SOLUTION BRIEF

Find Known and Unknown Threats Faster

React Quickly to Real Cloud Security Threats with Lacework FortiCNAPP

Executive Summary

As organizations increasingly embraced the cloud, cybercriminals saw it as a lucrative target. To curb the subsequent spike in threats, organizations initially deployed their traditional on-premises detection and response solutions to help protect against threats located inside cloud software. However, these "solutions" also introduced a whole new set of problems for security teams.

The security rules that historically powered detection solutions in traditional infrastructures, for example, were no match for dynamic cloud environments. Make the rules too broad, and you'll receive hundreds, possibly thousands, of alerts per day. Make the rules too narrow, and these solutions can't properly function. Security alerts were also of limited use. A lack of alert context made threat investigation a pain. And a lack of prioritization left teams guessing which alerts were most important.

The cloud demands more than what traditional security approaches can offer. Fortinet's cloud-native solution, Lacework FortiCNAPP, uses automation to analyze data from all across your environment and, ultimately, take the pain out of threat detection.

The Lacework FortiCNAPP Solution

The Lacework FortiCNAPP platform offers agentless cloud control plane protection and agent-based workload protection across Amazon Web Services (AWS), Google Cloud, and Microsoft Azure. It also monitors cloud activity in virtual machine (VM) workloads and containerized workloads, including Kubernetes (K8s), Google Kubernetes Engine (GKE), and others. At Fortinet, we can help you reduce threats and gain a comprehensive view across multiple clouds in a single platform.

Lacework FortiCNAPP uses a combined agentless and agent-based approach to gather the right level of information from cloud provider APIs as well as telemetry gathered directly from your workloads. Our agentless solution detects attacks, misuse, and misconfigurations in cloud accounts. At the same time, our lightweight agent-based approach monitors for workload vulnerabilities and known and potential threats related to users, applications, network connections, and files. This method provides greater visibility into your assets and their connections, along with their compliance with industry, governmental, and institutional standards from build time through runtime.

Challenges

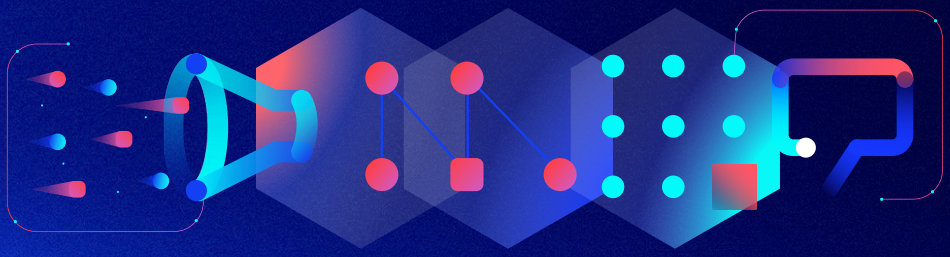
- Legacy tools and non-native cloud solutions are unable to detect unknown, ever-evolving threats.
- Your IT team is drowning in alert fatigue as full alert queues hide critical issues.
- Limited resources and security expertise limit hunts for threats and maintaining security rules.
- Fragmented data across cloud providers, services, and technologies make investigations a pain.

Lacework FortiCNAPP benefits

- Secure by design means your data never leaves your environment.
- Uncovering threats earlier reduces excessive querying and demand for significant expertise.
- Protecting your brand and revenue reduces the severity and scope of a major breach.
- Reducing the time spent managing alerts frees up resources for more strategic work.

The Power of the Lacework FortiCNAPP Platform

The Lacework FortiCNAPP platform ingests data, analyzes behavior, and detects anomalies across an organization's AWS, Google Cloud, Microsoft Azure, and Kubernetes environments without relying on rules. This patented approach significantly reduces noise while turning millions of data points into prioritized, actionable events.



