Prioritising cloud risk: Attack path and exposure-driven controls for Indian enterprises

March 2026

Contents

Executive summary

India's enterprises are accelerating multi-cloud adoption at an unprecedented pace, yet their security posture hasn't kept pace. Traditional cloud compliance approaches are checklist-based and fragmented, leaving critical exposures unaddressed and creating dangerous blind spots that sophisticated threat actors exploit with alarming regularity.

Attackers now exploit interconnected misconfigurations, exposed identities, and unpatched workloads to build attack chains that bypass traditional controls. Today, a single misconfigured identity and access management (IAM) role, combined with an exposed workload and overprivileged access, can provide attackers a direct pathway to an organisation's most sensitive data assets.

A shift to attack path-based risk prioritisation targets what matters most: breaking exploitable chains with business impact. Enhanced visibility and intelligence reduce the attack surface and better align resource allocation with risk.

The challenge

12,000+

alerts but limited context on actual risk

Approach

Attack

path analysis in a business context

The outcome

60–80%

reduction in critical exposures

The core philosophy behind this new approach is that visibility and context make organisations stronger. By seeing how exposure chains create attack paths, Indian enterprises can transform cloud security from a compliance task into a strategic risk management tool that builds board confidence and meets regulatory requirements.

The Indian cloud security context

India's digital transformation is occurring rapidly, with the banking, technology, and manufacturing industries moving to multi-cloud platforms such as AWS, Azure, and Google Cloud. Growth in AI, digital transformation, and Industry 4.0 initiatives is driving this shift, with the cloud becoming the backbone for all such initiatives.

While the tax holiday significantly lowers the cost of operating cloud infrastructure in India, it also accelerates the concentration of global and domestic data within Indian data centres, increasing the strategic importance of cloud security. Therefore, any breach, outage, or compromise will have cross-border economic and reputational impacts. For the tax holiday to translate into sustained global confidence, India's cloud ecosystem would need to be perceived as secure, resilient, and trustworthy.

With the current cloud adoption, many organisations struggle to understand how their different cloud assets and data connect and where they might be vulnerable. In addition, conventional security tools typically flood teams with numerous alerts, creating a scenario similar to identifying a needle in a haystack. For example, a small misconfiguration in one system may seem harmless on its own, but when combined with other weaknesses, it can create a path to a severe breach. Without a clear context, it is easy to miss these critical risks and leave an organisation exposed to sophisticated attacks.

Cloud adoption surge

Indian enterprises now operate 3+ cloud environments on average, managing thousands of workloads across hybrid infrastructure. The banking, financial services, and insurance (BFSI) sector has increased cloud spending by 40% year-over-year, whereas technology companies lead multi-cloud strategies.

Evolving threat landscape

Cloud-targeted ransomware attacks have increased by 156% in the Indian market. Credential theft, privilege escalation, and insider threats now represent the top three attack vectors, with adversaries specifically targeting misconfigured IAM policies and exposed storage buckets.

Regulatory pressure

The Reserve Bank of India (RBI)'s cloud guidelines, Securities and Exchange Board of India (SEBI)'s cybersecurity framework, Insurance Regulatory and Development Authority of India (IRDAI)'s data protection requirements, and the Digital Personal Data Protection Act, 2023 have created stringent accountability frameworks. Boards now face personal liability for data breaches.

Capability gap

Despite investments in cloud security tools, organisations struggle with siloed cloud teams, multiple cloud service provider (CSP)-specific dashboards, and lack of unified visibility. The talent shortage in cloud security expertise compounds these challenges.

Why traditional cloud security fails

Alert fatigue

Security teams typically receive numerous alerts, compliance findings, and vulnerability notifications from separate tools such as cloud security posture management, cloud workload protection, and cloud identity and entitlement management. These tools typically operate alone, identifying a single misconfiguration without seeing the bigger risk picture.

This creates thousands of alerts with little business or data context; thus, teams focus on minor issues and miss critical attack paths.

Individual risk - Medium
An unpatched virtual machine (VM) in a private subnet with no external connectivity and an overprivileged role receives a medium severity rating.
A privately accessible simple storage service (S3) bucket linked to the same overprivileged IAM role receives a medium severity rating.

