Paidy wendet sich an Orca Security für Multi-Cloud-Visibilität, spart zwei Vollzeitstellen und 500.000 Dollar pro Jahr an Kosten für Cloud Security Management



STANDORT
Tokio

BRANCHE
Finanzdienstleistungen

CLOUD-UMGEBUNG
AWS, Azure, GCP

„Wir haben 12 AWS-Konten. Wir kannten die Inhalte nicht und haben Sie daher mit Orca verknüpft. Innerhalb von 30 Minuten konnten wir uns ein besseres Bild machen, was in den jeweiligen Konten lief. Anders hätten wir das nie so schnell hingekriegt."



Jeremy Turner
Senior Cloud Security Engineer
Paidy

Herausforderungen der Cloud-Sicherheit

- Hunderte von Entwicklern, die Microservices in Dutzende von Konten über mehrere Clouds hinweg verlagern, machen es schwierig, jedes Asset in der Cloud-Umgebung des Unternehmens zu verfolgen und zu sichern.
- Die Kosten für den Bau einer eigenen Lösung würden sich auf mindestens zwei Vollzeitstellen für ein Jahr belaufen, anschließend 500.000 Dollar jährlich für die Wartung
- Proaktiver Schutz personenbezogener Daten und Einhaltung der japanischen Vorschriften wie der Verordnung über den grenzüberschreitenden Datenschutz und des Gesetzes zum Schutz personenbezogener Daten

Ergebnisse der Cloud-Sicherheit

- Es dauerte dreißig Minuten, um erste Einblicke in seine Cloud-Umgebung zu erhalten; zwölf AWS-Konten wurden in Orca Security integriert, das eine „drohende Kompromittierung" identifizierte.
- Einsparung von 500.000 Dollar pro Jahr an mühsamer Cloud-Sicherheitsarbeit
- Kann gegenüber Auditoren nachweisen, dass es in der Lage ist, personenbezogene Daten zu identifizieren und zu schützen
- Schnelleres Onboarding von Händlern steigert den Umsatz

Paidy – eine japanische Finanzinstitution in der Cloud

Paidy ist ein führendes Fintech-Unternehmen, das kartenlose Zahlungen und andere Finanzdienstleistungen für den japanischen Massenmarkt sowie Unternehmen anbietet. Die Lösungen des Unternehmens stehen an vorderster Front bei der Revolutionierung von Online- und mobilen Zahlungen, P2P-Überweisungen, persönlichen Finanzen und der Händlerabrechnung. Paidy ermöglicht es Kunden, nur mit ihrer E-Mail-Adresse und einer Handynummer zu bezahlen. Es wird keine Kreditkarte oder Voranmeldung benötigt. Um Betrug zu verhindern, wird jede Transaktion mit einer PIN per SMS authentifiziert. Kunden können jetzt einkaufen und eine konsolidierte Rechnung im folgenden Monat bezahlen.

Die gesamte Plattform von Paidy läuft in der Cloud – in erster Linie über mehrere AWS-Konten, aber auch über Azure und GCP. Es verfügt über mehrere Test- und Entwicklungsumgebungen. Da über die Plattform Finanztransaktionen abgewickelt werden, hat die Sicherheit höchste Priorität. CISO Felix Beatty ist für die Optimierung der gesamten Sicherheitslage von Paidy verantwortlich.

„Wir sind im Wesentlichen ein Finanzinstitut in der Cloud“, sagt Beatty. „Da wir so schnell gewachsen sind – mit einem Zuwachs von über drei Millionen Kunden in weniger als einem Jahr – gibt es Bereiche in unserem Unternehmen, die verbesserungsfähig sind; einer davon ist die Cloud-Sicherheit. Die meisten unserer Dienste laufen heute in der Cloud, daher brauchen wir Cloud-Sicherheitslösungen, die kritische Probleme sofort aufdecken, damit wir sie schnell beheben können.“



