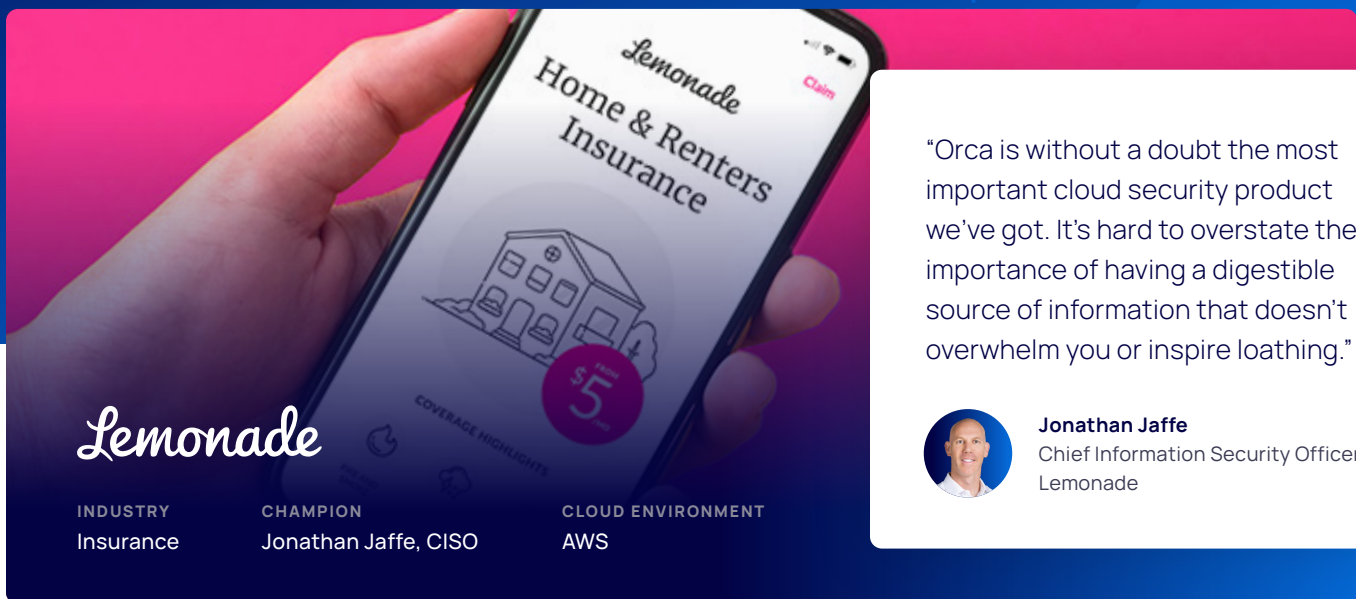


Insurance Innovator Lemonade Goes from 0 to 100% Cloud Visibility with Orca Security



Lemonade

INDUSTRY
Insurance

CHAMPION
Jonathan Jaffe, CISO

CLOUD ENVIRONMENT
AWS

Jonathan Jaffe
Chief Information Security Officer
Lemonade

"Orca is without a doubt the most important cloud security product we've got. It's hard to overstate the importance of having a digestible source of information that doesn't overwhelm you or inspire loathing."

Cloud Security Challenges

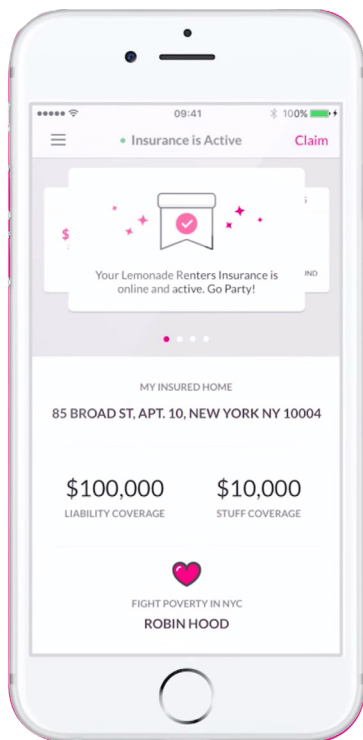
- ✗ Get complete visibility for the entire cloud estate
- ✗ Quickly prioritize important issues into "digestible bites"
- ✗ Minimize the impact on DevOps

