How to Source a Cloud Security and Compliance Platform

Cloud security is different. Traditional solutions rely on being in the path of traffic, deployed inside the application or operating system, or use network scanning techniques. But in the cloud, application stacks run on abstracted services or PaaS layers, or leverage API-driven services. Savvy cloud security buyers should consider what they want out of a cloud security platform and ask themselves these questions.

DO YOUR CURRENT CLOUD SECURITY POLICIES SUPPORT YOUR GROWTH PLANS?

You may need a solution that is able to support the ever-growing number of services that will likely be added over time to your environment.

HOW DOES COMPLIANCE FIT WITH YOUR OVERALL SECURITY PLANS?

If compliance is critical to your ability to operate within certain industries and for specific stakeholders, then you need a solution that automates compliance within development and deployment.

DO YOU HAVE AN EVALUATION AND VETTING PROCESS FOR CHOOSING A VENDOR?

While your CIO or CISO may do the final sign-off, make sure you include reps from DevOps, security engineering, and compliance.

IS CLOUD SECURITY TRAINING CRITICAL FOR YOUR TEAM'S DEVELOPMENT?

Not all your users are cloud superstars. Look for a solution that provides help for users who are new to the cloud in the form of guided remediation for risks that are uncovered by the tool.
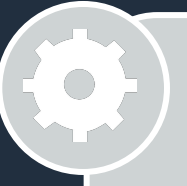
DO YOU EMPLOY DEVOPS OR CONTINUOUS DEPLOYMENT METHODOLOGIES?

If changes are made to your cloud environment many times each day, you should consider a solution that can monitor your infrastructure continuously, so you find vulnerabilities before the bad guys.

DOES YOUR ENTERPRISE NEED CONTINUOUS COMPLIANCE?

If you aren't comfortable working off of scanning reports and daily logs then you should seek a solution that operates continuously.

DO YOUR PROCESSES REQUIRE TICKETS TO BE OPENED WHEN REMEDIATION NEEDS TO COMPLY WITH SLAs?

Choose a solution that will easily integrate with ticketing and alerting tools

IS AUTOMATION CRITICAL TO YOUR DEVELOPMENT AND DEPLOYMENT CYCLES?

If so, you should be looking for a solution that takes DevOps principles into account and offers complete, real-time compliance assessment of your entire cloud infrastructure with simple, one-button compliance reports.
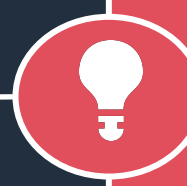
DO YOU REQUIRE CUSTOMIZATIONS TO RISK CHECKS SO THEY ALIGN WITH INTERNAL SECURITY POLICIES?

Having the ability to customize control checks can help ensure that the tool is able to monitor your environment and flag risks with the appropriate severity levels for your team.

DO YOUR DEVOPS TEAMS HAVE THE ABILITY TO SPIN UP NEW SERVICES WITHOUT NOTIFYING SECOPS?

Consider an agentless solution that will be able to detect and monitor all new services and regions from the minute they are spun up.

WHAT'S YOUR RESOURCE CAPACITY FOR COMPLIANCE ASSESSMENT?

If your team is unable to monitor all compliance elements, you should seek a solution that uses continuous compliance monitoring.

ARE YOU LOOKING TO EXTEND SECURITY RESPONSIBILITY ACROSS YOUR ORGANIZATION?

If you want more than just SecOps looking at security, then be sure to look for a solution that provides value to DevOps, Compliance & Risk, and executive management, as well as Security.