„Ein Agent kann auf diesem Linux-Kernel funktionieren oder auch nicht, und dasselbe gilt für Windows-Versionen. Es gibt einfach so viele Variablen, die ins Spiel kommen. Nachdem ich jahrelang mit Agenten zu tun hatte und dann gesehen habe, wie einfach Orca zu installieren und zu nutzen ist, wusste ich, dass der agentenlose Ansatz eine große Innovation und ein Wendepunkt ist.“

Jeremy Turner
Senior Cloud Security Engineer
Paidy

Mit der großangelegten Cloud-Umgebung von Paidy wird vollständige Sichtbarkeit zu einer Herausforderung

Eine der größten Herausforderungen ist es, einen Überblick über die gesamte Paidy-Plattform zu erhalten. „Wir haben eine große und komplexe Cloud-Umgebung; es ist schwierig, all diese dynamischen Assets zu verwalten“, sagt Beatty. „Wir haben Hunderte von Entwicklern, die versuchen, Microservices so schnell wie möglich in die Cloud zu verlagern, Instanzen auf- und abzuschalten, Backups zu erstellen, S3-Buckets anzulegen und die so schnell arbeiten, dass es sehr schwierig ist, zu jedem Zeitpunkt zu wissen, was wir haben. Wir müssen wissen: „Wie ist die aktuelle Sicherheitslage aller unserer Cloud-Assets?“

Jeremy Turner, Senior Cloud Security Engineer, ist seine rechte Hand bei der Sicherung der Cloud-Umgebung. Die beiden waren schon vor ihrer Zeit bei Paidy ein Team und wissen, wie sie die Sicherheitsherausforderungen angehen müssen.

Sicherheitsagenten sind großartig – wenn sie funktionieren (normalerweise tun sie das nicht)

„Ich mache das schon sehr lange“, sagt Turner. „Ich habe gelernt, dass alles, was mit Sicherheit und Schwachstellen zu tun hat, in der Regel die Installation einer Art von Agent erfordert. Wenn Sie eine Weile im Bereich der Informationssicherheit gearbeitet haben, wissen Sie, dass Agenten kaputt gehen, aktualisiert werden müssen und Vektoren für andere Sicherheitslücken sein können.“

Turner gibt zu, dass Agenten toll sind – wenn sie funktionieren. „Normalerweise tun sie das nicht. Es gibt so viele Abhängigkeiten und andere Dinge, die man bedenken muss. Ein Agent kann auf diesem Linux-Kernel funktionieren oder eben nicht, und das Gleiche gilt für Windows-Versionen. Es gibt einfach so viele Variablen, die ins Spiel kommen. Nachdem ich jahrelang mit Agenten zu tun hatte und dann gesehen habe, wie einfach Orca zu installieren und zu nutzen ist, wusste ich, dass der agentenlose Ansatz eine große Innovation und ein Wendepunkt ist“, sagt Turner.



Veraltete Schwachstellen-Scanner und AWS-Tools waren ungeeignet

Das Sicherheitsteam von Paidy hatte Erfahrung mit einer Vielzahl von alten Tools, die für die Cloud angepasst wurden. Turner sagt: „Ich habe Trend Micro, Qualys, und Tenable eingesetzt, entweder in einer Unternehmensumgebung oder zu Testzwecken. Tenable und Qualys machten beide den Eindruck, als hätten sie ihre bestehenden Unternehmensanwendungen locker an die Cloud angeknüpft. Jedoch funktioniert das nicht gut, da man sich immer noch mit Agenten abgeben muss. Wir müssen uns immer noch mit Technologien auseinandersetzen, die für Dinge wie Serverless oder Container nicht geeignet sind."

Paidy hat auch Netzwerkscanner ausgeschlossen. Laut Turner: „Aufgrund meiner Erfahrung mit nicht authentifizierten Scannern wusste ich, dass sie nur begrenzte Sichtbarkeit hatten und Ausfallzeiten verursachen können.

„Authentifizierte Scanner liefern zwar mehr Daten über Schwachstellen, erfordern aber immer noch viel Arbeit bei der Konfiguration sowie erweiterte Rechte. Dadurch wird Ihr Unternehmen einem Risiko ausgesetzt, da Sie im Grunde ein weiteres gemeinsames Konto und Passwort haben."

