Orca Security bringt Zip in weniger als einem Tag von 18 % Risikosichtbarkeit auf 100 % Deckung

BRANCHE
Finanzdienstleistungen

CHAMPION
Peter Robinson, Director der Cybersicherheit und Business IT

CLOUD-UMGEBUNG
AWS, Azure

„Nach jahrelangen Problemen endlich volle Transparenz – und das innerhalb eines Nachmittags! Ich habe schon einiges erlebt, aber so etwas noch nie."

Peter Robinson
Director der Cybersicherheit und Business IT, Zip

Cloud-Sicherheit: Herausforderungen

- Die rasche Expansion des Unternehmens führt zu einem schnellen Wachstum des Cloud-Bestandes
- Die flüchtige Natur der Infrastruktur erschwert die Suche nach Schwachstellen
- Verschiedene Umgebungen werden von mehreren Personen in mehreren Ländern betrieben

Cloud-Sicherheit: Ergebnisse

- 100 % Abdeckung von Cloud-Accounts mit vollständiger Transparenz, Bestandsaufnahme und priorisierten Abhilfemaßnahmen – alles ohne Auswirkungen auf Produktionsumgebungen
- Geringere Abhängigkeit von DevOps bei gleichzeitiger Sicherstellung ihrer vollen Unterstützung für priorisierte Abhilfemaßnahmen
- Massive Kosteneinsparungen, da keine Integrationskosten anfallen, keine sechs Vollzeitbeschäftigten erforderlich sind, um Risiken zu ermitteln und zu priorisieren, und das Pay-as-you-go-Lizenzierungsmodell von Orca nur für tatsächlich genutzte Assets gilt

Zip glaubt an unermüdliche Innovation

Zip Co ist ein führender Akteur in der nächsten Generation der Kundenfinanzierungs- und Zahlungsverkehrsbranche. Das Unternehmen bietet Point-of-Sale-Kredit- und digitale Zahlungsdienste für den Einzelhandel, die Haushalts-, Gesundheits-, Automobil- und Reisebranche. Zip wurde 2013 gegründet und hat seinen Hauptsitz in Sydney, Australien. Das Unternehmen ist schnell gewachsen und verfügt heute über Niederlassungen in Australien, Neuseeland, Südafrika, dem Vereinigten Königreich und den USA. Eine weitere Expansion in Nordamerika, Europa und im Nahen Osten ist geplant.

Die Rechenplattform von Zip ist komplett digital und in der Cloud gehostet. Die Plattform nutzt Big Data in ihrer proprietären Betrugs- und Kreditentscheidungstechnologie, um Antworten in Echtzeit zu liefern. Entsprechend dem Unternehmenswachstum wächst auch der Cloud-Bestand rasch. Vor einem Jahr waren es noch sechs AWS-Konten. Heute gibt es 22 AWS- und neun Azure-Konten – weitere sind in Vorbereitung.

> Vor Orca hatten wir insgesamt vielleicht eine Abdeckung von 18 % bei unserer Schwachstellenbewertung. Orca hat uns in weniger als einem Tag auf 100 % gebracht.“
>
> **Peter Robinson**
> Director der Cybersicherheit und Business IT, Zip

Peter Robinson ist Direktor der Cybersicherheit und Business IT, verantwortlich für die Cyber-Risiko- und Sicherheitslage des Unternehmens. „Zip wurde in der Cloud geboren und das ist eine schwierige Umgebung für die Sicherung unserer Assets, da herkömmliche Sicherheitstools hier nicht gut funktionieren“, erklärt er. Die meiste Zeit seiner zweijährigen Tätigkeit bei Zip hat er mit der Suche nach der richtigen Kombination von Tools verbracht, die einen guten Einblick in die Schwachstellen und Risiken von Zip und die Mittel zu deren Minderung bieten.

