FORTINET

SOLUTION BRIEF

4 Keys to Simpler SecOps Across Clouds

Executive Summary

SecOps difficulties remain high. The benefits of the cloud are undeniable: cost efficiency, limitless scale, ubiquitous access, and high application availability. Yet security has always been a trade-off. The cloud's limitless scale allows companies to expand or shrink their environments based on need. But it also means a growing attack surface with more ways for attackers to gain entry.

No one ever assumed cloud security would be easy. But now, decades into cloud adoption, research suggests cloud security difficulty is still high. A recent study by the Enterprise Strategy Group (ESG) indicates that 51% of SecOps practitioners and application developers believe that security operations are either as difficult or more difficult than they were 24 months ago.[1]

Respondents expressed frustrations with applying legacy tools and processes to an ever-changing cloud environment. But the research also supports four key reasons why Lacework can better support SecOps teams and move the needle in a positive direction.

Gain Full Visibility as Your Environment Grows or Shrinks

According to ESG, one of the most cited contributors to SecOps difficulty is the ever-changing, growing attack surface (chosen by 30% of respondents).[2] Visibility has been an issue in cloud security for some time. As organizations move data and applications to the cloud, they often lose oversight over their information. In these blind spots, threats can lurk, vulnerabilities can hide, and misconfigurations can go unnoticed.

With Lacework FortiCNAPP, organizations like yours can use agentless data ingestion to prioritize your environment's most critical vulnerabilities and misconfiguration within minutes. Organizations can then deploy the platform's lightweight agent into cloud environments to gain runtime visibility. This data is automatically analyzed, and insights from both build and runtime are served up in a single dashboard, providing full, effortless visibility into a cloud environment.

Use Automation to Efficiently Scale Operations

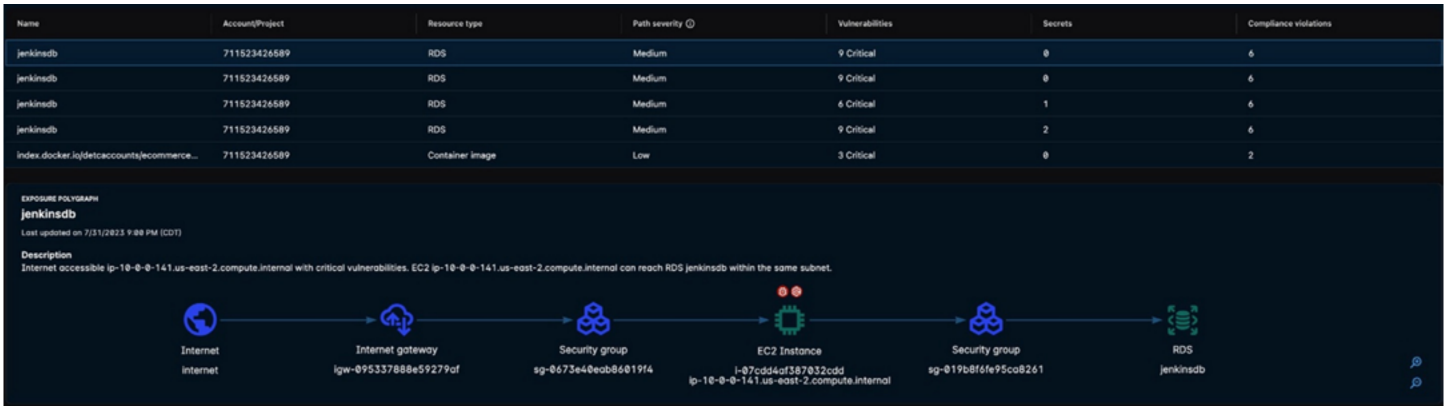
According to the study, the top contributor to SecOps difficulty is the lack of automation for complex cybersecurity tasks (chosen by 32% of respondents). Modern cloud security requires cybersecurity teams to piece together data points from across a myriad of sources. However, without automation, it's simply not possible for these bandwidth-deprived teams to perform these tasks adequately at scale.

