tcs TATA CONSULTANCY SERVICES

Cloud Migration in Insurance: Raising the Security Bar

Banking, Financial Services and Insurance

PURPOSE-DRIVEN

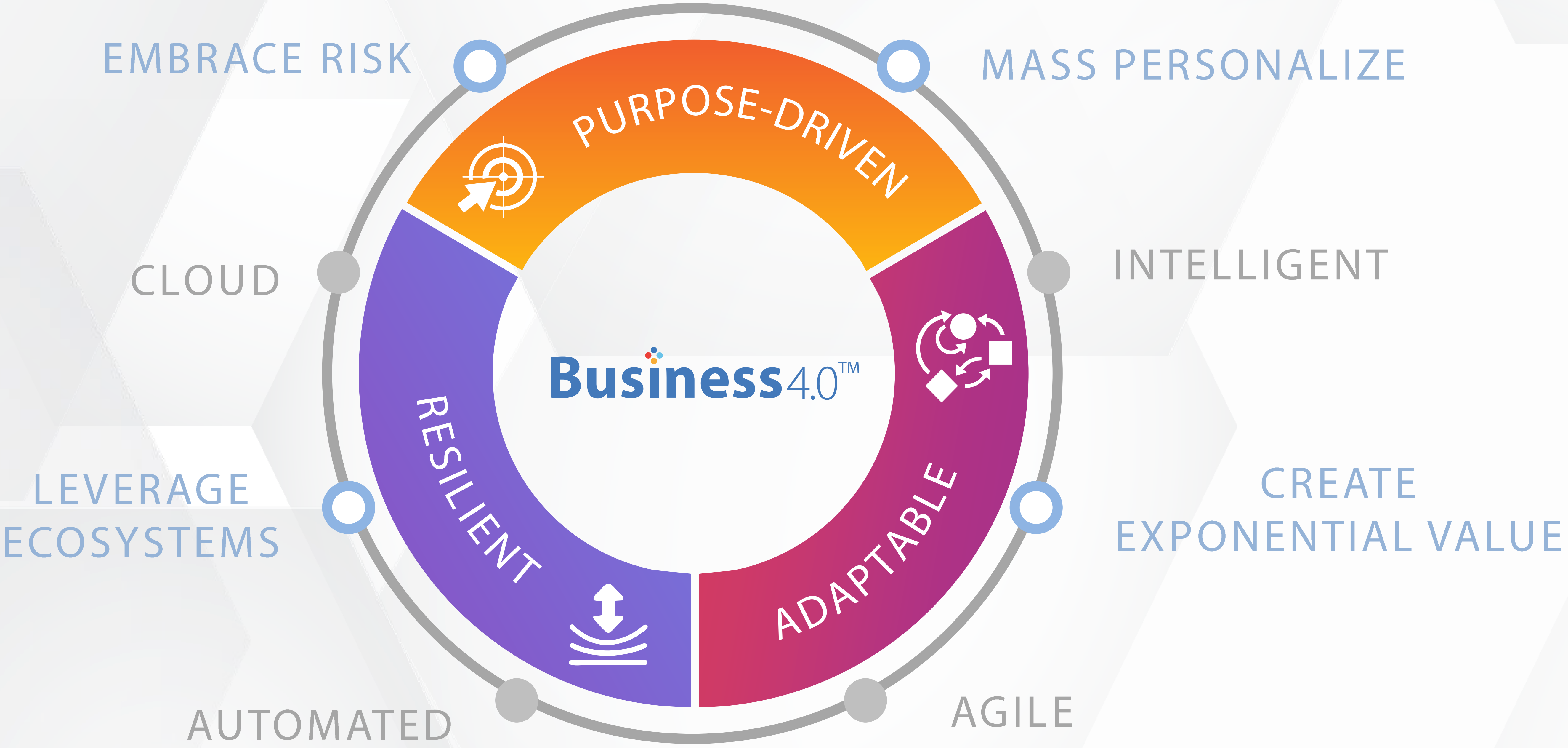
RESILIENT

ADAPTABLE

TATA CONSULTANCY SERVICES

PURPOSE-DRIVEN, RESILIENT, ADAPTABLE

BUSINESS 4.0™



About the Authors

Prasanna Sekhar

Prasanna Sekhar is an enterprise architect with the Guidewire Practice of TCS' Banking, Financial Services, and Insurance (BFSI) business unit. He has over 19 years of rich IT experience and has primarily worked with TCS' leading insurance clients worldwide, advising them on key transformation engagements pertaining to policy administration, underwriting, banking applications, electronic funds transfer, and legacy modernization. Prasanna holds a Bachelor’s degree in Computer Science Engineering from Madurai Kamaraj University, Tamil Nadu, India.

