Infosys® | CONSULTING

CAPITALIZING ON THE CLOUD

Financial Services and Insurance

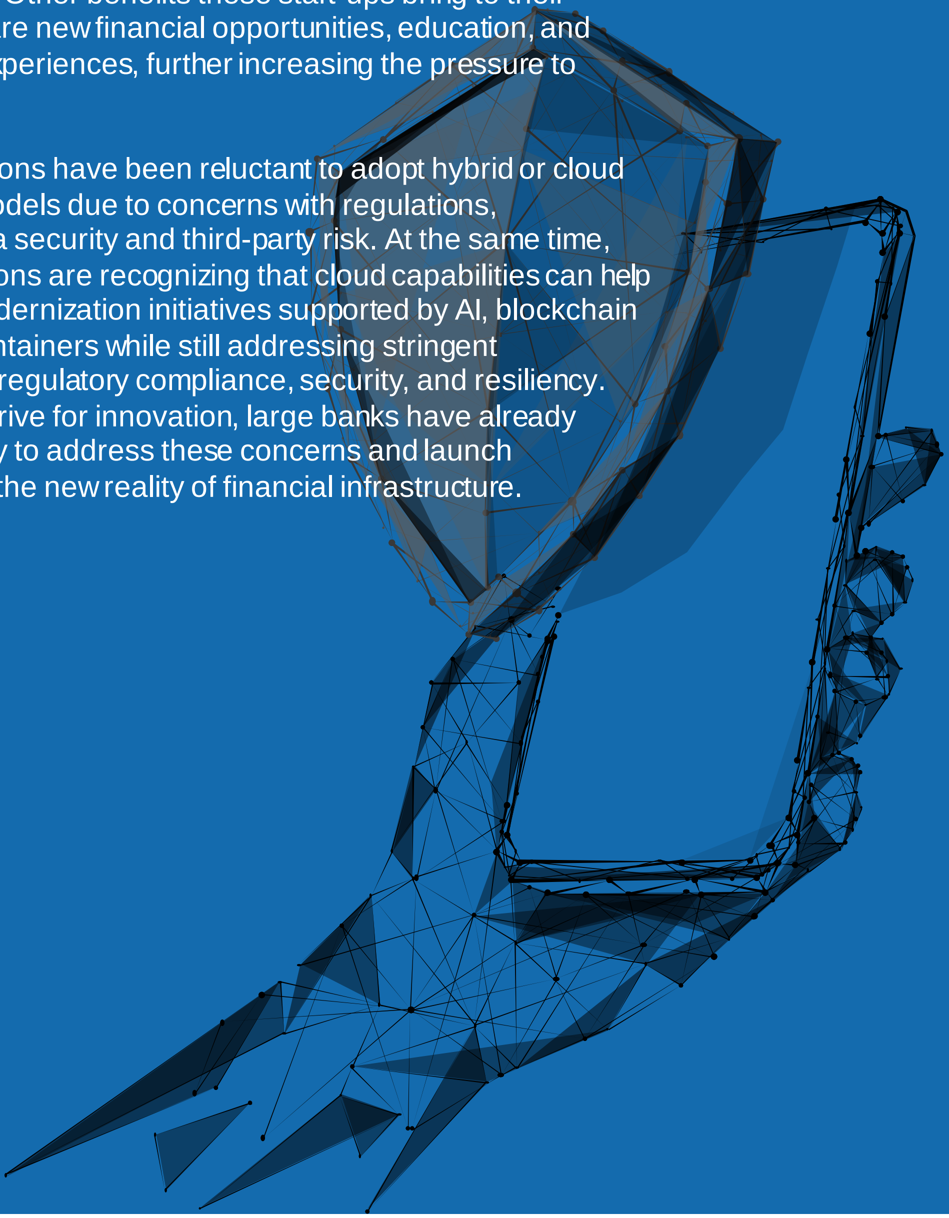
An Infosys Consulting Perspective
By Gerald Alston, Amber Boyle, Chad Williams and Sara Lind

Consulting@Infosys.com | InfosysConsultingInsights.com

Introduction

For financial institutions, embracing cloud computing is a matter of survival in a business environment where innovation and competition are pushing them to become more agile, while still adding value for their customers. These companies are facing fierce competition from financial sector technology start-ups built entirely on cloud technology who deliver a customer centric business model. Other benefits these start-ups bring to their customer base are new financial opportunities, education, and engaging app experiences, further increasing the pressure to innovate.

