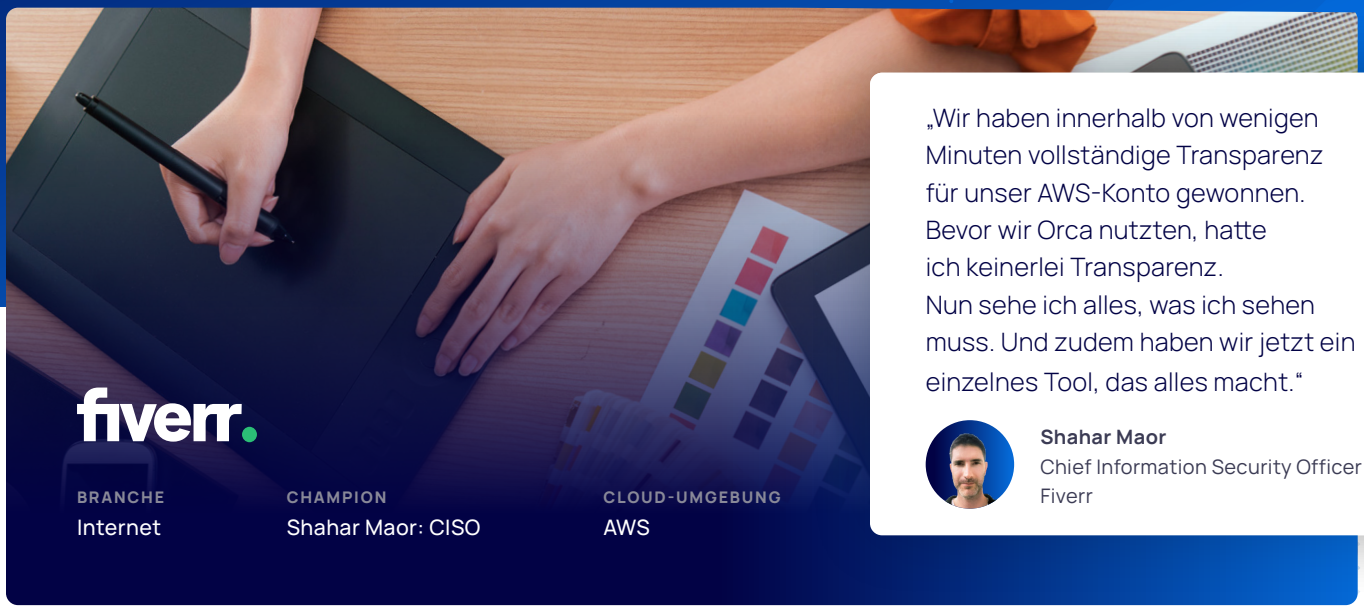
Fiverr ersetzt mehrere Werkzeuge durch Orca Security, um sofortige und vollständige Transparenz bei AWS Assets zu gewinnen



fiverr.

BRANCHE
Internet

CHAMPION
Shahar Maor: CISO

CLOUD-UMGEBUNG
AWS

„Wir haben innerhalb von wenigen Minuten vollständige Transparenz für unser AWS-Konto gewonnen. Bevor wir Orca nutzten, hatte ich keinerlei Transparenz. Nun sehe ich alles, was ich sehen muss. Und zudem haben wir jetzt ein einzelnes Tool, das alles macht."

Shahar Maor
Chief Information Security Officer
Fiverr

Herausforderungen der Cloud-Sicherheit

- Es war nicht möglich, den gesamten Zusammenhang der Vorgänge in AWS zu verstehen
- AWS und Open-Source-Tools waren zeitaufwändig und ineffektiv
- Wir wurden mit Tausenden von Warnmeldungen überflutet, für deren Überprüfung niemand Zeit hat

Ergebnisse der Cloud-Sicherheit

- Deep Cloud Inspection erkennt Malware, Fehlkonfigurationen, „Geheimnisse", schwache Passwörter und personenbezogene Daten
- Spart Woche für Woche viele Arbeitsstunden, schafft weniger Abhängigkeit von DevOps und sorgt dafür, dass keine Assets übersehen werden
- Warnungen werden jetzt auf der Grundlage des Umgebungskontexts priorisiert, an Slack weitergeleitet und behoben

Schnelle globale Expansion erfordert AWS-Cloud-Sicherheit im großen Maßstab

Das 2010 gegründete Unternehmen Fiverr (NYSE: FVRR) mit Hauptsitz in Tel Aviv ist ein riesiger globaler Online-Marktplatz für freiberufliche Dienstleistungen. Die Plattform ermöglicht es Freiberuflern, Kunden auf der ganzen Welt ihre Dienste anzubieten, und hilft Unternehmen, die von ihnen benötigten Dienstleistungen zu finden, indem sie einfach in einem Katalog blättern oder eine Suche durchführen.

Die Plattform von Fiverr hat bereits über 5,5 Millionen Unternehmen bedient und über 50 Millionen Transaktionen abgewickelt. Bei der großen Menge an Personen, die auf die Plattform zugreifen, ist die Gewährleistung einer sicheren AWS-Infrastruktur von entscheidender Bedeutung.