Ganesh Kumar Thiyagarajan

Ganesh Kumar Thiyagarajan is an insurance transformation consultant with the Insurance Transformation Group of TCS’ Banking, Financial Services, and Insurance (BFSI) business unit. Ganesh collaborates with TCS’ insurance clients in implementing core insurance platforms like policy administration, claims and billing. He has more than 20 years of IT experience and has worked with insurers across North America, Europe, the UK, and Asia Pacific regions. Ganesh holds a Certificate in General Insurance (AINS) from the Chartered Property Casualty Underwriter (CPCU) Society, USA and a Bachelor’s degree in Computer Science Engineering from Manonmaniam Sundaranar University, Tamil Nadu, India.

PURPOSE-DRIVEN RESILIENT ADAPTABLE

Abstract

Organizations across industries are having to revisit and reprioritize digital transformation journeys to accommodate new post pandemic realities. A trend that will gain traction is the migration of the IT infrastructure along with applications to cloud for better market reach and return of investment. In the insurance industry, the rate of cloud adoption is growing exponentially, and this will further accelerate in the post-COVID era. However, a surge in volume and consumption of data across the insurance industry will increase the risk of data breaches. This white paper examines the various data security aspects that need to be considered while moving core insurance platforms to the cloud.

Heading to the Cloud: Implications for Insurers

Insurers are increasingly migrating their core systems such as policy and claims to the cloud. However, the accountability and responsibility for securing critical customer data continue to lie with insurers. Security breaches and consequent data exposure are only rising – in the first half of 2019, the number of data breaches rose 54% to nearly 4000 compromising 4.1 billion records, an increase of 52%. [1] As a result, the need for establishing stringent security measures, enabling consistent monitoring, and improving stakeholders confidence have emerged as key imperatives for Insurers.

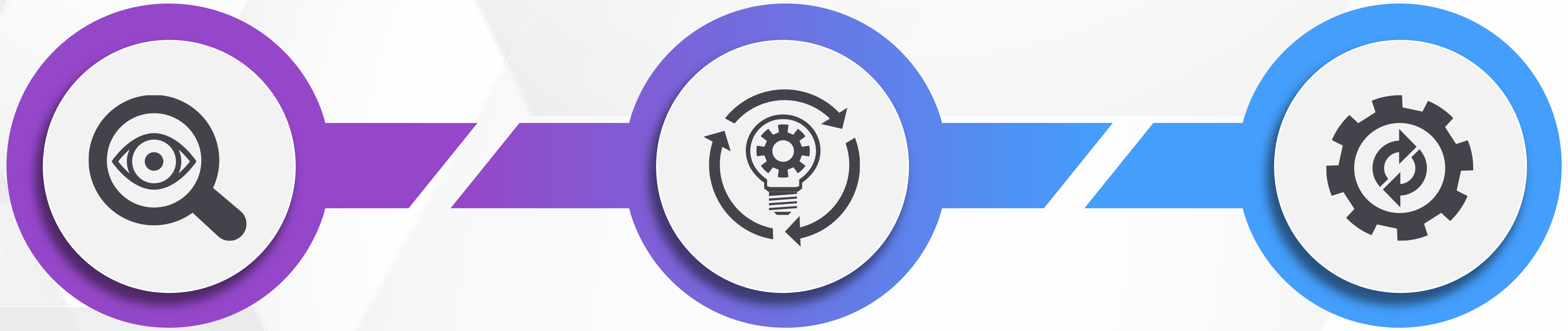
The common security threats faced by insurers while migrating to a public cloud or during on-premise implementation include data loss due to server outages and theft of personally identifiable information (PII) as well as customer information such as bank account details, payment card industry (PCI) data, and medical records. In our view, as insurers march forward on their cloud journey, a structured approach to ensure data security must form a key component of their cloud migration strategy.