Von geringer Sichtbarkeit zu 100 % an einem Nachmittag

Die Plattform von Zip ist auf dem neuesten Stand der Cloud-Technologien. „Wir haben uns stark in Richtung serverloses Computing und Infrastruktur als Code bewegt“, bemerkt Robinson. „Die flüchtige Natur unserer Umgebung bringt uns in eine Lage, in der wir keine Agenten auf diese Geräte bringen können, bevor sie verschwunden sind. Wir können sie nicht im herkömmlichen Sinne über das Netzwerk scannen, und es gibt keine Möglichkeit, eine Verbindung zu diesen Rechnern herzustellen, um ihren Sicherheitsstatus zu überprüfen, wenn sie nicht laufen.“

„Wir haben auch das Problem, dass viele Umgebungen von verschiedenen Gruppen betrieben werden. Wir haben sechs DevOps-Teams, die an verschiedenen Teilen der Infrastruktur und anderen Dingen arbeiten. Es ist fast unmöglich, Ressourcen für die Risikobewertung einzusetzen“, so Robinson. „Orca hat dieses Problem sofort für uns gelöst.“

Robinson erfuhr von Orca Security durch LinkedIn-Artikel. „Wir waren zunächst skeptisch gegenüber den Behauptungen von Orca, aber wir haben es ausprobiert. Nach jahrelangen Problemen endlich volle Transparenz – und das innerhalb eines Nachmittags! Ich habe schon einiges erlebt, aber so etwas noch nie.“

Orca übertrifft die Tools der Konkurrenz bei weitem

Robinson verbrachte zwei Jahre damit, herkömmliche Tools zum Scannen von Schwachstellen sowie andere, die speziell für containerähnliche Umgebungen entwickelt wurden, zu evaluieren. „Sie hatten alle die gleichen Probleme. Erstens benötigten sie zu viele Ressourcen für den Einsatz von Agenten und Scannern. Zweitens benötigen sie einen Berechtigungsnachweis, um sich zu authentifizieren, was das Lizenzierungsmodell aus unserer Sicht zum Scheitern verurteilt. Und drittens setzt keines der Tools automatisch Prioritäten und verfolgt Abhilfemaßnahmen."

Die Frage der Lizenzierung ist ebenfalls ein großer Nachteil bei diesen Tools. „Bei den anderen Anbietern müsste ich eine umfassende, unbegrenzte Asset-Lizenz erwerben. Sobald eine Lizenz verwendet wird – wenn auch nur für ein flüchtiges Asset – müssen wir dafür bezahlen. Ein Server war nur sechs Stunden in Betrieb, und schon hat er eine Lizenz gebraucht. Die Arbeit mit diesen Tools zu erledigen, würde mich fünfmal mehr kosten." Robinson berichtet, dass diese Art der Lizenzierung ihn eine Viertelmillion Dollar pro Monat gekostet hätte.

Das Hauptproblem bei all diesen Tools ist, dass es keine Priorisierung der Risiken gibt. Laut Robinson gibt es beispielsweise 129 Regeln, die bei 2.000 Assets fehlschlagen, und das Tool erstellt eine sechs- bis achtseitige Liste der Fehlschläge. „Aus diesem Feuerwehrschlauch kann man nicht trinken. Es ist nicht umsetzbar. Selbst das SIEM meldete in den letzten sieben Tagen 55.000 Fehlschläge. Das kann man gar nicht einschätzen."

Orca überwindet all diese Nachteile. Die Bereitstellung erfolgt im Handumdrehen und erfordert lediglich die Erstellung einer einzigen Rolle, was nur wenige Minuten dauert. Es müssen keine Agenten installiert werden. Die Lizenzierung ist viel überschaubarer und basiert auf den tatsächlich genutzten Assets.

Was Orca jedoch wirklich auszeichnet, sind seine Priorisierungsfunktionen. „Orca sagt mir, dass ich mich heute auf 28 Dinge konzentrieren muss. Bei 25 Cloud-Konten mit etwa 840 Rechenressourcen, VMs und Tausenden von anderen Assets beläuft sich das tatsächliche Risiko auf 28 Dinge, um die sich heute gekümmert werden muss", erklärt Robinson. „Das können wir schaffen."

