

Orca Security unterstützt die Live Oak Bank bei der Innovation und erleichtert die Einhaltung von Datenschutz- und Sicherheitsvorschriften



Herausforderungen der Cloud-Sicherheit

- ✘ Sicherheitsbewertungen müssen so nah wie möglich an der Echtzeit durchgeführt werden
- ✘ Die Cloud-Umgebung muss geschützt werden, ohne Entwickler einzuschränken oder für die IT-Abteilung ein Problem darzustellen
- ✘ Muss die FDIC-Anforderungen an die Cloud-Sicherheit erfüllen

Ergebnisse der Cloud-Sicherheit

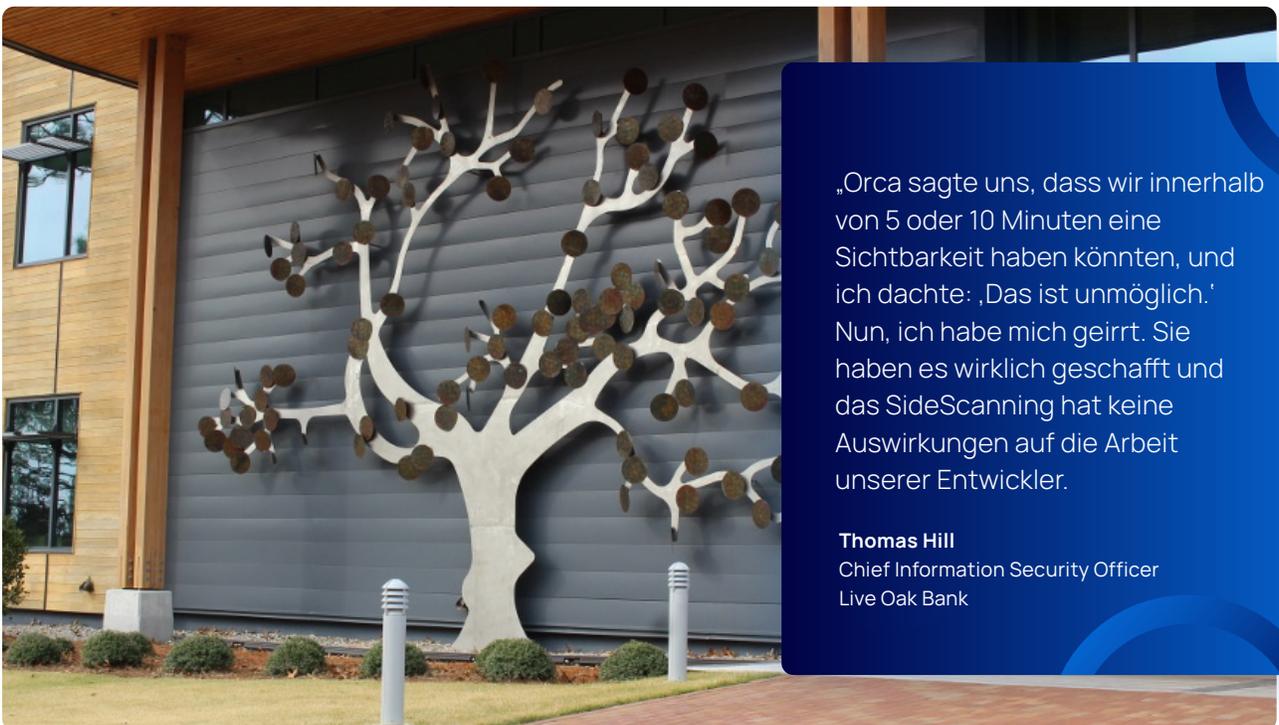
- ✔ Jetzt können Risiken und Schwachstellen nahezu in Echtzeit erkannt werden
- ✔ Kann DevOps-Prozesse ohne Unterbrechung des Betriebs- und Produktionszugriffs und ohne Installation von Agenten unterstützen
- ✔ Vollständige Unterstützung der FDIC-Richtlinien und künftiger Anforderungen an die Cybersicherheit in der Cloud

