Orca Security unterstützt BeyondTrust Secure Cloud-Dienste, die von Tausenden von Kunden genutzt werden

BeyondTrust

BRANCHE
IT-Sicherheit

CHAMPION
Morey Haber: CTO und CIO

CLOUD-UMGEBUNG
AWS, Azure

„Orca Security verwaltet heute alle unsere Cloud-basierten Lösungen für privilegierte Zugriffssteuerung (Privileged Access Management – PAM).“

Morey Haber
CTO und CIO
BeyondTrust

Herausforderungen der Cloud-Sicherheit

- Der Einsatz eines agentenbasierten Sicherheitstools erwies sich als zu komplex und kostspielig in der Verwaltung und bot zudem keine ausreichende Transparenz
- Agenten können nicht auf die angepassten Appliance-Images des Unternehmens geladen werden
- Erforderliche Berichterstattung zur Sicherstellung der Compliance für ISO, SOC, CIS und PCI

Ergebnisse der Cloud-Sicherheit

- Voller Produktionsbetrieb innerhalb von zwei Monaten; vollständige Integration durch Azure Sentinel Security Center – einschließlich Ticketing mit ServiceNow, Jira und einer Vielzahl anderer Integrationen
- Sicherstellung und Überwachung von Cloud-Lösungen, die an Kunden verkauft werden, ohne die Produktionsumgebung zu gefährden
- Verringerung der Entwicklungs- und Qualitätssicherungszeit um 1 ½ Vollzeitäquivalente bei gleichzeitiger Gewährleistung einer größeren Transparenz und besser umsetzbarer Bewertungsergebnisse
- Orca-Berichte zeigen Compliance-Nachweise zu Passwörtern, Firewall-Konfiguration, Schwachstellen und mehr

BeyondTrust bietet Cloud-basiertes Privileged Access Management für mehr als 70 % der Fortune-500-Unternehmen

BeyondTrust ist der weltweit führende Anbieter im Bereich der privilegierten Zugriffssteuerung und ermöglicht es Unternehmen, ihr gesamtes Universum an Berechtigungen zu sichern und zu verwalten. Mehr als 20.000 Kunden – darunter mehr als 70 % der Fortune-500-Unternehmen – nutzen die drei Kernlösungen von BeyondTrust, um ihre Umgebungen abzusichern und die Kontrolle zu erlangen, die sie benötigen, um Risiken zu reduzieren, Compliance zu erreichen und die betriebliche Leistung zu steigern.

Morey Haber erfüllt mehrere Rollen bei BeyondTrust. Als CTO überwacht er die Produktstrategie. Er ist auch der CISO des Unternehmens und damit für die interne und Cloud-Sicherheit von über 4.000 Cloud-Implementierungen bei Kunden verantwortlich. Außerdem beaufsichtigt er alle Bemühungen um Governance, Risiko und Compliance.

Zwanzig der 20 Jahre, die Haber in der IT-Branche tätig ist, hat er den Aspekten der Cybersicherheit gewidmet. Er hat mehrere Bücher über Angriffsvektoren und Strategien für Schwachstellenmanagement verfasst und war Direktor für Sicherheitstechnik bei einem Unternehmen, das von BeyondTrust übernommen wurde. Er weiß, worauf es ankommt, um technische Unzulänglichkeiten zu erkennen, die ein Unternehmen gefährden.

Orca setzt auf einen neuen Ansatz für Cloud-Sicherheit

Nach einer Demo von Orca Security war Haber fasziniert. „Ich war überwältigt. In all den Jahren, in denen ich mich auf Strategien und Produkte für das Schwachstellenmanagement spezialisiert habe, ist dies ein völlig neuer Ansatz mit enormem Potenzial."

Haber und sein Cloud-Team führten einen Testlauf mit der Orca-Plattform durch. „Wir haben das System installiert, und es hat innerhalb weniger Tage funktioniert. Es brachte bessere Ergebnisse und mehr Transparenz, als wir jemals von konkurrierenden Agenten erhalten haben. Vor Orca haben uns Agenten nur einen Überblick über die Laufzeiten gegeben, aber nicht den Rest der Umgebung gezeigt", sagt Haber. „Wir waren sehr beeindruckt. Orca ist jetzt vollständig implementiert und verwaltet alle Cloud-Lösungen, die wir heute verkaufen."

Orca sichert die Workloads der Kunden von BeyondTrust

BeyondTrust stellt einen einzigartigen Anwendungsfall für Orca Security dar. Während die meisten Orca-Kunden die Software nutzen, um ihre eigenen Cloud-Workloads zu bewerten, überwacht BeyondTrust als Sicherheitsanbieter Workloads, auf denen Cloud-Lösungen seiner Kunden laufen. Heute unterstützt das Unternehmen mehr als 4.000 Cloud-Implementierungen – und viele weitere sind geplant, zumal BeyondTrust sein schnelles Wachstum fortsetzt.

