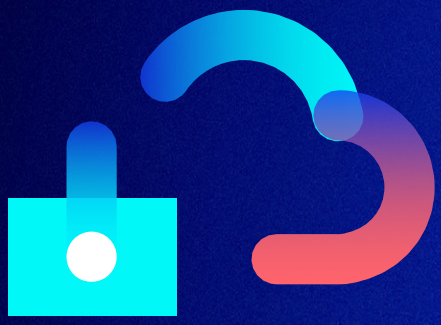
Agentless and agents

Protect your cloud with a layered strategy



LACEWORK®

The cloud is transformative, allowing for greater flexibility, efficiency, speed, and innovation.

While the benefits of cloud are undeniable, for security teams, the cloud introduces a new set of challenges. Cloud environments are complex and dynamic by nature, which means that you need an effective security strategy that keeps up with the rapid pace of change — and that requires a layered approach.

It's similar to the defense-in-depth methodology used to secure other parts of your infrastructure. For years, security practitioners have adopted a defense-in-depth strategy to protect the evolving network perimeter. Using products and services that monitor network, web, email, and endpoint activity, you can better defend against threats to employees. As organizations move to the cloud, it is vital to have a similar strategy to monitor the activity of your underlying cloud infrastructure and the workloads, applications, and customer data running on it.

By embracing microservices and a multicloud environment, the attack surface expands, along with the number of entities that need to be secured. Simply scanning cloud accounts and workloads for misconfigurations and vulnerabilities is not enough. And focusing only on regulatory and compliance requirements leaves security gaps. When looking for an effective approach to cloud security, consider one that is multi-faceted — that scans for risks and continuously monitors cloud account activity and workload behavior in runtime to immediately identify attacks, then ties those insights together to help you effectively prioritize and fix critical issues.

At Lacework, we're all about helping you achieve your desired outcomes.

Some vendors may focus on deployment methods as a means of getting your attention. We believe it's not simply a question of agentless or agent-based deployment mechanisms. Instead, it's about creating the most secure environment possible, by whatever means possible.

The Lacework Polygraph® Data Platform enables you to reach this goal. Not only can you better manage the risks from vulnerabilities and misconfigurations, but you can also continuously monitor runtime activity to detect threats faster and protect cloud workloads. By automatically tying together insights from build time to runtime with Lacework, your team can more effectively prioritize vulnerabilities and configuration errors based on what's actually running — going from thousands of issues to the dozen that need to be fixed first. To gather all of the data needed in the most effective way, Lacework uses both agentless and agent-based technology.

A layered approach to cloud security

To understand how our layered approach can help secure your cloud environment, consider the analogy of securing a multi-tenant office building. We can break this process into three progressive stages:

1 Uncover misconfigurations and vulnerabilities

Ensure windows and doors are locked

2 Monitor activity in cloud accounts for compromise

Watch badge-ins to different spaces

3 See what's happening in runtime and alerts on unusual activity

Use smart cameras to monitor 24-7

The first step in securing an office building is to make sure all the doors and windows are locked. In the cloud, this is the equivalent of uncovering vulnerabilities across your container images and workloads and finding and fixing misconfigurations in your cloud accounts, such as an open S3 bucket or a public BigQuery instance. Whether you're using virtual machines (VMs), containers, or Kubernetes, deployed manually or with Terraform, Lacework can help you uncover and remediate your misconfigurations and find vulnerabilities from build time to runtime.

The next step is to start monitoring who is entering the building, and where they are going. In the cloud, Lacework ingests activity logs to build a baseline of user and entity behavior, which helps us uncover deviations or anomalies. For example, we help you understand who deployed or modified a certain service in a specific region, and determine if this is expected behavior.