Das Zip von Robinson ist klein, daher muss es sich auf Tools verlassen können, um seine Ziele zu erreichen. „Mit Orca ist die gesamte Automatisierung, die Priorisierung, die Korrelation und der Null-Effekt-Einsatz in unseren Produktionsumgebungen einfach Gold wert. Das ist fantastisch", sagt er.

Orca verbessert die Zusammenarbeit und Produktivität von IT-Sicherheit und DevOps

Robinson sagt, dass die DevOps-Teams schnell arbeiten, um ihre Produkte auf den Markt zu bringen. Er kann nicht von ihnen verlangen, dass sie die Entwicklung eines Zip-Produkts einstellen, um Agenten und Netzwerkscanner einzurichten. Orca nimmt ihnen diese Last ab. Tatsächlich sind es die DevOps-Teams, die ihn bei der Einführung der Orca Security-Plattform am meisten unterstützt haben.

„Das Wichtigste ist, dass unsere DevOps-Mitarbeiter nichts tun müssen. Sie erstellen eine Rolle und fertig. Sie müssen in Zukunft nichts mehr tun. Es gibt keine Bereitstellung, keine Netzwerkregeln, keine Sicherheitsgruppen, die geändert werden müssen, keine Bereitstellung von Endpunktanwendungen oder Agenten, keine Anmeldedaten – nichts. Das hat meine Welt verändert“, sagt Robinson.

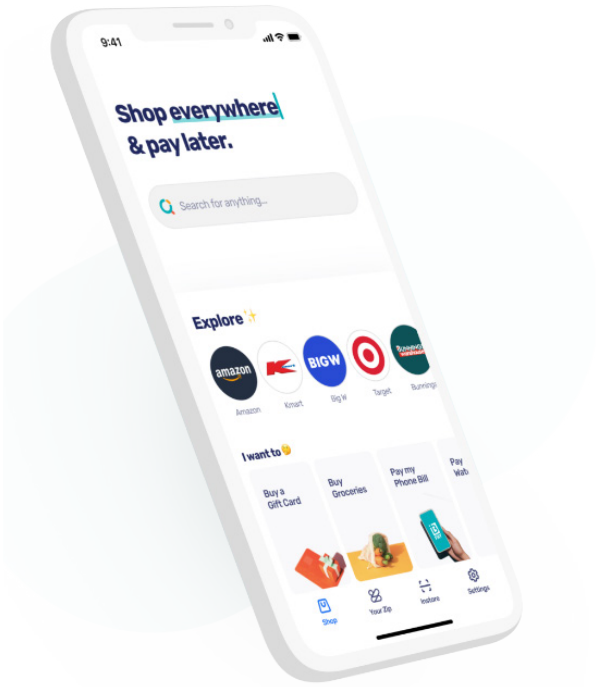
IT-Sicherheit und DevOps-Teams arbeiten jetzt gut zusammen. „Ich kann ihnen die von Orca empfohlenen Abhilfemaßnahmen nach Prioritäten geordnet vorlegen. Es gibt sehr klare Anweisungen zu Themen, die sehr wichtig sind“, erklärt Robinson. „Und es ist nicht nur eine Sache der Endpunkte. Angenommen, wir haben ein Problem mit der Sicherheitsgruppe dieser Netzwerk-ACL, diesem Load Balancer und diesem Endpunkt. Orca bietet eine Karte. Unsere Leute sagen: 'Oh, Orca zeigt, wie man CloudFlare und die internen Load Balancer umgehen kann. Es zeigt das Multipath Routing.' Wir wissen, dass das nicht passieren sollte, weil es bedeutet, dass jemand unsere WAF umgeht.“ Robinson sagt, dass diese Art von Informationen aus anderen Quellen nicht zu bekommen sind. „Orca bietet einen tiefen Einblick in ihre Fehlkonfigurationen. Sie können es visuell sehen. Sie wissen, dass sie es ändern oder die Sicherheitsgruppen so einrichten müssen, dass man nur durch den Load Balancer kommen kann. Und der Load Balancer nimmt nur Input von CloudFlare entgegen und man kann den Load Balancer nicht direkt aus dem Internet erreichen. Diese Art von Erkenntnis ist unglaublich hilfreich, um unsere Arbeitsbelastung zu verringern“, so Robinson.

