WHITE PAPER

# INFOSYS CLOUD SECURITY POSTURE ENHANCEMENT FRAMEWORK POWERED BY WIZ


## Abstract

This whitepaper highlights the new-age cyber challenges in cloud environments and explores ways to enhance cloud security posture using the Infosys framework with the Wiz Platform.


WIZ

Infosys®
Navigate your next

## Introduction

For today's enterprise digital footprint, cloud investments, infrastructure & application landscapes are ever expanding. Due to this accelerated pursuit of digitization, multiple convoluted threat patterns and attack surfaces have evolved. From the traditional lift and shift approach of three-tiered applications, to strategic multi-branched DevOps backed microservice architecture utilizing cloud native workloads, the evolution has been phenomenal. With expanding and evolving digital and cloud landscapes, demands for next generation security controls beyond the siloed and traditional cloud security platform has grown tremendously.

First generation Cloud Native Application Protection Platform (CNAPP), without having context awareness and ability to identify cyber risk in correlated manner across multiple parameters i.e. posture, identity, data, code etc., has been not able to offer comprehensive and centralized cloud security across multi or single clouds. Infosys Cloud Security Partner **Wiz** has revolutionized CNAPP platforms and technology with its Artificial Intelligence-driven technology and graphical view of all the variables of cyber risk and incident in cloud. Its capability to triage multiple correlated cloud security issues at an accelerated speed, while visualizing and magnifying the risks, is the way forward. Infosys has strategically collaborated and made significant investments in this evolving cyber value chain, with a focus on aggressive competency development and thought leadership for the Wiz-based cloud security program.

## Cloud Security Challenges faced by Enterprises

Following are some of the key cloud security challenges faced by today's organizations:

**Traditional Approaches Are Failing**

Legacy methods of managing security governance, which rely on paper-based processes, are not suitable for the dynamic nature of cloud environments.

**Compliance Failures**

Due to the rapid changes in cloud environments, it has been very challenging for enterprises to adhere to regulatory requirements in near real-time.

**Security Gaps**

Inadequate security controls to identify, detect, protect, respond, recover, and govern security create significant challenges in maintaining the security posture of the cloud.

**Security Misconfigurations**

Owing to the dynamic nature and ease of management of cloud services, enterprises face significant challenges in detecting security misconfigurations in real time.

**Limited Visibility**

One of the bigger challenges is to have a single pane of glass view of cloud assets and inventory across single or multi-cloud environment.

**Unprotected & Unattended Cloud Assets**

Unprotected and unattended cloud assets pose substantial risk due to missing patches, or having redundant cloud identity, public IP Address, sensitive data storage, and so on.

**Inadequate Policies and Processes**

Organizations often have security controls in place for cloud environments, but the lack of complementary security policies and processes weakens their cloud security posture.

**Correlated Risks In The Cloud Estate**

While there are native solutions from cloud hyperscalers to continuously assess security posture, the inability to effectively showcase correlated risks remains a challenge.

**Unified Security Platform For Cloud Security**

The cloud environment's attack surface expands with the advent of emerging workloads, such as serverless, containers, microservices, and other PaaS services. However, enterprises often lack unified platforms that can address multiple cloud security use cases effectively.

## Business Challenges and Return on Investment

According to leading analysts, 95% of security breaches in cloud environments occur due to misconfigurations. While many enterprises have already invested in NextGen Cloud Native Application Protection Platforms (CNAPP) like Wiz, which have significantly enhanced visibility into security posture, attack paths, vulnerabilities, and threats, this visibility needs to be amplified. Achieving this requires accelerated remediation and democratization of cloud security - areas where most enterprises are not currently making adequate progress. The intent of democratization of cloud security refers to identification of the security gaps, and quick as well as effective remediation by respective service owners following automation as a principle. As per Statista, the average cost of a cloud security breach in the US is approximately **$9.36 million**. Therefore, enhancing security posture and ensuring a cyber-resilient cloud environment can provide breach protection and mitigation, ultimately saving enterprises significant costs -either directly or indirectly.