Ingest

The platform collects data via an agentless and agent-based approach on activity related to:

- API calls
- User behavior
- Application launches
- Running processes
- Network behavior

Analyze

The platform's anomaly detection engine uses data to:

- Create groups for analysis
- Create a baseline from activity

Detect

The platform's anomaly detection engine detects changes and risks to:

- Identify unusual behavior
- Identify malware from threat feeds

Inform

Platform visualizations and alerts provide context to:

- Investigate more quickly
- Integrate with response tools

Anomaly Detection

The Lacework FortiCNAPP platform delivers automated anomaly detection to detect threats in multi-cloud environments, whether or not they're known. Its patented anomaly detection technology is fed by multiple distinct data sets, including activity data from an extremely lightweight agent and agentless cloud activity log data from your cloud providers. It also continuously analyzes hundreds of terabytes of data around processes, applications, APIs, files, users, and networks. Machine learning is combined with behavioral analytics to correlate and analyze these disparate datasets, building a baseline for your normal cloud activity. Then, any abnormal activities that fall outside of that baseline are surfaced and labeled based on criticality.

This layered approach discovers new behaviors without the need for human intervention. This data-driven approach to security means that the more data the platform analyzes, the smarter it becomes. This automated intelligence drives better efficacy and a higher return on your investment.

Composite Alerts

Lacework FortiCNAPP composite alerts automatically combine multiple detections to define more specific alert conditions without excessive querying or significant expertise and effort. The platform can accurately detect active cloud attacks by automatically combining multiple low-severity alerts that may often go unnoticed by security teams into a single, meaningful alert.

These composite alerts successfully detect attacks such as cloud ransomware, cryptomining, and compromised credentials. When applicable, composite alerts also integrate Amazon GuardDuty findings to enrich evidence of an ongoing security issue. This allows users to gain greater insights from a single location without the need to correlate data from multiple products.

Alert Context and Visualizations

As threats are surfaced, security event details are provided in a comprehensive event card that displays each event's who, what, why, where, and when. This information includes the username associated with the event, machine details, process-related information, any related alerts, and more. This rich context is sourced and organized from cloud audit and configuration data, workload context from its agent, and agentless vulnerability and security scanning.

These alert cards also include visualizations to arm you with rich context so you can quickly investigate and remediate issues. By analyzing audit logs and workload data, the Lacework FortiCNAPP platform builds detailed visualizations that track network, application, process, and user activities across hosts. Security analysts can then zero in on suspicious activity, trace an intruder's steps, and remediate the situation.

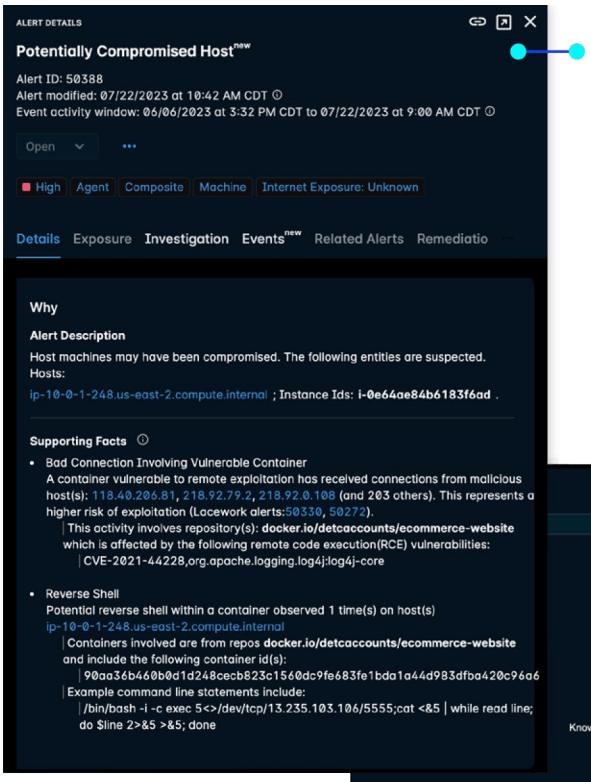


Figure 1: Lacework FortiCNAPP composite alerts combine multiple low-severity alerts into a single high-severity alert, pointing to potential malicious activity.