The stark reality: These two medium severity findings can make security teams defer remediation. When viewed with an attacker's lens, they represent a stark difference. The isolated VM poses minimal threat; however, an insider using the overprivileged IAM role can reach the private S3 bucket containing sensitive data to which they should not have access. Without an attack path context, security teams cannot distinguish between theoretical vulnerabilities and exploitable exposures. This fundamental flaw explains why organisations with mature compliance programmes still suffer breaches, because they secure against checklists rather than actual attack scenarios. The board receives reports that show high compliance scores; however, critical attack paths remain wide open.

Anatomy of an attack

The attack path understanding of how different security weaknesses combine to form attack chains is key to setting priorities for fixes. This shows why context matters more than just vulnerability counts.

Initial access: Internet-exposed endpoint

A web application with public access sits behind an application load balancer. Although this exposure is intentional, it represents an adversary's entry point into a target cloud environment.

Vulnerability exploitation

The application contains an unpatched remote code execution vulnerability (CVE-2023-XXXXX). In isolation, this may appear as one finding among thousands, but when positioned at a public endpoint, it becomes immediately exploitable.

Identity compromise

The compromised application runs under an IAM service account with overly broad permissions for access to S3, DynamoDB, and Lambda functions. The attacker now has legitimate cloud credentials with extensive privileges.

Lateral movement

Using the compromised identity, the attacker discovers an S3 bucket containing database backups. The bucket lacks encryption and uses default access policies, allowing the stolen credentials full read access.

Data exfiltration

The database backups contain customers' personal identifiable information, payment card data, and financial records. The attacker thus reaches high-value data through a series of individually moderate findings that together create a critical path.

The risk prioritisation insight

Traditional security tools will flag each component separately: the CVE as "High", the overprivileged IAM role as "Medium", and the unencrypted bucket as "High". However, without understanding the path, security teams cannot distinguish this critical chain from thousands of other findings. Attack path analysis reveals that breaking any single link, patching the CVE, restricting the IAM permissions, or encrypting the bucket, will collapse the entire attack scenario. This is the power of context-driven prioritisation.

This example demonstrates why Indian enterprises must evolve beyond vulnerability management to attack path analysis. The Digital Personal Data Protection (DPDP) Act, 2023 and RBI guidelines hold organisations accountable for protecting customer data; such accountability that cannot be satisfied by counting patched systems, but rather requires understanding and closing exploitable paths to regulated data.

Using risk graphs: A new paradigm

An attack path is a series of exposures that attackers use to reach valuable assets. To analyse these paths, it is important to see how vulnerabilities, misconfigurations, and permissions work together.

Misconfigured identity

Overprivileged IAM role or compromised credentials

Vulnerable workload

Unpatched application or exploitable service

Public exposure

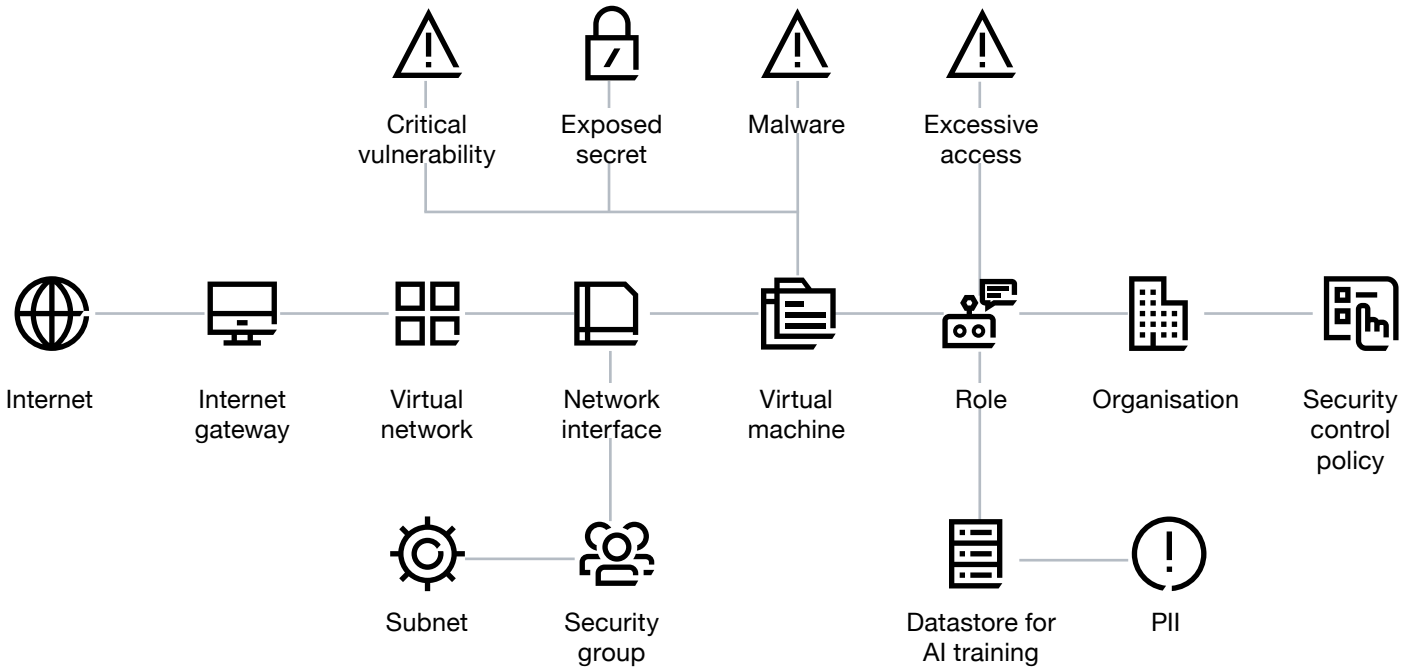
Internet-facing endpoint or accessible storage

