Lacework™

THE DEFINITIVE GUIDE TO PUBLIC CLOUD SECURITY

Comparing Security Vendors for AWS, Azure, & GCP

Lacework™

THE CLOUD'S UNIQUE SECURITY CHALLENGES

One of the greatest cloud security challenges comes from the fact that the cloud delivers its infrastructure components, things like gateways, servers, storage, compute, and all the resources and assets that make up the cloud platform environment, as virtual services. There is no traditional network or infrastructure architecture in the cloud.

Deploying workloads into 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.

Here are some of the common security challenges presented by the cloud:

1) **Microservices**
2) **The DevOps process**
3) **Ephemeral workloads**
4) **Containers**

1) 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 each and every microservice that makes up a cloud app.

2) THE DEVOPS PROCESS

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.

3) 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 a dynamic cloud environment, and the way they are delivered to users is constantly changing. Sometimes these workloads come and go in seconds.

4) CONTAINERS

Containers make it possible to easily deploy applications, functions, and microservices in tightly controlled containerized environments. Although containers are inherently secure, they introduce a whole new level of complexity and potential vulnerability.

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. Also, it's 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 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 eight to ten billion events per month, which makes threat detection a much more challenging proposition. Of course attackers are well aware of these vulnerabilities and are working frantically to exploit them.

TRADITIONAL APPROACHES NO LONGER WORK IN THE CLOUD

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 like the cloud.

Traditional data center defenses were designed to protect a defined perimeter by monitoring and controlling data that moves in and out of the 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.

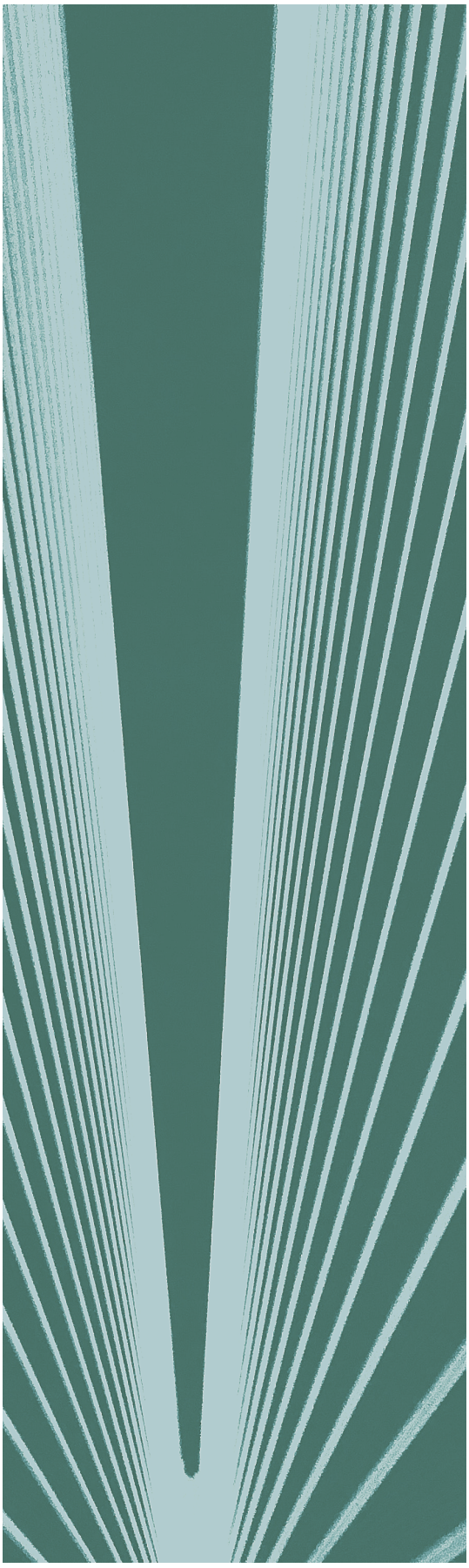
That goal of the layered defense strategy is to block unauthorized access to the network and prevent unauthorized activity inside the network. For an attacker to be successful, he, she, or it must bypass all these layers of security.

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 on planet earth (and beyond) 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.

Cloud changeability also works against the traditional tools. 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 that can reconfigure itself every few minutes to meet operational demands, the computing environment changes too quickly to be secured by a traditional rules-based approach.