> „Ich arbeite seit über 20 Jahren mit Lösungen zur Schwachstellenanalyse. Ich habe sogar ein Buch über die Erstellung einer Strategie für Schwachstellenmanagement geschrieben. Ich habe noch nie zuvor so etwas wie die Orca Security-Plattform gesehen. Dieses Produkt ist brillant."
>
> **Morey Haber**
> CTO und CIO
> BeyondTrust

Haber nennt ein Beispiel für den gegenwärtigen Einsatz von Orca. „Der Privileged Remote Access von BeyondTrust ermöglicht den Zugriff Dritter auf die Umgebung eines Kunden, um z. B. das HVAC-System zu überprüfen, sicherzustellen, dass die Drucker funktionieren, oder was auch immer der Bedarf ist. Unsere Lösung führt eine Credential-Injection auf den Zielsystemen durch, sodass Dritte die Passwörter weder kennen noch sehen. Sobald sie sich angemeldet haben, zeichnet das Produkt sämtliche Vorgänge auf dem Bildschirm auf und dokumentiert diese. So entsteht eine echte Zero-Trust-Architektur für den Fernzugriff."

„Orca stellt sicher, dass nichts offen oder falsch konfiguriert ist, dass Instanzen keine Patches vermissen und dass keine Schwachstellen in der Cloud-Umgebung unserer Kunden existieren", sagt Haber. „Hier ist ein weiteres Beispiel für den signifikanten Wert von Orca. Wir haben eine neue Firewall für eines unserer Produkte installiert. Orca wies uns schnell auf eine Fehlkonfiguration in den Standardeinstellungen hin und wir konnten sie sofort korrigieren. Wie sonst hätten wir das gesehen? Ein Agent hätte nicht helfen können, da es extern passierte, aber Orca erfasste es. Für mich ist das von unschätzbarem Wert."

„Orca stellt sicher, dass nichts offen oder falsch konfiguriert ist, dass Instanzen keine Patches vermissen und dass keine Schwachstellen in der Cloud-Umgebung unserer Kunden existieren."

Morey Haber
CTO und CIO
BeyondTrust

Probleme mit agentenbasierten Lösungen

BeyondTrust verwendet eine in der Branche konkurrierende Lösung für das traditionelle Schwachstellenmanagement seiner internen Ressourcen und Laptops. Bevor das Unternehmen auf Orca stieß, experimentierte es mit der agentenbasierten Technologie für seine cloudbasierten Lösungen, begegnete allerdings zahlreichen Problemen. „Mit der Infrastruktur und den Kenntnissen dieses Tools haben wir uns entschlossen, ihre Agenten in unseren Produkten einzusetzen. Die Idee war, für jede unserer virtuellen Maschinen einen Agenten einzusetzen", sagt Haber.

„Es sind mehrere virtuelle Maschinen erforderlich, um eine Instanz für einen Kunden zu bilden – und zusätzlich die gesamte Backend-Installation. Die Kosten waren überschaubar, aber die DevOps-Kette – die Pipeline für die Zertifizierung, den Aufbau, die Anbindung, die Laufzeit, die Aktualisierung und alles andere – nahm etwa sechs Monate in Anspruch. Und es war mühsam, all diese Agenten am Laufen zu halten, während wir im Zuge unseres außergewöhnlichen Wachstums das Onboarding von Hunderten von Kunden organisierten. Sehr schnell wurde deutlich, dass dies nur schwer zu bewältigen sein würde."

Haber erklärt mit Blick auf die Cloud, dass er, wenn er ein Agentenpaket in eines seiner Produktangebote aufnehmen will, dieses von der frühen Entwicklungsphase über die Qualitätssicherung bis hin zur Produktion einbeziehen muss. „Wir müssen die Umgebungen einrichten, um den Agenten in den einzelnen Phasen zu steuern, um dafür zu sorgen, dass er funktioniert, die Daten ausgibt und anschließend sicherstellen, dass er nicht abstürzt. Bei Tausenden von Agenten kommt es vor, dass einer oder mehrere kaputt gehen oder nicht mehr aktualisiert werden können. Dann müssen wir eine Fehleranalyse durchführen und anschließend die Produktionsumgebung eines Kunden aktualisieren. Das ist ein Albtraum für die Änderungskontrolle und die Compliance, der am besten ganz vermieden werden sollte."

