# Das innovative Versicherungsunternehmen Lemonade verbesserte mit Orca Security seine Cloud-Sichtbarkeit von 0 auf 100 %

Lemonade

| BRANCHE | CHAMPION | CLOUD-UMGEBUNG |
|---|---|---|
| Versicherung | Jonathan Jaffe, CISO | AWS |

„Orca ist zweifelsohne das wichtigste Cloud-Sicherheitsprodukt, das wir haben. Man kann gar nicht hoch genug einschätzen, wie wichtig es ist, eine leicht verdauliche Informationsquelle zu haben, die einen nicht überwältigt oder Abneigung hervorruft."



**Jonathan Jaffe**
Chief Information Security Officer
Lemonade

## Herausforderungen der Cloud-Sicherheit

- Vollständige Transparenz für den gesamten Cloud-Bestand
- Schnelle Priorisierung wichtiger Themen in „leicht verdauliche Häppchen"
- Minimierung der Auswirkungen auf DevOps

## Ergebnisse der Cloud-Sicherheit

- 100-prozentige Abdeckung von Cloud-Konten mit vollständiger Transparenz und priorisierter Behebung – ohne Auswirkungen auf DevOps und die Produktionsumgebung
- Fähigkeit zur Erfüllung von Compliance-Vorgaben und zum Nachweis von Kontrollen gegenüber Prüfern
- Das Orca-Dashboard zeigt verwertbare Erkenntnisse über priorisierte Probleme
- Die Gewissheit, dass es keine Lücken im Deckungsschutz gibt

## Lemonade revolutioniert den Versicherungsmarkt

Lemonade bietet Versicherungen in den USA und Europa an. Es ist Teil des „Insurtech"-Marktes, auf dem Versicherungsanbieter fortschrittliche Technologien nutzen, um innovative Produkte und Dienstleistungen anzubieten, mit denen traditionelle Unternehmen nicht mithalten können. Als relativ junges Unternehmen verfügt Lemonade über einen Cloud-nativen Technologie-Stack, mit dem es zu 100 % online arbeiten kann. Das macht Lemonade zu einem gewandten Konkurrenten auf dem Versicherungsmarkt. So liefert Lemonade beispielsweise Versicherungsangebote durch einen Bot mit künstlicher Intelligenz über das Internet und über seine mobilen Anwendungen. Gleichzeitig verfügt Lemonade über ein A-Rating, ist vollständig reguliert und wird von den vertrauenswürdigsten Namen der Versicherungsbranche rückversichert.

## Frühere Orca-Erfahrungen des CISO sind wegweisend

Die Infrastruktur von Lemonade befindet sich vollständig in der AWS-Cloud, wo es eine Herausforderung sein kann, in Echtzeit Erkenntnisse über Schwachstellen und Sicherheitsrisiken zu erhalten. Selbst die nativen Tools von Amazon liefern nicht alle Informationen, die Sicherheits- und DevOps-Fachleute benötigen.

Jonathan Jaffe kam 2020 als CISO zu Lemonade. Er bemühte sich sofort um eine vollständige Transparenz des gesamten Cloud-Bestands, um Sicherheitsrisiken besser einschätzen zu können. „Als ich anfing, gab es keine angemessene Lösung, die mich über unsere Schwachstellen informiert hätte", sagt er. „Ich wollte viel mehr Transparenz in Bezug auf Schwachstellen in der Cloud, als wir sie hatten.

## Orca übertrifft die agentenbasierten Mitbewerber Lacework und Palo Alto Prisma Cloud

„Wir haben sowohl Orca Security als auch Palo Alto Prisma Cloud und Lacework geprüft", sagt Jaffe. „Wir haben bei meinem letzten Unternehmen über ein Jahr lang mit Lacework gearbeitet. In den letzten vier Monaten meiner Zeit dort haben wir auch Orca in einem PoC eingesetzt, sodass es einfach war, den Orca-Vergleich Seite an Seite zu machen. Und wir haben Prisma Cloud ausgiebig evaluiert."