The rules can't keep up, and it's not humanly possible to adjust the rules fast enough. 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.

"...there will always be millions of others, including bad actors, sharing the same cloud infrastructure as you."



Yet enforcing security at this level can be a real challenge when developers, who necessarily have access to everything, are constantly deploying new functions and services.

Another weakness of the old tools is limited visibility into what's going on inside the cloud environment as a whole. Unlike traditional intrusion detection tools that can watch everything happening inside your isolated data center, 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.

And that's not the only limitation to visibility in the cloud. As noted earlier, visibility into your own cloud activity can be difficult because of the way containers and microservices are deployed.

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.

PUBLIC CLOUD SECURITY VENDORS

	Lacework	Palo Alto Networks: Redlock, Evident.io	Check Point: Dome 9	TwistLock	Threat Stack
AWS, Azure, GCP Support	✓	AWS, Azure only	✓		AWS only
Security Automation	✓				
Multicloud Configuration Compliance (AWS, Azure, GCP)	✓	✓	✓		AWS only
Cloud Server Compliance (PCI, SOC 2, HIPAA, NIST)	✓			✓	✓
Host IDS	✓			Container only	
Runtime Threat Detection - Host infrastructure	✓	Network only			✓
Runtime Threat Detection - Container infrastructure	✓			Container only	✓
Kubernetes Security	✓			✓	✓
Anomaly Detection	✓				
File Integrity Monitoring (FIM)	✓				✓

AWS, Azure, GCP Support: Lacework delivers threat detection of behavioral anomalies for cloud and container environments as a single pane of glass across AWS, Azure, and GCP. With so many of our customers opting to distribute workloads into different environments, this now gives them security coverage over their entire infrastructure. One solution for one problem – security of cloud environments. Grow with Lacework's platform as your security needs evolve a) Multi-Cloud (AWS/Azure/GCP) b) Host, container and K8s c) Machine Learning that goes beyond location and service anomalies c) Operate at scale (100's accounts and 1000's of containers and hosts).

Security Automation: Using a combination of expert systems and unsupervised machine learning, Lacework fully automates repetitive, labor-intensive processes to provide continuous security monitoring, intrusion detection, and configuration compliance to protect all of your assets in the cloud.

Multicloud Configuration Compliance (AWS, Azure, GCP): Lacework provides continuous cloud configuration monitoring and audit reports across AWS, Azure, and GCP environments to detect any violations in compliance across the data storage, networking, user access, and logging aspects of your cloud infrastructure.

Cloud Server Compliance (PCI, SOC 2, HIPAA, NIST): Lacework builds compliance into your infrastructure from Day One. With capabilities for host intrusion detection (host IDS), file integrity monitoring (FIM), & anomaly detection, Lacework will give you the ability to quickly comply to the primary infrastructure security requirements for SOC 2, PCI DSS, NIST, & HIPAA. Lacework eliminates manual auditing in the evidence collection process for compliance.

Host IDS: Lacework Host-based IDS automatically identifies intrusions and raises the alarm so you can stay a step ahead of attackers. We give you the visibility and context you need to resolve intrusion events before they turn into damaging breaches. Delivered as a service, Lacework can be deployed at scale in minutes.

Runtime Threat Detection - Host infrastructure: Lacework provides security monitoring and alerting for active threats and security risks across cloud host infrastructure. At runtime, Lacework continuously identifies, analyzes, and alerts on anomalous behavior across applications, virtual resources, hosts, network traffic, and all user activity.

Runtime Threat Detection - Container infrastructure: Lacework is fully container-aware and monitors all container activities regardless of the container distribution. At runtime, any malicious activity in a containerized environment will generate an anomaly at one layer or another – Lacework's threat detection and behavioral analysis identifies anomalous activities across your cloud and containers so issues can be remediated before any damage is done.

Kubernetes Security: Lacework provides deep security monitoring visibility into your Kubernetes deployment. This includes high-level dashboards of your clusters, pods, nodes, and namespaces combined with application level communication between all of these at the application, process, and network layer.

Anomaly Detection: Lacework provides real-time anomaly detection for all modern cloud and container environments. It uses machine learning to identify and analyze behavioral deviations from normalized behaviors in cloud and container infrastructures that result from vulnerabilities.

