SOLUTION BRIEF

Efficient Cloud Security Risk Management

Prevent Exploits by Fixing Your Biggest Issues First

Executive Summary

Most cloud risk management solutions only go so far. Identification alone isn't enough. In a world where the U.S. government's National Vulnerability Database (NVD) holds over 200,000 vulnerabilities, 18,000 of which are listed as critical, modern security tools must go further. In a study conducted by the Enterprise Strategy Group, 38% of respondents indicated that the biggest challenge with security operations was having to prioritize a growing number of security alerts.[1]

Identification is only step one. Prioritization is the key. The Lacework FortiCNAPP platform automatically correlates data from build to runtime to help organizations prioritize the top issues specific to their environments. Our single platform provides a consolidated, actionable source of cloud security truth so that security, operations, and developer teams can ensure they're fixing risks that matter.

The Lacework FortiCNAPP Solution

The Lacework FortiCNAPP platform analyzes risks and threats from all major cloud service providers and Kubernetes configurations. It addresses multiple cloud security use cases without ever putting your data at risk. Lacework FortiCNAPP is also secure by design, which means that, unlike other cloud security providers, it can analyze your data without ever leaving your environment.

The platform can assess and continuously monitor your cloud infrastructure and applications, find weak spots, and prevent risks from being deployed into production. With Lacework FortiCNAPP, you can quickly gain complete visibility into what is deployed, what has been added, and how it is configured. Users can also see which vulnerabilities are tied to running workloads to effectively eliminate up to 90% of critical vulnerabilities in your cloud environment.

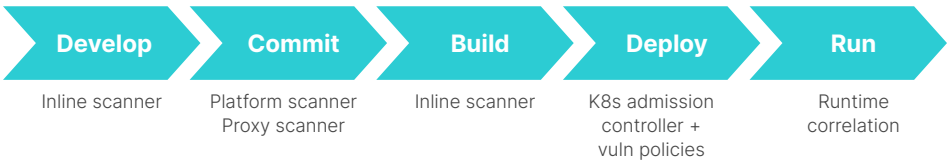


Figure 1: Lacework FortiCNAPP detects and prioritizes vulnerabilities throughout the software development life cycle.

Challenges

- Inability to prioritize fixes leads to confusion and burnout
- Delegation of inactive vulnerabilities hurts trust with developer teams
- Lack of context makes remediation difficult
- Post-deployment risk fixes result in higher costs

Lacework benefits

- Secure by design: Your data never leaves your environment
- Reduce risk and exposure and minimize impact due to security incidents
- Increase employee productivity and focus on meaningful work
- Innovate with speed and security and address issues pre-production

Vulnerability Management

The Lacework FortiCNAPP platform can identify your cloud vulnerabilities and then surface those risks that matter most to your unique environment. With its agentless workload scanning, FortiCNAPP allows security teams to detect vulnerabilities across active hosts, containers, and application language libraries. Security teams can then tie these vulnerabilities to active workloads to ensure they're not prioritizing vulnerabilities that will not reduce their environment's overall risk.

The platform assigns each vulnerability a proprietary risk score that combines your data with third-party risk data to surface your most critical risks. This risk score takes your vulnerabilities and then automatically applies a number of filters to find your most serious issues. The platform determines which vulnerabilities are internet exposed, which are being actively exploited in the wild, and which are tied to running software. What's left? The one in 10 vulnerabilities that actually matter.

Lacework FortiCNAPP covers vulnerability detection during build, ship, deployment, and runtime. It also offers shift-left security capabilities to ensure vulnerabilities are fixed before reaching production. Inline scanning detects and reports on vulnerability risks within CI/CD pipelines and offers remediation guidance on how to resolve these issues before they become bigger problems.

Cloud Security Posture Management

Lacework FortiCNAPP helps you automatically inventory cloud resources and understand your risk posture, even as configurations change. It also continuously assesses and validates compliance against industry best practices like NIST and CIS and uncovers discrepancies between your current state and regulations like SOC 2, ISO, HIPAA, and more.

Within minutes of deployment, you can easily check for policy violations, catch misconfigurations, and automate compliance reporting from a single platform. With custom compliance assessment, you can create policies and define how configurations and access controls should behave in your cloud operating model. Lacework FortiCNAPP also offers Infrastructure-as-Code security, which allows developers to build within guardrails determined by the security team and remediate any issues with one click.

Attack Path Analysis

Lacework FortiCNAPP attack path analysis combines insights from cloud audit and configuration data, workload context from our lightweight agent, and agentless vulnerability and security scanning to provide context for any anomaly or policy-related event. Agentless scanning capabilities can also point out exposed data assets (such as RDS databases and S3 buckets), compliance violations, and hard-coded secrets like SSH private keys exposed on a host.

These factors are all combined into a single visualization, referred to as an Exposure Polygraph, that maps out real ways attackers can exploit your environment and reach your critical data assets. This way, security professionals can quickly determine if a host is affected, which entities are exposed to the internet, whether compliance violations exist, and more.

Customer outcomes

- 76% of respondents in a customer survey identified CSPM functionality as the top factor that led them to choose Lacework
- 86% of respondents to a customer survey agreed: With Lacework FortiCNAPP, I gain a complete understanding of my cloud environment and the actions needed to improve my security posture
- 81% of respondents to that survey also saw value within one week of deploying the Lacework FortiCNAPP platform

"We turned Lacework FortiCNAPP on and immediately started seeing the things in our environment that we wanted to know about. Our DevOps engineers saw it in action and fell in love. They couldn't believe it was so simple."

David Ramsay
Head of Engineering
COO, DECTA

All attack paths within a cloud environment are listed within a dedicated attack path dashboard and prioritized based on several factors, including the value of the data assets at risk. Users can also see their most at-risk hosts, container images, data assets, and attack paths with exposed secrets from a single dashboard. This way, teams can focus on fixing the items within their cloud environment that will have the most impact.