Finally, similar to how smart cameras can be used to watch and alert on exactly what's happening in hallways and meeting rooms, Lacework continuously monitors runtime activity and alerts on suspicious activity. In the cloud, you need to see what's happening with your workloads, so you can quickly identify unusual behavior, like changes to files or an application talking to an external IP for the first time. This way, you can identify potential attacks early, including ones that may be taking advantage of a zero-day vulnerability. Behavior-based threat detection that leverages a baseline of known activity in your specific environment is the key to effective security without a ton of false positives.

Just like securing an office building, these steps become even more powerful when you combine insights across all elements together. Consider having a centralized security team that is constantly analyzing this information and correlating data together. They could alert on suspicious activity. And if there was an attempted burglary, they would have all of the recorded activity to aid in investigations. By having all of these pieces working together, you can be alerted sooner and investigate and respond faster, with less manual effort.

Benefits of combining agentless and agents

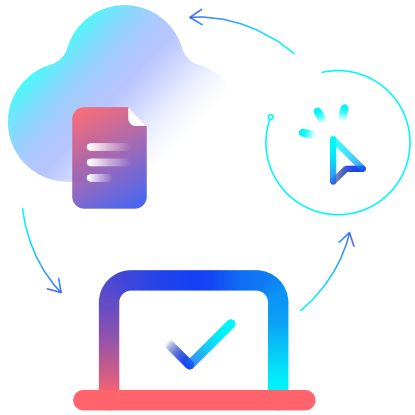
Understanding your complex cloud environment and knowing where the biggest risks are hiding is a continuous journey. Depending on where you are in your cloud security journey, you may need different approaches or a combination of methods to achieve the aforementioned outcomes. Cloud security can be deployed in different ways — in both agentless and agent-based approaches. As we mentioned, it's not an "either or" discussion; it really comes down to what kind of data is needed to fully secure your cloud and the most effective way to gather that data. And to achieve the most comprehensive security for your cloud, a combination of agentless and agents is essential. Here are three benefits to this approach:

Start with a simple first step

For many organizations, especially those in the early stages of cloud security maturity levels that don't have the time or resources to fully deploy agents everywhere, an agentless method is a great way to start getting quick visibility into cloud assets, possible risks, and attack surfaces — and it's painless. All it takes is a simple one-time connection of your cloud accounts with Lacework, making it easy for your teams to collect valuable cloud security data near-instantly, without the use of agents.

An agentless approach is especially helpful for gaining full coverage where a traditional agent can't reach, or quickly assessing security posture across your entire environment, including shadow IT hosts and new accounts that you may have onboarded due to mergers and acquisitions. Agentless allows you to gather data about vulnerabilities, misconfigurations, cloud audit log anomalies, and unusual account activities with the least amount of overhead possible. Armed with this data, you can meet compliance guidelines, detect account compromises, and much more. An agentless method gives comprehensive visibility across your cloud workloads from build time to runtime, with a high degree of choice and flexibility.

With agentless, you can identify risks stemming from vulnerabilities and misconfigurations in your cloud environments during build time. You can scan and detect vulnerability risks across all your hosts, containers, and language libraries at runtime. Your security teams can detect anomalous activities, such as a new user trying to create or delete an EC2 or S3 instance, change keys or policies on a cloud account, or add new privileged users. And Lacework allows your organization to take actions on the most critical of these risks, exactly when you need to.



The Lacework approach

Our agentless approach helps you gather data from places within your cloud accounts and services that an agent simply can't reach. We continuously monitor your cloud configuration, detect threats in your accounts, and provide container vulnerability assessment for software supply chain risks. Lacework also offers application programming interfaces (APIs) that collect necessary data from your cloud service providers (CSPs) and performs compliance checks, which are mapped to industry standard frameworks. Our agentless capabilities include:

- Cloud services configuration scanning
- Container registry scanning
- Cloud-native Kubernetes admission controller
- Cloud services anomaly detection
- Kubernetes activity log monitoring
- Infrastructure as code (IaC) scanning
- Cloud workload scanning at runtime

Gain continuous runtime workload security

As we mentioned, an agentless approach, while simple, can only go so far. To gain the best picture of your cloud environment, it's critical to monitor workloads during runtime to discover any active threats, such as an attack that's exploiting an unknown or zero-day vulnerability. Relying solely on agentless scanning can potentially cause you to miss critical activity and information.

