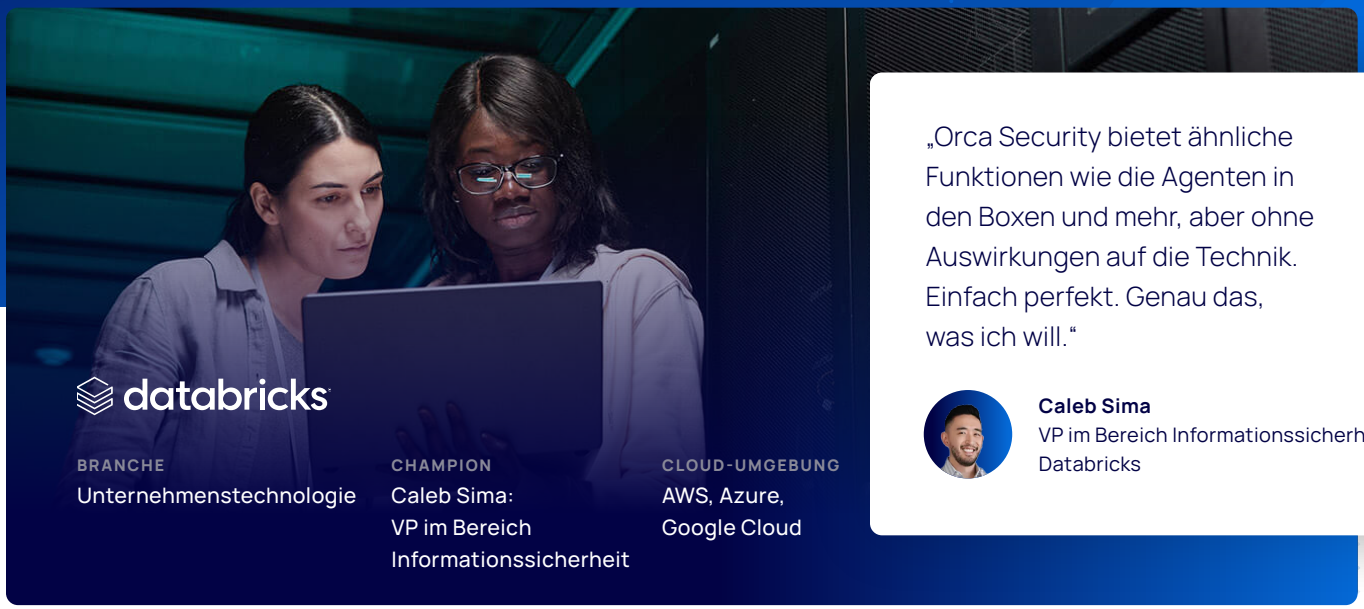
Orca Security ist die erste Wahl von Databricks



databricks

BRANCHE
Unternehmenstechnologie

CHAMPION
Caleb Sima:
VP im Bereich Informationssicherheit

CLOUD-UMGEBUNG
AWS, Azure, Google Cloud

„Orca Security bietet ähnliche Funktionen wie die Agenten in den Boxen und mehr, aber ohne Auswirkungen auf die Technik. Einfach perfekt. Genau das, was ich will."

Caleb Sima
VP im Bereich Informationssicherheit
Databricks

Herausforderungen der Cloud-Sicherheit

- Transparenz über alle laufenden Vorgänge, ohne Agenten einsetzen zu müssen
- Genaue Bewertung von Schwachstellen und Risiken und Festlegung von Prioritäten für Abhilfemaßnahmen
- Support für einen Multi-Cloud-Bestand
- Vermeiden von Konflikten im Software-Engineering

Ergebnisse der Cloud-Sicherheit

- Erhöhte Transparenz durch risikopriorisierte Warnungen, die präzise, handlungsorientiert und kontextbezogen sind
- Alle größeren Sicherheitsprobleme können gelöst werden; derzeit Überwachung kleinerer Probleme
- Ein einziges Out-of-Band-Tool ermöglicht die Identifizierung von Schwachstellen, die Bestandsaufnahme von Assets sowie das Überwachen und Erkennen von Vorgängen auf allen Cloud-Systemen
- Die Technologie liegt vollständig in der Kontrolle des Sicherheitsteams

Databricks verwaltet Risiken, um Kunden zum Erfolg zu verhelfen

Databricks ist ein führendes Unternehmen in den Bereichen Datenanalyse und maschinelles Lernen. Heute vertrauen mehr als fünftausend Organisationen weltweit auf Databricks – darunter eine Reihe von Fortune-500-Unternehmen – um massives Data Engineering, kollaboratives Data Science, maschinelles Lernen über den gesamten Lebenszyklus und Geschäftsanalysen zu ermöglichen. Das Unternehmen verfügt über Hunderte von globalen Partnern, darunter namhafte Unternehmen wie Microsoft, Amazon, Informatica und Cap Gemini.

Als Technologieunternehmen, das Teil der Lieferkette seiner Kunden und Partner ist, legt Databricks großen Wert auf die Überwachung und das Management seiner eigenen Risiken, um deren Vertrauen zu gewinnen und zu erhalten. Um diese Sicherheit zu gewährleisten, investiert das Unternehmen in hochwertige Sicherheitsprodukte und -anbieter.

Databricks arbeitet in einer Multi-Cloud-Umgebung mit AWS, Azure und GCP. Durch den Betrieb auf allen drei Plattformen ist es schwierig, die nativen Tools der Cloud-Betreiber für eine einheitliche Sicherheit in der gesamten Umgebung zu nutzen. Daher ist die Auswahl der richtigen Tools zur Aufrechterhaltung einer sicheren Umgebung von entscheidender Bedeutung.