Privilege escalation

Lateral movement to critical systems

Consider a real-world scenario in which an internet-facing web application with a structured query language (SQL) injection vulnerability (component one) runs with an IAM role that has excessive S3 permissions (component two). This role can access a bucket containing database backup files (component three), which include encryption keys stored in plaintext (component four). Individually, each finding may appear manageable; however, when connected, they form a complete attack path from the public internet to the most sensitive data.

Figure 1. Attack path graph



The power of attack path analysis lies in visualisation through risk graphs—dynamic maps showing relationships between assets, exposures, identities, and data. These graphs illuminate not only what is vulnerable but also what is reachable and what is at stake. The critical insight: you don't need to patch everything simultaneously. Instead, identify and break the most dangerous paths. Removing a single link, perhaps restricting the overprivileged IAM role, can collapse multiple attack scenarios, considerably reducing risk with focused effort. This approach transforms security from an endless game of whack-a-mole into strategic risk management

Contextual risk prioritisation in practice

Modern cloud security platforms have evolved beyond traditional vulnerability scanning to provide contextual intelligence that transforms how organisations understand and manage risk.

These capabilities democratise cloud security, making sophisticated risk analysis accessible beyond specialist security teams. Developers and DevOps engineers receive intuitive, actionable insights into their existing workflows, enabling them to remediate exposures during the development process rather than discovering them in production.

The result: Organisations shift from reactive firefighting to proactive risk management.

60–80%

Exposure reduction

Critical open exposures reduced within the first 90 days

10min

Full visibility

Complete cloud estate discovery

50%+

Democratised security

Users/developers or DevOps teams

01 Unified visibility

Agentless discovery scans every layer of cloud environments across Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP) in minutes, providing complete visibility into every technology, workload, identity, and data store without performance impact or deployment complexity.

02 Contextual mapping

Security graph technology connects vulnerabilities, identities, network paths, and data sensitivity into a unified model. This correlation reveals how a misconfigured security group relates to an overprivileged service account, which connects to sensitive customer data.

03 Intelligent prioritisation

Advanced engines analyse the security graph to highlight risks that form active attack paths to critical assets. Rather than presenting 10,000 findings of equal severity, the system identifies 50 exposures that could lead to material business impact.

04 Business translation

Risk scoring incorporates business context, not simply technical severity. A vulnerability affecting revenue-generating systems or regulated data receives appropriate prioritisation, whereas identical technical issues in development environments are deprioritised.

05 AI-accelerated response

AI streamlines security operations by offering quick visibility into threats, accelerating remediation workflows, and suggesting context-aware fixes that address root causes rather than symptoms.

Framework for prioritised cloud risk management

Indian enterprises need a clear and practical way to shift cloud security from compliance-focused to risk-driven. This approach helps organisations handle more attack vectors in multi-cloud environments by focusing on the most effective defences, rather than simply counting vulnerabilities.

Prioritise remediation based on business impact

- Rank risks by combining reachability (can an attacker reach there?), data sensitivity (what is at stake?), and business criticality (what is the impact?). Focus remediation efforts on chokepoints—single fixes that collapse multiple attack paths. This strategic approach maximises security improvement per unit of effort.