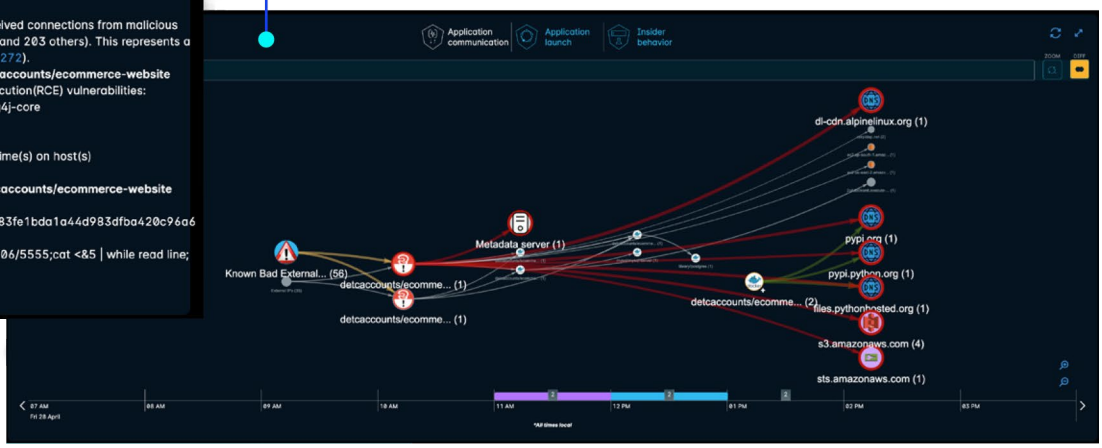


Figure 2: Lacework FortiCNAPP maps all activities and communications throughout your cloud environment. These visualizations automatically highlight any anomalous activities hour by hour and can track cloud exploits from the malicious source through the vulnerability to any affected cloud entities.

Continuous File Integrity Monitoring

The Lacework FortiCNAPP platform can monitor changes in files and directories in near real-time. Lacework FortiCNAPP users can choose to watch for file or directory creation, deletion, modification, and move or attribute changes in specific folders or files. This way, security analysts can monitor critical files or directories for change control, files for indications of tampering, and directories for evidence of malware activity.

A Deep Network of Integrations

Lacework FortiCNAPP is easy to operationalize due to its extensive roster of integrations with other workflow tools. Our integration partners include (but are not limited to):

- Monitoring and logging tools (such as Splunk, Snowflake, and New Relic)
- Incident response and ticketing tools (such as Splunk, Jira, PagerDuty, and ServiceNow)

- Messaging tools (like Slack)
- Remediation and compliance tools (for example, Kaholo and Tines)
- Developer tools (Buildkite, Puppet, Chef, and Hashicorp)

Each alert within Lacework FortiCNAPP is actionable because of its detailed alert context. The platform integrations ensure that each actionable alert is seamlessly routed to the right tools for the next steps.

Customer outcomes

- 100:1 reduction in alerts
- 95% reduction in false positives
- 90% reduction in manual cloud security tasks
- 81% of customer see value in <1 week

Why Lacework FortiCNAPP?

Prioritize cloud security risks with visibility and context

Quickly gain complete visibility into deployments, configurations, and workloads to pinpoint and prioritize the most critical vulnerabilities and misconfigurations for remediation.

Find known and unknown threats faster

Discover threats within your dynamic cloud environment with anomaly detection and threat intelligence. Gain rich context surrounding each alert to promptly investigate and remediate cloud security issues.

Increase operational efficiency

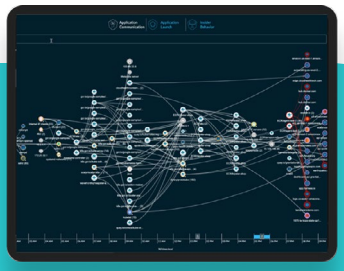
Accomplish more with less and know where to focus. Lower the total cost of ownership through a single platform and improve time to value with automated, DevOps-friendly cloud security.

Achieve continuous compliance

Prove and maintain continuous compliance across your entire cloud estate for requirements like SOC 2, ISO 27001, HIPAA, and more. Automate audit requests and free up time for high-value security tasks.

Ready to chat?

REQUEST A DEMO



FORTINET

www.fortinet.com

August 1, 2024 6:16 PM / 2802111-0-0-EN