Cloud Security Results

- ✓ 100% coverage of cloud accounts with full visibility and prioritized remediation all with zero impact to DevOps and the production environment
- ✓ Able to meet compliance mandates and demonstrate controls to auditors
- ✓ Orca dashboard shows actionable insights of prioritized issues
- ✓ Peace of mind that there are no gaps in coverage

Lemonade is Revolutionizing the Insurance Market

Lemonade provides insurance in the US and Europe. It's part of the "insurtech" market, whereby insurance providers use advanced technology to offer innovative products and services that traditional entities can't match. As a relatively young company, Lemonade has a cloudnative technology stack that lets it operate 100% online. This makes Lemonade an agile competitor in the insurance market. For example, Lemonade delivers policy quotes by an artificial intelligence bot over the web and through its mobile apps. At the same time, Lemonade is A-rated, fully regulated, and reinsured by the most trusted names in insurance.



CISO's Prior Orca Experience Leads the Way

Lemonade's infrastructure is entirely in the AWS cloud, where it can be a challenge to get real-time insights about vulnerabilities and security risks. Even Amazon's native tools don't provide all the information that security and DevOps practitioners need.

Jonathan Jaffe joined Lemonade as its CISO in 2020. He immediately sought to get complete visibility for the entire cloud estate to better assess security risks. "When I came on board, there wasn't an adequate solution in place telling me about our vulnerabilities," he says. "I wanted much more visibility into cloud vulnerability issues than what we had."

Orca Beats Agent-Based Competitors Lacework and Palo Alto Prisma Cloud

"We assessed Orca Security, as well as Palo Alto Prisma Cloud, and Lacework," says Jaffe. "At my last company, we used Lacework for over a year. In the last four months of my time there, we also ran Orca in a PoC, so it was easy to do the Orca comparison side-by-side. And, we evaluated Prisma Cloud, extensively."

At Lemonade, the evaluation team had to rely on product demos for Prisma Cloud and Lacework, though Jaffe was already intimately familiar with both Orca and Lacework. "Unlike Orca, the others require agents. DevOps wasn't excited about installing and maintaining agents. DevOps also feared the performance hit agents could have on

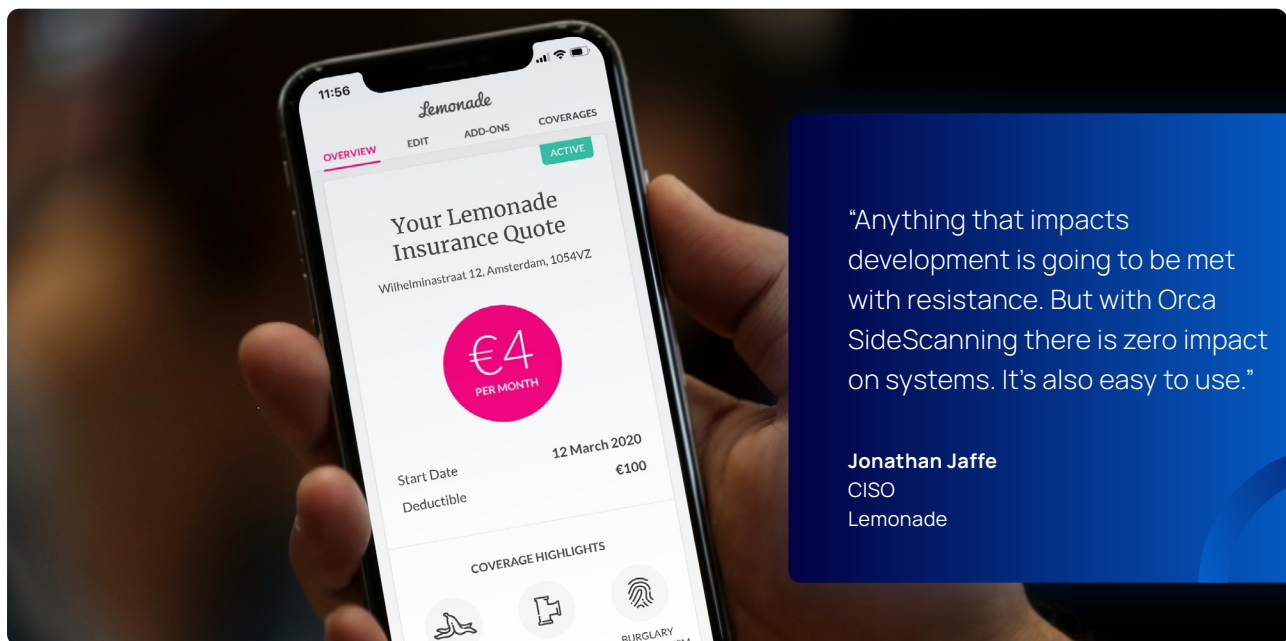
our systems, especially production. And, based on my prior experiences with Laceworks, I knew I'd be fighting with missing visibility because of missing agents." Orca took half an hour to set up and fully deploy for the PoC. "It was nothing to get it going," Jaffe says. "We saw results immediately. In under 24 hours, we could see all the resources and the environment in all of our AWS accounts. Moreover, we could quickly and easily see the issues that Orca found, which, fortunately, were small and manageable.