Communicate to the board in risk language

- Transform technical exposure data into executive-ready risk heatmaps and KPI dashboards.
- Report key metrics, including closure of critical paths, mean time to remediate exploitable exposures, reduction in attack surface over time, and alignment with regulatory requirements.
- Make security outcomes visible and measurable.

Correlate exposures into attack paths

- Utilise security graph analytics to map relationships between assets, identities, and data.
- Identify exploitable paths—for example, an internet-exposed workload with vulnerable components that runs under an overprivileged identity with access to production databases.
- Visualise these paths to understand the attacker's perspective.

Integrate with descopes and continuous assurance

- Embed security checks into continuous integration/continuous deployment (CI/CD) pipelines to prevent new exposures from reaching production. Implement policy-as-code to enforce secure by-default configurations.
- Monitor continuously for configuration drift and the reappearance of risky patterns, closing the loop between detection and prevention.

Establish cloud inventory and context

- Deploy automated discovery to identify all assets, configurations, identities, and data stores across your cloud estate.
- Implement business-aligned tagging that identifies critical systems, regulated data, and revenue-generating applications. This foundation provides the raw material for contextual risk analysis.

This framework shifts the conversation from "How many vulnerabilities do we have?" to "What are our most critical exposures and how quickly are we closing them?" It provides chief information security officers (CISOs) with the structure required to demonstrate security effectiveness to boards and regulators, while giving security teams clear priorities and measurable progress.

Governance, metrics, and continuous improvement

Strong cloud security depends on good measurement systems that turn technical improvements into business value. The appropriate metrics build accountability, show progress, and help guide investment decisions for regulators and boards.

Reduction in reachable critical exposures	Mean time to remediate exploitable paths	DevOps pipeline security integration	Cloud misconfiguration recurrence rate
Track the percentage decrease in attack paths that can lead to sensitive data or critical systems. This metric directly measures risk reduction rather than vulnerability counts. Target: 60%+ reduction within 90 days of programme initiation	Measure the average time from detection to the remediation of critical attack paths. This operational metric demonstrates security team efficiency and responsiveness. Industry benchmark: Under 48 hours for critical paths in production environments	Calculate the percentage of CI/CD pipelines with integrated security scanning and policy enforcement. This leading indicator predicts future security posture by measuring prevention capabilities. Target: 80%+ coverage across development teams	Monitor how frequently remediated issues reappear, indicating whether fixes address root causes or merely symptoms. Low recurrence demonstrates effective policy implementation and developer education. Target: Below 5% recurrence rate

These governance practices and metrics create the foundation for continuous security improvement. They enable CISOs to demonstrate value, justify security investments, and maintain board confidence while providing security teams with clear objectives and measurable progress indicators.

Enterprise risk framework integration

Align cloud security metrics with established enterprise risk management frameworks, including ISO 27001, NIST Cybersecurity Framework, and CIS Controls. This integration ensures that cloud risk receives appropriate visibility within broader organisational risk registers and audit programmes.

Map cloud security controls regulatory requirements from RBI, SEBI, IRDAI, and DPDP 2023. Maintain evidence of control effectiveness through automated compliance reporting that references attack path analysis and risk reduction metrics.

Executive review cadence

Establish quarterly executive reviews of cloud attack surface with board-level risk committees. Present risk heatmaps showing high-value assets, current exposures, and remediation progress. Include trend analysis demonstrating security postural improvement over time.

Prepare concise executive summaries that translate technical metrics into business language: “We’ve reduced the attack surface for customer financial data by 73%, closing 45 critical paths in Q3. Mean time to address critical exposures improved from 12 to 2 days.”

Cultivating a reliable, context-aware cloud security strategy

Enterprises should move beyond compliance-based security because modern threats exploit exposure gaps to circumvent fragmented controls. Only risk-based security strategies can keep up with changing attack methods, because exposures can create attack paths that bypass standard controls.

Context-aware cloud security	**Attack path analysis**	Understanding exploitable risk chains
	Intelligent prioritisation	Focus on key exposures
	Automated response	Rapid remediation of critical paths
	Team empowerment	Actionable insights for all stakeholders
	Continuous improvement	Metric-driven security evolution
	Contextual visibility	Unified view across multi-cloud environments

01 Move from checklist to context

a. Abandon the false security of compliance scores that ignore actual risk. Instead, implement security graph analytics that reveal how assets, identities, and data interconnect to form exploitable paths.

02 Prioritise key issues

a. Direct remediation efforts towards exposures that form critical attack paths to sensitive data and essential systems.

b. Recognise that closing seven exploitable paths provides more security value than addressing 7,000 low-context findings.

c. Measure success by attack surface reduction, not vulnerability counts.