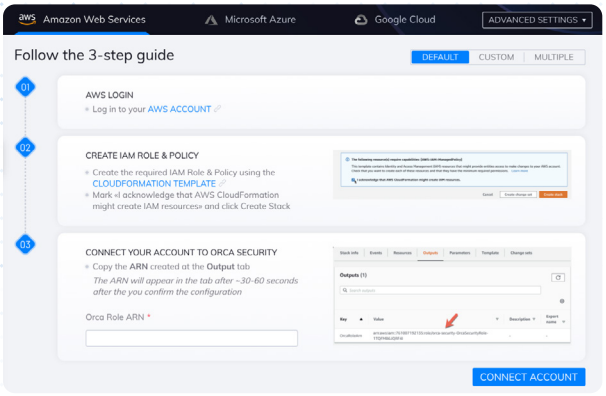
Cloud-Anbieter wie Amazon bieten Tools für Sicherheitsscans. „Amazons AWS Inspector, ein Schwachstellen-Scanner, benötigt einen Agenten. Normalerweise ist er in die Amazon AMI integriert, aber er funktioniert nur mit bestimmten AMIs", fährt er fort. „AWS GuardDuty ist die ideale Lösung für einen Schwachstellen-Scan und eine Überprüfung der Compliance. Aber Berichterstattung ist sein größtes Thema; die Verwendung der Daten kann eine Herausforderung darstellen. Es wird einfach eine Liste von Schwachstellen angezeigt, und dann müssen wir herausfinden, was wir dagegen tun können."

Beatty fügt hinzu: „Da wir mehrere AWS-Konten haben und mehrere Clouds nutzen, war es schwierig, eine einzige Übersicht zu haben, in der wir alles, was passiert, überwachen konnten. Die Multi-Cloud-Transparenz war unser wichtigstes Thema. Außerdem haben wir nicht die Zeit und die Ressourcen, um ein Tool zu entwickeln,



> „Tenable und Qualys machten beide den Eindruck, als hätten sie ihre bestehenden Unternehmensanwendungen locker an die Cloud angeknüpft. Jedoch funktioniert das nicht gut, da man sich immer noch mit Agenten abgeben muss. Wir müssen uns immer noch mit Technologien auseinandersetzen, die für Dinge wie Serverless oder Container nicht geeignet sind."
>
> **Jeremy Turner**
> Senior Cloud Security Engineer
> Paidy

das z. B. AWS-Dienste oder etwas Ähnliches nutzt. Wir wollen einen Dienst nutzen, der keinen Agenten benötigt, den wir nicht ständig aktualisieren müssen und der einfach funktioniert.“ Für Paidy erfüllt Orca Security all diese Bedürfnisse und mehr.



Orca SideScanning™ bietet dringend benötigte Sichtbarkeit

Die Orca Security-Plattform unterscheidet sich erheblich von anderen Sicherheits-Tools. Die als SaaS angebotene Lösung liest den Cloud-Blockspeicher nach dem Out-of-Band-Prinzip, also von der Seite – daher auch die Bezeichnung SideScanning™. Innerhalb der Cloud-Umgebung des Kunden wird kein Code ausgeführt. Stattdessen baut Orca ein reines Lesemodell der Cloud-Umgebung, das dann gescannt wird, um potenzielle Sicherheitsprobleme zu bewerten.

Die volle Transparenz ist das, was Turner am meisten schätzt. „Sichtbarkeit ist ein Problem, das jede Organisation betrifft. Orca hat uns sofort einen umfassenden und tiefen Einblick in unsere Bedrohungslandschaft gegeben“, sagt Turner. „Wenn wir diese Daten nehmen und sie den Leuten zeigen, gehen ihnen die Augen auf. Wir hatten einen Fall, in dem Orca eine ‚drohende Kompromittierung‘ eines Systems aufgedeckt hat, das wahrscheinlich schon seit zwei oder drei Jahren in einer Testumgebung im Einsatz war. Das System hat ein völlig veraltetes Betriebssystem ausgeführt. Nachdem Orca das Problem erkannt hatte, erstellten wir ein Ticket, das ein Techniker sofort bearbeiten konnte. Wir hatten das Glück, die Schwachstelle zu erschließen, bevor das System in die UAT und Produktion ging.“