## Infosys Cloud Security posture enhancement framework

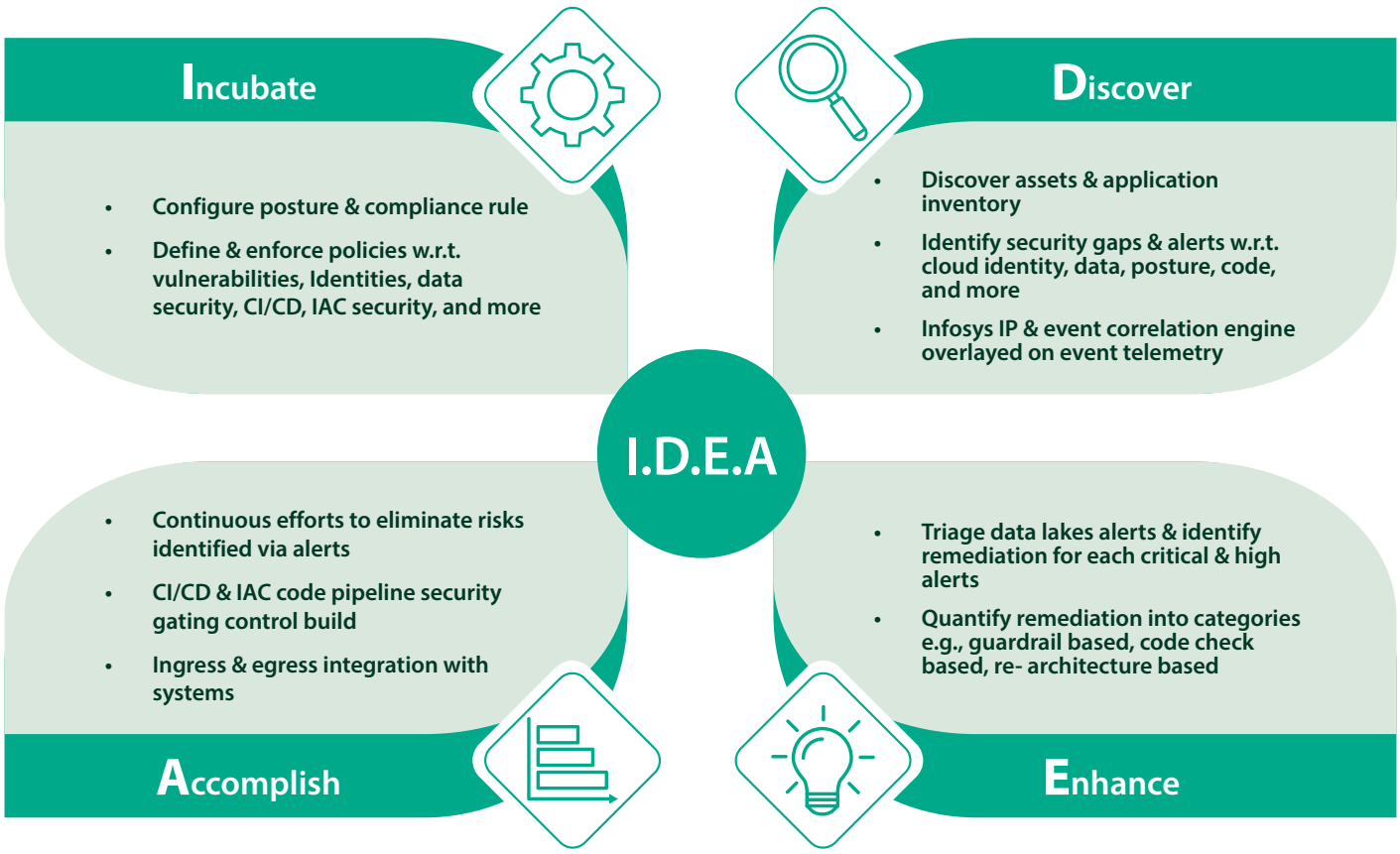
This whitepaper highlights Infosys' approach to conducting Cloud Security Advisory engagements for global enterprises, based on its proprietary service model and leveraging the next-generation Wiz CNAPP. This solution combines Wiz's advanced CNAPP capabilities with Infosys' proven service expertise and intellectual property (IP), delivering a comprehensive and effective cloud security advisory. The focus is to offer customers speed, measurable ROI, and continuous cloud security governance model through Infosys Cloud Security posture enhancement framework, powered by Wiz platform. In this custom framework, we have developed the Infosys Risk Compliance Ruleset, designed to assess industry compliance and best practices posture requirements for any enterprise. All security alerts, findings, and emerging

threats identified through the enablement of this ruleset are forwarded to a security data lake, powered by the **Infosys Cyber Next** platform. Further, this Infosys-built algorithm will provide a mitigation plan and business case including resource requirements, duration to mitigate the identified findings, etc., against the Infosys Risk Compliance Ruleset.