Mit Orca geht BeyondTrust diesen Problemen aus dem Weg. „Dank Orca entfällt für mich der Zeit- und Investitionsaufwand, den Agenten benötigen. Ich bezahle nicht für die Laufzeit eines Agenten, der eine CPU belastet, und ich habe kein Risiko der Änderungskontrolle, wenn ich ein Mitglied des Betriebsteams in eine Produktionsumgebung einführe.“ Zu den Kosteneinsparungen sagt Haber: „Die Agentenkosten pro Client liegen bei 20 bis 30 USD pro Jahr. Bei Hunderten bzw. Tausenden von Kunden steigen die Kosten für den Einsatz von Agenten erheblich. Mit Orca müssen wir all das nicht berücksichtigen. Ich schätze, dass wir etwa 2 % der Laufzeitkosten pro Kunde einsparen und unsere DevOps- und QA-Zeit um 1 ½ Vollzeitäquivalente reduziert haben.“

Ein weiterer entscheidender Grund, warum Agenten bei BeyondTrust nicht funktionieren, ist die Tatsache, dass eines der Produkte des Unternehmens einen kundenspezifischen, gehärteten und angepassten Kernel verwendet. Agenten lassen sich auf dieses System einfach nicht laden. Die SideScanning™-Technologie von Orca hat kein Problem damit, dies zu erkennen.

„Für Unternehmen auf regionalem Expansionskurs bietet Orca einen äußerst effizienten Ansatz. Er verkürzt die Einrichtungs- und Amortisationszeit und bringt deutlich weniger Risiken mit sich.“

Morey Haber
CTO und CIO
BeyondTrust

Die Compliance-Module und Integrationen von Orca sind von unschätzbarem Wert

Für BeyondTrust sind mehrere Aspekte der Einhaltung gesetzlicher und branchenspezifischer Vorgaben von wesentlicher Bedeutung. Um das Vertrauen der Kunden zu gewinnen, hält BeyondTrust die SOC- und ISO-Compliance ein – beide sind für seine AWS- und Azure-Plattformen vollständig zertifiziert. Und obwohl BeyondTrust für seine Zwecke keine PCI-Compliance benötigt, könnte ein Kunde seine Technologie lizenzieren und in einer PCI-Zone einsetzen. Daher ist die PCI-Zertifizierung von entscheidender Bedeutung. Orca verfügt über integrierte Compliance-Module, die Haber bei der Dokumentation von Compliance-Anforderungen unterstützen (z. B. bei Passwörtern, Firewall-Konfigurationen, PII-Exposition usw.)

Die Integration von Orca mit Azure Sentinel Security Center und ServiceNow macht die Lösung für BeyondTrust noch wertvoller. Das Security Center wird wie ein SIEM verwendet, sodass die Ergebnisse von Orca direkt in das Azure Sentinel Security Center einfließen. Orca Security kann ein Ticket in ServiceNow starten, wenn eine Untersuchung oder Abhilfe erforderlich ist.

Ein Dashboard des Azure Sentinel Security Center wird kontinuierlich überwacht, sodass Probleme schnell behoben werden können. „Wir haben diese Integrationen in weniger als einer Woche eingerichtet, und es funktioniert einwandfrei“, sagt Haber. „Ein Dashboard-Diagramm zeigt mir die Zeit bis zur Einstufung ab dem Zeitpunkt, an dem Orca ein Problem feststellt. Unsere durchschnittliche Zeit bis zur Lösung hat sich bei kritischen Fällen halbiert“, sagt er. „Sobald ein Ticket geschlossen ist und Orca das Problem nicht mehr anzeigt, ist der Kreislauf geschlossen. Das ist wichtig für unser Governance-Team und für diejenigen, die die Einhaltung unserer SLAs gewährleisten müssen“, sagt Haber.

Die Auswirkungen auf die Sicherheitstechnik

Durch die Integration mit ServiceNow kann Orca Tickets mit spezifischen Details generieren, die von der Sicherheitstechnik bearbeitet werden können. Dies spart im Vergleich zur Verwendung eines agentenbasierten Tools viel Zeit. „Wir sind in mehreren Regionen weltweit tätig – in Nordamerika, Europa und Südamerika, berichtet Haber. „Wenn man bedenkt, wie viele Komponenten wir pro Region mit einer agentenbasierten Technologie im Vergleich zu einer einfachen Orca-Verbindung bereitstellen müssten, kann man sehen, dass meine Technik- und Betriebsteams mit Orca viel zufriedener sind.“

In Bezug auf die Geschwindigkeit des Einsatzes und die Genauigkeit von Orca sagt Haber: „Es ist ein effizienter Weg, um komplexe Daten für eine handlungsorientierte Anleitung zu erhalten. Es unterstützt uns beim Schwachstellenmanagement, bei der Compliance und bei sicheren Konfigurationen. Nach nur wenigen Monaten im Einsatz stellt Orca für uns eine sehr wertvolle Lösung dar.“

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