[1] SC Media, First half 2019 sees 4,000 data breaches exposing 4B records, Aug 2019, Accessed Nov 2020, https://www.scmagazine.com/home/security-news/data-breach/first-half-2019-sees-4000-data-breaches-exposing-4b-records/

Ensuring Data Security: A Continuous Journey

Given the time, effort, and investment involved in cloud migration, we recommend that insurers future-proof their strategy to accommodate evolving security requirements that will arise due to rapid digitalization, connected devices, and hyper personalization. Thestrategy must cover three phases to cater to cloud security requirements.

- **Identify** security threats and potential data breaches
- **Implement** fool-proof security design in alignment with the enterprise cloud strategy
- **Improvise** continuously to adapt to the changing needs of insurance and associated security needs



Identify
Identify organization specific data and security requirements
Implement
Design and implement data and security architecture
Improvise
Improvise continuously to accommodate evolving future requirements

Figure 1: Proposed Approach for Cloud Migration

Identify

Defining a comprehensive security strategy will require insurers to identify security compulsions, ascertain applicable regulations on data privacy and security, and determine ecosystem needs.

Regulations

Insurers will need to abide by government regulations related to protecting the PII and PCI data as well as associated laws governing the industry in the concerned jurisdiction. For instance, during our engagements with US insurers, we learned that the definition of PII is different across different US states. Similarly, the General Data Protection Regulation (GDPR) mandates that PII can be stored outside the European Union only in compliance with GDPR provisions.[2] Likewise, the National Association of Insurance Commissioners (NAIC) in the US provides guidance on the security of insurance applications.[3] Insurers should therefore pay special attention to cybersecurity while migrating applications to the cloud.

Several cloud service providers and commercial off-the-shelf (COTS) products comply with local laws and regulations. Insurers need to examine aspects of compliance with current laws in addition to evaluating the vendor's capability to accommodate future changes without impacting insurers' business operations.

[2] Intersoft Consulting, General Data Protection Regulation, General principle for transfers, Accessed November 2020, https://gdpr-info.eu/art-44-gdpr/

[3] National Association of Insurance Commissioners, Cybersecurity, April 2020, Accessed November 2020,https://content.naic.org/cipr_topics/topic_cybersecurity.htm

Ecosystem data needs

Insurers must assess their existing landscape as well as that of their ecosystem partners to ascertain the potential data (data at rest and data in motion) that needs to be secured. In the insurance value chain functions, core systems integrate with multiple systems, both internally and externally, and consume confidential data in the course of routine business operations (see Table 1). In this process, PII, payment card industry information (PCII), or protected health information (PHI) data are exchanged between the systems. While designing systems for the cloud, insurers will need to carefully safeguard the data at rest by encrypting it and use secure protocols such as HTTPS for data in motion.

PCII Data	PHI Data	PII Data
Credit score	Medical reports	Contact creation
Policy creation	Police reports	Address standardization
Policy renewal		CRM integrations
Mid term policy changes		Customer prefill
Rating		Quote
Claim payments		Agent setup
Agency billing		Claims inquiry
Disbursement		Policy inquiry
IVR payments		Datawarehouse
List bill		Operational data store
Collections		Rental car
Authentication		Document generation
Accounting and general ledger		First notice of loss (FNOL)
Note: Some of the PCI and PHI integrations could also have PII data		

Table 1: A Sample of the Integration Scenarios to be Considered to Ensure Data Security

Backup and future data needs

Apart from data exposure, there are other potential security risks including data loss due to server crash and ransomware attacks. The onus of data backup is on insurers when they partner with public cloud providers. Hence, insurers need to identify data backup requirements in their cloud journey.

By 2025, the Internet of Things (IoT) will gain traction and the insurance industry will witness widespread use of sensor data from connected homes, cars, and devices for risk assessment. Insurers' applications will need to collect and process data from IoT devices. Insurers will therefore need to design the security architecture considering such future requirements.