Some organizations have been reluctant to adopt hybrid or cloud infrastructure models due to concerns with regulations, compliance, data security and third-party risk. At the same time, financial institutions are recognizing that cloud capabilities can help them pursue modernization initiatives supported by AI, blockchain and software containers while still addressing stringent requirements of regulatory compliance, security, and resiliency. Embracing the drive for innovation, large banks have already proven the ability to address these concerns and launch themselves into the new reality of financial infrastructure.



Cloud Adoption: Financial Services Concerns

- **Regulation/compliance concerns**: Financial institutions should select providers with specialized knowledge of financial industry laws and regulations, that offer transparency with their internal controls, provide access to audit reports, and have templates for service contracts compatible with local laws and regulations. Major cloud providers such as Microsoft, Google and IBM have already demonstrated specialization and success with these capabilities.

- **Data protection and security concerns:** Keeping data safe from unauthorized access, damage and corruption is a primary concern for most companies, especially when dealing with money. Implementation of data protection and privacy controls like encryption, tokenization, loss prevention, and digital rights management are available with cloud services but more importantly speed and straightforward facilitation of implementation can rapidly increase responsiveness and reduce cost and time to market. As an example, client-side encryption is used to protect data in transit by ensuring the cloud service provider nor an outsider will have readable access to the information.

- **Third party risk concerns:** Running critical systems in the cloud is not inherently riskier than on-premises deployments, provided the user is leveraging cloud service provider compliance settings in alignment with financial regulations (e.g., for data retention, data access, auditability) and design and security best practices are implemented. Physical security of the cloud service provider equipment, software and hardware updates, internal governance processes and technical controls typically cannot be independently assessed but compliance bodies accept corporate level attestations in accordance with regular compliance assessments.

- **Transformational challenges:** Many financial institutions rely heavily on legacy applications. Migrating these applications to the cloud can provide some serious challenges for organizations as frequently the application was designed before cloud services were an option. To fully take advantage of the benefits of cloud services, applications may need to go through re-design which can be a costly and time-consuming step. To mitigate unforeseen challenges, independent evaluation of a cloud migration strategy by someone with a track record of success is critical to on-time delivery of capabilities. This process begins with clearly defining objectives, assessing the current governance constraints, and effectively implementing a sound migration strategy. Ultimately, this proven method can achieve greater operational efficiency, flexibility, increased revenue, reduced costs, enhanced security, better risk mitigation, and return on investment.

