Devo Security Operations - Cloud Security Detections

Monitor and Defend Your Cloud Environment with Ready-to-Deploy Detections

SOLUTION BRIEF

UNLOCK INNOVATION FROM DIGITAL TRANSFORMATION WHILE KEEPING YOUR CLOUD DATA SECURE

As organizations move their workloads to the cloud to accelerate innovation and capitalize on cloud efficiencies and scalability, they are realizing that the cloud presents visibility and control challenges which can make them vulnerable to cyberattacks.

Some organizations take a siloed security approach when it comes to protecting their data in the cloud, leading to fragmented environments that create visibility challenges. In other cases, organizations mistakenly assume that the cloud is inherently secure.

A poor understanding of the shared responsibility model can put organizations at greater risk because they are not adequately securing their data. Typically, this is due to misconfigurations or relying on default access controls, which can lead to overly permissive privileges on accounts, insufficient logging and an inadequate understanding of security vulnerabilities related to public cloud environments.

Keeping your public cloud environments safe requires unified visibility, effectively secured workloads, and the ability to detect misconfigurations fast.

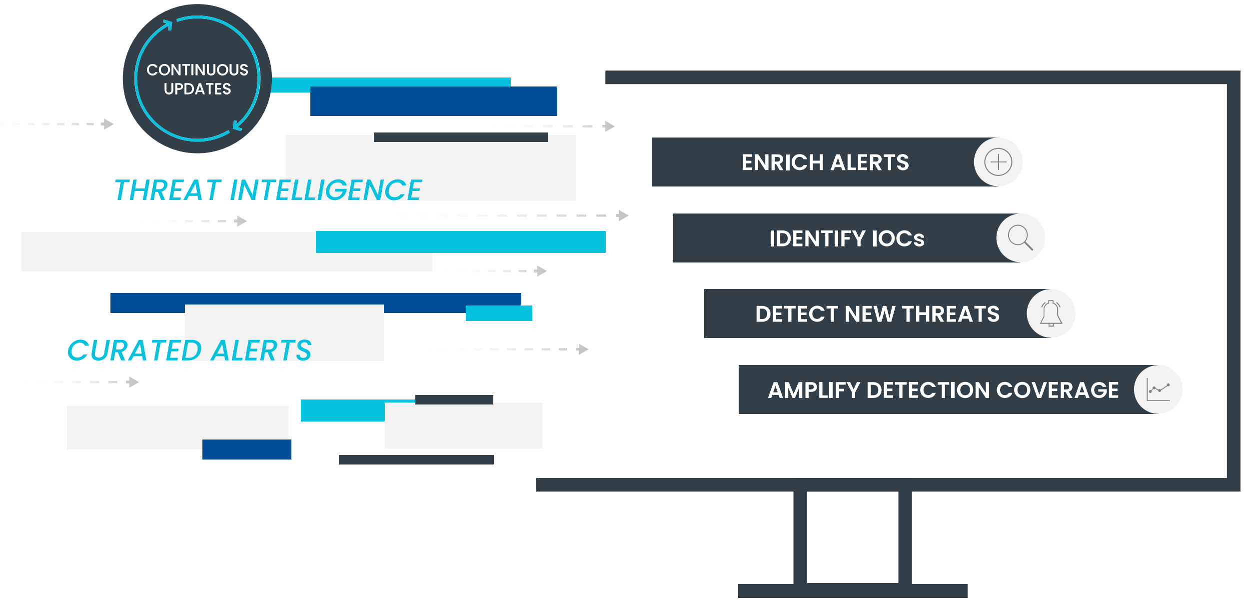
ACHIEVE UNIFIED VISIBILITY AND MONITOR DATA AT SCALE ACROSS YOUR CLOUD ENVIRONMENT

Devo Security Operations empowers your team to continuously monitor and protect your cloud environment by enabling you to ingest your cloud data while providing you with ready-to-install cloud security detections.

These detections, carefully curated by Devo and validated against real-world data, provide your team with the confidence to act and mitigate threats quickly. The pre-built detections make it easy for your team to protect their cloud data by reducing the time needed to research attack vectors and engineer detections, giving them back valuable time to focus on higher-order investigations.

RAPIDLY DEPLOY CLOUD SECURITY USE CASES WITH EXPERT-CREATED AND VETTED DETECTIONS

Devo makes it easy for your security team to put cloud security detections into action. Delivery of cloud security detections is via the Devo Content Stream, a delivery mechanism that enables your analysts to browse the detections and install them with only a few clicks. When they have fully deployed the detections, your team will be able to confidently monitor and defend your cloud data and applications.



The following cloud security use cases depict how Devo's cloud security detections help protect your cloud environments:

Use Case 1:
Cloud Monitoring

To quickly identify potential attacks and breaches in your cloud environment, you should adopt a cloud monitoring strategy that enables you to identify patterns and uncover security risks within your infrastructure. Tools such as AWS CloudWatch make it easy to collect monitoring and operational data for detecting anomalous behaviors in your environment.

A subset of the Devo-curated cloud security detections maximizes the integration between Devo and AWS CloudWatch to empower your security team to implement automated and continuous monitoring with alerts based on suspicious cloud usage.

Use Case 2:
Privilege Escalation

Bad actors exploit different assets to increase their chances of a successful breach. Once they gain initial access, they will move within your network to seize valuable assets. Collecting logs from technologies such as AWS CloudTrail, which records account activity across your AWS infrastructure, gives you the visibility and insight to quickly detect lateral movement.

A number of the cloud security detections in Security Operations provide granular visibility into application, user or file access behavior across different environments to uncover identity-based threats. These detections will enable you to identify a range of suspicious activities, such as multiple failed logins from a user within a short period of time, changing logging configurations from mission-critical services, and increased permissions to investigate further and remediate faster.

Use Case 3:
Analyze VPC Traffic

VPC logs are an optimal source of information for understanding the traffic patterns that reach your public cloud instance. By carefully observing and analyzing the traffic you will be able to identify unauthorized traffic destinations that may indicate a malicious actor has gained initial access to your network and is planning its next move.

Certain cloud security detections in Security Operations alert you of suspect actions that may signal an intruder performing reconnaissance in your network. These detections will fire when an IP is denied multiple times in a short window of time or if large files are uploaded or sent.

Are you ready to learn more about Devo Security Operations?
Contact your sales representative to schedule a demo or visit Devo Docs for more information.

Devo
255 Main Street
Suite 702
Cambridge, MA 02142

Devo is the only cloud-native logging and security analytics platform that releases the full potential of your data to empower bold, confident action. With unrivaled scale to collect all of your data without compromise, speed to give you immediate access and answers, and clarity to focus on the signals that matter most, Devo is your ally in protecting your organization today and tomorrow. Devo is headquartered in Cambridge, Mass. Learn more at **www.devo.com**.