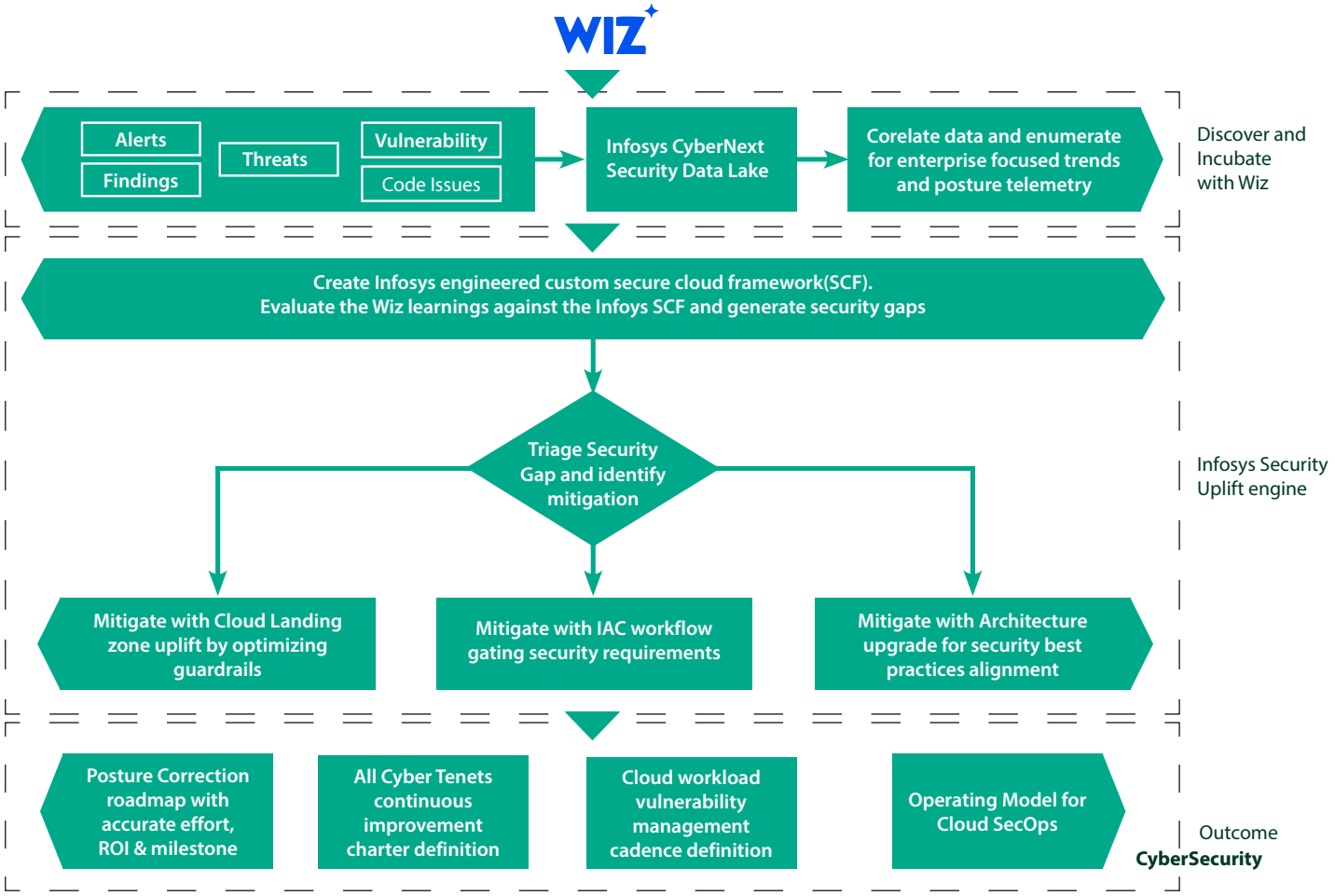
The below representation showcases Infosys' approach to deliver the benefits via **Infosys cloud security posture enhancement framework**.