Cloud Adoption: General Concerns

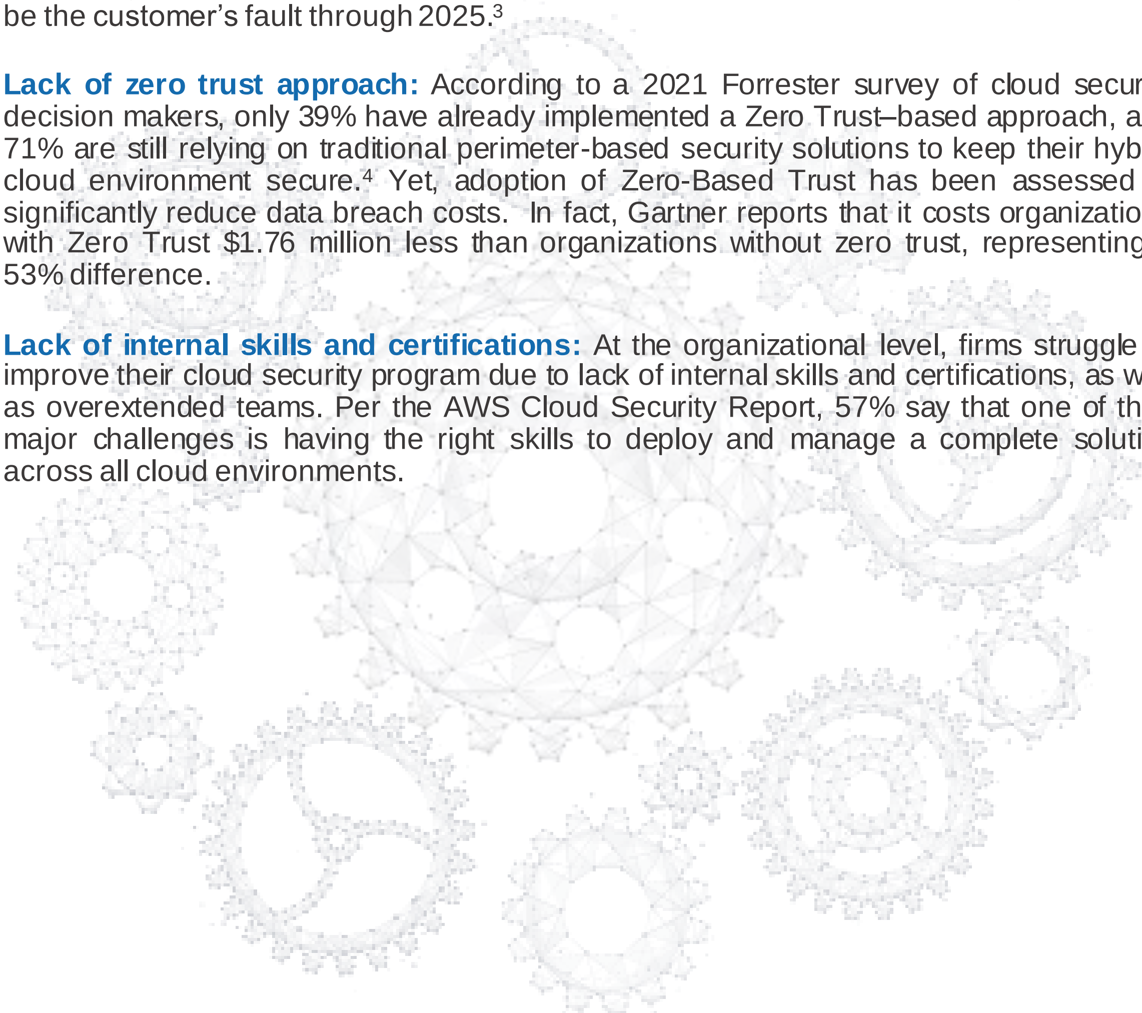
- **Interoperability and visibility**: Per the 2021 AWS Cloud Security Report, over half of the organizations surveyed reported challenges in understanding how different solutions fit together and to having to use between three to six different dashboards to configure cloud security policies alone.[1] Coupled with other security dashboards, security professionals are finding it difficult to maintain overall visibility into the security posture of an organization and maintain consistency across platforms, applications and services.

- **Multi-cloud support:** According to a Gartner cloud adoption survey, 75% of organizations are leveraging multi-cloud architectures and native capabilities do not support them. For this reason, third-party tools are often required to provide full cloud security across the hyper-scalers and to secure multi-cloud environments.[2]

- **Misconfigurations:** According to Gartner's 2021 Cloud Security Report; nearly all successful attacks on cloud services are the result of customer misconfiguration, mismanagement, and mistakes. It is also estimated that 99% of cloud security issues will be the customer's fault through 2025.[3]

- **Lack of zero trust approach:** According to a 2021 Forrester survey of cloud security decision makers, only 39% have already implemented a Zero Trust–based approach, and 71% are still relying on traditional perimeter-based security solutions to keep their hybrid cloud environment secure.[4] Yet, adoption of Zero-Based Trust has been assessed to significantly reduce data breach costs. In fact, Gartner reports that it costs organizations with Zero Trust $1.76 million less than organizations without zero trust, representing a 53% difference.