„Unsere DevOps-Mitarbeiter konzentrieren sich auf unser Produkt, was sie auch tun sollten. Ich kann nicht von ihnen verlangen, dass sie ihre Bemühungen darauf verwenden, überall Endpunkt-Agenten einzusetzen und Scanner-Anmeldeinformationen zu erstellen.“

Peter Robinson
Director der Cybersicherheit
und Business IT
Zip

Orca unterstützt unternehmenstaugliche Funktionen wie die rollenbasierte Zugriffskontrolle. „Es ist wirklich gut, dass wir Personen Konten zuweisen können, wenn wir sie hinzufügen. Ich kann es so einstellen, dass meine Quadpay-Mitarbeiter in den USA nur Quadpay-Daten sehen und an Quadpay-Konten arbeiten können, anstatt das gesamte Unternehmen zu sehen. Sie können nur sehen, was sie sehen müssen“, sagt Robinson.

Wenn Zip Orca nicht unternehmensweit einsetzen würde, müsste nach Robinsons Schätzungen in jedem der sechs Länder mindestens ein Vollzeitmitarbeiter beschäftigt sein. „Wir bräuchten wahrscheinlich sechs zusätzliche Vollzeitkräfte, um eine lange, nicht priorisierte Liste von Schwachstellen zu durchforsten, herauszufinden, woran wir arbeiten müssen, Tickets für Abhilfemaßnahmen zu erstellen – und das alles, während wir versuchen, Agenten auf die Rechner zu bringen und alles Weitere.



Es ist also mehr als nur eine Sache des Risikomanagements. Es geht auch um Zeit, Kosten und Mühe“, so Robinson. „Orca schlägt zwei Fliegen mit einer Klappe – das Risiko ist sofort beseitigt, zumindest was die Sichtbarkeit angeht, und die Kosten sind auch sofort erledigt.“

Orca fügt sich in den Risikomanagementprozess von Zip ein

Robinson verfügt über eine Methode zur Erkennung von Problemen – sei es durch Penetrationstests, externe Schwachstellenscans, interne Scans, Beobachtungen, Vorfälle oder andere Mittel – und leitet sie durch einen Risikomanagementprozess zu Jira. „Wir haben ein Risikoboard in Jira, auf dem wir das inhärente Risiko bewerten. Wir weisen dann dem verantwortlichen Eigentümer ein Subticket oder eine Aufgabe zu und bewerten die erforderlichen Abhilfemaßnahmen“, so Robinson. „Die Integration von Orca in Jira ist perfekt, das funktioniert also auf jeden Fall für uns.“

