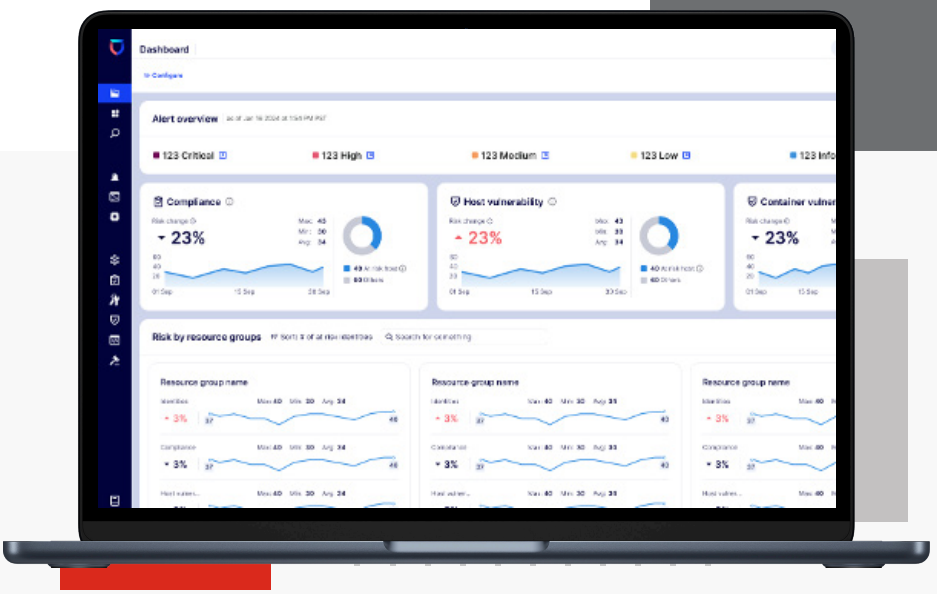
Lacework FortiCNAPP



Key Lacework use cases

- Automated threat detection that eliminates the need to write and maintain rules
- Build time and runtime vulnerability management across hosts and containers, plus risk scores to help with prioritization
- Configuration assessments and checks for compliance standards like SOC2, ISO 27001, HIPAA, HITRUST, PCI, NIST, FISMA, PII, and CIS Benchmarks

Simplifying security for multicloud and hybrid environments

Overview: securing your cloud environments

Adopting cloud architectures can be transformative, allowing for greater flexibility, efficiency, speed, and innovation. But these benefits come with a new set of challenges. Cloud environments are complex and dynamic by nature, which means that legacy security approaches can't offer adequate protection from configuration errors, vulnerabilities, and threats.

For any combination of Amazon Web Services (AWS), Google Cloud, Microsoft Azure, or Kubernetes that you're using, it's important to protect your business by securing your cloud accounts and workloads. Lacework partners with you to address these concerns by offering an automated, end-to-end security solution for multicloud and hybrid infrastructures that is global, secure, and trusted. We monitor for threats to workloads and accounts across your multicloud and containerized environments. With Lacework, you can keep your data and resources safe.

Challenges: minimizing risks in multicloud

There are many reasons to prioritize the security of your multicloud environment. Cyberattacks can be harmful for your business and your data, costing money and compromising customer trust. No matter the size of your security team, manual monitoring can be slow, eating up your valuable time. And whether you are in a regulated space or your customers require it, the continuous need to prove compliance can be time-consuming – not to mention expensive. Luckily, Lacework is here to help with all of this, and more. We automatically find true threats, which reduces your false positives and alerts to help you stop danger in its tracks.

Our Approach

Available in

Cloud

A data-driven solution

Lacework reduces risks with a data-first approach. We begin by collecting the most important information: gathering data through our combined agentless and agent-based approach. Our agentless approach collects the data to build a complete multicloud asset inventory across accounts and services, while our agent collects data on cloud compute resources. Through cloud service provider logs, we continuously observe your cloud resources, monitoring the behavior of users, apps, processes, and networks to identify indicators of compromise.

Once the initial data is collected, Lacework moves on to detection so we can find the greatest risks to your business, including misconfigurations and vulnerabilities. For runtime threats, Lacework surfaces indicators of compromise based on unusual activity through our patented Polygraph® Data Platform. We can find vulnerabilities throughout your build time and runtime processes, identify cloud misconfigurations in cloud resources like storage services, and discover issues that concern cloud best practices as well as compliance requirements.

Finally, we tell you what we discovered, so you can decide how best to proceed. Lacework surfaces only the most critical risks, eliminating alert fatigue, and provides context-rich visualizations and notifications so you can take quick action. We also offer comprehensive reporting to help you prove compliance. And by integrating with ticketing, messaging, SIEM, and more, we allow you to solve issues more efficiently.

Use Cases

Advanced protection for multicloud environments

Lacework provides a modern security solution for the modern cloud. Not only do we help you ensure continuous compliance and protect your data from unauthorized exposure, but we do it all in a way that requires minimal maintenance. We offer more protection with less hassle.