100% Coverage and Prioritization of Security Issues

Jaffe sought several important features in a security solution. "The first is 100% coverage, which is something we'd never get from anything that requires agents to be installed. I have to feel comfortable that we don't have gaps in coverage."

Another must-have feature is the ability to prioritize what needs fixing. "Lacework provides loads of information, but we didn't find it useful; To the contrary, we found it impaired our ability to remediate issues. Having too much diluted the value of the few gems it might have surfaced. Moreover, it doesn't prioritize information in a useful way. When we used Lacework, our security analyst spent most of his time struggling to understand which problems he should spend his time to solve. If he could get past this problem and choose an issue to chase, he'd run into the next problem: was there really an intrusion, or is it yet another false positive?—All of this had to occur before he could get to remediation. Before Orca, we'd give up seeing an issue to resolution because the information was organized so poorly.

"Orca is the opposite. With the information presented in a matrix, we can look at it by threat type, vulnerability, account, affected resource, and so on. We can view the top five items by categories, such as neglected assets or vulnerabilities.



"Anything that impacts development is going to be met with resistance. But with Orca SideScanning there is zero impact on systems. It's also easy to use."

Jonathan Jaffe
CISO
Lemonade

This puts problems into small bites we can chew through, one at a time. Instead of being overwhelmed, which is how many other products make you feel. We can quickly address prioritized issues, putting off or altogether dismissing those of lesser importance.”

For Jaffe and his team, the Orca dashboard provides a calming effect because it doesn't overwhelm them by providing too much information. He says, “Orca's real value is in covering a huge amount of my cloud security, notifying us about vulnerabilities and—by a highly reduced degree—actual threats.”

Evidence of Controls for Audits

With its headquarters being in New York, that state's Department of Financial Services (NYDFS) regulates Lemonade's business. In addition, the company is subject to various EU regulations and has its own SOC 2 audits. Orca's reports help Jaffe provide evidence for controls for the various regulations and audits. “Orca has helped reduce my audit effort; for example, I can run reports that show we maintain least privilege controls and that we use multi-factor authentication.”

Orca also alerts Jaffe if there are potential data loss issues or if personal data is exposed in risky areas. The Lemonade team can remediate such issues long before they become a problem that would show up in audit reports. “Orca is great at detecting potential exposure of credit card data, email addresses, and social security numbers or other national IDs,” says Jaffe. “These are priority issues that we can quickly remediate.”

“Orca alleviates our number one pain: where are our cloud-related security risks? Before Orca, we simply didn't have the visibility I needed.”

