Deloitte.

Cloud Security Policy Orchestration

Shift-left with policy-as-code to achieve multi-cloud security

MARKET CONTEXT

Cloud Security Policy Orchestration, a policy-driven approach to shift-left security, can help with broad visibility into cloud assets across the multi-cloud landscape. The solution enforces security policy-as-code uniformly across the software development lifecycle to help you feel confident that your cloud security requirements are being applied throughout your cloud environments. This approach works to help enhance compliance and security across your enterprise while freeing up your developers to focus on what matters most: growing your business.

Cloud Security Policy Orchestration can help protect the enterprise and facilitate **secure, intelligent operations** while also driving **agile, secure modernization**. Through each solution in the platform, we will work with you to help you transform security and **make cyber core to the organization**.

We can work with you wherever you are in your cloud journey and help you feel confident in tackling your security requirements, providing the outcomes you need to help you spearhead business enablement. Cloud Security Policy Orchestration can help protect the enterprise and enable secure, intelligent operations while also driving agile, secure modernization.

We will work with you to help you transform security and make cyber core to the organization.

CLOUD SECURITY MANAGEMENT BY DELOITTE

Cloud Security Policy Orchestration	Attack Surface Management	Cyber Predictive Analytics	Cyber Cloud Managed Services

Cloud Security Policy Orchestration is one component of the Cloud Security Management by Deloitte platform and can be consumed as part of the broader suite of services or individually by clients.

COMMON TRENDS, CHALLENGES AND OUTCOMES OF CLOUD SECURITY POLICY ORCHESTRATION

Common challenges
that we help address

- Lack of contextualized visibility into the overall cloud security posture across a multi-cloud infrastructure deployment
- Fatigue from multiple security alerts making it challenging to determine the real security issues that require attention
- Lack of tooling to achieve proactive security via DevSecOps and shift-left methodologies
- Inability to uniformly apply security policies across the every stage software development lifecycle
- Limited integration and automation to uniformly handle security responses including alerting, ticketing, and remediation
- Challenges around identifying potential policy visualizations that can lead to service interruption or security incidents

Desired outcomes
of a policy-driven, shift-left approach

- Enhanced response and recovery capabilities by identifying potential policy violations that could lead to service interruptions or security incidents
- Quicker time to security insights and fewer, more relevant alerts through better filtering of signal from the noise
- Increased efficiency of security operations via automation (e.g., alerting, remediation, and response workflows)
- Ability to uniformly apply policies across the each stage software development lifecycle to enable DevSecOps and proactive security methodologies
- Enable governance and optimization that provides vision and drives growth by leveraging leading practices across different libraries of information to help you reduce cloud security and compliance risks

A SET OF GOVERNING POLICIES

Cloud Security Policy Orchestration has a set of governing policies that provides for continuous evaluation of proposed, developed and deployed code. From a central location, it can help you create, customize, test, and manage policies as well as decide when and where (i.e., to which workloads) policies should be applied.
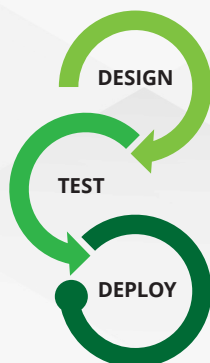
DESIGN — Developers check in code to the central policy repository and then Cloud Security Policy Orchestration evaluates it against policies.