For the strongest runtime security, you need an agent that is tracking activity to investigate and respond faster. Unlike an agentless approach, an agent is uniquely positioned to perform activities such as runtime threat detection of known and unknown threats, file integrity monitoring, host-based intrusion detection, configuration checks, and host vulnerability scans.

The Lacework approach

Unlike many legacy agents (and some modern ones), the Lacework agent is lightweight and easy to install. It deploys in minutes with minimal overhead, but still provides the depth and continuous monitoring necessary for your investigations into all process activity. By deploying directly into your workload, whether it's a virtual machine or container, or uses Kubernetes, the Lacework agent grants continuous visibility that isn't available from any other location.

Lacework takes a distinctive approach

to runtime threat detection for files, applications, memory, network, and user activity.

Using machine learning, our Polygraph® technology automatically learns activities and behaviors unique to each customer environment and surfaces unusual activity — all without requiring excessive rules to be created and constantly maintained. Not only do we provide the continuous monitoring needed in runtime, but our approach helps you prioritize risks with accuracy, removing alert fatigue and speeding up investigations. Lacework is the only company that leverages behavior-based anomaly detection across AWS, Google Cloud, Microsoft Azure, and Kubernetes environments to automate cloud security so you can easily detect threats at scale.

Combine breadth and depth

To stay safe in the face of known and unknown threats, you need broad protection that combines risk posture analysis with continuous threat detection. For example, with the recent Log4j vulnerability, businesses had to both quickly identify vulnerable systems and prioritize remediation for ones actively running and most at risk of exploit activity. The impact of this protection can't be overstated. It's the difference between trying to deal with hundreds or thousands of vulnerable systems and narrowing it down to a few dozen that need immediate attention. The former is an impossible task; the latter is both feasible and within reach by tying together vulnerability and runtime data.

In addition, identifying exploit activity quickly is critical to preventing a breach. By continuously monitoring cloud behavior and identifying abnormal activity, you can better detect attacks — even those involving a zero-day exploit.

Just as you would take multiple steps to secure a building, you must do the same in your cloud environment. A layered approach can help you find and fix vulnerabilities and misconfigurations, uncover behavioral deviations, and check workloads for suspicious activity — all in one place.

Consider the "agent versus agentless" debate settled. Modern cloud security requires a holistic security approach — a breadth of coverage that layers security capabilities for accounts, services, and workloads. Only this combination of abilities can help you get secure — and stay secure.

The Lacework approach

Gain the full level of visibility you need to truly protect your business. If you want to know what's happening in your cloud accounts and on your systems, the combined agentless and agent-based approach that Lacework offers gives you better data and insights, enabling you to take more effective action.

"Lacework combines an agentless and agent-based approach to collect data about our environment in the most efficient way possible. The agent allows us to quickly detect when something is wrong because we get constant information right in the Lacework dashboard. If you only rely on a snapshot, you're going to miss important activity and information. We want as much detail as possible to aid in investigations, and Lacework gives us that."

AUSTIN GREGORY, INFORMATION SECURITY ENGINEERING MANAGER, NYLAS

Case Study: Reltio

Needs

- Ease anxieties by uncovering cloud misconfigurations and vulnerabilities
- Cut costs by eliminating redundant tools
- Regain control with visibility into a multicloud environment

Results

- Deployed Lacework across 3,000 systems in a few days
- Investigated and resolved issues 4x faster than before, across all criticality levels
- Gained deep visibility across all highly ephemeral and dynamic clouds

Read the full Reltio story

Learn more about Lacework

Watch a webinar

Get a custom walkthrough

Request a demo