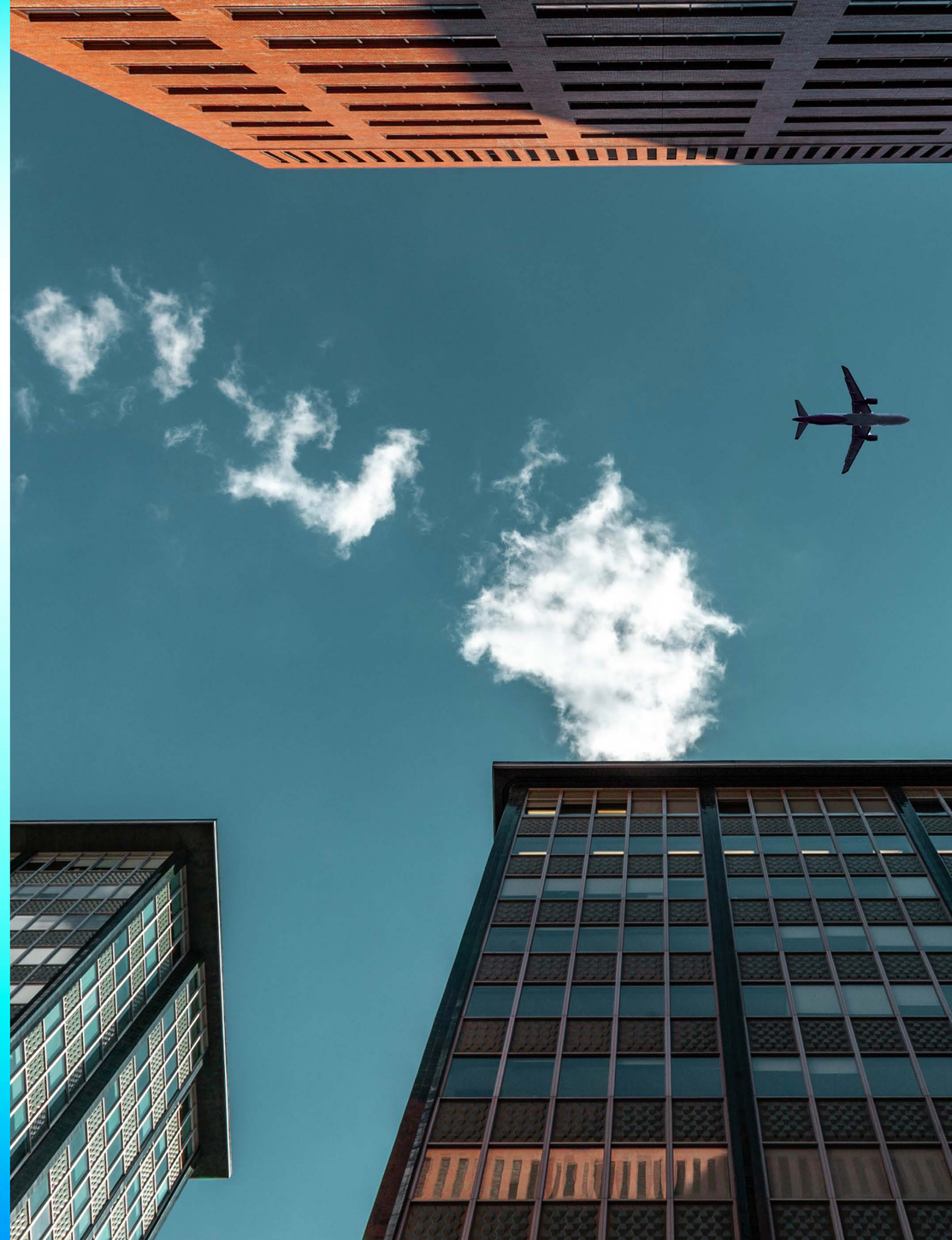
LACEWORK

Cloud security fundamentals



Protecting a cloud environment requires a dedicated, comprehensive effort across the policies, processes, technologies, and controls that are involved in securing the data and resources that make up the overall cloud infrastructure.

There is no traditional network or infrastructure architecture in the cloud — instead, this security dynamic requires a unique approach of shared responsibility between cloud users and their cloud service providers.

When moving workloads and resources into a public cloud like AWS, Azure, and GCP, customers receive an inherent layer of security delivered by the cloud provider — this is considered security of the cloud. Customers then must establish and manage security for all the data, transactions, and other activity happening in that environment — their responsibility is security in the cloud. The challenge is that each public cloud provider delivers their own level of security controls and policies. Customers must understand these differences so they can make informed decisions about which cloud environments are best suited to their individual needs.