Shahar Maor, CISO von Fiverr, ist sich bewusst, dass die Sicherung von Cloud-Umgebungen eine komplexe Angelegenheit ist

„Ich war der erste Sicherheitsexperte, den Fiverr in Vollzeit eingestellt hat“, verrät CISO Shahar Maor. „Obwohl die Sicherheit bereits tief in die Kultur von Fiverr eingebunden war.“

Maors erste Analysen der AWS-Infrastruktur wiesen auf mögliche Angriffe von externen Vektoren, Hackern, bösartigen Bots und Viren hin. Aber er wusste, dass es in einer Cloud-Umgebung mehr gibt, als man auf den ersten Blick sieht.

„Oftmals gehen Unternehmen davon aus, dass es ausreicht, wenn sie den Außenbereich schützen und übersehen dabei oft die Cloud-Infrastruktur“, so Maor. „Möglicherweise denken Sie nicht daran, dass eine Fehlkonfiguration auf der Plattform selbst ein Problem sein könnte. Es ist ein Irrglaube, zu denken, dass man mit einer Cloud-nativen Infrastruktur einen besseren Überblick hat. Bei der Absicherung von Cloud-Umgebungen gibt es eine Menge komplexer Aspekte.“

Maor zeigte sich besorgt über die schwachen Passwörter der Plattformbenutzer und die Möglichkeit, dass Malware auf AWS-Servern ausgeführt wird. „Als ich zum ersten Mal eine Übersicht der Risiken für unsere wertvollen Assets sah, war direkt klar, dass wir zuvor keine vollständige Sichtbarkeit gehabt hatten. Außerdem verbrachte ich viel zu viel Zeit mit der manuellen Überwachung von Assets, insbesondere der AWS S3-Buckets, um sicherzustellen, dass nichts offengelegt wurde. Das war sehr mühsam.“

Die ideale Lösung zur Gewährleistung einer umfassenden Transparenz über alle AWS-Ressourcen

Mit spezifischen Anforderungen im Hinterkopf machte sich Maor auf die Suche nach einer AWS-Cloud-Sicherheitslösung. Wir brauchten eine Lösung,

> „Oftmals gehen Unternehmen davon aus, dass es ausreicht, wenn sie den Außenbereich schützen und übersehen dabei oft die Cloud-Infrastruktur.“
>
> **Shahar Maor**
> Chief Information Security Officer
> Fiverr

die einen vollständigen Einblick in unsere AWS-Umgebung bietet und gleichzeitig nach Malware scannt, Fehlkonfigurationen erkennt und PII schützt."

Das optimale Cloud-Sicherheits-Tool bietet eine umfassende Lösung für identifizierte Risiken und liefert umsetzbare Erkenntnisse und Werte für IT, DevOps und Technik. Zu den weiteren Zielen und Anforderungen an eine AWS-Sicherheitslösung gehören:

- Keine zu verwaltenden Agenten
- Vollständige Transparenz, keine übersehenen Assets
- Suche nach und Schutz von PII
- Durchführung von Gesundheitskontrollen auf Servern
- Identifizieren schwacher Passwörter
- Aufspüren von Fehlkonfigurationen
- Suche nach verbleibenden „Geheimnissen" im bestehenden Code
- Überwachen von exponierten Assets wie z. B. S3-Buckets
- Vereinfachung der Einhaltung von Vorschriften, insbesondere für PCI

> „Wir brauchten eine Lösung, die einen vollständigen Einblick in unsere AWS-Umgebung bietet und gleichzeitig nach Malware scannt, Fehlkonfigurationen erkennt und PII schützt."
>
> **Shahar Maor**
> Chief Information Security Officer
> Fiverr

Native Tooling, Legacy-Scanner und agentenbasierte Ansätze reichten nicht aus

Maor erkannte, dass die Cloud-Umgebung von Fiverr einzigartige Anforderungen stellte, die viele verfügbare Cloud-Sicherheitstools nicht erfüllen konnten. „Native Tools wie Amazon Inspector oder GuardDuty bieten grundlegende Funktionen, aber sie korrelieren die Logik nicht mit den Vorfällen oder verstehen den vollständigen Kontext des Geschehens nicht. Die Protokolle müssen immer noch analysiert werden und der Zeitaufwand ist höher, um die Daten sinnvoll zu nutzen. Das ist besser als gar nichts, ebenso wie Open-Source-Tools, aber es gibt keinen Workflow für die Weitergabe von Ergebnissen an Ihre Teams, damit diese Maßnahmen ergreifen können."

Maor fügte hinzu, dass Scanner und agentenbasierte Tools sehr begrenzt sind. „Einige handelsübliche Tools scannen einen Server auf Schwachstellen, aber das war's auch schon. Kurz gesagt, diese Tools verursachen mehr Arbeit, und sie erfordern Fachwissen und zusätzliche Tools, um effektiv zu arbeiten."