Entrepreneur der Sicherheitsbranche nennt Orca „Einfach und Brillant“

Caleb Sima ist der Vizepräsident für Informationssicherheit des Unternehmens. Während eines Großteils seiner Karriere war er ein Serien-Entrepreneur, der mehrere Cybersicherheitsunternehmen gegründet, entwickelt und verkauft hat. Vor einigen Jahren änderte Sima seine Karriere vom Gründer und Entrepreneur zum Verteidiger innerhalb von Unternehmen. Dadurch verfügt er über eine einzigartige Perspektive für die besten Technologien, die zur Verteidigung und zum Schutz der Anwendungen und Cloud-Umgebungen von Databricks eingesetzt werden können.

„Der Entrepreneur in mir sagte: ‚Das ist es!' Das ist so offensichtlich und einfach, einfach nur brillant. Das ist ein Selbstläufer.“

Caleb Sima
VP im Bereich Informationssicherheit
Databricks

„Als ich zu Databricks kam, hatte ich die Möglichkeit, mein Sicherheitsteam von Grund auf zu entwickeln. Gemeinsam haben wir die Tools für unseren Sicherheits-Stack bewertet und ausgewählt“, sagt er. Ein wichtiges Kriterium bestand darin, dem Softwareentwicklungsteam von Databricks nicht in die Quere zu kommen. „Wir sind ein schnelllebiges Unternehmen und ich möchte nichts tun, was den Fortschritt unserer Ingenieure verlangsamt. Unser Technologie-Stack verändert sich so schnell, dass die Installation von Agenten auf den Ressourcen eine Herausforderung und sehr komplex wäre.“

„Nachdem ich davon gehört hatte, wollte ich unbedingt die Orca-Demo sehen. Mein Interesse erwachte, als ich erfuhr, wie es funktioniert: Es werden Momentaufnahmen von Festplatten erstellt und diese auf Aktivitäten und Schwachstellen analysiert.“

Agenten schaffen Komplexität, Komplexität erhöht das Risiko

Für Sima war klar, dass er kein Produkt wollte, das Agenten auf Maschinen einsetzt – vor allem dann nicht, wenn es sich um kritische Infrastrukturen und Hosts handelt.

> „Orca priorisiert Warnungen so, dass Sie auf Basis der bereitgestellten Informationen und des Sicherheitsniveaus direkt handeln können. Das ist hochmodern und pure Magie.“
>
> **Caleb Sima**
> VP im Bereich Informationssicherheit
> Databricks

„Es ist ein großer Aufwand – sowohl für die Sicherheit als auch für die Technik – eine agentenbasierte Lösung zum Laufen zu bringen“, sagt er. „Jeder Anbieter mit einem Agenten sagt, dass sie sehr leicht sind. Dabei geht es nicht um die CPU-Leistung, sondern um ein höheres Risiko. Je mehr Dinge man in ein System einbaut, desto komplexer wird es und desto größer ist das Risiko, dass etwas schiefgehen kann.“

Der Wert von Orca war von Anfang an offensichtlich

Databricks meldete sich für einen POC an und hatte Orca schnell einsatzbereit. Es mussten lediglich einige Cloud-Kontoberechtigungen eingerichtet werden. Innerhalb weniger Stunden zeigte Orca Ergebnisse in seinem Dashboard an. Sima und seine Kollegen aus der Sicherheitsabteilung konnten nicht glauben, was sie zu sehen bekamen. „Ich kann mich noch daran erinnern, dass ich Warnungen durchgegangen bin und einfach nur überrascht war“, so Sima. „Zunächst dachten wir, es handele sich um Falschmeldungen. Dann haben wir es selbst überprüft und festgestellt, dass jede Warnung richtig war.“

Databricks stand vor mehreren Herausforderungen, die es mit einer Lösung wie Orca zu lösen hoffte. Ursprünglich ging es darum, einen Überblick über die laufenden Prozesse zu erhalten, ohne Agenten auf den Systemen installieren zu müssen. Gesucht wurde zudem ein Tool, das bei der Überwachung, Erkennung und Reaktion auf Clouds helfen kann. Zudem wollte das Unternehmen Risiken in all seinen Cloud-Umgebungen identifizieren. „Irgendwie gelang es Orca, einen Ausgleich zwischen diesen Bedürfnissen zu schaffen und alle unsere Kriterien zu erfüllen. „Die Tatsache, dass alle Cloud-Umgebungen miteinander – und mit Orca – kommunizieren können, gibt uns ein übergeordnetes Bild über unser Gesamtrisiko.“

„Unser größter Schmerzpunkt lag in der Transparenz unserer Cloud-Workloads, Instanzen und Maschinen“, berichtet Sima. „Der POC hat uns gezeigt, dass wir nicht nur sehen können, was passiert, sondern dass Orca uns auch sagen konnte, dass etwas passieren könnte. Das heißt: „Hier sind die möglichen Seitwärtsbewegungen und die Art der Ressourcen, auf die ein Angreifer potenziell zugreifen könnte. Solche Einblicke waren unglaublich, also haben wir den Wert sofort erkannt.“

Sima schätzt an Orca vor allem die Genauigkeit und den Tiefgang der Ergebnisse. „Sie können z. B. feststellen, dass es eine große Anzahl fehlgeschlagener SSH-Anmeldungen auf dieser Box gibt, die zufällig auch Schlüssel enthält, die auf diese Boxen zugreifen, die auch eine AWS-Anmeldeinformation enthalten, die auf diese Infrastruktur zugreifen kann. Es ist offensichtlich, dass diese Box einem Angriff ausgesetzt ist und auch übermäßig privilegiert ist, was ja auch alles stimmt. Und Sie können das tun und es jedem in der Organisation auf ziemlich verständliche Weise vermitteln“, sagt Sima. Das ist sehr hilfreich.

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