File Integrity Monitoring (FIM): Lacework's FIM solution automates setup and eliminates labor-intensive rule development, ACL specification, and configuration. With our innovative baselining technology, Lacework keeps up with cloud changes while dramatically reducing false positives so security teams can focus on the FIM events that really matter.

CLOUD SECURITY NEEDS 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;

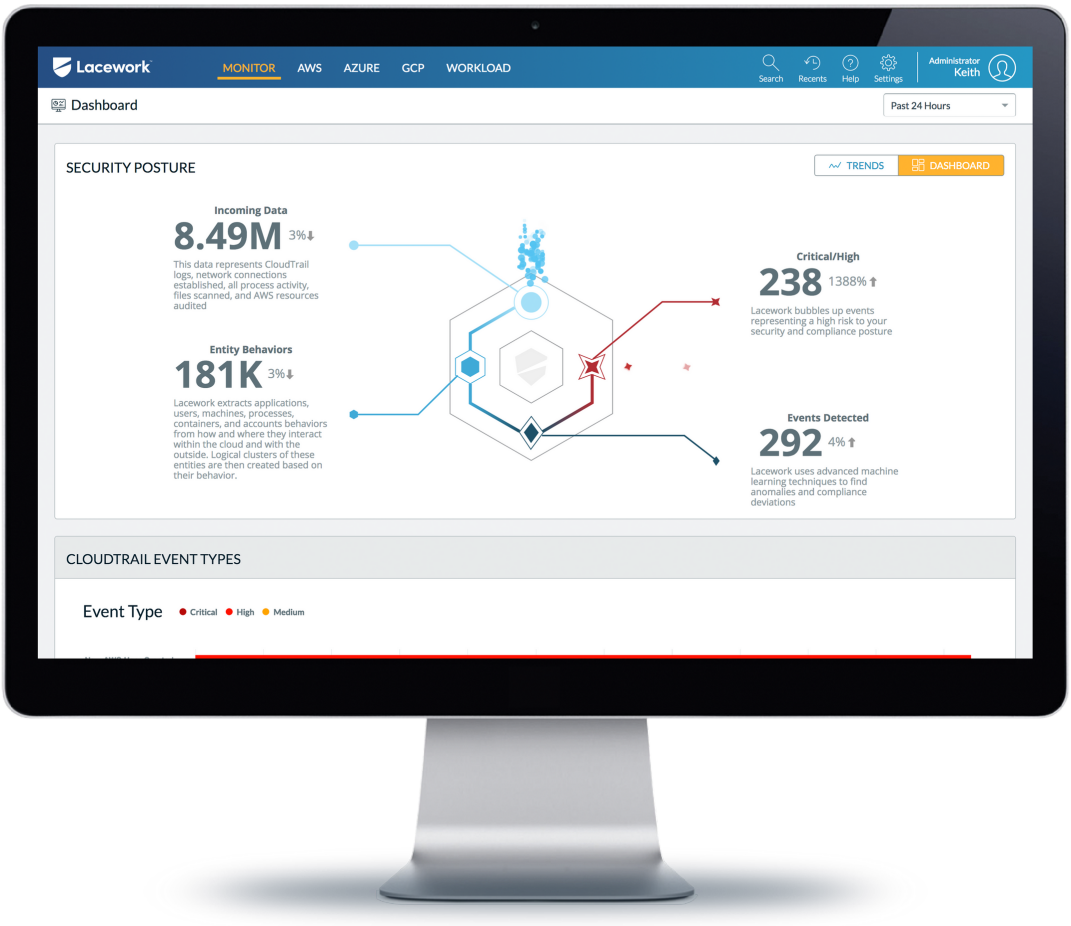
Continuous, real time workload and deep container activity monitoring, abstracted from the network. A public cloud environment provides limited visibility into network activity, so this requires having agents on containers that monitor orchestration tools, file integrity, and access control.

Today many companies make a choice between speed and security. That is a false choice. 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.

LACEWORK: AUTOMATED SECURITY AND COMPLIANCE FOR AWS, AZURE, & GCP

Lacework automates security and compliance across AWS, Azure, GCP, and private clouds, providing a comprehensive view of risks across cloud workloads and containers. Lacework's unified cloud security platform 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.



Streamline security for AWS, Azure, and GCP. Gain unmatched visibility, ensure compliance, and enable actionable threat intelligence.

FREE ASSESSMENT