Implement

Insurers should identify the right cloud solution considering their risk appetite and the risk they intend to transfer to cloud vendors. Across various geographies, most of the insurance COTS vendors provide software-as-a-service (SaaS) options apart from infrastructure-as-a-service (IaaS) and platform-as-a-service (PaaS) options for cloud implementation. Several insurers are adopting SaaS options for core applications.Table 2 provides the three different cloud options along with the ownership of the associated infrastructure and data entities.

Cloud options =>	Infrastructure-as-a-Service (IaaS)			Platform-as-a-Service (PaaS)			Software-as-a-Service (SaaS)		
Category	Insurer	COTS vendor	Cloud provider	Insurer	COTS vendor	Cloud provider	Insurer	COTS vendor	Cloud provider
Customer data	X			X			X		
Application	X	X		X	X			X	
Identity and access management	X	X		X	X		X	X	
Operating system	X					X		X	
Network	X			X		X		X	
Firewall	X			X		X		X	
Storage	X			X				X	
Database	X	X				X		X	
Infrastructure			X			X			X
Business continuity	X			X				X	

Table 2: Ownership of Infrastructure and Data Entities for Different Cloud Options

Based on the chosen cloud platform, building a resilient security architecture will be of paramount importance. For any application, security is the most important factor – adopting the security-by-design approach while designing the application in the early phases of application architecture is critical. Figure 2 depicts a reference cloud architecture incorporating security aspects.

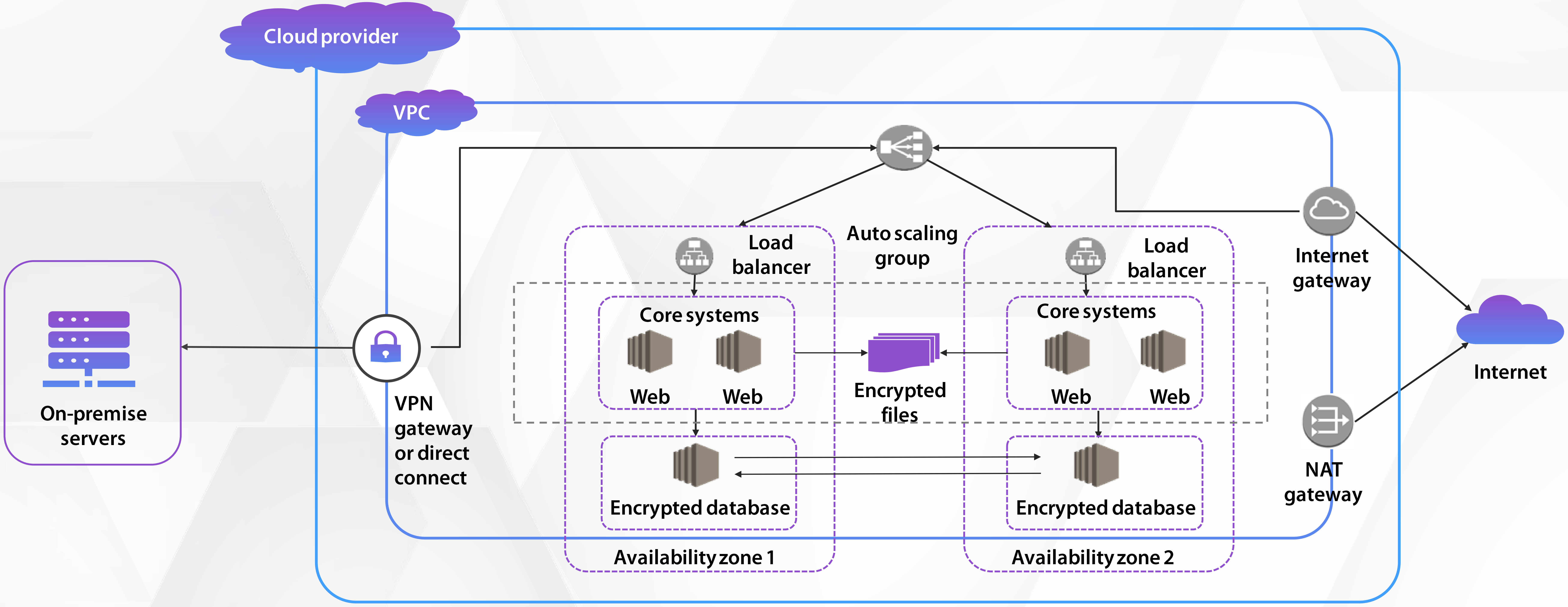


Figure 2 – Reference Security Architecture

Certain key components can be embedded into the proposed architecture to address cloud specific data security aspects (see Table 3). Distinct components to address organization specific security challenges can also be added to arrive at a comprehensive architecture that addresses end-to-end data security requirements.