Infosys **I.D.E.A**. framework breaks down the entire cloud security posture enhancement life cycle process into 4 phases, namely - **I**ncubate, **D**iscover, **E**nhance & **A**ccomplish. In each phase, a set of activities will be carried out using specific tools and technologies, with detailed descriptions provided in the subsequent sections.

## Infosys I.D.E.A. Framework




While Wiz CNAPP platform highlights very deep insights of the security gaps in the cloud environment of the customers hyperscalers, the remediation of these gaps has been a real challenge for customers




The above workflow highlights our in-house devised framework and methodology to remediate any cloud security gaps while considering the maturity of server owner team, opportunity to bring automation strategy to remediate, change management at cloud guardrails level or any re-architecture following secure landing zone practice. Our methodology offers an accelerated approach to enhance cloud security, while Wiz offers greater visibility of security gaps across multiple parameters. The subsequent sections detail the Infosys **I.D.E.A.** framework.

### Phase 1: Incubate

Standup Infosys cloud security posture enhancement framework on Wiz platform to cover critical cyber threat vectors w.r.t. cloud security posture, data, identity & code. Reference of compliances such as NIST, CIS, ISO27K1, CSA and industry experience is foundation of the framework. This framework will ensure the coverage for customer risk and cloud business footprint with custom policies and controls. Wiz-provided magnified risk and correlated attack paths will also be part of the eventual framework assessment

### Phase 2: Discover

Subsequently, the Wiz SaaS tenant will assess the customer's cloud environment over a condensed timeframe (e.g., 3-4 weeks), encompassing the security posture and associated risk factors. Following this period, an evaluation will be conducted against the Infosys framework to generate a comprehensive report on cloud security findings. All findings identified by Wiz during the discovery phase will be transmitted to the security data lake, which is powered by the Infosys Cyber Next Platform. The discovery telemetry forwarded to the data lake will include inventories of cloud assets, applications, and associated service utilization metrics. Customized parsing methods developed by Infosys will correlate findings from the Infosys Cloud Security Posture Enhancement Framework with other telemetry data fed into the security data lake. This correlation aims to provide a diagnostic threat view of the cloud landscape. The security data lake correlation engine will also be empowered with Infosys IP of industry specific and cloud secure landing zone tenets.

### Phase 3: Enhance

This is the most important step in the operating model offered. The telemetry triage in phase 2 resulting in diagnostic threat view will be

enhanced using Infosys IP-based algorithm to orchestrate remediation business case, including effort, cost, remediation duration, and so on. The stated Infosys IP is described further in compilation steps below. The report from "Infosys cloud security posture enhancement framework" will also be fully pushed into the algorithm as an input variable. The algorithm will then compile the received data to generate roadmap for posture enhancement.

Compilation will include below critical steps amongst others:

- Identify actionable mitigation for each finding, alert, and threat reported in the Infosys Cloud Security Posture Enhancement framework report from Wiz console.
- Deep dive into each security gap to identify one of the mitigation approaches listed below:
    - **Option 1**: Mitigation with cloud landing zone foundation empowerment with cloud guardrails enrichment. This is permanent fix of the finding and prevents recurrence. Thereby reducing the cloud attack surface, cloud security architect will validate & sign-off on the guardrail redesign.
    - **Option 2**: Mitigation with Cloud Infra as a code (IAC) security gating check addition. This is an enhancement to existing DevOps workflow. With this approach, Infosys will also democratize cloud security and make it incumbent upon application teams pushing cloud IAC to follow security guidelines. Cloud SecOps governance team will hold accountability for this value add to DevOps workflow.
    - **Option 3**: These steps offer mitigation with architecture optimization. This is typically a retro fit path where initial landing zone design due diligence for cloud adoption has not been followed secure by design principles. Typically exhibits of such an environment have no hub-spoke cloud architecture, no firewalling between prod & lower environments and other security gaps. The pivot cycle for this mitigation option is extended but is required to ensure long term cloud security success metrics for the organization are met.
- After mitigation option is finalized for the findings, the algorithm will evaluate and provide variables to create business cases, such as effort estimation for initial minimum viable cloud maturity milestone, remediation duration, etc.
- Certain options for tool adoption and downstream integration into customer SIEM or threat emulation engines will also be output from the algorithm.