Bei Lemonade musste sich das Evaluierungsteam auf Produktdemos für Prisma Cloud und Lacework verlassen, obwohl Jaffe sowohl mit Orca als auch mit Lacework bereits bestens vertraut war. „Im Gegensatz zu Orca benötigen die anderen Agenten. DevOps waren nicht begeistert von der Installation und Wartung von Agenten. DevOps befürchtete außerdem, dass Agenten die Leistung unserer Systeme beeinträchtigen könnten, insbesondere in der Produktion. Und aufgrund meiner früheren Erfahrungen mit Laceworks wusste ich, dass ich aufgrund fehlender Agenten mit fehlender Transparenz zu kämpfen haben würde."

Es hat eine halbe Stunde gedauert, bis wir Orca eingerichtet und für den PoC vollständig implementiert hatten. „Es war im Handumdrehen fertig“, so Jaffe. „Und die Ergebnisse waren sofort zu sehen. In weniger als 24 Stunden konnten wir alle Ressourcen und die Umgebung in allen AWS-Konten sehen. Außerdem konnten wir die von Orca gefundenen Probleme schnell und einfach erkennen, die zum Glück klein und überschaubar waren.

## 100 % ige Abdeckung und Priorisierung von Sicherheitsfragen

Jaffe wünschte sich mehrere wichtige Merkmale einer Sicherheitslösung. „Das erste ist die 100 %ige Abdeckung, die wir bei einem System, das die Installation von Agenten erfordert, nie erreichen würden. Ich muss mich darauf verlassen können, dass wir keine Lücken in der Abdeckung haben.“

Eine weitere unverzichtbare Funktion ist die Möglichkeit, die zu behebenden Probleme zu priorisieren. „Lacework bietet eine Fülle von Informationen, die wir aber nicht als nützlich empfunden haben; im Gegenteil, wir fanden, dass sie unsere Fähigkeit, Probleme zu beheben, beeinträchtigt haben. Zu viel davon verwässerte den Wert der wenigen Kostbarkeiten, die es vielleicht zum Vorschein gebracht hatte. Außerdem werden die Informationen nicht sinnvoll nach Prioritäten geordnet. Als wir Lacework einsetzten, verbrachte unser Sicherheitsanalyst die meiste Zeit damit, herauszufinden, für welche Probleme er seine Zeit aufwenden sollte, um sie zu lösen. Wenn er dieses Problem überwinden und ein Problem auswählen konnte, dem er nachgehen wollte, stieß er auf das nächste Problem: Gab es wirklich einen Angriff, oder handelt es sich um einen weiteren Fehlalarm? All dies musste geschehen, bevor er sich an die Behebung machen konnte. Vor Orca haben wir oft aufgegeben, ein Problem zu lösen, weil die Informationen so schlecht organisiert waren.

„Orca ist das Gegenteil. Die in einer Matrix dargestellten Informationen können nach Bedrohungstyp, Schwachstelle, Konto, betroffener Ressource usw. betrachtet werden. Wir können die fünf wichtigsten Punkte nach Kategorien, wie z. B. vernachlässigte Assets oder Schwachstellen, anzeigen.

„Wenn etwas die Entwicklung beeinträchtigt, regt sich Widerstand. Aber mit Orca SideScanning gibt es keinerlei Auswirkungen auf die Systeme. Es ist auch einfach zu bedienen.“

**Jonathan Jaffe**
CISO
Lemonade

Dadurch werden die Probleme in kleine Häppchen zerlegt, die wir nach und nach durchkauen können, anstatt uns zu überfordern, wie es bei vielen anderen Produkten der Fall ist. Wir können uns schnell um die vorrangigen Probleme kümmern und die weniger wichtigen aufschieben oder ganz verwerfen."

Für Jaffe und sein Team hat das Orca-Dashboard eine beruhigende Wirkung, weil es sie nicht mit zu vielen Informationen überfordert. Er sagt: „Der wahre Wert von Orca liegt darin, dass es einen großen Teil meiner Cloud-Sicherheit abdeckt und uns über Schwachstellen und – in einem stark reduzierten Ausmaß – über tatsächliche Bedrohungen informiert."