Die selbst entwickelte Technologie der Live Oak Bank ist ein wichtiges Unterscheidungsmerkmal

Live Oak Bank unterscheidet sich in vielerlei Hinsicht von den meisten Banken. Live Oak wurde als Internet-Bank gegründet und ist weiterhin ohne physische Standorte tätig. Das Unternehmen konzentriert sich auf kleine Unternehmen und verfügt über Fachwissen in mehr als 20 spezifischen Branchen, wie z. B. Tierarztpraxen, Apotheken, Landwirtschaft, Gesundheitswesen und anderen Branchen. Im Gegensatz zu ihren Konkurrenten engagieren sich die Banker von Live Oak stark dafür, ihre Kunden bei der Führung ihrer eigenen Geschäfte zu unterstützen – und das mit Erfolg. Der partnerschaftliche Ansatz hat zu einer Kreditausfallquote von weniger als 1 % geführt – weit unter dem Branchendurchschnitt von 3 %.

Das Unternehmen hat sich von Anfang an die Cloud zu eigen gemacht. Anstatt sein Geschäft auf einer herkömmlichen, rechenzentrumsbasierten Bankplattform aufzubauen, entwickelte Live Oak seine eigene Software. Ein Teil der Technologie des Unternehmens wurde in neue Softwareunternehmen ausgegliedert. Viele dieser Fintech-Unternehmen arbeiten nach wie vor mit der Live Oak Bank zusammen, um einen API-gesteuerten In-the-Cloud-Kern zu schaffen. Die Cloud-Technologie ist ein zentraler Bestandteil aller Aktivitäten von Live Oak.

Thomas Hill kam vor sechs Jahren als CIO zur Live Oak Bank. Als das Unternehmen wuchs und sein eigenes Technologieportfolio ausbaute, wurde es notwendig, die Rollen von IT und Sicherheit zu trennen, sodass Hill die Position des CISO übernahm. „Wir wollen, dass unser Geschäft schnell und in Echtzeit abläuft. Wir wollen, dass sich das Unternehmen mit Lichtgeschwindigkeit bewegen und verändern kann“, sagt Hill. „Meine Aufgabe ist es, dafür zu sorgen, dass wir dies sicher und im Rahmen aller gesetzlichen Vorgaben tun können.“



„Orca sagte uns, dass wir innerhalb von 5 oder 10 Minuten eine Sichtbarkeit haben könnten, und ich dachte: ‚Das ist unmöglich.‘ Nun, ich habe mich geirrt. Sie haben es wirklich geschafft und das SideScanning hat keine Auswirkungen auf die Arbeit unserer Entwickler.“

Thomas Hill
Chief Information Security Officer
Live Oak Bank

DevOps fördern (ohne im Weg zu stehen)

Als Unternehmen, das seine eigene Software entwickelt, wird das DevOps-Team bestärkt, mutig und innovativ zu sein. Ein traditioneller Sicherheitsverantwortlicher kann DevOps behindern, indem er von ihnen verlangt, dass sie langsamer werden und bei jedem Schritt die Sicherheit berücksichtigen. Hill weigert sich aber, ein Hindernis für das Entwicklerteam zu sein. „Das Letzte, was wir tun wollen, ist, unsere Entwickler einzuschränken“, sagt er. „Wir wollen, dass sie über den Tellerrand hinausschauen und neue Dinge schaffen, also geben wir ihnen die Macht, das zu erfinden, was sie brauchen, aber auf eine verantwortungsvolle Weise.“

„Das Wichtigste für einen Sicherheitsmitarbeiter ist es, zu wissen, was es gibt, um die richtigen Kontrollen auf die richtige Umgebung auszuweiten. Mit Orca haben wir volle Sichtbarkeit, sodass wir wissen, worauf wir unsere Energie konzentrieren müssen.“

