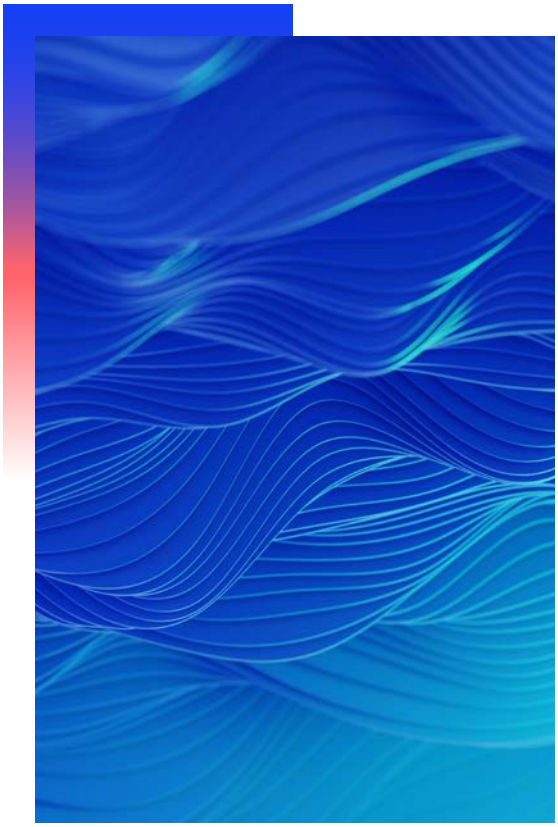
FEATURE BRIEF

Agentless workload scanning

OVERVIEW
What is the feature?

Lacework provides a simple, frictionless way to gain comprehensive visibility into risks across cloud workloads, without requiring an agent. Our new agentless scanning provides organizations with more flexibility and choice in how they scan and detect vulnerabilities and exposed secrets across their active hosts, container images, and application language libraries. They can understand what is actively running in their cloud environment and prioritize their vulnerability work items to improve their overall security posture. By combining this approach with agent-based runtime insights, organizations can collect more data about their environment in the most effective way possible for maximum value and security.



Benefits

- **Simple, frictionless deployment**
  Achieve a faster time to value while reducing risk. Connecting cloud accounts to Lacework easily operationalizes security across your entire environment.
- **More flexibility and choice to gain broader scan coverage**
  Efficiently scan and detect vulnerabilities and exposed secrets across all hosts, containers, and application language libraries for comprehensive visibility into risks.
- **Easy-to-build layered security**
  Monitor all critical file changes, plus identify and get optional alerts on new, changed, malicious, and non-package-installed files.

VALUE

Why is the feature important?

With the dynamic nature of cloud environments, organizations need more flexibility and choice to secure their workloads at scale. While agents provide the best level of continuous monitoring and security, they may not be feasible — or even preferred — in every customer situation. For some customers, it may be enough to simply assess the risk of their environment. For others, continuous monitoring and runtime insights are required for threat detection and investigation. Consider, too, the different priorities of security, development, and platform teams. From triaging incidents to building faster to managing organizational infrastructure, everyone has a unique role that a one-size-fits-all approach can't encompass.

What challenges does this feature solve?

- **Increased threats and attack surface**
  Ephemeral workloads, containers, and serverless functions are being added and removed at a rapid speed. Vulnerabilities and exposed secrets hidden in source code and services can lead to major breaches.
- **Complex environments and hard-to-reach workloads**
  While agents provide deeper insights, they are not always operationally feasible. Sometimes, organizations need a frictionless way to perform a quick assessment of risks across an entire environment.
- **Different personas and priorities lead to organizational friction**
  Teams need to strike a balance between patching every vulnerability and keeping applications and infrastructure up and running, which can cause conflict.
- **One formula does not fit all use cases**
  Specific business and security needs can vary widely, requiring different methods to collect all relevant data about cloud environments.

DEPLOYMENT

How is the feature implemented?

Your security administrators connect your cloud accounts to Lacework with a simple, one-time deployment use cloud-native capabilities (e.g., CloudFormation). Businesses leveraging AWS Organizations can leverage cloud-native capabilities to provision the necessary infrastructure to all regions.