This guide identifies the security needs of cloud providers and offers requirements that an informed buyer should consider. It looks at how different security vendors address these challenges in order to deliver on the end user needs to address their part of the shared responsibility model, and ultimately, to keep their data and assets safe.

To start, let's look at some of the unique security challenges presented by the cloud.

LACEWORK

The cloud changes everything, including security

A cloud environment is a virtual one. All infrastructure components —gateways, servers, storage, compute, and all the resources and assets that make up the entirety of a cloud platform environment, are presented and operate as virtual services.

This type of architecture simplifies things in many ways: hardware doesn't need to be installed, storage is provided, and compute capabilities can efficiently be scaled up or down depending on need, rather than at datacenter capacity.

Deploying workloads in the cloud can quickly involve complex sets of microservices and serverless instances that function in fluid architectures that change every few minutes or seconds, creating a constantly changing security environment.

That rate of change is happening on the backs of the following resources and processes, each of which have their own level of security needs and requirements:

Microservices

In a cloud environment, applications are often broken down into many discrete functions. These microservices enable greater run time flexibility and more efficient resource utilization, but they also make security more complex. Where before you had to manage authentication and access control for an application, now you have to do that for every microservice that makes up a cloud app.

DevOps

In a cloud environment, new code is continuously being deployed. This can happen daily or even hourly, and in practice, DevOps deployments are often way ahead of security. Every newly deployed function or service represents a growth in the attack surface.

Ephemeral workloads

To optimize the use of cloud platform resources, it's common to recycle things like drives, IP addresses, data, firewalls, and other operational components. These functions and assets are constantly destroyed and recreated in an ever-changing cloud environment, and the way they are delivered to users is constantly changing. Often, these workloads come and go in seconds.

Containers

Containers make it possible to easily deploy applications, functions, and microservices in tightly controlled containerized environments. Although containers seem secure on the surface, at the same time, they introduce a whole new level of complexity, along with a slew of potential new vulnerabilities.

All containers in an environment share a common operating system kernel which, if compromised by a poorly configured container, can compromise all the other containers in that environment. It's also not always easy to see what's happening between containers. For instance, monitoring traffic to and from an EC2 instance is one way to make sure you are operating securely. But if there are several containers sharing data inside one EC2 instance, a lot can be happening that is not visible to the monitoring tool. Additionally, using lots of container instances increases the chances of simple human errors like overprovisioning the container with functions and privileges it does not need.

The combined effect of the activity from all these parts is an exponential growth in a cloud environment's attack surface. There's also an enormous amount of event activity in the cloud. A busy cloud environment can generate 8 to 10 billion events per month, which makes threat detection a much more challenging proposition. Attackers are well aware of these vulnerabilities and are working frantically to exploit them.

Traditional approaches no longer work in the cloud

Traditional datacenter defenses were designed to protect a defined perimeter by monitoring and controlling data that moved in and out of a network environment. Defending the perimeter requires a layered defense strategy that typically includes these components:

Router

Provides connectivity between the datacenter and the outside world, and can provide a first layer of defense through pre-set TCP/IP filtering

Firewall

Monitors IP address, port, and application traffic in and out of the network, and filters traffic based on a set of established rules and lists

Antivirus/Malware protection

Scans for malicious code using known code signatures to identify threats

Intrusion detection and prevention

Monitors traffic inside the datacenter network to identify activity that violates defined policies

Access and identity management

Sets role and account-based policies to manage application and data access, and manages identity authentication

Dynamic, ever-changing cloud environments are not well served by traditional security tools. That's because those tools were never designed for fluid, high access environments.

The goal of this layered defense strategy is to block unauthorized access to the network and prevent unauthorized activity inside the network. For an attacker to be successful, they must bypass all these layers.

That approach works reasonably well in an isolated datacenter environment that doesn't change very much. But the cloud is neither isolated nor unchanging. The cloud is a shared environment whose entire purpose is to provide easy access to anyone who can connect to the internet. Although you can use cloud security tools to control access to your own cloud assets, there will always be millions of others, including bad actors, sharing the same cloud infrastructure as you.

Much of what is happening is not user-facing. For example, servers connect to each other through API calls that run in the background, and automated scaling changes workload capacity and performance levels. Users can think of this activity in this way: they are not only configuring your local on-premises equipment to talk to the cloud, they are configuring the cloud, too. To be able to grant secure access when necessary, users need to leverage the tools, identity sources, and federation capabilities of the cloud provider. Additionally, a great deal of autonomous connections are being made, which is why access control list (ACLs) is critical.