Challenges

- The attack surface has grown and is continuously changing.
- Security operations are based on manual processes and can't scale.
- Gaps in security monitoring tools and processes increase risk.
- Teams can't develop detection rules in a timely manner.

Lacework solutions

- Gain full visibility into your cloud environment in minutes.
- Use automation to streamline and scale SecOps use cases.
- Close security gaps with a single, interconnected platform.
- Employ anomaly detection to detect threats, with or without rules.



Name	Account/Project	Resource type	Path severity ⓘ	Vulnerabilities	Secrets	Compliance violations
jenkinsdb	711523426589	RDS	Medium	9 Critical	0	6
jenkinsdb	711523426589	RDS	Medium	9 Critical	0	6
jenkinsdb	711523426589	RDS	Medium	6 Critical	1	6
jenkinsdb	711523426589	RDS	Medium	9 Critical	2	6
index.docker.io/detcaccounts/ecommerce...	711523426589	Container image	Low	3 Critical	0	2

EXPOSURE POLYGRAPH

jenkinsdb

Last updated on 7/31/2023 9:00 PM (CDT)

Description

Internet accessible ip-10-0-0-141.us-east-2.compute.internal with critical vulnerabilities. EC2 ip-10-0-0-141.us-east-2.compute.internal can reach RDS jenkinsdb within the same subnet.

Figure 1: See all possible attack paths, prioritized in one place.

The Lacework FortiCNAPP platform offers automation that covers the entire software development life cycle (SDLC) and even precedes application development. With Lacework Infrastructure-as-Code (IaC) security, developers can see and address security and compliance issues as cloud environments are being built and configured. Security teams also have visibility into IaC issues through the Lacework dashboard, alongside all other risk and threat information.

Lacework FortiCNAPP uses automation to make risk management more efficient. Our platform analyzes your cloud data and automatically prioritizes which cloud risks are most critical. It can determine which vulnerabilities are tied to active software packages and prioritize these fixes. The platform can prioritize your top risks using attack path analysis, which ties together disparate risks and creates an attacker's roadmap from the internet to your crown jewels.

During runtime, our automation can drastically enhance threat detection and investigation. Our platform features patented tools that detect abnormal cloud behaviors, with or without rules. For example, our platform detected activity tied to the Log4j vulnerability before the risk was publicly disclosed. Lacework FortiCNAPP features composite alerts, which tie together disparate, low-severity alerts occurring in succession that may indicate more severe security activity like compromised credentials or cloud ransomware.

Lacework FortiCNAPP helps companies:

- Prioritize cloud risks through visibility and context
- Find known and unknown threats faster
- Do more with their existing security teams
- Achieve continuous cloud compliance

Close Security Gaps with a Single Platform

In the ESG report, 28% of respondents indicated that security gaps caused by disparate tools and processes were a significant source of SecOps pain.[3] Recent studies indicate that the average organization works with 10 to 15 security vendors and 60 to 70 security tools.[4]

Each new tool has a different dashboard, a fresh learning curve, a siloed data set, and a new licensing cost. During incident investigation, SecOps teams are forced to manually piece insights together across multiple interfaces. And, as the ESG survey data suggests, even with multiple solutions in place, organizations can't easily detect or respond to threats or attacks in time to prevent incidents or efficiently respond to mitigate their impact. At what point do these "solutions" actually become problems?

In 2021, Gartner created a new security category called the cloud-native application protection platform (CNAPP), where a single platform would secure cloud applications from development through production. Gartner predicted that by 2025, 60% of enterprises will consolidate posture management and workload protection to a single platform.[5]

With Lacework FortiCNAPP, Fortinet offers a single CNAPP platform that ingests data through agentless and agent-based means to efficiently handle cloud security. The platform is more than a collection of loosely integrated functions under a single umbrella; it automatically correlates data across build time and runtime to augment existing security teams.