- **Lack of internal skills and certifications:** At the organizational level, firms struggle to improve their cloud security program due to lack of internal skills and certifications, as well as overextended teams. Per the AWS Cloud Security Report, 57% say that one of their major challenges is having the right skills to deploy and manage a complete solution across all cloud environments.



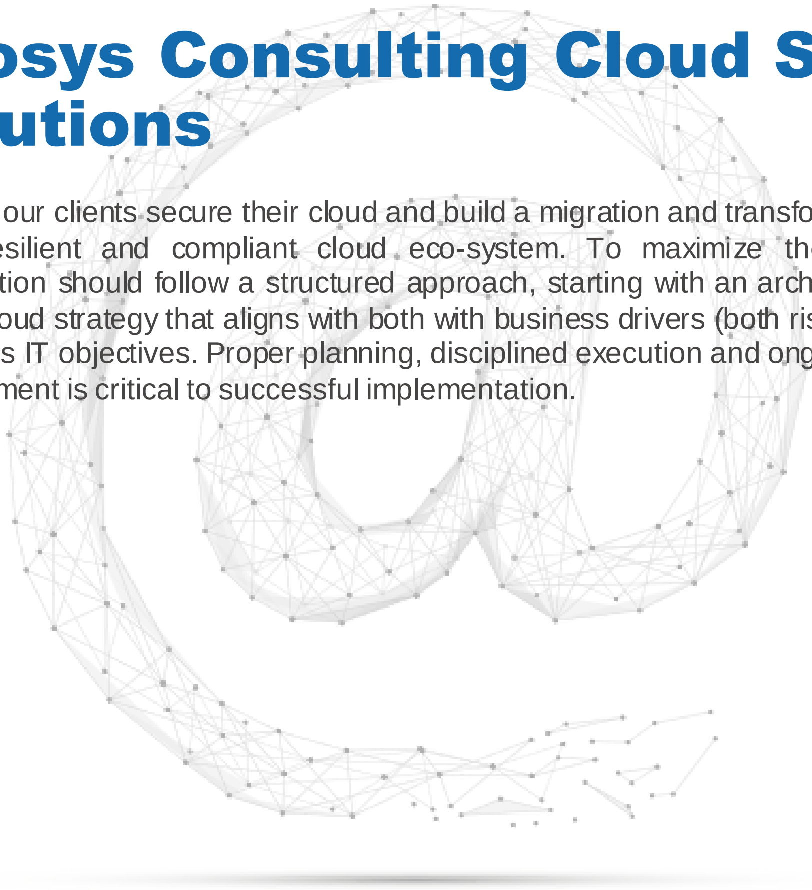
Goals/Objectives for Cloud Security

While organizations should not take the move to the cloud lightly in terms of security concerns, successful cloud adoption is possible by maintaining the following objectives:

- Maintain cloud posture and compliance.
- Uncover and manage vulnerabilities.
- Streamline threat detection and response.
- Continuously audit for security risks and misconfigurations.
- Provide actionable response and auto-remediation.
- Achieve consistent security across hybrid, or multi-cloud environments with CSPs (AWS, Azure, Google, and Kubernetes).
- Track and enforce configurations to meet policies.
- Provide continuous visibility of multi-cloud environments to identify cloud misconfiguration vulnerabilities.
- Prevent cloud drift.

Infosys Consulting Cloud Security Solutions

We help our clients secure their cloud and build a migration and transformation strategy for a cyber resilient and compliant cloud eco-system. To maximize the cloud's value, an organization should follow a structured approach, starting with an architecture review and a sound cloud strategy that aligns with both with business drivers (both risks and opportunities) as well as IT objectives. Proper planning, disciplined execution and ongoing governance and management is critical to successful implementation.



Cloud security strategy: Align your business needs and strategic vision with your cloud architecture:

- Understand key business priorities and align with IT security directives driving cloud transformation.
- Understand risk and business impact analysis affected by cloud provider contracts and SLAs.
- Decide the cloud computing environment that's right for the organization – e.g., private, public or hybrid.
- Decide the type of workload to be migrated to private cloud, public cloud, or hybrid cloud.
- Decide the security and privacy controls for the workloads that are being migrating to cloud.