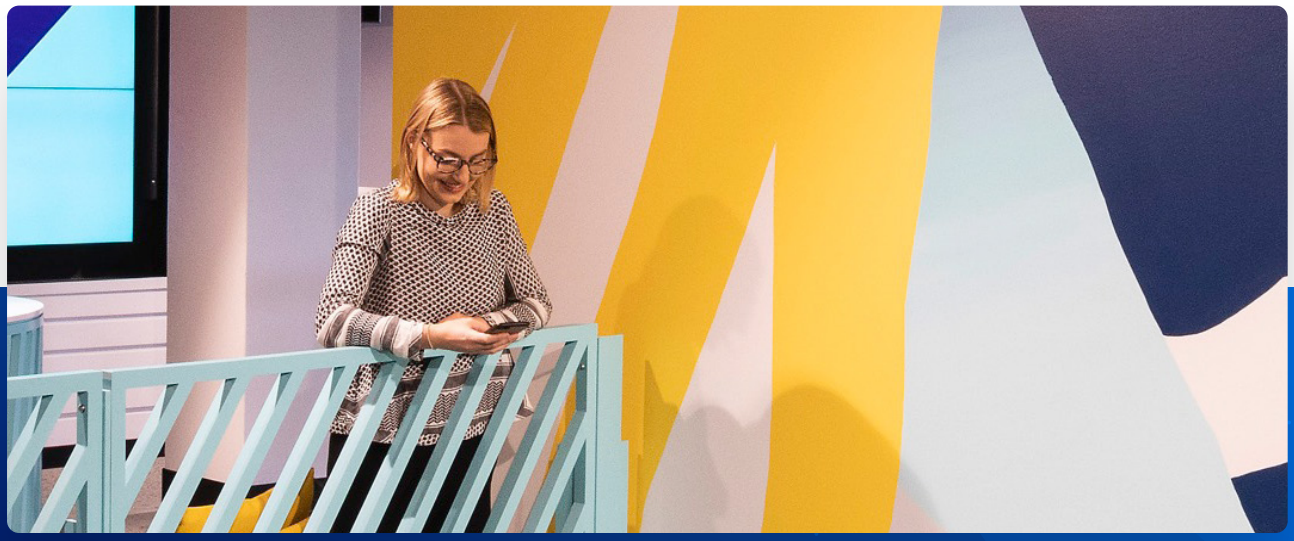
Ein einzigartiges Merkmal von Orca ist, dass es Probleme selbst lösen kann. Wenn ein Problem erkannt und gelöst wird, vermerkt Orca, dass es behoben wurde. „Früher mussten die Jungs eine manuelle Bewertung und einen Test durchführen, um festzustellen, ob die Sache tatsächlich behoben wurde oder nicht. Während Orca einfach sagt: ‚Es ist weg. Danke.‘ Wir können unser Restrisiko auf null setzen und das Ticket schließen“, sagt Robinson. „Das spart ziemlich viel Zeit.“

Als Zip kürzlich ein Unternehmen aufkaufte, wurde Robinson gebeten, dessen Vermögenswerte unter seine Verwaltung zu stellen. „Ich brauchte buchstäblich nur wenige Minuten, und schon waren zwei brandneue Amazon-Konten zu 100 % unter meinem Schwachstellenmanagement.“

Orca gewinnt den ROI und den Business Case

Zip verfügt über Tools, die ihre Assets von außen scannen. „Wir geben Domänennamen ein, es führt eine Erkennung durch und nutzt Bugbounty-Techniken, um unsere externen Schwachstellen zu bewerten“, berichtet Robinson. „Bevor wir Orca gefunden haben, waren interne Bewertungen jedoch eine größere Herausforderung. Ich habe dafür gekämpft, dass wir die notwendigen internen Scans bekommen. Wir haben die Budgets überarbeitet und versucht, den Aufwand, die Arbeit und die Ablenkung von unserem Zip-Produkt zu beziffern. Ich habe den Business Case geschrieben, um diese immateriellen Werte einzubeziehen. Ich habe unseren Führungskräften erzählt, wie viel Zeit es kostet, die Mitarbeiter von ihrer eigentlichen Arbeit abzulenken, um Agenten zu installieren und Dinge einzurichten, und wie viel Zeit es kostet, Schwachstellen zu durchsuchen, um diejenigen zu finden, die wichtig sind, und all die manuellen Korrekturen vorzunehmen. Das kostet enorm viel Zeit. Außerdem sind die Integrationskosten riesig.“

Er sagt, dass mit Orca das Risiko erheblich reduziert wird, weil die Deckung 100 % beträgt. Und die Zeitersparnis beträgt im Vergleich zu jedem anderen Produkt fast 100 %. „Die Bereitstellung dauert nur 20 Minuten und ist im Backend mit Jira integriert“, so Robinson. „Aus Sicht eines Systemadministrators, der Infrastruktur oder von DevOps gibt es nichts anderes zu tun – und zwar für immer. Der Business Case für Orca ist sehr überzeugend.“



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.