Configuration assessment

Understand your configurations with Lacework, which lets you automatically find, monitor, and inventory all assets across your multicloud environments. Simplify your configuration assessment process by leveraging just one platform to easily track configuration changes, find vulnerabilities, and detect threats. We also provide a consolidated view to all team members who might not otherwise have access to your consoles for the cloud providers that you use.

Cloud and industry compliance audits

In addition to helping with configuration assessment, Lacework allows you to check your environment against industry standards. We audit your configuration daily and alert you of any concerning changes, ensuring continuous compliance in your multicloud environments. Lacework can help you meet compliance standards including SOC2, ISO 27001, HIPAA, HITRUST, PCI, NIST, FISMA, PII, and CIS Benchmarks. Not only do we generate reports in formats like PDF and CSV, giving you context-rich recommendations to help with all your audits, but we also integrate with tools like Jira and Slack to accelerate your remediation efforts.

Lacework also offers the latest and greatest Center for Internet Security (CIS) Benchmarks for AWS, Google Cloud, and Azure, which enables you to assess your security posture according to industry best practices, as well as measure security improvements over time. During container image development and container deployments, we scan across CIS Benchmarks for secure configurations for cloud accounts and workloads.

> *" [Before Lacework] we would need to combine three different security solutions together to get the right coverage across Kubernetes, Google Cloud, and AWS. We needed a platform that could centralize every aspect of our security approach."*
>
> NABIL MISSOUM, DEVSECOPS
>
> ENGINEER, AB TASTY

Threat detection

Reduce alert noise and surface only the most critical events with Polygraph anomaly detection support for multicloud. Lacework gives you actionable alerts so you can stay on top of behavior changes in your environment, offering automatically built and updated baseline models of a data center's behavior. We'll alert you to all kinds of anomalous behavior, such as a process communicating with an external IP address for the first time ever. And we're flexible: our automated detection lets you cut down on writing rules, while giving you the ability to create custom policies when you need to.

Vulnerability management

With our end-to-end vulnerability management, Lacework helps you identify vulnerabilities sooner, making it easier for you to proactively manage risks across your hosts and containers. We continually assess container images and hosts for new vulnerabilities, as well as changes to existing ones. Plus, once we've identified which vulnerabilities pose the greatest risk to your multicloud environment, we provide you with a risk score so you can decide what to prioritize.

Why Lacework?

- Assess vulnerabilities at both build and runtime with continuous monitoring
- Detect abnormal activity during runtime, even before a vulnerability is identified, without requiring rules
- Speed investigations with Polygraph visualizations to better understand what happened before, during, and after a specific event

Customer outcomes

- Reduced costs and consolidated technology from several security vendors
- Gained deep visibility across cloud environments
- Improved productivity by investigating alerts 4x faster than before
- Grew business value while preparing for compliance audits
- Reduced risk by building security into the development process

> *"We're currently running agents in AWS, but we're looking to extend the same thing to Google Cloud. We're also looking into Azure, so we will want to leverage Lacework there as well. It will be interesting when we adopt Azure to see how much time we shortcut. Lacework will help guide us and provide evidence that we're doing the right things to secure the Azure cloud."*
>
> JOSH BEEMSTER, HEAD OF TECHNICAL OPERATIONS, AND
>
> STEVE COPPIN-SMITH, VICE PRESIDENT OF ENGINEERING, SNOWPLOW

Technical Specifications

ENVIRONMENTS SUPPORTED				
Amazon Services	Amazon CDK Amazon Control Tower Amazon EC2 Amazon EKS	Amazon ECS (EC2) Amazon ECS Fargate Amazon EKS Fargate Amazon Linux	Amazon Linux AMI Amazon Systems Manager (SSM Agent)	✓
Google Services	Google Kubernetes Engine (GKE) Standard	Google Anthos		✓
Azure Services	Azure Kubernetes Services (AKS)			✓
Technologies/OS	ARM64 Docker Docker Swarm Kubernetes Kubernetes Helm Kustomize	CentOS Container Linux by CoreOS CoreOS Debian Fedora	Kali Oracle Linux Red Hat Enterprise Linux Scientific SUSE Ubuntu	✓
Container Registries	Amazon Elastic Container Registry (ECR) Docker Hub	Docker V2 Registry Github Container Registry	Google Artifact Registry (GAR)	✓
Container Runtimes	Containerd	Docker		✓
CI/CD Tooling – Automation and Pipelining	Ansible BuildKite Chef	CircleCI Github Harness	Jenkins Spinnaker Terraform	✓
Integrations – SIEM/ Alerting/Ticketing/ Performance	ArcSight (Microfocus) AWS CloudWatch Cisco Webex Teams Datadog Elastic/ELK Stack Google Pub/Sub	IBM QRadar JIRA Microsoft Teams New Relic OpsGenie PagerDuty	ServiceNow Slack Splunk Sumo Logic VictorOps Webhook	✓