- Cloud security architecture review: Review and document your overall architecture and controls environment:
  - Review cloud architecture for adherence to security frameworks.
  - Review application-level security.
  - Review identity services.
  - Review IsaaS, PaaS and SaaS.
  - Review data security, logging systems.
  - Review compliance controls.
  - Review virtualized infrastructure.
  - Review networking security.

- Cloud security assessment services: Cloud security assessment services enable best practices and leverage expertise with multiple security disciplines in cloud application security, cloud API and integration security, and cloud migration readiness.
  - Identify security risks and potential vulnerabilities.
  - Understand security requirements and IT objectives.
  - Provide tailored recommendations aligned with the business requirements.
  - Provide scorecard and recommendations report on existing infrastructure.
  - Provide migration readiness report in alignment with architecture evaluation.

- Cloud security policy and data governance: Design, build, and implement a cloud security governance program. Understand how risk is articulated and managed (policies, procedures, culture) across your organization.
  - Review regulatory and compliance requirements specific to your organization.
  - Establish security governance model and structure that align with business requirements.
  - Create/modify security policies, processes, and tools for cloud governance.
  - Build a security governance framework.
  - Recommend best practices to address security risks and misconfigurations.
  - Ensure polices enforce and track key configurations and change management processes.

Infosys Use Case

Infosys has demonstrated success in helping major financial institutions reach their full potential with cloud migration.

A prominent wealth management company was challenged with migrating over 600 business applications from traditional data centers to AWS. The challenge was to quickly migrate those applications in a secure manner while implementing an effective vulnerability management solution.

Infosys was able to create a comprehensive migration plan that included key governance tenants as well as monitoring and compliance mechanisms to ensure cloud security from start to finish. Infosys was also able to effectively implement End Point Security (EPS) to address vulnerability concerns. The following are more specifics on the solutions provided and the value delivered.

Solution

- Established security governance to provide strategies for cloud security policies, procedures, incident management, security alerts, continuous monitoring, security audits, and compliance.
- Developed comprehensive End Point Security (EPS) solution for cloud workloads using Trend Micro Deep Security.
- Designed and implemented all end point modules viz. AV, FIM, HIPS and McAfee DLP.
- Established lifecycle process for cloud infrastructure vulnerability management thus ensuring continuous assessment and mitigation.