TEST — If Cloud Security Policy Orchestration does not identify issues with the proposed code, it's deployed and continuously evaluated for deviations.
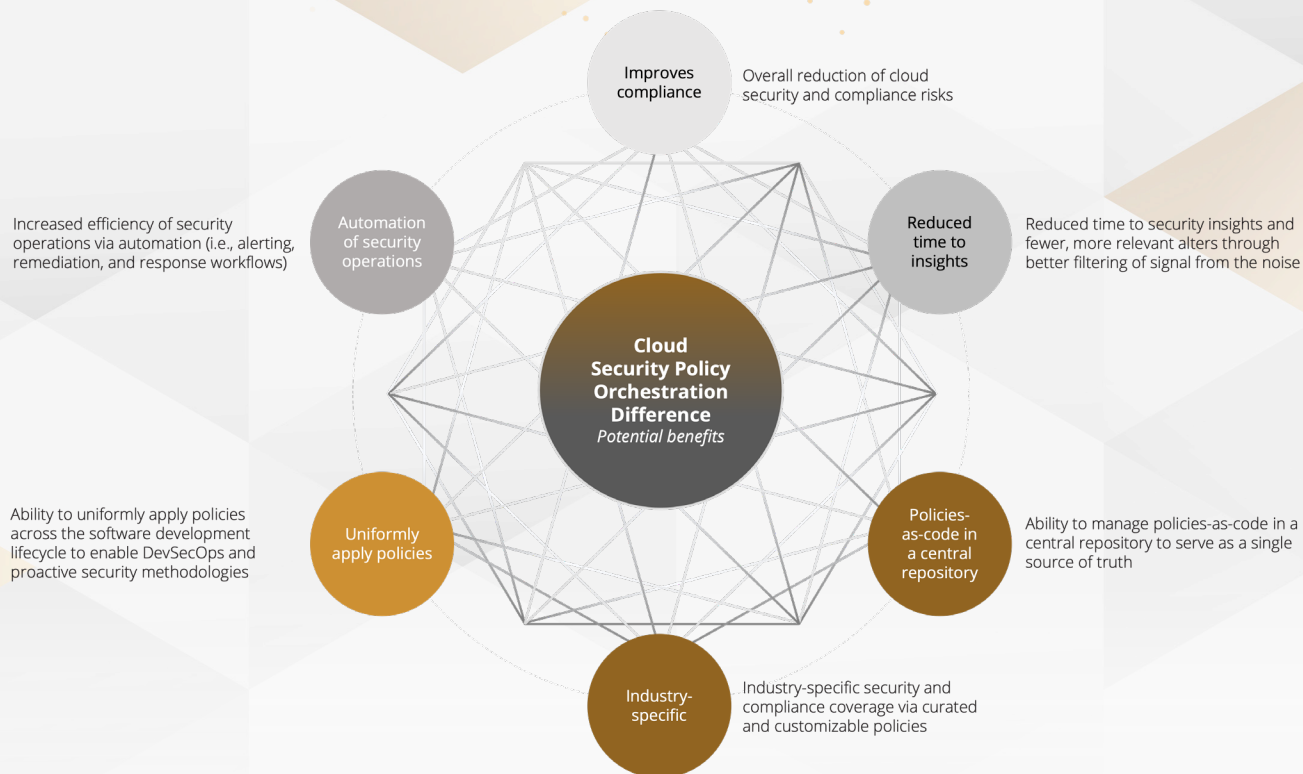
This code-driven approach enables policy application and response actions to by dynamically applied at the organization or data classification layer instead of individual workloads.

DEPLOY — If Cloud Security Policy Orchestration detects a policy violation, it routes the code for remediation accordingly.

The Hub for Security Policy and Posture Management

Cloud Security Policy Orchestration provides a broad view of your multi-cloud posture and serves as the hub for managing policy-as-code security policies to enable DevSecOps and shift security left.

- Uses Rego as the policy language of choice and uses Open Policy Agent (OPA) as the policy engine that enables the application and enforcement of policies
- Policy as Code support aligns well with the GitOps model to enable policy customization and management
- Cloud Security Policy Orchestration's policy library can align with leading practices across National Institute of Standards and Technology Special Publication 800-53, Health Information Trust Alliance Common Security Framework, Center for Internet Security, and Payment Card Industry Data Security Standard frameworks (among others)

The central diagram:

Cloud Security Policy Orchestration Difference
Potential benefits

- **Improves compliance** — Overall reduction of cloud security and compliance risks
- **Reduced time to insights** — Reduced time to security insights and fewer, more relevant alters through better filtering of signal from the noise
- **Policies-as-code in a central repository** — Ability to manage policies-as-code in a central repository to serve as a single source of truth
- **Industry-specific** — Industry-specific security and compliance coverage via curated and customizable policies
- **Uniformly apply policies** — Ability to uniformly apply policies across the software development lifecycle to enable DevSecOps and proactive security methodologies
- **Automation of security operations** — Increased efficiency of security operations via automation (i.e., alerting, remediation, and response workflows)

SERVICES AND DESCRIPTIONS

Policy Updates
- Policy-as-Code library is updated for Cloud Service Providers and regimen changes

Policy Customization and Enhancement
- Policies can be customized and enhanced to the client's circumstances

Automated Remediation & Workflows
- Remediation workflows trigger the appropriate actions to resolve violations

Customized Reporting
- The premium offer includes customization of reports through use of the filtering capabilities inherent to the tool

Operate Services
- The premium offer include operate services (e.g., cloud transformation migration assistance and security incident response)

Day 0 Security Baseline Posture
- Solution installs performed in one day to provide broad Day 0 visibility into the organization's cloud security posture

Periodic Assessments
- Quarterly (or more frequently for clients in our Premium tier) assessments provide updates and recommendations for improving effectiveness of security policies

A SOLUTION CUSTOMIZED TO YOUR BUSINESS

Cloud Security Policy Orchestration is one solution within Cloud Security Management by Deloitte.
All solutions within Cloud Security Management by Deloitte are able to be implemented and maintained for an end-to-end cloud security solution or can be provided individually to help you address specific challenges within your cloud environments.

That works for you
We help protect your enterprise by bringing the technology to secure your cyber estate, enabling secure, intelligent operations while providing efficient workforce that can work for you. In doing so, we help you with business enablement, allowing you to be agile in modernization.
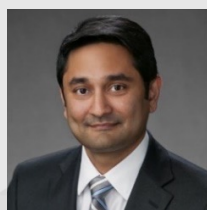
Vikram Kunchala
Principal
Deloitte & Touche LLP
vkunchala@deloitte.com

Vijay Sarathy
Managing Director
Deloitte & Touche LLP
vsarathy@deloitte.com

Ramesh Menon
Managing Director
Deloitte & Touche LLP
ramemenon@deloitte.com