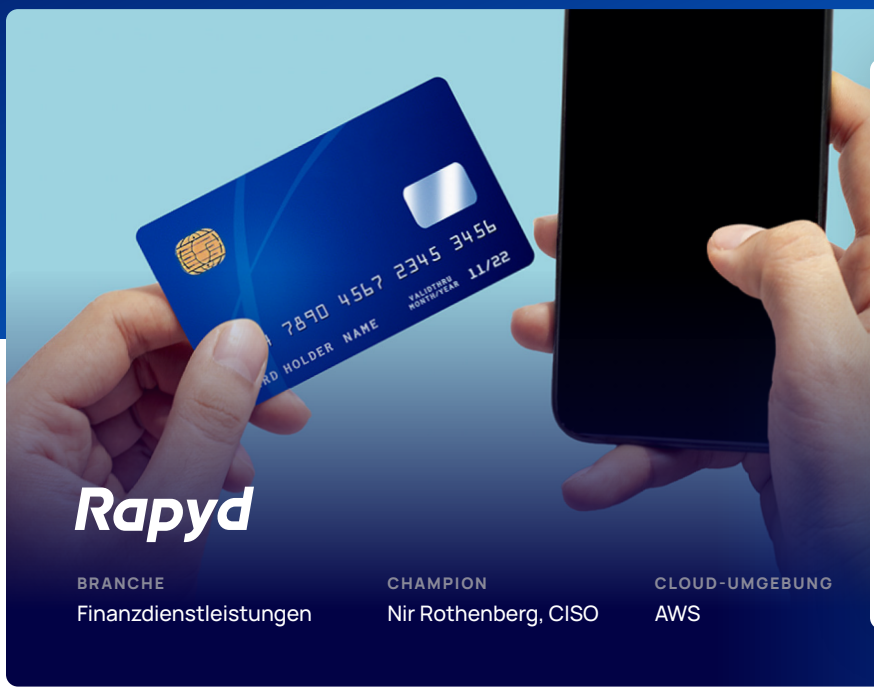
Rapyd nutzt die von Orca Security gewonnenen, tiefen Einblicke in die Cloud zum Schutz globaler Zahlungssysteme



Rapyd

BRANCHE
Finanzdienstleistungen

CHAMPION
Nir Rothenberg, CISO

CLOUD-UMGEBUNG
AWS

„Orca ist eine große Hilfe für unsere Arbeit mit DevOps. Mein Systemadministrator kann DevOps jetzt zeigen und erklären, was wir gefunden haben. Wir sind jetzt kooperativer und hilfreicher für sie. Das ist ein großer Schritt in Richtung DevSecOps – die organisatorische Reibung zwischen DevOps und meinem Sicherheitsteam ist weg."

Nir Rothenberg
Chief Information Security Officer
Rapyd

Herausforderungen der Cloud-Sicherheit

- Vollständige kontextuelle Transparenz zur Förderung von priorisiertem Patch-Management
- Nachweis guter Governance und Einhaltung von Vorschriften gegenüber Auditoren
- Vereinfachung der Sicherheit

Ergebnisse der Cloud-Sicherheit

- Sofortige und vollständige Transparenz seiner Cloud-Infrastruktur
- Integration von Orca mit Jira zur Automatisierung der CI/CD-Pipeline für sicherheitsrelevante Aufgaben
- Erstellung einer kooperativen Umgebung mit DevOps für den Wechsel zu DevSecOps

Rapyd beseitigt die Hindernisse für universelle Zahlungen

Rapyd bekämpft die Fragmentierung in der globalen Zahlungsverkehrsbranche. Das Unternehmen entwickelt die Technologie, die die Komplexität des grenzüberschreitenden Handels beseitigt und gleichzeitig das Know-how für lokale Zahlungen bereitstellt.

Globale E-Commerce-Unternehmen, Technologiefirmen, Online-Marktplätze und Finanzinstitute nutzen die Fintech-as-a-Service-Plattform von Rapyd, um lokalisierte Fintech- und Zahlungsfunktionen reibungslos und einfach in ihre Anwendungen einzubinden. Das Rapyd Global Payments Network ermöglicht Unternehmen den Zugang zum weltweit größten lokalen Zahlungsnetzwerk, das über 900 lokal bevorzugte Zahlungsmethoden umfasst. Dazu gehören Banküberweisungen, elektronische Geldbörsen und Bargeld in mehr als 100 Ländern.

Mit Orca wird Patch-Management zum Kinderspiel

Jedes globale digitale Zahlungssystem muss heute unablässig auf Sicherheit ausgerichtet sein. Das ist es, was Nir Rothenberg, den CISO von Rapyd, antreibt, der den IT- und Sicherheitsbetrieb leitet. Sein Unternehmen verfügt zwar über gute Sicherheitspraktiken, doch war es stets eine Herausforderung, dies gegenüber Prüfern nachzuweisen.

