SOLUTION BRIEF

Discover Known and Unknown Threats with Lacework FortiCNAPP and Amazon GuardDuty

Executive Summary

There's an enormous amount of auditable activity in the cloud. This makes threat detection a real challenge. A busy cloud environment can generate 8 to 10 billion data points per month, from Amazon Web Services (AWS) cloud account activities and workload changes to the network-level relationships between your workloads and the public internet. Moreover, in the cloud, where ephemeral servers and containers come and go on-demand, malicious activity can escape detection unless the visibility into events and behaviors is deep and continuous.

Often, gaining this visibility means the security teams will employ a combination of tools, but trying to gain this at cloud scale becomes difficult. Assessing, investigating, and remediating cloud security events from multiple sources requires high operational overhead to tune and the ability to quickly react to changes in the environment. In that situation, it's a struggle to apply security policies consistently across the organization. This creates gaps in security coverage, putting organizations at risk of breach.

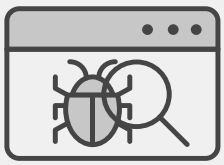
The Importance of Threat Detection

Active intrusion monitoring and alerting are critical to a modern security solution. There isn't a bank in the world without motion sensors and security cameras protecting their vault. Similarly, you can't rely solely on patching misconfigurations if you operate your business-critical applications on the public internet. Identifying and prioritizing existing risks and preventing future attack vectors and vulnerabilities is a big part of securing your cloud. Attackers only need one mistake, one minor misconfiguration, one new vulnerable application package deployed, or some other crack in your defenses to compromise your cloud account. That's a tough challenge when charged with the security of your organization—and your customers.

Knowns and Unknowns

Your security solution must be data-driven, filtering millions or billions of security data points to understand what is normal for you and your unique cloud environments and workloads. The solution must deliver the right, fully contextualized alert at the right time.

The security landscape changes quickly. Attack vectors often exist in the wild before Common Vulnerabilities and Exposures (CVE) databases and best-practice guidelines are updated. This means it is still possible to be breached while you are 100% patched and following all cloud configuration security guidance.



A threat detection solution for your cloud environment must be equipped to:

- Filter the chaos from millions of logged events and remove false positives
- Establish a behavioral baseline for your cloud and data center environment
- Automatically identify deviations from the behavioral baseline and generate real-time alerts if the deviations indicate malicious activity
- Seamlessly scale up and down with your infrastructure
- Provide clear visualization and high levels of contextual correlation for urgent, targeted action on alerts

To reduce the risk of being the target of a zero-day attack, effective security tools use context-heavy behavior baselining and anomaly detection to produce events of concern for analysts to review. Context means understanding what is changing and how those changes relate to your resources. Context is used both to determine activity of interest and to speed up investigation of specific alerts. This allows you to understand whether behaviors are normal and innocuous or abnormal and potentially malicious without having to gather data from additional sources or tools.

Leveraging solutions that are only focused on risk reduction or the likelihood of an attack will leave you exposed with no understanding of your runtime environment during an active breach. And without data correlation that spans across your entire security solution, investigation times will increase significantly as your teams sift through cloud-scale amounts of data.

"Amazon GuardDuty and Lacework FortiCNAPP together give us greater insight and efficiency. Looking at AWS CloudTrail logs can be tedious. The technologies working together have been a huge benefit for our organization"

Russel K.
Information Security Engineer, RapidSOS

Further, Faster

As an AWS customer, you might be utilizing the AWS native tool Amazon GuardDuty. This threat detection service continuously monitors your AWS accounts and workloads for malicious activity and delivers detailed security findings for visibility and remediation. Amazon GuardDuty is good for getting started in your AWS cloud and finding known bad behaviors.

However, you really need to be monitoring for known AND unknown threats, because knowing threats is great, but knowing what you don't know is even better.

Here's where the combined solution of Amazon GuardDuty and Lacework FortiCNAPP makes sense. Amazon GuardDuty enables threat detection on AWS native services, and the Lacework FortiCNAPP platform extends this by providing rich, workload-level data for process and container threat detection, compliance assessments, and user behavior auditability all in one place. In addition, the Lacework FortiCNAPP platform offers deeply integrated, build-through-runtime coverage, enabling comprehensive visibility, risk reduction, and actionable insights. To do this, Lacework FortiCNAPP uses combined techniques of behavioral analytics, unsupervised machine learning, threat intelligence, vulnerability and misconfiguration scanning, and compliance auditing that enables customers to understand risk and vulnerabilities in context across all aspects of the runtime environment, including Linux workloads, servers, containers, cloud account activity, and build time workflows. In summary, the Lacework FortiCNAPP platform is a cloud-native approach to security that provides actionable insights to help you build more securely in the AWS Cloud.