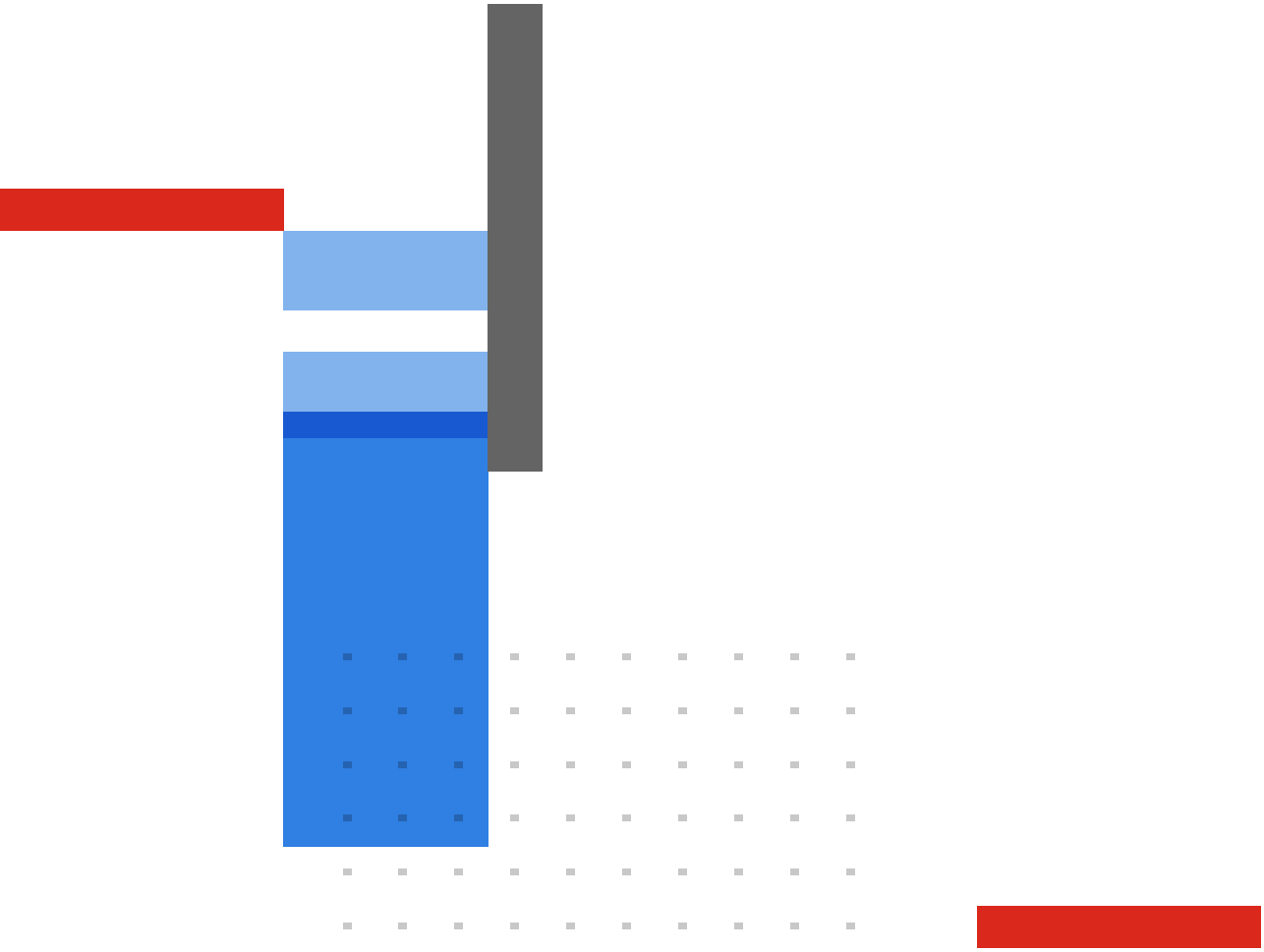
Ordering Information

Product	SKU	Description
Standard	FC1-10-LACWK-1063-02-12	1 Year Lacework FortiCNAPP - Standard tier. Entitlement per-vCPU.
	FC1-10-LACWK-1063-02-36	3 Year Lacework FortiCNAPP - Standard tier. Entitlement per-vCPU.
	FC1-10-LACWK-1063-02-60	5 Year Lacework FortiCNAPP - Standard tier. Entitlement per-vCPU.
Pro	FC1-10-LACWK-1064-02-12	1 Year Lacework FortiCNAPP - Pro tier. Entitlement per-vCPU.
	FC1-10-LACWK-1064-02-36	3 Year Lacework FortiCNAPP - Pro tier. Entitlement per-vCPU.
	FC1-10-LACWK-1064-02-60	5 Year Lacework FortiCNAPP - Pro tier. Entitlement per-vCPU.
Enterprise	FC1-10-LACWK-1065-02-12	1 Year Lacework FortiCNAPP - Enterprise tier. Entitlement per-vCPU.
	FC1-10-LACWK-1065-02-36	3 Year Lacework FortiCNAPP - Enterprise tier. Entitlement per-vCPU.
	FC1-10-LACWK-1065-02-60	5 Year Lacework FortiCNAPP - Enterprise tier. Entitlement per-vCPU.

Visit https://www.fortinet.com/resources/ordering-guides for related ordering guides.

Fortinet Corporate Social Responsibility Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy.



FORTINET

www.fortinet.com

September 10, 2024

FCNAPP-DAT-R01-20240910