## Nachweis von Kontrollen für Audits

Da sich der Hauptsitz des Unternehmens in New York befindet, unterliegt die Geschäftstätigkeit von Lemonade der Aufsicht des dortigen Department of Financial Services (NYDFS). Darüber hinaus unterliegt das Unternehmen verschiedenen EU-Vorschriften und führt eigene SOC-2-Audits durch. Die Berichte von Orca helfen Jaffe, Nachweise für die Kontrollen im Rahmen der verschiedenen Verordnungen und Audits zu erbringen. „Orca hat dazu beigetragen, meinen Aufwand für Audits zu reduzieren; zum Beispiel kann ich Berichte abrufen, die zeigen, dass wir die Kontrolle der geringsten Privilegien gewährleisten und Multi-Faktor-Authentifizierung verwenden."

Orca alarmiert Jaffe auch, wenn es Probleme mit potenziellen Datenverlusten gibt oder wenn persönliche Daten in Risikobereichen exponiert sind. Das Lemonade-Team kann solche Störungen beheben, lange bevor sie zu einem Problem werden, das in den Prüfungsberichten auftauchen würde. „Orca ist bestens in der Lage, potenziell gefährdete Kreditkartendaten, E-Mail-Adressen, Sozialversicherungsnummern oder andere nationale IDs zu erkennen", sagt Jaffe. „Dies sind vorrangige Probleme, die wir schnell beheben können."

> „Orca lindert unser größtes Problem: Wo liegen unsere Cloud-bezogenen Sicherheitsrisiken? Vor Orca hatten wir einfach nicht die Sichtbarkeit, die ich brauchte."
>
> **Jonathan Jaffe**
> Chief Information Security Officer
> Limonade

## Die Zahl der Risikopositionen wurde stark reduziert

Lemonade hat seine Risikopositionen erheblich reduziert. „Wir haben sie auf ein Sechstel reduziert, und jetzt können wir sie unter Kontrolle halten, indem wir sie überwachen“, sagt Jaffe. „Mit Orca können wir die Dinge unter die Lupe nehmen, damit wir wissen, was wir in Ordnung bringen müssen und worüber wir uns keine Sorgen machen müssen.“

Was Jaffe am meisten an Orca gefällt, ist die Art und Weise, wie es priorisierte Themen auflistet. „Man kann die fünf wichtigsten Punkte nach Kategorien, wie z. B. vernachlässigte Assets oder Schwachstellen, anzeigen. Dadurch werden die Probleme in kleine Häppchen zerlegt, die wir nach und nach durchkauen können, anstatt uns zu überfordern, wie es bei vielen anderen Produkten der Fall ist.

Er ist auch von der Benutzeroberfläche begeistert und meint, dass das Dashboard eine beruhigende Wirkung hat, weil es ihn nicht mit zu vielen Informationen überfordert. Jaffe sagt: „Der wirkliche Wert von Orca liegt darin, dass es einen großen Teil meiner Cloud-Sicherheit abdeckt – es benachrichtigt mich über Schwachstellen und in geringerem Maße auch über tatsächliche Bedrohungen.“

## Über Orca Security

Mit seiner einzigartigen, zum Patent angemeldeten SideScanning™-Technologie bietet Orca Security cloudumfassende, workloadintensive Sicherheit und Compliance für AWS, Azure und GCP. Nach einer sofortigen, nur Lesegriff zulassenden und folgenlosen Integration in den Cloud-Provider erkennt es Schwachstellen, Malware, Fehlkonfigurationen, Risiken durch Seitwärtsbewegungen, Authentifizierungsrisiken und unsichere Daten mit hohem Risiko und priorisiert das Risiko auf der Grundlage des zugrunde liegenden Problems, seiner Zugänglichkeit und des Explosionsradius – ohne Einsatz von Agenten.

Verbinden Sie Ihr erstes Cloud-Konto in wenigen Minuten und überzeugen Sie sich selbst: Besuchen Sie orca.security

© Copyright Orca Security 2021. Alle in diesem Material genannten Marken, Dienstleistungsmarken und Handelsnamen sind Eigentum ihrer jeweiligen Inhaber.