For example, with active vulnerability detection, the platform can tie vulnerabilities to active software packages to better help teams prioritize issues. With traditional cybersecurity, this data would have been siloed within different tools. However, now, it's possible to benefit from analyzing this data in one place, within a single platform.

Become Less Dependent on Rules and Signatures

According to ESG, 26% of respondents cited difficulty developing security rules in a timely manner as a primary source of SecOps frustration.[6] Reliance on rules and signatures may have worked traditionally; however, to be effective in the cloud, threat rules need to be constantly tweaked and maintained.

Rule maintenance is a balancing act. If the rules are too broad, organizations will be overloaded with false positive alerts. If they're too narrow, they won't detect any cloud threats. On top of that, teams need to consider that rules and signatures only detect known threats, leaving organizations vulnerable to any unknown, never-before-seen malicious activity.

As the ESG study suggests, rule writing and maintenance takes time; it can be easy for SecOps teams to constantly feel like they're catching up from behind. Lacework takes a different approach. Rather than relying solely on rules, our platform features patented ML-based anomaly detection. This technology automatically builds a baseline for normal behavior in your environment and flags any abnormalities.

Organizations can still write and maintain rules within the Lacework FortiCNAPP platform if desired. However, since our platform doesn't solely rely on these rules, SecOps teams no longer have to feel like they're catching up from behind. Threats will be flagged regardless of whether or not a rule has been developed for them.

"By adopting a single platform, we fully eliminated five tools, which has saved us valuable time and reduced our costs."

Hans-Michael Odenthal
Systems Expert
AOK Systems GMBH

"I've been in the industry for many years. When we sat down with our infrastructure and DevOps teams to review Lacework FortiCNAPP, that was the only time I've ever seen all of the teams agree on a solution."

John Turner
Senior Solutions Architect
LendingTree

Why Lacework FortiCNAPP?

- Gain complete visibility into risks and threats with a single integrated platform covering the entire SDLC and control and data planes.
- Have coverage across all hyperscale cloud providers, Kubernetes, hosts, containers, and more.
- Leverage a range of capabilities, including threat detection, vulnerability and configuration checks, compliance reporting, IaC security, and more.
- Speed investigations with Polygraph visualizations to better understand what happened before, during, and after a specific event.
- Leverage remediation guidance to quickly act on issues uncovered.

Customer Outcomes

John Turner, senior security architect at LendingTree, was able to reduce alerts for his organization by 90%. "Lacework FortiCNAPP helped us deal with the firehose of information we were getting out of our cloud environment."

Mario Duarte, director of security at Snowflake, was able to reclaim hours of his team's time every day. "Lacework FortiCNAPP has freed up my team from spending two to three hours a day configuring, tweaking, and looking at alerts to less than 15 minutes. It's freed up so much time to do other things that are security related."

Bren Briggs, VP of DevSecOps at Hypergiant, successfully deployed Lacework FortiCNAPP across 30+ AWS accounts in two hours. "The effort-to-pay-off ratio was fantastic. I've never had an easier-to-install product. In under two hours, I was done deploying it, had a multi-account CloudTrail, and had completely aggregated all the CloudTrail for 30+ AWS accounts. How much easier can it be?"

[1] Cloud Detection and Response: Market Growth as an Enterprise Requirement, Lacework, July 2023.

[2] Greenberg, Karl. "Cloud Security, Hampered by Proliferation of Tools, Has a 'Forest for Trees' Problem," TechRepublic, March 13, 2023.

[3] 2023 Gartner® Market Guide for Cloud-Native Application Protection Platforms (CNAPP), Lacework, 2023.

[4] Gartner, Simplify Cybersecurity With a Platform Consolidation Framework, 26 March 2024.

[5] 2023 Gartner® Market Guide for Cloud-Native Application Protection Platforms (CNAPP), Lacework, 2023.

[6] Cloud Detection and Response: Market Growth as an Enterprise Requirement, Lacework, July 2023.

Continue the Conversation

REQUEST A DEMO

www.fortinet.com