The cloud is malleable, which is one of its most important attributes. That creates tension if it is operating with strict, unbending rules. Notice how almost all the tools in the traditional security stack rely on checking monitored activity against pre-set rules, policies, lists, and known signatures. In a cloud environment that can reconfigure itself every few minutes to meet operational demands, the computing function changes too quickly to be secured by a traditional rules-based approach.

Rules and controls are unable to keep pace with the rate of change, and it's not possible to adjust the rules manually. It's largely because of this that the old security groups and policies become less important in a cloud environment than service meshes and Layer 7 firewalls that limit the scope of applications by controlling which microservices talk to which APIs.

Using the cloud also demands a level of visibility unlike that needed for legacy environments. Unlike traditional intrusion detection tools that can watch everything happening inside your isolated datacenter, you will always be limited in what you can see in a cloud infrastructure because it's a shared infrastructure, and you won't be permitted to monitor activity of other cloud clients or deeper cloud operations.

Cloud providers typically do not deliver comprehensive visibility to give users a clear, precise picture of activity and anomalies. The issue gets even more complicated (and less visible) because the dynamic addition and removal of containers and microservices changes the environment's landscape, which means every change brings new things to understand and investigate.

The dynamic nature of a cloud environment also limits the value of activity logs that many traditional tools inspect to detect and investigate unusual activity. In an environment where servers can spin up and spin down in minutes, log information is of limited use or it is non-existent. An IP address associated with one function or resource may have a totally different role in 10 minutes. This makes incident detection and forensics difficult.

Cloud security needs a new approach

The only way to secure a continuously changing cloud environment is through continuous, real-time approaches to security. These security functions need to include the following capabilities:

Continuous real time anomaly detection and behavioral analysis that is capable of monitoring all event activity in your cloud environment, correlate activity among containers, applications, and users, and log that activity for analysis after containers and other ephemeral workloads have been recycled.

This monitoring and analysis must be able to trigger automatic alerts. Behavioral analytics makes it possible to perform non-rules based event detection and analysis in an environment that is adapting to serve continuously changing operational demands.

- Continuous, real-time configuration and compliance auditing across cloud storage and compute instances
- Continuous real time monitoring of access and configuration activity across APIs as well as developer and user accounts
- Continuous, real time workload and deep container activity monitoring, abstracted from the network

A public cloud environment provides limited visibility into network activity, so this requires having agents on containers that monitor orchestration tools, file integrity, and access control.

Today many companies make a choice between speed and security, which is a bad bargain. New security tools designed to deeply monitor cloud infrastructure and analyze workload and account activity in real time make it possible to deploy and scale without compromising security. When operating in the cloud, businesses need to know that their infrastructure remains secure as it scales.

They need assurance that they can deploy services that are not compromising compliance or introducing new risk. This can only happen with new tools designed specifically for highly dynamic cloud environments, tools that provide continuous, real-time monitoring, analysis, and alerting.

How the security market has evolved to address these challenges

The first generation of cloud security solutions were either on-prem solutions ported over to the cloud, or primarily focused on protecting the perimeter. This was a good place to start, but did not meet the requirements of fast paced cloud innovation.

The second generation of cloud security solutions took this legacy technology, and applied it in a way that tried to identify known threats around new technology like containers. Many of these vendors were incorporated into larger organizations through acquisitions, which was reflective of their single solution set.

Most recently, there have been newer point solutions that take novel approaches to more easily identify known threats and vulnerabilities, like operating off incremental data snapshots, or try to apply endpoint security to the cloud, which only solves a piece of the puzzle, rather than addressing true runtime behaviors or addressing data complexity.

That's why Lacework was built — to solve the cloud security problem with a data at scale approach, built in the cloud and for the cloud to collect, analyze, store, and secure the massive amounts of dynamic cloud data.

Covering the full range of specific security needs

Cloud configuration

Cloud misconfigurations can result in severe vulnerabilities that put your entire infrastructure at risk. Lacework integrates directly into AWS, Azure, or GCP cloud deployments and audits configuration against the CIS benchmark standard. Lacework generated reports rank findings by severity and categorize by service (e.g., IAM, EC2, and CloudTrail).

Cloud log detection

Lacework ingests AWS CloudTrail, Azure Activity Log, and GCP Audit Trail logs and streams them to the Lacework data warehouse to build a baseline of normal behavior, which is updated hourly. From this, Lacework provides detailed in-context alerts for anomalous behavior by comparing each hour to the previous one.