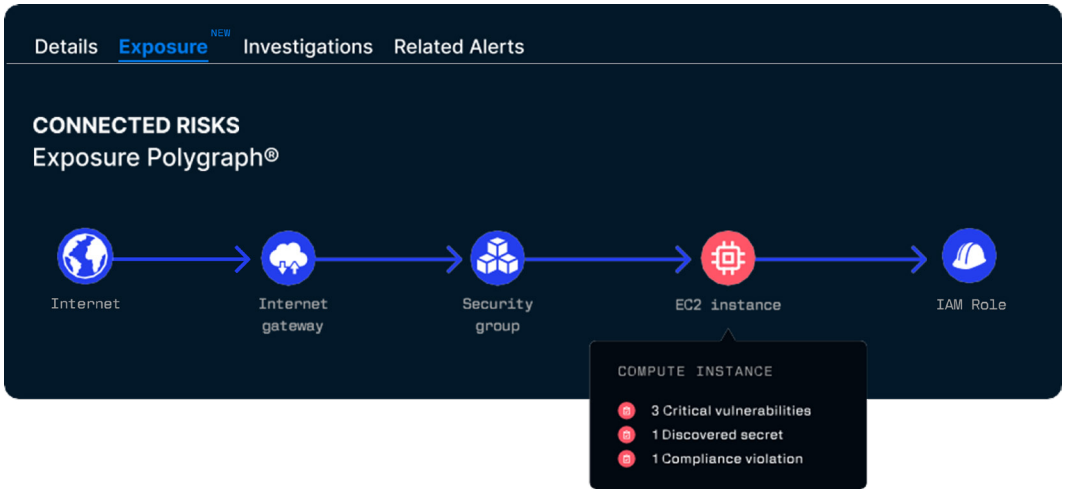


Figure 2: Exposure Polygraph visualizations map different ways attackers can enter a cloud environment and access data assets.

Cloud Infrastructure Entitlement Management

In the cloud, identity is the new perimeter. Pressure to innovate rapidly leaves many identities over-privileged. There's no easy solution. AWS, Google Cloud, and Azure alone have over 35,000 different unique permissions (and counting). In the cloud, human and non-human resources need the appropriate access to perform certain tasks. Even with decent cloud visibility, many companies can't see all their identity-related risks and have no idea how to get the needle moving in the right direction.

Lacework FortiCNAPP grants security teams the visibility and context necessary to prioritize and right-size their most at-risk cloud identities. Organizations gain continuous visibility into all cloud identities, know precisely who can perform what actions, easily see which identities pose the greatest risk, and understand what has changed over time. Users can also know which identities are over-privileged by seeing which entitlements each cloud identity is actually using. Users can then receive detailed recommendations on how to right-size the most critical cloud identities.

> *"It's not just having all the context, but also presenting it in a way that we can easily digest. There are millions of things that can be associated with a security event, and Lacework pulls out four or five of those to give an engineer or analyst an obvious next step."*
>
> **Steve Lukose**
> Director of Security Engineering
> CLARI

A Safety Net for Better Defense

Even the best defenses are fallible. When it comes to security posture, you should put your best foot forward. But what happens when an exploit happens?

Fortinet has you covered. The Lacework FortiCNAPP platform is built around its industry-leading threat detection capabilities. Lacework FortiCNAPP offers both agentless cloud control plane protection and agent-based workload protection.

With the Lacework FortiCNAPP platform, you get:

Composite alerts: Lacework FortiCNAPP composite alerts detect active cloud attacks by automatically correlating disparate alerts, including lower-severity security events that may otherwise go unnoticed. Fortinet customers receive high-fidelity composite alerts flagging compromised credentials, cloud ransomware, cloud cryptomining, and more. These alerts can also consider Amazon GuardDuty findings when building evidence for suspected threats.

Known and unknown threat detection: Lacework FortiCNAPP takes data from across your cloud and automatically builds a baseline for normal activity in your environment. It then automatically surfaces any concerning abnormalities, which means threats are uncovered in your cloud environment whether or not they're tied to known rules.

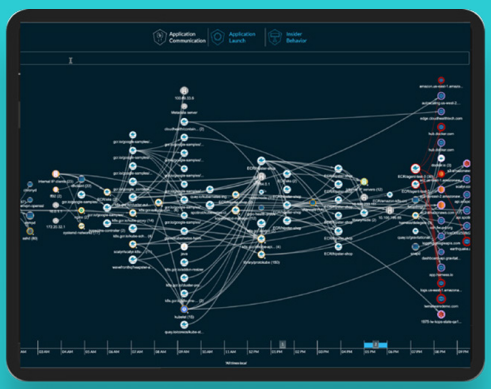
Detailed cloud activity visualizations: By analyzing audit logs and workload data, the Lacework FortiCNAPP platform builds detailed visualizations that can track network, application, process, and user activities across hosts. Security analysts can then zero in on any suspicious activity, trace an intruder's steps, and remediate the situation.

A lightweight, proven cloud-optimized security agent: The Lacework FortiCNAPP agent was built for the cloud—not retrofitted to the cloud from legacy systems—which means it's lightweight, scalable, proven, and requires little to no user maintenance.

See it in action.

REQUEST A DEMO

READ ABOUT OUR LAYERED SECURITY APPROACH



[1] Enterprise Strategy Group, a division of TechTarget, Inc. Research Survey, Cloud Detection and Response: Market Growth as an Enterprise Requirement, July 2023.

FORTINET

www.fortinet.com

July 30, 2024 11:44 AM / 2803810-0-0-EN