### Phase 4: Accomplish

This phase offers true ROI to enhance enterprise's cloud security posture. The outcomes from the Infosys Cloud Security Posture Enhancement framework, along with the Infosys algorithm and the power of Wiz compute capability, will be made available to the customer. Additionally, Infosys IP, thought leadership, and industry experience would function as catalysts to continuously enhance the outcome.

Below are key highlights of the customer initialization into this journey of continuous cloud governance and democratization:

- **Roadmap with actionable steps** for cloud posture optimization with efforts, cost, duration and technology requirement
- Offer primary cloud threat tenets of Identity & Data Protection process and policy runbooks, customized to customer landscape and security maturity
- Approach to enterprise **tool rationalization** w.r.t. Cloud Security, both in terms of cost and integration for best Return on Investment
- DevOps workflow optimization charter based on the existing cloud IAC and version control scan findings to streamline CI/CD pipeline & **democratize cloud security**
- Recommend operational models to ensure vulnerability and security baseline standard maintenance for all cloud workloads

## Experience & Typical Benefits

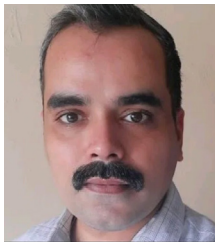
Infosys utilized the in-house I.D.E.A. framework for one of the multinational communication majors based in Britain. This simplified the cloud account onboarding process and **ensured 100% asset coverage** for over **~550 cloud accounts**. It also enhanced triaging and prioritisation by highlighting vulnerabilities which are especially risky through "Toxic Combinations", as well as easy-to-use filters to check internet exposure. **This reduced the open critical and high vulnerabilities by 37%** in the **first 90 days itself**. Further, we streamlined the threat detection and reporting capability for Kubernetes container workloads, **automatically ingesting**, **analysing**, and **triaging** over **9.5 million events per a day.**

Another American Retail company wanted to protect their AWS cloud deployments, meet compliance, and scale to support rapid expansion and a growing global user base. Infosys' framework based on Wiz **improved the overall cloud security posture from 52% to 85% within 6 months**, by offering real time visibility of multi-cloud asset inventory, vulnerabilities, misconfigurations, and ensuring compliance maturity against **CIS benchmarking**. We further enabled easy onboarding of the new AWS cloud accounts and offered **automated remediation**.

## Conclusion

To summarize, **Infosys I.D.E.A. framework** powered by Wiz not only provide visibility of cloud security posture across multiple parameters i.e. identity, data, code etc. but also accelerate enterprise journey to establish secure and resilient cloud platforms by democratization of cloud security. Infosys framework enables enterprises to get full value of the Wiz platform by automating the remediation of cloud security gaps & vulnerabilities in a seamless manner.

## About the Authors

### Vinit Ajgaonkar

Cloud Security Architect & Principal Consultant

Vinit brings over 15 years of deep cybersecurity experience. He is currently a key part of our Cyber Innovation, Strategy & Excellence Team, focusing on building and deploying next-gen cybersecurity solutions. As a cloud security architect, Vinit actively helps clients on their digital transformation paths. He possesses a unique blend of thought leadership in technology, complemented by a hands-on approach and a keen interest in exploring new tools and technologies.

### Darshan Singh

Industry Principal

Darshan has nearly two decades of extensive experience in Cybersecurity. As a key member of the Infosys Cyber Innovation and Practice team, he focuses on developing NextGen security solutions and strategies to counter evolving cyber threats. His versatile expertise spans numerous domains, including cloud security, cyber resiliency, infrastructure security, data security, Zero Trust, OT security, vulnerability management, and security monitoring and analytics.



For more information, contact askus@infosys.com


Navigate your next