Jonathan Jaffe
Chief Information Security Officer
Lemonade

Lemonade

Renters Policy Declarations

POLICY NUMBER	START DATE	EXP. DATE
1234	Jun 06, 2018	Jun 06, 2019

NAME	ADDRESS
John Doe	123 Main St, Portland, OR 1234

COVERAGE SUMMARY

Personal Property	\$10,000
Loss Of Use	\$3,000

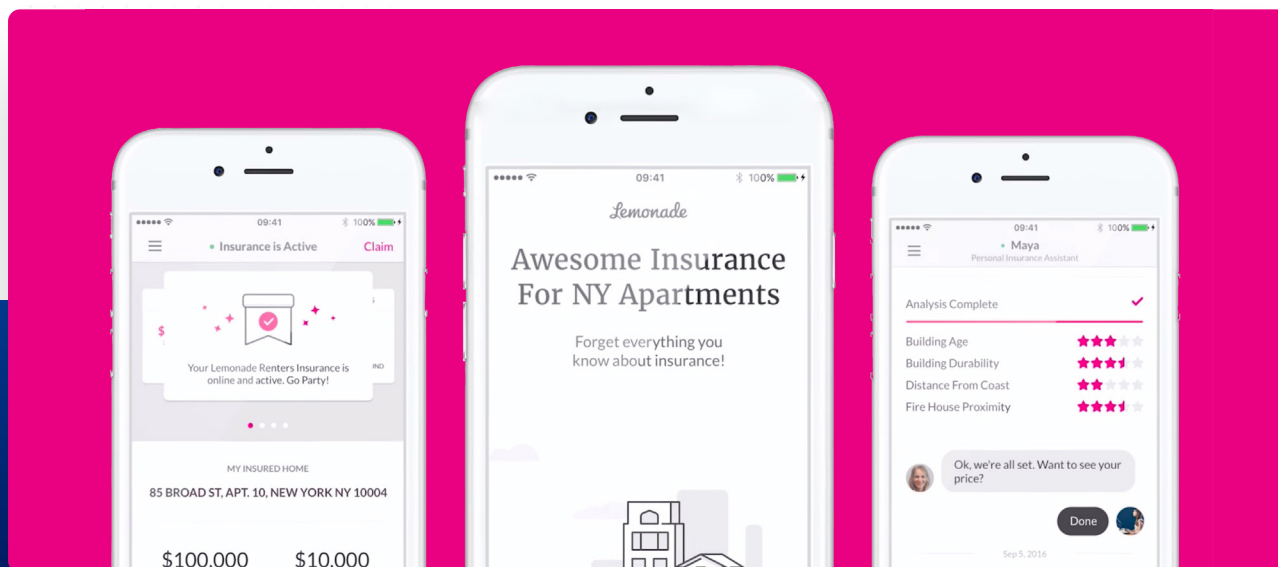
At-Risk Items Have Been Vastly Reduced

Lemonade has significantly reduced its at-risk items. “We cut them down to one-sixth of what they were, and now we can keep that under control by monitoring them,” says Jaffe. “Orca lets us shine a light on things so we know what to fix and what we don’t have to worry about.”

What Jaffe likes most about Orca is the way it lists prioritized issues. “You can see the top five items by categories, such as neglected assets or vulnerabilities. That puts problems into digestible

amounts so we can chew through them one at a time, instead of being overwhelmed, like a lot of other products make you feel.”

He also loves the interface, stating that the dashboard provides a calming effect because it doesn’t overwhelm him by providing too much information. Jaffe says, “Orca’s real value is in covering a huge amount of my cloud security— notifying me about vulnerabilities, and to a lesser degree, actual threats.”



About Orca Security

Utilizing its unique patent-pending SideScanning™ technology, Orca Security provides cloud-wide, workload-deep security and compliance for AWS, Azure, and GCP. After an instantaneous, read-only and impact-free integration to the cloud provider, it detects vulnerabilities, malware, misconfigurations, lateral movement risk, authentication risk, and insecure high-risk data— then prioritizes risk based on the underlying issue, its accessibility, and blast radius - without deploying agents.



Connect your first cloud account in minutes
and see for yourself: [Visit orca.security](https://www.orca.security)