The Lacework FortiCNAPP Platform

- **Delivers behavior-based threat detection**
  With patented technology that uses cloud behavioral analytics, the Lacework FortiCNAPP platform automatically correlates behaviors at scale to find deviations and threats across workloads and cloud and Kubernetes control planes.

- **Continuously ingests data**
  We continuously gather configuration, user, and resource activity data from your environment, not relying solely on sampling or periodic snapshots. We collect data at the host, container, and process level (with or without agents), understanding network connectivity, interactions between resources and cloud services, and how users interact with hosts and applications.

- **Understands your cloud topology and adapts to change**
  The Lacework FortiCNAPP technology builds a view of your cloud topology by automatically grouping system components. This helps you understand how your cloud operates. You can visualize and understand what your applications are doing and how they're interacting. Within one hour, a baseline of normal cloud activity is created by continuously collecting, correlating, and analyzing activity data. The platform automatically learns and tunes itself based on your unique environment.

- **Correlates behaviors**
  Once the baseline is established, it continually monitors for new activity or changes in behavior for early detection of bad actors or compromised credentials or hosts. The Lacework FortiCNAPP platform uses a variety of behavioral models to answer two simple questions: "Is this normal?" and "Should this be happening?" For every service you're running and every behavior we encounter—per cloud account basis, per workload basis, and per user basis—the platform gets smarter. We model resources and interactions at a functional level (applications, processes, privilege changes) to ensure normal cloud changes will not result in false alarms. This approach is much more granular than what native cloud service tools offer. Results are highly tailored to each customer and how they use the cloud.

- **Detects unknown threats**
  The platform uncovers threats that are hardest to detect by continuously monitoring for deviations in user and cloud resource behavior in your unique environment with our FortiCNAPP technology. By automatically learning how your environment operates and finding anomalous behavior, FortiCNAPP can help you can find potential exploits before an attack or vulnerability is known, widely publicized, or patched.

When using Amazon GuardDuty and Lacework FortiCNAPP, all alerts can be consolidated in AWS Security Hub. From Lacework, the integration with Security Hub pushes normalized AWS Security Finding Format (ASFF) like compliance deviations, user and API activity anomalies, software vulnerabilities, and runtime workload protection anomalies. With the ability to view all of your AWS security events from one place, whether from AWS native services or the Lacework FortiCNAPP platform, you can make the most of your response and remediation workflows.

It is undeniable that cloud computing has fueled business growth and increased efficiencies, but, as we've discussed, consistent and effective cloud security is a real challenge. Depending on the maturity levels of your cloud security program and business needs, native tools like Amazon GuardDuty provide a threat detection service that gets an organization started. As you grow, though, you will need an automated, data-driven solution like Lacework FortiCNAPP to complement native security tools that may have become too noisy, siloed, and complicated to manage effectively. The Lacework FortiCNAPP platform on AWS simplifies overall security management while quickly and automatically delivering visibility and actionable insights that truly matter to you and take your business to the next level.

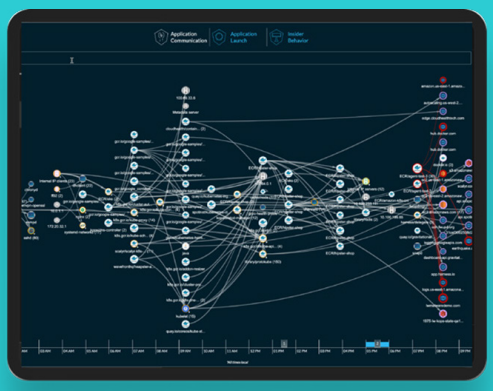
Fortinet Cloud Security empowers organizations to achieve digital acceleration by securing every application journey on any cloud. Delivering consistent policies, centralized management and visibility, and security automation across all clouds and hybrid clouds, organizations can securely build, deploy, and run applications while reducing complexity and increasing effective security and response.

Get started now

Visit Fortinet in AWS Marketplace

Contact awssales@fortinet.com

Visit fortinet.com/AWS for more details, demo videos, white papers, case studies, and customer testimonials.



FORTINET

www.fortinet.com

September 11, 2024 8:55 PM / 2802041-0-0-EN