Host & network intrusion detection system (HIDS, NIDS)

Workload security depends on how well the host-based intrusion detection system identifies insider attacks that otherwise wouldn't be caught inside network traffic. The Lacework host-based intrusion detection system (HIDS) identifies any activity happening across all cloud workloads and accounts. Our host-based intrusion detection overcomes the limitations of network intrusion detection systems (NIDS) that are traditionally used in enterprise datacenters and non-cloud-based infrastructures.

Host vulnerability assessment

Lacework continuously assesses the risk of vulnerabilities found on hosts, containers, and pods within an environment. This means that users can identify and take action on software vulnerabilities in their environment and manage that risk proactively.

Host configuration assessment

Lacework provides continuous assessments of configurations of AWS Config, CloudTrail, and S3 buckets by creating the SQS queue and IAM Role and then configures both integrations with Lacework.

Container runtime detection (Container IDS)

Container runtime and orchestration platforms like Docker and Kubernetes accelerate deployment velocity, but vulnerabilities in the orchestration layer adds to the attack surface. Lacework delivers native container security support, reducing the attack surface, and detecting threats in a containerized environment. Our cloud container security monitoring platform automatically discovers every container across a user's environment and clusters them based on different behaviors.

LACEWORK

Covering the full range of specific security needs continued

Container vulnerability assessment

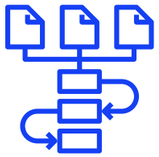
Lacework assesses, identifies, and reports on vulnerabilities found in the operating system software packages in container images before the container image is deployed. This means you can identify, manage, and take action on software vulnerabilities in your risky container images.

< 5 Minute investigation time

Lacework applies machine learning analytics to all cloud activity, including workloads and containers across the environment, which vastly reduces the amount of data processed by a SIEM, all of which happens continuously and with feedback in under five minutes.

Application relationships

In complex cloud environments, there are multiple applications and resources interacting, all of which demand behavioral insights against normalized activity. Lacework allows users to recognize and monitor in-scope application workloads, collect data about activity about commissioning/decommissioning all connections in the cloud environment.



Orchestration runtime detection

Lacework identifies vulnerabilities in the host OS, container images and the containers themselves using real-time analytical data collected across the infrastructure. This dashboard simplifies orchestration and cloud administration.

Serverless monitoring

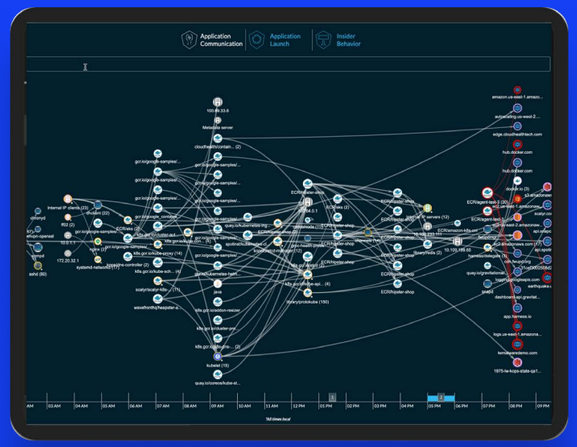
Lacework provides the ability to identify and monitor all resources and services in real-time. This includes traditional sources like on-prem servers, databases, caches, and load balancers, but also for containers, VMs, and other serverless resources.

LACEWORK

Automated security and compliance for the cloud generation

Lacework automates security and compliance across AWS, Azure, GCP, and private clouds, providing a comprehensive view of risks across cloud workloads and containers. Lacework delivers a unified cloud security platform that provides unprecedented visibility, automates intrusion detection, delivers one-click investigation, and simplifies cloud compliance.

Lacework was built specifically to deliver contextual data about cloud events, because changes can lead to new vulnerabilities and potential threats, potentially impacting your security posture and in turn your compliance goals. Every update, configuration change, access point, and a million other activities that might represent potential threats are identified and analyzed for their risk potential.



Ready to chat?

Request a demo

Lacework delivers security and compliance for the cloud generation. The Polygraph® Data Platform is cloud-native and offered as-a-Service, delivering build-time to run-time threat detection, behavioral anomaly detection, and cloud compliance across multi-cloud environments, workloads, containers, and Kubernetes. Trusted by enterprise customers worldwide, Lacework significantly drives down costs and risk, while removing the burden of unnecessary toil, rule writing, and inaccurate alerts. Lacework is based in San Jose, California, and backed by Sutter Hill Ventures, Liberty Global Ventures, Spike Ventures, the Webb Investment Network (WIN), and AME Cloud Ventures.

Get started at www.lacework.com

LACEWORK®