„Unser Geschäft ist der Zahlungsverkehr, also müssen wir PCI DSS-konform sein – und das sind wir auch“, sagt Rothenberg. „Jedes Jahr wollen die Auditoren sehen, dass wir ein gutes Patching-Verfahren anwenden. Wir patchen unermüdlich, aber aus verschiedenen Gründen ist es nie 100%ig. Alles zu dokumentieren, um zu zeigen, dass wir die Sache im Griff haben, war ein echter Schmerzpunkt, bevor wir Orca gefunden haben.“

Rapyd wird vollständig in der Cloud betrieben, wobei alles auf AWS läuft. Rothenberg wollte ein intelligentes Tool, das einen vollständigen Überblick über die Server bietet, die wirklich einen Patch benötigen. Er bemühte sich um eine nach Prioritäten geordnete Liste, auf der alles im Kontext steht. Viele Tools können scannen und auflisten, was gepatcht werden muss, aber ohne Kontext ist die Liste lang und vieles davon bedeutungslos.

„Den nativen AWS-Tools fehlt es an Intelligenz. Ein AWS-Inspector-Scan kann uns zwar Ergebnisse liefern, aber diese Ergebnisse passen nicht immer in unseren Kontext“, so Rothenberg. „Wir erhalten eine Liste mit tausend Patches, die alle als kritisch eingestuft werden. Einige können jedoch nicht eingesetzt werden, weil sie nicht mit unserer Distribution übereinstimmen, oder sie sind für Offline-Server gedacht, bei denen Patches keine Rolle spielen. Wenn ich einem Auditoren einen solchen Bericht zeige, denkt er noch, dass wir uns nicht um die Geschäfte kümmern. Nehmen wir an, es gibt einen Server mit einer kritischen Sicherheitslücke. Es gibt einen Patch, der auf Ubuntu 18.04 funktioniert, aber wir haben 18.9. In diesem Kontext können wir also nicht patchen. Außerdem ist der Server nicht mit dem Internet verbunden, sodass dies ohnehin nicht wirklich wichtig ist. Orca sagt uns: 'Kritischer Patch, mittleres Risiko.' Das kann ich einem Auditoren zeigen, um unser Handeln zu rechtfertigen.“

Rothenberg bewertete verschiedene AWS-Tools, darunter GuardDuty, Inspector und Detective, sowie traditionelle agentenbasierte Sicherheitstools und Netzwerkscanner. Er bemerkte, dass diese Tools nur mit großem Aufwand funktionieren – zu viel, um dem nahezukommen, was Orca direkt aus einer Hand liefert. „Bei agentenbasierten Tools müssten wir Server einrichten, einen Agenten einsetzen, Skripte schreiben und ausführen, unsere Umgebung kennen und ein Dashboard konfigurieren, das anzeigt, was wir sehen wollen. Wir müssten ihm beibringen, was ein Risiko ist und was nicht, und einen Großteil der Analysearbeit selbst erledigen. Und wir würden immer wieder nachbessern, denn Risiko ist dynamisch, es ändert sich. All diese Schritte laufen mit Orca automatisch ab."

Orca identifiziert Nichteinhaltung der CIS-Kontrollen und Risiko für personenbezogene Daten

Rothenberg beaufsichtigt die Einhaltung der Vorschriften des Center for Internet Security Controls durch Rapyd. Auch hierfür probierte er systemeigene AWS-Tools aus und fand sie unzureichend. „Wir müssen selbst herausfinden, was ihre Scan-Ergebnisse bedeuten. Aber mit Orca sind die Scanergebnisse verarbeitet und auf den Punkt gebracht. Nichtkonformitäten mit CIS, die ein sofortiges Handeln erfordern, sind direkt zu erkennen. Wir haben Orca mit Jira integriert. Wenn die Arbeit DevOps zugewiesen werden muss, klicken wir einfach auf eine Schaltfläche."

Laut Rothenberg ist die Erstellung von Tickets für die interne Aufgabenverfolgung unerlässlich. „Da wir die Aufgaben und die damit verbundenen Risiken zu jedem Zeitpunkt kennen, können wir die Aufgaben, die wir DevOps zuteilen, priorisieren, um sie nicht zu überfordern. Wenn wir geprüft werden, können wir zeigen: 'Das ist unsere Pipeline, das ist unser Arbeitsplan.' Es ist alles in Jira und alles hat einen Prüfpfad."

Der CISO wendet sich auch an Orca, um Situationen zu erkennen, in denen personenbezogene Daten in Dateien gefährdet sind, die möglicherweise nicht ordnungsgemäß geschützt sind. „Als Zahlungsverkehrsunternehmen sind wir sehr sensibel, was die Gefährdung von personenbezogenen Daten angeht. Wenn ein Server personenbezogene Daten enthält oder Verschlüsselungsschlüssel offengelegt sind, erkennt Orca dies sofort und zeigt uns die Risiken für diesen Rechner und das jeweilige Asset an. Wir sind in der Lage, den Vorfall schnell zu beheben."