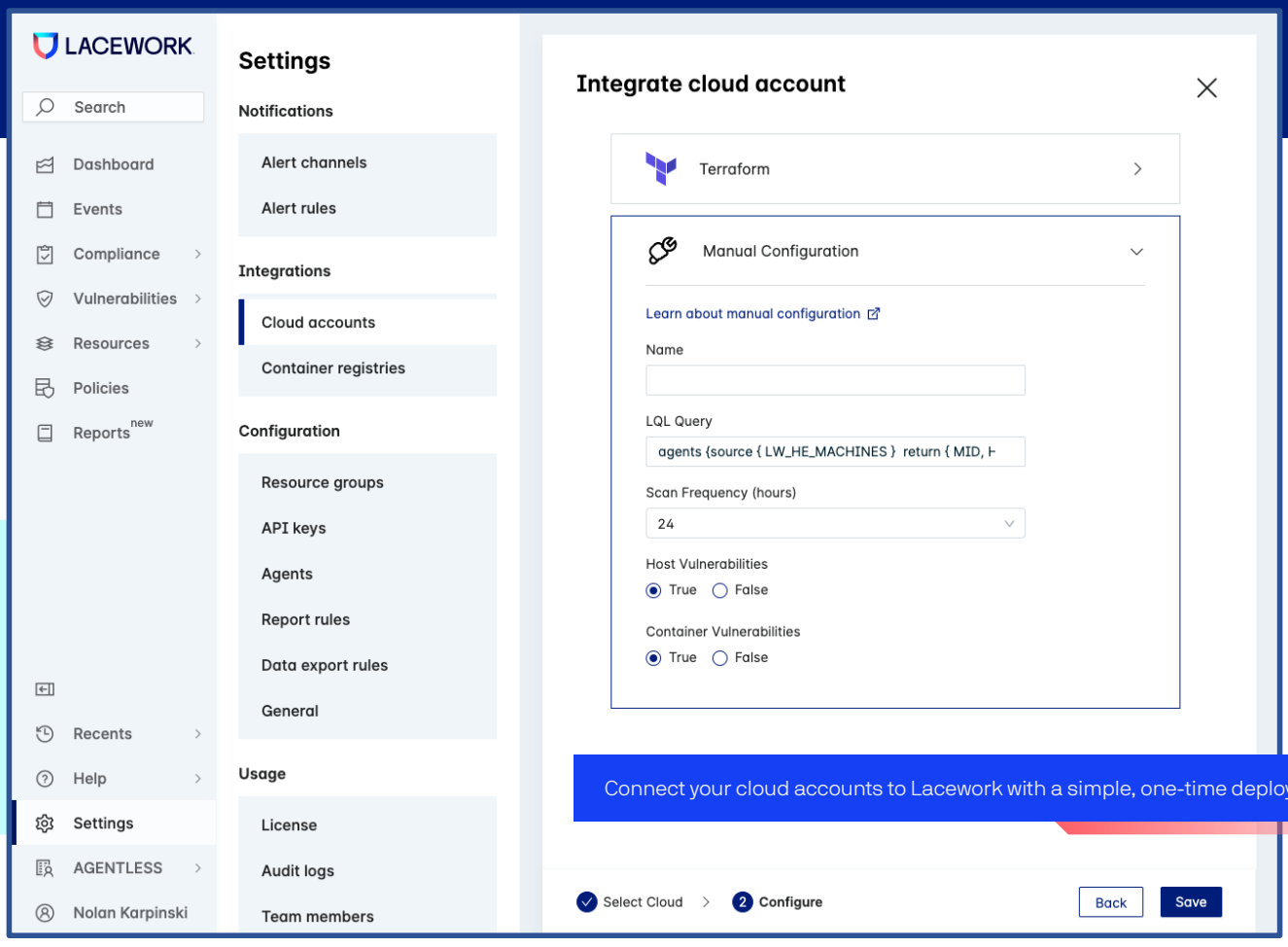
The setup itself takes just minutes. Then, Lacework streams snapshot data through a serverless analysis engine that scans for vulnerabilities and exposed secrets within the target scanning account. This effectively creates an inline file cache, and requires no additional resources to manage. The serverless functions run with optimized privileges to create the most secure environment possible for analyzing your cloud data.