Beatty stimmt dem Stellenwert der Sichtbarkeit zu: „Es gibt keine Entschuldigung dafür, dass man Probleme übersieht, wenn sie einem direkt vor Augen geführt werden. Und deutlicher als die Meldung ‚Drohende Kompromittierung‘ auf dem Orca-Dashboard kann es kaum werden.“

Orca hilft Paidy auch bei Problemen mit der Ausweitung von Konten. „Wir betreiben 12 AWS-Konten“, sagt Turner. „Wir wussten nicht, was sich in ihnen allen befindet, daher haben wir sie mit Orca verknüpft. Innerhalb von 30 Minuten hatten wir einen Überblick über die Gesamtlage aller Konten. Anders hätten wir das nie so schnell hingekriegt.“

Die Vermögensverwaltung ist eine weitere Funktion, die Orca Security für Paidy bereitstellt. Orca bietet ein Inventar des Standorts jedes Assets, Metadaten und eine Liste der Schwachstellen. „Es ist ziemlich cool, wenn ich eine Instanz auswählen und sehen kann, wer sich dort angemeldet hat, wie viele fehlgeschlagene Anmeldeversuche es gibt oder welche Pakete dort installiert sind. Ich schätze es, dass ich das tun kann, ohne für jede Instanz von einem Agenten abhängig zu sein“, sagt Turner.

Orca Security identifiziert und schützt personenbezogene Daten und erleichtert Paidys Compliance-Bemühungen

Je mehr Erfahrung Paidy mit der Orca Security-Plattform sammelt, desto mehr Möglichkeiten findet das Team, die von ihr generierten Daten zu nutzen. Als Fintech-Unternehmen sind wir sehr auf toxische Datenkombinationen bedacht – Orca hilft uns dabei“, sagt Turner. „Zum Beispiel müssen Kunden ihre Handynummer angeben, um unseren Service zu nutzen. Aber wenn es um Privat- oder E-Mail-Adressen in Verbindung mit möglichen Bankkontoinformationen

und Kaufhistorie geht, dann haben wir es mit personenbezogenen Daten und japanischen Datenschutzbestimmungen zu tun."

Turner erklärt, wie Orca zum Schutz personenbezogener Daten beiträgt." Eine Funktion lässt uns wissen, wenn Orca personenbezogene Daten vermutet. Es ist wie ein Alarm, der uns mitteilt: „Dieser Server enthält E-Mail-Adressen, die nicht zu paidy.com gehören. Was ist los?' Dann können wir nachforschen. Im Moment sagt das Tool nicht: ‚Hier ist eine toxische Datenkombination', aber es zeigt uns, wo wir jagen müssen. Wir hatten eine Situation, in der das Data-Science-Team einen Datenbank-Joiner erstellte, der zu einer äußerst toxischen Kombination von Daten führte. Orca hat uns geholfen, dies rechtzeitig zu erkennen und im Keim zu ersticken."

Paidy muss eine Reihe von Datenschutzgesetzen einhalten. Japans Verordnung über den grenzüberschreitenden Datenschutz ähnelt der DSGVO der EU, und das japanische Gesetz zum Schutz personenbezogener Daten wurde 2004 erlassen. Orca hilft dabei, den Auditoren zu beweisen, dass Paidy in der Lage ist, persönliche Daten zu identifizieren und zu verschlüsseln. Paidy hat die Gewissheit, dass es in der Lage ist, nach gefährdeten personenbezogenen Daten zu suchen.

Turner nutzt die Integration von Orca Security in Jira, um Tickets zu öffnen. Diese lösen wiederum Workflows aus, sodass Personen und Prozesse geeignete Maßnahmen ergreifen können, um beispielsweise sensible Daten zu verschlüsseln oder andere von Orca aufgespürte Probleme zu beheben.



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

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