Thomas Hill
Chief Information Security Officer
Live Oak Bank

„Früher – und damit meine ich buchstäblich vor drei Monaten – haben wir unsere Umgebung einmal im Monat gescannt“, so Hill. „Im Hinterkopf hatte ich die Sorge, dass ein Entwickler ein Skript erstellt, das eine ganze Umgebung und einen neuen Stack aufbaut, und dann mit dem Testen

der Dinge beginnt. Sie könnten nur eine Fehlkonfiguration davon entfernt sein, das alles ins Internet zu stellen. Wir müssen das aufspüren, aber einmal im Monat zu scannen reichte nicht aus. Wenn man in Echtzeit arbeitet, muss man alles in Echtzeit sehen.“

An dieser Stelle kommt Orca ins Spiel. „Wir wollen unsere gesamte Umgebung sehen können – nicht nur die Geräte, die eine IP-Adresse haben, die möglicherweise zugänglich sein könnten und von denen wir wissen“, sagt Hill.

„Orca ist eine großartige Lösung für uns, weil wir Entwicklern die Möglichkeit geben wollen, innovativ zu sein, aber gleichzeitig in Echtzeit scannen müssen, ohne den Betrieb zu beeinträchtigen.“

Orca übernimmt die Arbeit mehrerer Tools aus der Sicherheits-Toolbox

Hills Team führte einen PoC mit Orca durch und wusste innerhalb weniger Tage, wie nützlich es sein würde. Die Sichtbarkeit, die das Sicherheitsteam damit erhält, ist mit anderen Tools nicht zu vergleichen – auch nicht mit solchen, bei denen Agenten auf den Geräten installiert sind. „Ich kann gar nicht genug betonen, wie wichtig es ist, die gesamte Cloud offline einzusehen, um den Betriebs- und Produktionszugang nicht zu unterbrechen. Das SideScanning™-Verfahren von Orca ist wirklich innovativ“, sagt Hill. „Das nimmt uns jegliche Unstimmigkeiten mit unserer IT-Gruppe.“

Live Oak hatte herkömmliche branchenführende Schwachstellen-Scanner für die Cloud eingesetzt. Hill ist der Meinung, dass Orca die Cloud-Assets umfassender scannt, ohne dass dafür umständliche Agenten erforderlich sind. „Die beste Praxis für die Ausführung von Agenten-basierten Tools ist die monatliche Ausführung. Ich fühle mich nicht wohl dabei, solange zwischen den Scans zu warten“, sagt Hill. Mit Orca kann er sie täglich ausführen, ohne dass die Produktion beeinträchtigt wird.

Orca erleichtert Finanzinstituten die Einhaltung von Bundesvorschriften

Die Live Oak Bank verfügt über einen ausgedehnten AWS-Bestand. Hill sagt, dass sie mehr als ein Dutzend Organisationen haben – jede ist ihr eigenes AWS-Mini-Rechenzentrum. Darüber hinaus hat die Bank Fintech-Partner, die sowohl AWS als auch Azure nutzen, wobei die Systeme von Live Oak diese miteinander verbinden.

Als staatlich anerkannte Bank muss Live Oak die Vorschriften zum Datenschutz und zur Datensicherheit einhalten. In diesem Zusammenhang hat die FDIC als Mitglied des Federal Financial Institutions Examination

Council (FFIEC) eine Erklärung abgegeben, die sich mit der Nutzung von Cloud-Computing-Diensten und den Grundsätzen des Sicherheitsrisikomanagements im Finanzdienstleistungssektor befasst. „Das FDIC-Statement ist heute nur ein Leitfaden, aber wir gehen davon aus, dass es bald zu einer Vorschrift wird“, sagt Hill. „Orca hilft uns, die Sicherheitslage unserer Cloud-Umgebungen zu verstehen, was für uns als Bank extrem wichtig ist. Unsere Unternehmensrisiko-Gruppe findet es sehr vorteilhaft, ein Tool wie Orca zu haben, das diesen Bedarf deckt.“

Aufgrund gesetzlicher Vorschriften für Finanzdaten verwendet Live Oak eine Hybrid-SaaS-Version von Orca Security, genannt Orca Pod. Es ermöglicht der Bank, ihre Daten in ihrer eigenen Umgebung zu behalten und nur Metadaten an Orca zu übertragen.



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](https://www.orca.security)