Component	Challenges addressed
Virtual private network (VPN)	Protects data from hackers and allows secure internal communication across the application landscape
Network address translation (NAT) gateway or internet gateway	Allows the core application to communicate with the other service providers by protecting the data on the cloud; blocks inbound internet traffic from malicious servers
Load balancer / availability zones	Makes applications resilient to cyberattacks and natural calamities by enabling other zones to take over service when service is disrupted in one zone; restores data quickly and protects against attacks
Encrypted database / files	Ensures compliance with government regulations; prevents unauthorized access by employees
Virtual private cloud (VPC)	Provides an isolated cloud environment

Table 3: Solution Components of the Proposed Cloud Architecture

Lastly, given a chain is only as strong as its weakest link, security measures should not be restricted to core insurance applications but extended to all the applications in the ecosystem.

Improvise

Constantly evolving business scenarios and emerging vulnerabilities will mandate data security becoming a continuous journey with focus on some primary aspects.

Data governance

Gartner's annual Audit Plan Hot Spots Report reveals that data governance has risen to become the top audit concern for 2020, up from second place in the 2019 report.[4] Establishing a comprehensive data governance framework and continuously tweaking it in response to the evolving needs of the business is critical.

Monitoring mechanisms

Mechanisms to monitor security architecture will need to be implemented and strategies to adapt to changing scenarios must be defined. We recommend security process automation to eliminate repetitive tasks and collaboration between IT security and operations (SecOps) teams to ensure effective monitoring and achieve system and data security. Multiple monitoring tools are available in the market; cloud service providers also offer tools to monitor systems. Insurers will need to utilize these tools effectively to continuously enhance their data security.

Vulnerability assessment

Insurers need to leverage the ethical hacker community and offer bug bounty programs to its employees to identify vulnerabilities in their systems. In addition, insurers should engage with service providers to carry out independent vulnerability assessments to identify deficiencies and strengthen their security architecture.

[4] Gartner, Gartner Says Data and Cyber-Related Risks Remain Top Worries for Audit Executives, November 2019, Accessed November 2020, https://www.gartner.com/en/newsroom/press-releases/2019-11-7-gartner-says-data-and-cyber-related-risks-remain-top-worries-for-audit-executives

In a Nutshell

Cloud migration is fast becoming an important component of digital transformation strategies in the insurance industry. Coupled with the increased use of data from IoT devices, the data needs of insurers and associated security risks is bound to grow and evolve. Insurers that take steps to design a comprehensive security architecture as part of their cloud strategy will be able to address the full spectrum of security challenges and ensure successful cloud migration as well as reap the benefits of digitalization, improved operational efficiency, and the ability to deliver superior customer experience.

TATA CONSULTANCY SERVICES

Contact

For more information on TCS' Insurance Services,
please visit https://www.tcs.com/insurance

Email: bfsi.marketing@tcs.com

About Tata Consultancy Services Ltd (TCS)

Tata Consultancy Services is an IT services, consulting and business solutions organization that delivers real results to global business, ensuring a level of certainty no other firm can match.

TCS offers a consulting-led, integrated portfolio of IT and IT-enabled infrastructure, engineering and assurance services. This is delivered through its unique Global Network Delivery Model^{TM}, recognized as the benchmark of excellence in software development. A part of the Tata Group, India's largest industrial conglomerate, TCS has a global footprint and is listed on the National Stock Exchange and Bombay Stock Exchange in India.

For more information, visit us at **www.tcs.com**

PURPOSE-DRIVEN

RESILIENT

ADAPTABLE