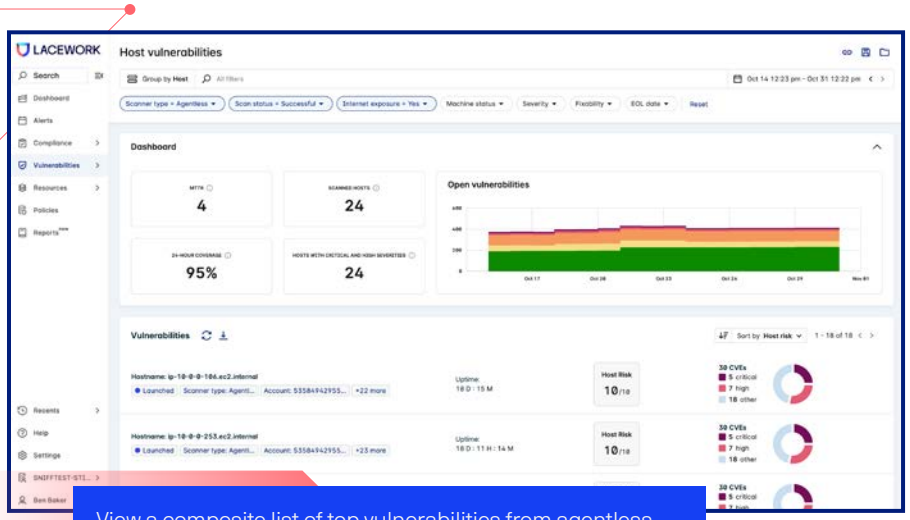
Our solution is secure by design and does not require root administrator privileges to deploy. We do not "auto deploy" infrastructure into your cloud environment because we believe that those decisions should be driven by your needs and the principle of least privilege.

Lacework agentless workload scanning is robust and requires no maintenance. It is automatically upgraded when a new version is released. Your security administrators have the flexibility to schedule assessments based on metadata such as tags and VPC, at a frequency of their choice (the default configuration is for daily scans).

Security operators can view a composite list of top vulnerabilities and secrets discovered from agentless workload scanning, alongside agent-based, registry-based, or pipeline-based scans.

For maximum security, you can use agentless workload scanning and agents for the same assets. For efficiency when dealing with workloads that are enabled for both agentless and agent, Lacework will use the agentless method for vulnerability and secrets scanning and will disable scanning with the agent.



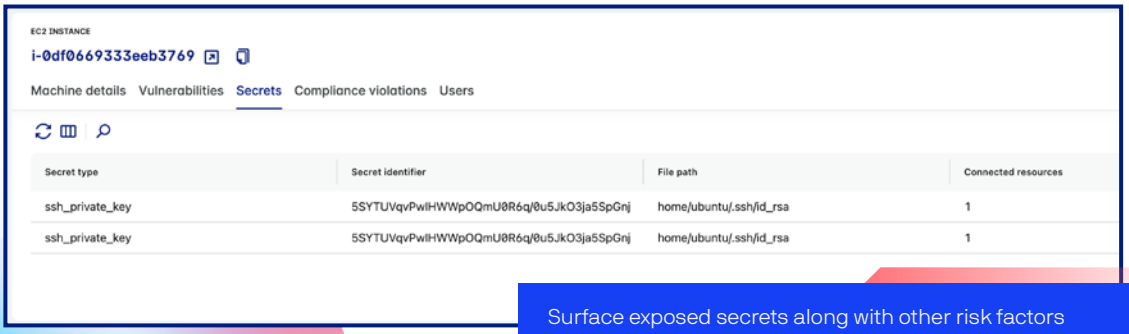


View a composite list of top vulnerabilities from agentless workload scanning, alongside other scans

COMPATIBILITY

Where is the feature supported?

- Available in AWS today, with other cloud service providers to be added in future releases
- Includes native EC2 hosts, EKS, and ECS in addition to the operating system supported by the Lacework Linux agent
- Enables optimized deployment via AWS Organizations, but can also be deployed on single accounts

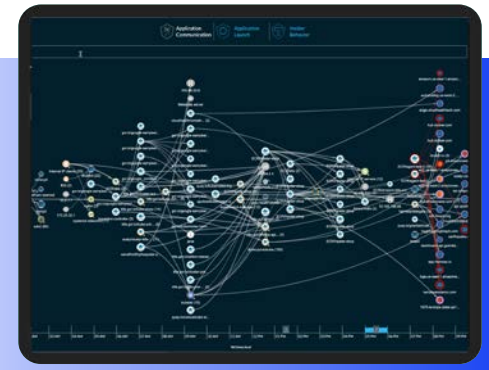


Surface exposed secrets along with other risk factors through agentless workload scanning

Learn about our layered approach

Book a demo

Read the whitepaper



LACEWORK

Lacework is the data-driven security company for the cloud that delivers end-to-end visibility and automated insight into risk across cloud environments. Trusted by enterprise customers worldwide to reduce risk, Lacework significantly drives down costs so you can securely innovate in the cloud with speed.

 | 888.292.5027 | lacework.com 11/22