Value Delivered

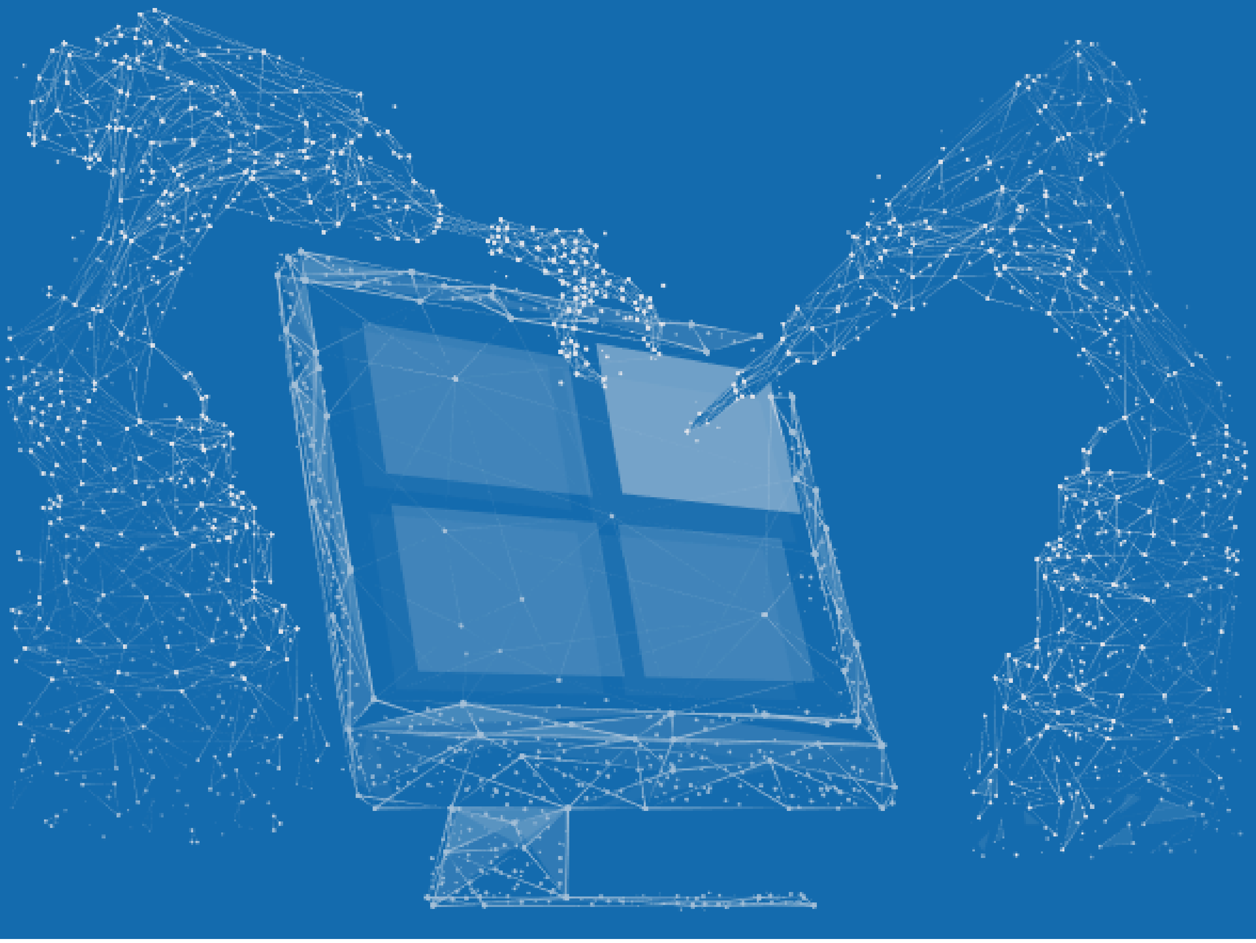
- Embedded defense in-depth solution for cloud hosted infrastructure.
- Optimized costs for cloud security controls.
- Ensured that client’s data privacy policies were compliant to Australian law.
- Integrated cloud autonomics platform to facilitate automation on cloud.

Final thoughts

Cloud provides transformative opportunities for organizations and is a vital competitive component in today's challenging marketplace. While it is not an easy technology to adopt, the potential benefits and opportunities outweigh the challenges and risks associated with cloud transformation.

References

1. Cybersecurity Insiders: 2021 AWS Cloud Security Report
2. Gartner: Emerging Technologies: Venture Capital Growth Insights for Cloud Security
3. Gartner: Hype Cycle for Cloud Security, 2021
4. Forrester: A Strong Hybrid Cloud Security Program Drives Tangible Business Benefits



Meet the Experts

Gerald Alston

Associate Partner – Cybersecurity

gerald.alston@infosys.com

Amber Boyle

Senior Principal – Cybersecurity

amber.boyle@infosys.com

Chad Williams

Senior Principal – Cybersecurity

chad.williams@infosys.com

Sara Lind

Principal – Cybersecurity

sara.lind@infosys.com

Infosys® | CONSULTING

consulting@Infosys.com
InfosysConsultingInsights.com

LinkedIn: /company/infosysconsulting
Twitter: @infosysconsltng

About Infosys Consulting

Infosys Consulting is a global management consulting firm helping some of the world's most recognizable brands transform and innovate. Our consultants are industry experts that lead complex change agendas driven by disruptive technology. With offices in 20 countries and backed by the power of the global Infosys brand, our teams help the C-suite navigate today's digital landscape to win market share and create shareholder value for lasting competitive advantage. To see our ideas in action, or to join a new type of consulting firm, visit us at www.InfosysConsultingInsights.com.

For more information, contact consulting@infosys.com