03 Collaborate for operational excellence

a. Partner with experienced advisers who understand cloud security technology and the unique regulatory landscape facing enterprises.

b. Leverage combined expertise in RBI guidelines, DPDP compliance, and multi-cloud risk management to operationalise sophisticated security programmes that satisfy both technical and governance requirements.

The path forward requires commitment to transformation, not merely implementing new tools but fundamentally rethinking how your organisation identifies, prioritises cloud risk, and builds a resilient, context-aware cloud security strategy.

How AI enhances risk prioritisation

AI is making cloud security smarter and more automated. Machine learning facilitates security graph analysis, natural language processing supports threat intelligence, and predictive analytics improves risk scoring. AI enables security teams to handle threats as quickly and widely as the cloud requires. Instead of replacing human judgement, AI supports it, allowing professionals to focus on strategy while automating attack path analysis. Nevertheless, organisations should look out for risks such as false positives and privacy issues.

Intelligent pattern recognition

Machine learning algorithms analyse millions of cloud configurations across organisations to identify subtle patterns that indicate exploitable attack paths.

AI recognises that certain combinations of IAM permissions, network configurations, and workload vulnerabilities create higher risk than individual findings suggest.

Accelerated threat response

When new vulnerabilities are disclosed or threat actors change tactics, AI rapidly assesses exposure across your entire cloud estate. Rather than waiting for security teams to manually correlate threat intelligence with asset inventories, AI instantly identifies which workloads are affected, whether they are reachable through attack paths, and what data may be at risk.

Context-aware remediation suggestions

AI does not only identify risks but also recommends specific remediation actions based on the analysis of successful fixes across similar environments.

These suggestions consider the business context, understanding that the optimal fix for a development environment differs from production systems.

Predictive risk analytics

By analysing historical data on configuration changes, security incidents, and attack techniques, AI predicts which types of exposures are most likely to be exploited in your specific environment.

This predictive capability enables proactive security, allowing teams to address emerging risks before adversaries discover them.

For Indian enterprises managing complex multi-cloud environments with limited security expertise, AI represents a force multiplier that enables small teams to achieve security outcomes previously requiring significantly larger organisations. The technology does not replace human judgement but augments it, freeing security professionals to focus on strategic initiatives, while AI handles the computational heavy lifting of analysing millions of potential attack paths.

Appendix

Cloud risk prioritisation maturity model

Level 1

Ad hoc: Reactive security, tool-generated alerts without context, manual processes

Level 2

Managed: Defined security processes, compliance-focused, siloed tools

Level 3

Integrated: Unified visibility, some attack path analysis, policy-as-code adoption

Level 4

Optimised: Full attack path-driven prioritisation, automated remediation, and DevSecOps integration

Level 5

Predictive: AI-enhanced risk prediction, continuous improvement, and security as competitive advantage

Cloud security terminology

Attack path

A sequence of interconnected exposures that an adversary can exploit to reach high-value assets

Security graph

A data model representing relationships between cloud assets, identities, configurations, and data

Cloud Security Posture Management (CSPM)

Tools that assess cloud configuration against security best practices

Cloud Workload Protection Platform (CWPP)

Security for containerised and virtual machine workloads

Cloud Infrastructure Entitlement Management (CIEM)

Governs and secures cloud identity permissions

DevSecOps

Integration of security practices into DevOps development workflows

Lateral movement

An attacker's progression from initial access to additional systems within the environment

About PwC

We help you build trust so you can boldly reinvent

At PwC, we help clients build trust and reinvent so they can turn complexity into competitive advantage. We're a tech-forward, people-empowered network with more than 364,000 people in 136 countries and 137 territories. Across audit and assurance, tax and legal, deals and consulting, we help clients build, accelerate, and sustain momentum. Find out more at www.pwc.com.

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

Contact us

Sundareshwar Krishnamurthy
Partner, India Cyber Leader
PwC India
sundareshwar.krishnamurthy@pwc.com

Sricharan Saripalli
Partner, Cyber and Digital Risk
PwC India
sricharan.saripalli@pwc.com

Terence Gomes
Partner, Cyber and Digital Risk
PwC India
terence.gomes@pwc.com

Sandeep Kumar
Director, Cyber and Digital Risk
PwC India
sandeep.d.kumar@pwc.com

pwc.in

HS/February 2026 - M&C 5747