Ein einziges Tool für alles

Für Maor ist Orca Security ein One-Stop-Shop zur Reduzierung von Risiken, die sich in der AWS-Infrastruktur von Fiverr verbergen. „Orca bietet eine ganzheitliche Lösung zur Minimierung von Risiken im Datencenter von Fiverr. Die einzigartige Methode von Orca zum Scannen von AWS erwies sich für uns als am besten geeignet und überzeugte unser DevOps-Team. Und zudem haben wir jetzt ein einzelnes Tool, das alles macht."

Orca SideScanning™ eliminiert den Bedarf an Agenten und hat keine Auswirkungen auf die Leistung

Der Einsatz von Sicherheitsagenten auf einzelnen virtuellen Maschinen erfordert eine kontinuierliche Verwaltung und Administration. Anstelle dieses Ansatzes läuft Orca als SaaS-Service mit Lesezugriff auf den Laufzeit-Blockspeicher der AWS-, Azure- und/oder GCP-Workloads des Kunden. Aus der Momentaufnahme rekonstruiert Orca Bits und Bytes und erstellt eine virtuelle, schreibgeschützte Ansicht der Betriebssysteme, Anwendungen und Daten. Anschließend erfolgt eine Überprüfung auf Schwachstellen und Risiken.

„Orca ist besonders leicht und hat keinerlei Auswirkungen auf das Netzwerk", sagt Maor. „Die Transparenz ist gegeben, ohne dass die Instanz selbst beeinträchtigt wird. Orca erstellt einfach eine Kopie, liest sie, analysiert die Ergebnisse und stellt sie dann in einem Dashboard dar, damit wir sie überprüfen können."

Bedeutsame, hochwertige Warnmeldungen ohne störende Effekte

Die patentierte SideScanning™-Technologie von Orca Security erkennt automatisch alle Assets in der Umgebung eines Kunden. Dadurch erhalten die Sicherheitsteams unmittelbare Transparenz über gefährdete Ressourcen, Schwachstellen, Malware und Fehlkonfigurationen. Durch die Kombination solcher Informationen mit Umgebungsmetadaten sendet Orca Warnmeldungen im Kontext, um eine effektive Priorisierung zu ermöglichen.

„Orca sendet bedeutsame, handlungsorientierte Warnungen in Echtzeit, um unsere Aufmerksamkeit auf eine Bedrohung zu lenken, anstatt Tonnen von Protokollen und Tausende von Warnungen zu erstellen, die niemand liest oder Zeit hat, sie zu überprüfen. Wir erhalten Slack-Benachrichtigungen über jedes kritische Ergebnis. Wenn Orca eine neue Schwachstelle aufdeckt, erfahren wir sofort davon."

Vereinfachung der Einhaltung gesetzlicher Vorgaben

Zusätzlich vereinfacht Orca Security die Einhaltung der gesetzlichen Vorgaben. „Laut den PCI-Richtlinien müssen wir unsere Umgebung überprüfen – und da es sich um eine serverlose Umgebung handelt, stellt dies eine besondere Herausforderung dar. Mit der Lösung von Orca überprüfen wir sowohl EKS- als auch ECS-Container und erhalten so eine gute Abdeckung für den PCI-Bereich."

> „Orca Security sendet bedeutsame und handlungsorientierte Warnungen in Echtzeit, um unsere Aufmerksamkeit auf eine Bedrohung zu lenken. Wenn Orca eine neue Schwachstelle aufdeckt, erfahren wir sofort davon."
>
> **Shahar Maor**
> Chief Information Security Officer
> Fiverr

Vollständige Sichtbarkeit, minimaler Aufwand

Kurz nach der Implementierung zeigte Orca Schwachstellen auf, die das Team von Maor beheben konnte. „Orca Security liefert wertvolle Erkenntnisse und die Fähigkeit, die Sicherheitslage von Fiverr zu erweitern. Vor Orca hatte ich keinerlei Transparenz. Jetzt sehe ich alles, was ich sehen muss."

Für Maor war das die Bestätigung, dass Orca Security genau das Richtige für ihn ist. „Ich habe immer noch sowohl Orca als auch einen CASB implementiert, aber bei der nächsten Erneuerung werde ich den CASB entfernen, weil er keine Erkenntnisse liefert", sagte er. „Ich werde mich bei der End-to-End-Überwachung der AWS-Produktionsumgebung ausschließlich auf Orca verlassen."

Wöchentlich Stunden einsparen, ohne auf DevOps angewiesen zu sein

Maor verbringt jetzt nur noch die Hälfte seiner bisherigen Zeit mit der Arbeit an der Cloud-Sicherheit. „Orca hat uns im Hinblick auf die Wartung und Verwaltung der Cloud-Sicherheit jede Woche viele Arbeitsstunden erspart. Außerdem bin ich beim Support nicht auf DevOps angewiesen."

Als zusätzlichen Bonus profitiert Maor von den Empfehlungen und dem Fachwissen des Teams von Orca Security. „Das Team von Orca verfügt über ein umfangreiches Hintergrund- und Praxiswissen im Bereich Sicherheit sowie über eine erstaunliche Agilität und Flexibilität. Wir sehen bereits jetzt einen enormen Nutzen von Orca und freuen uns darauf, mit ihm als unsere wichtigste AWS-Sicherheitsplattform zu wachsen."

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.

orca security

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