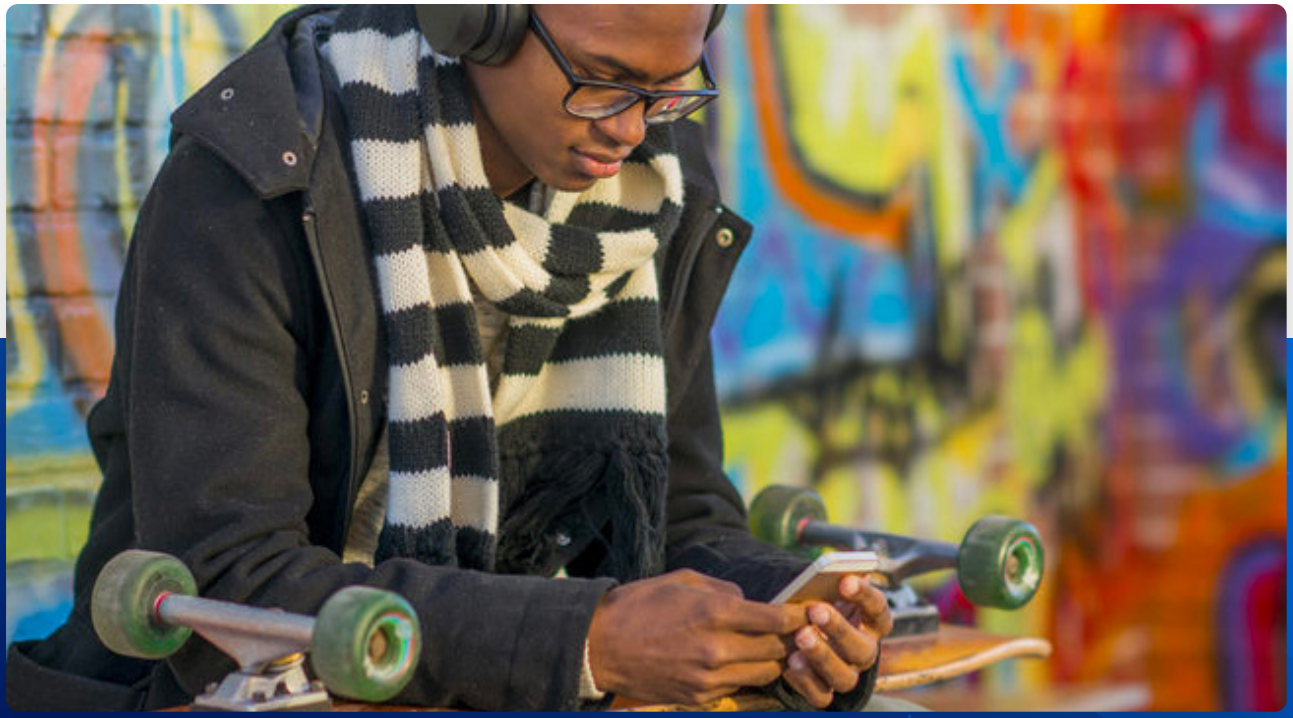
In früheren Jahren hat Rapyd Schwachstellen in Excel-Tabellen erfasst. Orca hat dieses Verfahren hinfällig gemacht. „Jetzt ist alles automatisiert und hat eine CI/CD-Pipeline. Wenn wir das nächste Mal geprüft werden, kann ich unsere Orca- und Jira-Berichte vorlegen, um zu zeigen, welche Risiken wir verfolgen und was wir tun, um sie zu beheben", sagt Rothenberg. „Mit der Art und Weise, wie wir heute unsere Assets überwachen, wird es sehr einfach, Patching und Compliance nachzuweisen."

> „Nach der Überprüfung durch Orca wird ein aussagekräftiger Bericht mit handlungsrelevanten Informationen ausgegeben, der alles in Kontext setzt. Neben den Erkenntnissen liefert er auch Randüberlegungen, die unseren Patch-Management-Prozess unterstützen."
>
> **Nir Rothenberg**
> Chief Information Security Officer,
> Rapyd

Einfachheit führt zu besserer Sicherheit

Orca hat das Leben von Rothenbergs Sicherheitsteam vereinfacht. „Gleich nachdem wir Orca mit unserer Umgebung verknüpft hatten, fand es sofort eine Menge interessanter Dinge. Ohne Orca hätten wir niemals diese Transparenz erreicht."

„Orca ist eine große Hilfe für unsere Arbeit mit DevOps", sagt Rothenberg. „Mein Systemadministrator kann jetzt mit DevOps auf Augenhöhe sprechen. Er kann erklären, was wir gefunden haben, er kann es ihnen zeigen. Das hilft uns, professioneller zu werden, die Umgebung besser zu sehen und besser zu verstehen. Jetzt arbeiten wir stärker mit DevOps zusammen und sind ihnen eine größere Hilfe. Das ist ein echter Schritt in Richtung DevSecOps. Jetzt läuft alles wie bei einer gut geölten Maschine. Die organisatorische Reibung zwischen Security und DevOps ist weg."



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.